



DES-3350SR

Layer 3 Switch

Command Line Interface Reference Manual

Second Edition
(April 2004)

6ES3350SRC02
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. Verwenden 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 ist 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 sollte 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 autorisiertem 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 sind beschädigt.
 - b – Flüssigkeit ist in das Gerät eingedrungen.
 - c – Das Gerät war Feuchtigkeit ausgesetzt.
 - d – Wenn das Gerät nicht der Bedienungsanleitung entsprechend 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 Originalersatzteile bzw. den Originalteilen entsprechende Teile verwendet werden. Der Einsatz von ungeeigneten Ersatzteilen kann eine weitere Beschädigung hervorrufen.
17. Wenden Sie sich mit allen Fragen die Service und Reparatur 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, NEGLIGENCE, 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 OF 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 ©2003 D-Link Corporation.

Contents subject to change without prior notice.

D-Link is a registered trademark of D-Link Corporation/D-Link Systems, Inc. All other trademarks belong to their respective proprietors.

Copyright Statement

No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from D-Link Corporation/D-Link Systems Inc., as stipulated by the United States Copyright Act of 1976.

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

Introduction.....	11
Using the Console CLI.....	16
Command Syntax.....	24
Basic Switch Commands.....	28
Switch Port Commands.....	48
Network Management Commands.....	53
Download/Upload Commands.....	89
Network Monitoring Commands.....	93
Spanning Tree Commands.....	101
Forwarding Database Commands.....	112
Broadcast Storm Control Commands.....	124
QOS Commands.....	128
Port Mirroring Commands.....	147
VLAN Commands.....	153
Link Aggregation Commands.....	167
IP Interface Commands.....	177
ARP Commands.....	185

Routing Table Commands	193
Route Redistribution Commands	198
IGMP Commands	210
IGMP Snooping Commands.....	215
802.1X Commands	230
Access Control List (ACL) Commands.....	253
BOOTP Relay Commands.....	273
DNS Relay Commands	280
RIP Commands	290
DVMRP Commands.....	299
PIM Commands.....	308
IP Multicasting Commands	315
MD5 Configuration Commands	319
OSPF Configuration Commands.....	324
SNTP Commands	360
Command History List	365
Technical Specifications	371
Switch System Messages	374

1

INTRODUCTION

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

This manual provides a reference for all of the commands contained in the CLI. Configuration and management of the switch via the Web-based management agent is discussed in the User's Guide.

Accessing the Switch via the Serial Port

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

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

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

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

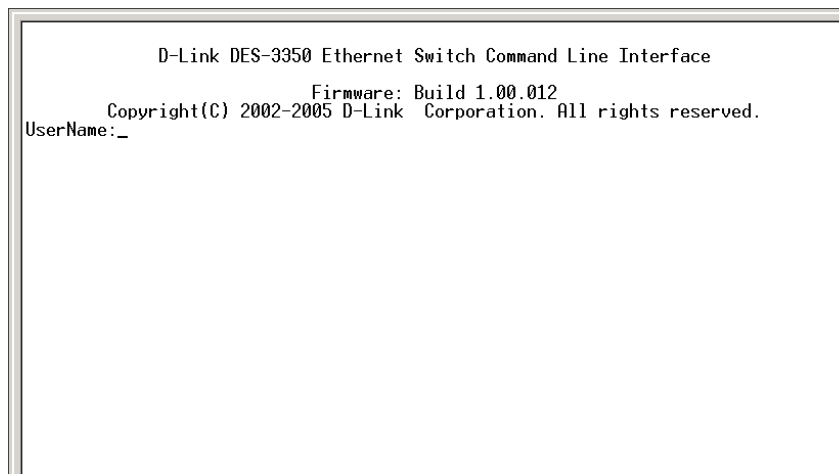


Figure 1-1. Initial Console screen.

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

Setting the Switch's IP Address

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

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

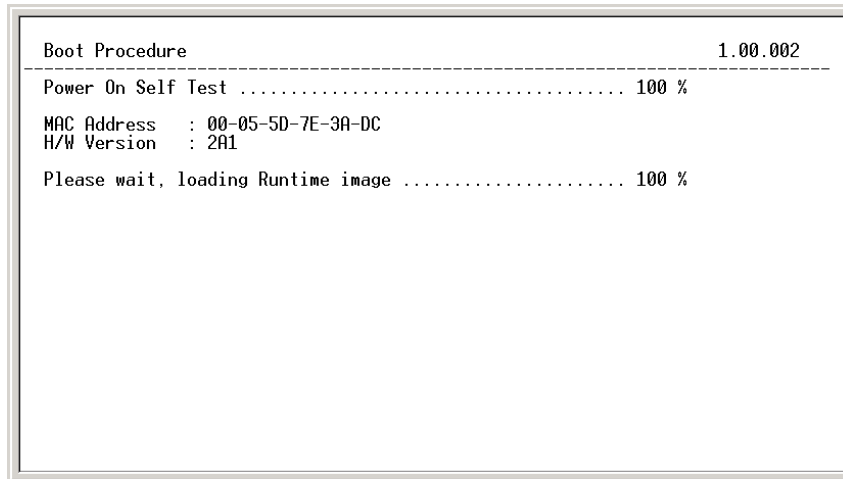


Figure 1-2. Boot Screen

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

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

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

1. Starting at the command line prompt, enter the commands **config ipif System ipaddress xxx.xxx.xxx.xxx|yyy.yyy.yyy.yyy**. Where the **x**'s

represent the IP address to be assigned to the IP interface named **System** and the **y**'s represent the corresponding subnet mask.

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

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

```
D-Link DES-3350 Ethernet Switch Command Line Interface
Firmware: Build 1.00.012
Copyright(C) 2002-2005 D-Link Corporation. All rights reserved.
UserName:
Password:
local>config ipif System ipaddress 10.24.22.9/255.0.0.0
Command: config ipif System ipaddress 10.24.22.9/8

Success.
local>_
```

Figure 1-3. Assigning the Switch an IP Address

In the above example, the switch was assigned an IP address of 10.24.22.9 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-3350SR 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 compatible
- 9,600 baud
- 8 data bits
- No parity
- One stop bit
- No flow control

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

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

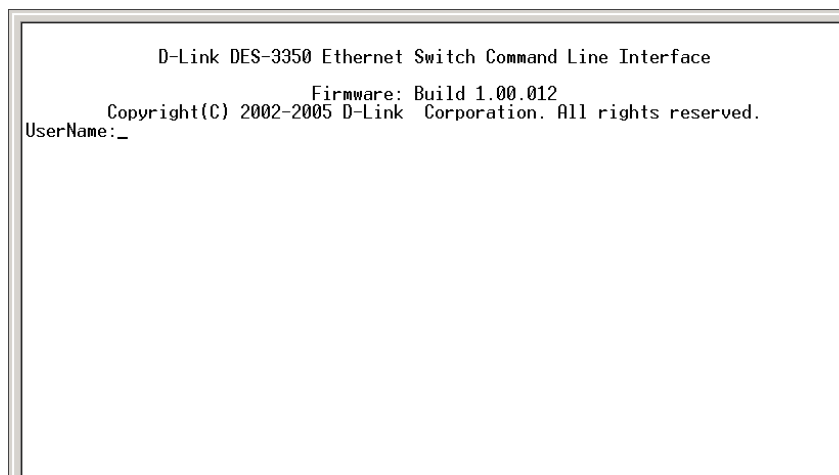


Figure 2-1. Initial Console Screen

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

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

```
..  
?  
clear  
clear arptable  
clear counters  
clear fdb  
clear log  
config 802.1p default_priority  
config 802.1p user_priority  
config 802.1x auth_mode  
config 802.1x auth_parameter ports  
config 802.1x capability ports  
config 802.1x init  
config 802.1x reauth  
config access_profile profile_id  
config account  
config aggport  
config aggport_actor_admin_state  
config aggport_partner_admin_state  
config aggregator  
config arp_aging time  
config arpentry  
CTRL+C ESC Quit SPACE Next Page ENTER Next Entry 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.

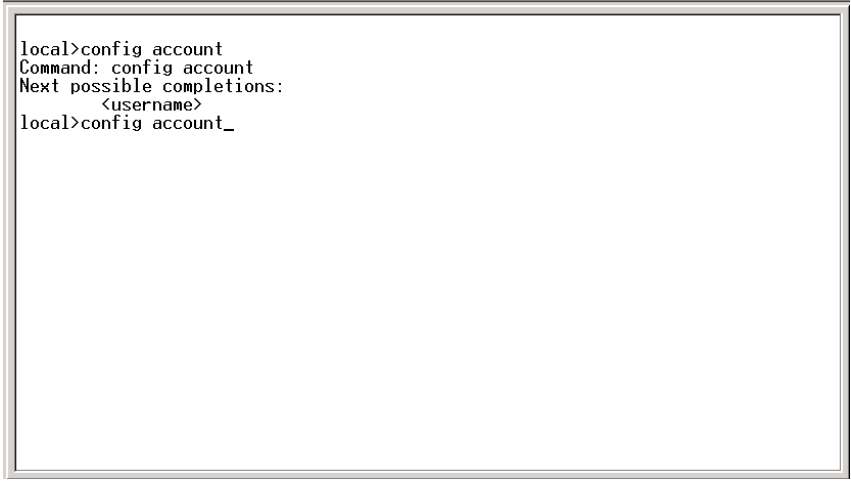
Alternatively, if you hit the **Tab** key immediately after you have entered a command, the CLI will display all the next available parameters sequentially.

```
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.



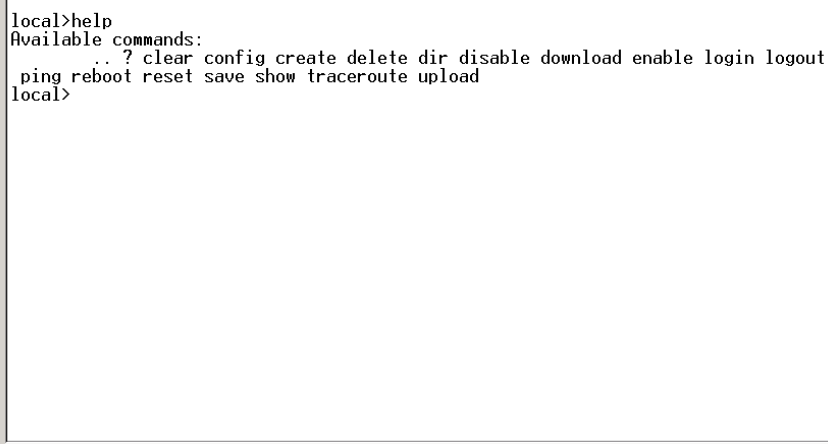
```
local>config account
Command: config account
Next possible completions:
      <username>
local>config account_
```

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 traceroute 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 802.1x access_profile account aggport aggport_actor_state aggport
_partner_state aggregator arprentry bandwidth_control bootp_relay command_history
_dnsr dvmrp error fdb gvrp igmp igmp_snooping ipfdb ipif ipmc iproute lacp link_
aggregation log
      md5 mirror multicast_fdb ospf packet pim port_security ports radius rip
route router_ports scheduling serial_port session snmp snmp stp switch time traf
fic 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	configure ipif System ipaddress <network_address>
Description	In the above syntax example, you must supply the network address in the <network_address> space. Do not type the angle brackets.
Example Command	configure ipif System ipaddress 10.24.22.5/255.0.0.0

[square brackets]	
Purpose	Encloses a required value or set of required arguments. One or more values or arguments can be specified.
Syntax	create account [admin user]
Description	In the above syntax example, you must specify either an admin or a user level account to be created. Do not type the square brackets.
Example Command	create account admin

 vertical bar	
Purpose	Separates two or more mutually exclusive items in a list – one of which must be entered.
Syntax	create account [admin user]
Description	In the above syntax example, you must specify either admin or user. Do not type the vertical bar.
Example Command	create account user

{braces}	
Purpose	Encloses an optional value or set of optional arguments.
Syntax	config serial_port {baud_rate[9600 19200 38400 115200] auto_logout [never 2_minutes 5_minutes 10_minutes 15_minutes]}
Description	In the above syntax example, baud_rate, auto_logout, never, 2_minutes, 5_minutes, 10_minutes, and 15_minutes are all optional arguments. You can specify any or all of the arguments contained by braces. Do not type the braces.
Example command	config serial_port baud_rate 9600

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

Line Editing Key Usage

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.
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 1-65535>
disable telnet	
enable web	<tcp_port_number 1-65535>

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 account [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.
	Username can be between 1 and 15

config account

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.
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

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-3350 Fast-Ethernet Switch
Ext. Ports        : 1000TX + 1000TX
MAC Address       : 00-01-02-03-04-00
IP Address        : 10.24.22.9 (Manual)
VLAN Name         : default
Subnet Mask       : 255.0.0.0
Default Gateway   : 0.0.0.0
Boot PROM Version : Build 1.00.002
Firmware Version  : Build 1.00.012
Hardware Version   : 2A1
System Up Time    : 0 days 04:41:06
Time              : Unknown
Time Source       : System Clock
System Name       :
System Location    :
```

```
System Contact      :  
Spanning Tree      : Disabled  
GVRP               : Disabled  
IGMP Snooping      : Disabled  
RIP                : Disabled  
DVMRP              : Disabled  
PIM-DM             : Disabled  
OSPF               : Disabled  
TELNET             : Enabled (TCP 23)  
SNTP               : 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.
Parameter s	<p>[9600 19200 38400 115200] – The serial bit rate that will be used to communicate with the management host.</p> <p>never – No time limit on the length of time the console can be open with no user input.</p> <p>2_minutes – The console will log out the current user if there is no user input for 2 minutes.</p> <p>5_minutes – The console will log out the current user if there is no user input for 5 minutes.</p> <p>10_minutes – The console will log out the current user if there is no user input for 10 minutes.</p> <p>15_minutes – The console will log out the current user if there is no user input for 15 minutes.</p>
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure 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 1-65535>
Description	This command is used to enable the Telnet protocol on the switch. The user can specify the TCP or UDP port number the switch will use to listen for Telnet requests.
Parameters	<tcp_port_number> – 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 1-65535>
Description	This command is used to enable the Web-based management software on the switch. The user can specify the TCP port number the switch will use to listen for Telnet requests.
Parameters	<tcp_port_number 1-65535> – The TCP port number. TCP ports are numbered between 1 and 65535. The “well-known” port for the Web-based management software is 80.
Restrictions	Only administrator-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	<p>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.</p> <p>system – If system is specified all of the factory default settings are restored on the switch.</p> <p>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.</p>

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] state [enabled disabled] description <desc32>
show ports	[<portlist all>] {description}

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] state [enabled disabled]} description <desc32>
Description	This command allows for the configuration of the switch's Ethernet ports. Only the ports listed in the <portlist> will be affected.
Parameters	<p>all – Displays all ports on the switch to be configured.</p> <p>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.</p> <p>auto – Enables auto-negotiation for the specified range of ports.</p> <p>[10 100 1000] – Configures the speed in Mbps for the specified range of ports.</p> <p>[half full] – Configures the specified range of ports as either full- or half-duplex.</p> <p>state [enabled disabled] – Enables or disables the specified range of ports.</p>

config ports

description <desc 32> - Enter an alphanumeric string of no more than 32 characters to describe a selected port interface.

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 state enabled
```

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

Success.

show ports

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

Syntax **show ports {<portlist|all>}**

description

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

show ports

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.

{description} – Adding this parameter to the **show ports** command indicates that the port description will be included in the display.

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 State	Settings Speed Duplex	Connection Speed Duplex
----	-----	-----	-----
1	Enabled	Auto	Link Down
2	Enabled	Auto	Link Down
3	Enabled	Auto	Link Down
4	Enabled	Auto	Link Down
5	Enabled	Auto	Link Down
6	Enabled	Auto	Link Down
7	Enabled	Auto	Link Down

Example usage:

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

```
local>show ports all description
Command: show ports all description
Port Port  Settings  Connection
      State  Speed/Duplex Speed/Duplex
-----
 1  Enabled  Auto      Link Down
   Desc: 12
 2  Enabled  Auto      Link Down
   Desc: 12
 3  Enabled  Auto      100M/Full
   Desc: 12
 4  Enabled  Auto      Link Down
   Desc: 12
 5  Enabled  Auto      Link Down
   Desc: 12
 6  Enabled  Auto      Link Down
   Desc: 12
 7  Enabled  Auto      Link Down
   Desc: 12
 8  Enabled  Auto      Link Down
   Desc: 12
 9  Enabled  Auto      100M/Full
   Desc: 12
10  Enabled  Auto      Link Down
   Desc: 12
```

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 32> view <view_name 32> [read_only read_write]
delete snmp community	<community_string 32>
create snmp user	<username 32> <groupname 32> {encrypted(1) [by_password(1) auth [md5(2) <auth_password 8-16 > sha(3) <auth_password 8-20 >] priv [none(1) des(2) <priv_password 8-16>] by_key(2) auth [md5(2) <auth_key 32-32> sha(3) <auth_key 40-40>] priv [none(1) des(2) <priv_key 32-32>]]}
delete snmp user	<usmusername 32>
create snmp view	<view_name 32>

Command	Parameters
	<oid> view_type [included excluded]
delete snmp view	<view_name 32> [all <oid>]
show snmp view	{<view_name 32>}
config snmp engineID	<snmp_engineID>
show snmp engineID	
create snmp group	<groupname 32> [v1 v2c v3 [noauth_nopriv auth_nopriv auth_priv]] {read_view <view_name 32> write_view <view_name 32> notify_view <view_name 32>}
delete snmp group	<groupname 32>
create snmp host	<ipaddr> [v1 v2c v3 [noauth_nopriv auth_nopriv auth_priv]] <auth_string 32>
delete snmp host	<ipaddr>
show snmp host	(<ipaddr>)
enable rmon	
disable rmon	
config snmp system_contact	<sw_contact>
config snmp system_location	<sw_location>
config snmp system_name	<sw_name>
enable snmp traps	
disable snmp traps	
enable snmp authenticate traps	

Command	Parameters
disable snmp authenticate traps	
create trusted_host	<ipaddr>
show trusted_host	<ipaddr>
delete trusted_host	<ipaddr>
show snmp	community {<community_string 32> engine ID groups host <ipaddr> user view
ping	<ipaddr> times <value 1-255> timeout <sec 1-99>
traceroute	<ipaddr> ttl <value> port <value> timeout <sec> probe <value>
show ipfdb	{<ipaddr>}

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 32> view <view_name 32>

create snmp community**[read_only | read_write]**

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	<p><community_string 32> – An alphanumeric string of up to 32 characters used to authentication of users wanting access to the switch's SNMP agent.</p> <p>view_name – An alphanumeric string of up to 32 characters used to define the subset of all MIB objects accessible to the given community.</p> <p>read_only – 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.</p> <p>read_write – 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.</p>
Restrictions	Only administrator-level users can issue this command. A maximum of four community strings can be specified.

Example Usage:

To create a read-write level SNMP community “dlink”:

```
local>create snmp community dlink view
CommunityView read_write
Command: create snmp community dlink view
CommunityView read_write

Success.

local>
```

delete snmp community

Purpose	Used to delete an SNMP community string previously entered on the switch.
Syntax	delete snmp community <community_string 32>
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 32> – An alphanumeric string of up to 32 characters used to authenticate 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 “dlink”:

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

Success.

```
local>
```

create snmp user

Purpose	Used to create a new SNMP user to an SNMP group that is also created by this command.
Syntax	create snmp user <username 32> <groupname 32> {encrypted (1) [by_password(1) auth [md5(2)<auth_password 8-16> sha](3) <auth_password 8-20>] priv [none(1) des(2) <priv_password 8-16>] by_key(2) auth [md5(2) <auth_key 32- 32> sha](3) <auth_key 40-40>] priv [none(1) des(2) <priv_key 32-32>]]}
Description	The create snmp user command creates a new SNMP user and adds the user to an SNMP group that is also created by this command.
Parameters	<p><username 32> – An alphanumeric name of up to 32 characters that will identify the new SNMP user.</p> <p><groupname 32> – An alphanumeric name of up to 32 characters that will identify the SNMP group the new SNMP user will be associated with.</p> <p>encrypted – Specifies whether the password</p>

create snmp user

appears in encrypted format.

by_password – Indicates input password for authentication and privacy.

by_key – Indicates input key for authentication and privacy.

auth [md5 | sha] – Initiate an authentication-level setting session.

md5 – Specifies that the HMAC-MD5-96 authentication level will be used.

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

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

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

<auth_key> – An authentication key used by MD5 or SHA1. It is a hex string type.

<priv_key> –A privacy key used by DES. It is a hex string type.

Restrictions

Only administrator-level users can issue this command.

Example Usage:

To create an SNMP user on the switch:

```
local>create snmp user dlink D-Link_group encrypted  
by_password auth md5 12345678 priv des 12345678
```

```
Command: create snmp user dlink D-Link_group encrypted  
by_password auth md5 12345678 priv des 12345678
```

Success.

```
local>
```

delete snmp user

Purpose	Used to remove a user from an SNMP group and delete the associated group in SNMP group.
Syntax	delete snmp user
Description	The delete SNMP user command removes a user from an SNMP group and deletes the associated group in the SNMP group.
Parameters	<usmusername 32> – An alphanumeric string of up to 32 characters used to identify the user on the host that connects to the agent.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete an SNMP user named “dlink”:

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

Success.

local>
```

create snmp view

Purpose	Used to assign views to community strings to limit which MIB objects an SNMP manager can access.
Syntax	create snmp view <view_name 32> <oid> view_type [included excluded]
Description	The create SNMP view assigns views to community strings to limit which MIB objects an SNMP manager can access.
Parameters	<p><view_name 32> – View name to be created.</p> <p><oid> – Object-Identified tree, MIB tree.</p> <p>view_type – Specify the access type of the MIB tree in the view.</p> <p>included – Includes for this view.</p> <p>excluded – Excluded for this view.</p>
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To create an SNMP view:

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

delete snmp view

Purpose	Used to remove a view record.
Syntax	delete snmp view <view_name 32> [all <oid>]
Description	The delete SNMP view command removes a view record.
Parameters	<view_name 32> – View name of the user who will be deleted. all – All view records. <oid> – Object-Identified tree, MIB tree.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete an SNMP view:

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

Success.

local>
```

show snmp view

Purpose	Used to display the SNMP view record.
Syntax	show snmp view {<view_name 32>}
Description	The show SNMP view command displays the SNMP view record.
Parameters	<view_name 32> – View name of the user you would like to show.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To show an SNMP view:

```
local>show snmp view
Command: show snmp view

Vacm View Table Settings
View Name      Subtree      View Type
-----
```

restricted	1.3.6.1.2.1.1	Included
restricted	1.3.6.1.2.1.11	Included
restricted	1.3.6.1.6.3.10.2.1	Included
restricted	1.3.6.1.6.3.11.2.1	Included
restricted	1.3.6.1.6.3.15.1.1	Included
CommunityView	1	Included
CommunityView	1.3.6.1.6.3.	Excluded
CommunityView	1.3.6.1.6.3.1	Included

Total Entries: 8

local>

local>

config snmp engineID

Purpose	Used to configure an identifier for the SNMP engine on the switch.
Syntax	config snmp engineID
Description	This config snmp engineID command configures an identifier for the SNMP engine on the switch. Associated with each SNMP entity is a unique engineID.
Parameters	snmp_engineID – Identity for the SNMP engine on the switch. It is an octet string type.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure an SNMP engine on the switch:

```
local>config snmp engineID 1023457890
Command: config snmp engineID 1023457890

Success.

local>
```

show snmp engineID

Purpose	Used to display the identification of the SNMP engine on the switch.
Syntax	show snmp engineID
Description	This show snmp engineID command displays the identification of the SNMP engine on the switch. The default value is suggested in RFC 2271. The very first bit is 1, and the first four octets are set to the binary equivalent of the agent's SNMP management private enterprise number as assigned by IANA, D-Link is 171. The fifth octet is 03 to indicate the rest is the MAC address of this device. The 6 th through 11 th octets are the MAC address.
Parameters	none.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To display an SNMP engine on the switch:

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

SNMP Engine ID : 1023457890

local>
```

create snmp group

Purpose	Used to create a new SNMP group, or a table that maps SNMP users to SNMP views.
Syntax	create snmp group <groupname 32> [v1 v2c v3 [noauth_priv auth_nopriv auth_priv]] {read_view <view_name 32> notify_view <view_name 32> notify_view <view_name 32>}
Description	The create snmp group command creates a new SNMP group.
Parameters	<p><groupname 32> – An alphanumeric name of up to 32 characters that will identify the new SNMP group.</p> <p>v1 – The least secure of the possible security models.</p> <p>v2c – The second least secure of the possible security models.</p> <p>v3 – The most secure of the possible security models.</p> <p>noauth_nopriv – Specifies neither support for packet authentication nor encrypting.</p>

create snmp group

auth_nopriv – Specifies support for packet authentication.

auth_priv – Specifies support for packet authentication and encrypting.

<view_name 32> – View name, the MIB view.

Restrictions Only administrator-level users can issue this command.

Example Usage:

To create an SNMP group on the switch:

```
local>create snmp group dlink D_Link_group v3 auth_priv  
read_view CommunityView write_view CommunityView  
notify_view CommunityView
```

Command: create snmp group dlink D_Link_group v3 auth_priv
read_view CommunityView write_view CommunityView
notify_view CommunityView

Success.

```
local>
```

delete snmp group

Purpose Used to delete an SNMP group.

Syntax **delete snmp group <groupname 32>**

Description The delete snmp group command removes

delete snmp group

an SNMP group.

Parameters	<groupname 32> – An alphanumeric name of up to 32 characters that will identify the SNMP group that will be deleted.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete an SNMP group on the switch:

```
local>delete snmp group D_Link_group
```

```
Command: delete snmp group D_Link_group
```

Success.

```
local>
```

create snmp host

Purpose	Used to create a recipient of an SNMP trap operation.
Syntax	create snmp host <ipaddr> [v1 v2c v3 [noauth_priv auth_nopriv auth_priv]] <auth_string 32>
Description	The create snmp host command creates a recipient of an SNMP operation.
Parameters	<ipaddr> – The IP address of the recipient for which the traps are targeted.

create snmp host

v1 – The least secure of the possible security models.

v2c – The second least secure of the possible security models.

v3 – The most secure of the possible security models.

noauth_nopriv – Specifies neither support for packet authentication nor encrypting.

auth_nopriv – Specifies support for packet authentication.

auth_priv – Specifies support for packet authentication and encrypting.

<auth_string> – The authentication string.

Restrictions Only administrator-level users can issue this command.

Example Usage:

To create an SNMP host on the switch:

```
local>create snmp host 10.48.74.100 v3 noauth_nopriv initial
```

```
Command: create snmp host 10.48.74.100 v3 noauth_nopriv  
initial
```

```
Success.
```

```
local>
```

delete snmp host

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

Example Usage:

To delete an SNMP host on the switch:

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

Success.

local>
```

show snmp host

Purpose	Used to display the identification of the SNMP engine on the switch.
Syntax	show snmp host {<ipaddr>}

show snmp host

Description	This show snmp host command displays the recipient for which the traps are targeted.
Parameters	<ipaddr> – The IP address of the recipient for which the traps are targeted. If no parameter is specified, all SNMP hosts will be displayed.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To display an SNMP engine on the switch:

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

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

Total Entries : 2
local>
```

enable rmon

Purpose	Used to enable RMON on the switch.
---------	------------------------------------

enable rmon

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

Example Usage:

To enable RMON:

```
local>enable rmon
Command: enable rmon

Success.

local>
```

disable rmon

Purpose	Used to disable RMON on the switch.
Syntax	disable rmon
Description	This command is used, in conjunction with the enable rmon command above, to enable and disable remote monitoring (RMON) on the switch.

disable rmon

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

Example Usage:

To disable RMON:

```
local>disable rmon
Command: disable rmon

Success.

local>
```

config snmp system_contact :

Purpose	Used to enter the name of a contact person who is responsible for the switch.
Syntax	config snmp system_contact <sw_contact>
Description	This command is used to enter the name and/or other information to identify a contact person who is responsible for the switch. A maximum of 255 characters can be used.
Parameters	<sw_contact> – A maximum of 255 characters used to identify a contact

config snmp system_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>
```

config snmp system_location

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

config snmp system_location

this command.

Example Usage:

To configure the switch location for “Rota”:

```
local>config snmp system_location Rota
Command: config snmp system_location Rota

Success.

local>
```

config snmp system_name

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

Example Usage:

To configure the switch name for “DES-3350”:

```
local>config snmp system_name DES3350
Command: config snmp system_name DES3350

Success.

local>
```

enable snmp traps

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

Example Usage:

To turn on SNMP trap support:

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

Success.

local>
```

disable snmp traps

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

Example Usage:

To prevent SNMP traps from being sent from the switch:

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

Success.

local>
```

enable snmp authenticate traps

Purpose	Used to enable SNMP authentication trap support.
Syntax	enable snmp authenticate traps

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.

disable snmp authenticate traps

this command.

Example Usage:

To turn off SNMP authentication trap support:

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

Success.

local>
```

create trusted_host

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

Example Usage:

To create a trusted host:

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

Success.

local>
```

show trusted_host

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

Example Usage:

To display the list of trusted hosts:

```
local>show trusted_host
Command: show trusted_host
```


Management Stations**IP Address:**-----
10.1.1.1**Total Entries: 1****local>****delete trusted_host**

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

Example Usage:

To delete a trusted host with an IP address 10.48.74.121:

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

Success.
```

```
local>
```

show snmp

Purpose	Used to display various SNMP configuration information entered on the switch.
Syntax	show snmp [community <community_string 32> engineID groups host <ipaddr> user view]
Description	This command will display the current SNMP configuration on the switch.
Parameters	<p>community – This command is used to display SNMP community strings that are configured on the switch.</p> <p><community string 32> – An alphanumeric string of up to 32 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the switch's SNMP agent.</p> <p>engineID – This command displays the identification of the SNMP engine on the switch.</p> <p>groups – This command displays the group-names of SNMP groups currently configured on the switch. The security model, level, and status of each group is</p>

show snmp

also displayed.

host – This command is used to display the IP addresses and configuration information of remote SNMP managers that are designated as recipients of SNMP traps that are generated by the switch's SNMP agent.

<ipaddr> – The IP address of a remote SNMP manager that will receive SNMP traps generated by the switch's SNMP agent.

user – This command displays information about each SNMP username in the SNMP group username table.

view – This command displays an SNMP view previously created on the switch.

<view_name 32> – An alphanumeric string of up to 32 characters that identifies the SNMP view that will be displayed.

Restrictions none.

Example Usage:

To display SNMP community community strings configured on the switch:

```
local>show snmp community  
Command: show snmp community
```

Community Name	View Name	Access Right
private	CommunityView	read_write
public	CommunityView	read_only
Total Entries: 1		
local>		

ping

Purpose	Used to test the connectivity between network devices.
Syntax	ping <ipaddr> {times <value 1-255>} {timeout <sec 1-99>}
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	<p><ipaddr> – The IP address of the remote device.</p> <p>times <value 1-255> – The number of individual ICMP echo messages to be sent. A value of 0 will send an infinite ICMP echo messages. The maximum value is 255. The default is 0.</p>

ping

timeout <sec 1-99> – Defines the time-out period while waiting for a response from the remote device. A value of 1 to 99 seconds can be specified. The default is 1 second.

Restrictions Only administrator-level users can issue this command.

Example Usage:

To send ICMP echo message to “10.48.74.121” for four times:

```
local>#ping 10.48.74.121 times 4
Command: ping 10.48.74.121
Reply from 10.48.74.121, time<10ms
Reply from 10.48.74.121, time<10ms
Reply from 10.48.74.121, time<10ms
Reply from 10.48.74.121, time<10ms
Ping Statistics for 10.48.74.121
Packets: Sent =4, Received =4, Lost =0
local>
```

traceroute

Purpose Used to determine the network path between two devices.

Syntax **traceroute <ipaddr> {ttl <value>} {port <value>} {timeout <sec>} {probe <value>}**

traceroute

Description	This command allows you to trace a route between the switch and a given host on the network.
Parameters	<p><ipaddr> – The IP address of the remote device.</p> <p>ttl <value> – The time to live value of the trace route request. This is the maximum number of routers the traceroute command will cross while seeking the network path between two devices. The maximum value is</p> <p>port <value> – The port number. Must be above 1024.</p> <p>timeout <sec> – The age-out time.</p> <p>probe <value> – The number of probing.</p>
Restrictions	Only administrator-level users can issue this command.

Example Usage:

Trace the routed path between the switch and 10.48.74.121.:

```
local>traceroute 10.48.74.121 probe 3
Command: traceroute 10.48.74.121 probe 3

1 <10 ms.  10.48.74.121
1 <10 ms.  10.48.74.121
```

```
1 <10 ms. 10.48.74.121
local>
```

show ipfdb

Purpose	Used to show the IP forwarding database.
Syntax	show ipfdb {<ipaddr>}
Description	This command allows you to display the IP forwarding database.
Parameters	<ipaddr> – The IP address of the forwarding database.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To show the IP forwarding database table:

```
local>show ipfdb
Command: show ipfdb
```

Interface	IP Address	Port	Learned
-----	-----	-----	-----
System	10.0.0.2	17	Dynamic
System	10.0.0.168	17	Dynamic
System	10.0.34.1	17	Dynamic
System	10.0.46.1	17	Dynamic
System	10.0.51.1	17	Dynamic
System	10.0.58.4	17	Dynamic
System	10.0.85.168	17	Dynamic
System	10.1.1.4	17	Dynamic
System	10.1.1.88	17	Dynamic

System	10.1.1.101	17	Dynamic
System	10.1.1.102	17	Dynamic
System	10.1.1.151	17	Dynamic
System	10.1.1.154	17	Dynamic
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 127> configuration <ipaddr> <path_filename 127> {increment}
upload	configuration log <ipaddr> <path_filename 127>

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 127> configuration <ipaddr> <path_filename 127> {increment}]
Description	This command is used to download a new firmware or a switch configuration file from a TFTP server.
Parameters	<p>firmware – Download and install new firmware on the switch from a TFTP server.</p> <p>configuration – Download a switch configuration file from a TFTP server.</p> <p><ipaddr> – The IP address of the TFTP server.</p> <p><path_filename 127> – The DOS path and filename of the firmware or switch configuration file on the TFTP server. For example, C:\3350.had.</p> <p>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.</p>
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 127>
Description	This command is used to upload either the switch's current settings or the switch's history log to a TFTP server.
Parameters	<p>configuration – Specifies that the switch's current settings will be uploaded to the TFTP server.</p> <p>log – Specifies that the switch history log will be uploaded to the TFTP server.</p>

upload

<ipaddr> – The IP address of the TFTP server. The TFTP server must be on the same IP subnet as the switch.

<path_filename 127> – 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 utilization	[cpu ports {<portlist>}]
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
65-127	755	10	RX Frames	4395
128-255	316	1		19
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+CESCQuitSPACENext PagePrevious PageRefresh

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 and cpu utilization statistics.
Syntax	show utilization [cpu ports {<portlist>}]
Description	<p>cpu - Entering this parameter will display the current cpu utilization of the switch.</p> <p>ports - Entering this parameter will display the current port utilization of the switch.</p> <p><portlist> Specifies a port or range of ports to be displayed</p>
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

To display the cpu utilization statistics:

```
local>show utilization CPU
Command: show utilization CPU
CPU utilization :
-----
Five seconds - 39%    One minute - 82%    Five minutes - 39%

Success.
local>
```

clear counters

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

Example Usage:

To clear the counters:

```
local>clear counters ports 7-9
Command: clear counters ports 7-9

Success.

local>
```

clear log

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

show log

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 auto <value 1-200000000> priority <value 0-240> migrate [yes no] edge [true false] p2p [true false auto] state [enabled disabled]
config stp	maxage <value 6-40> hellotime <value 1-10> forwarddelay <value 4-30> priority <value 0-61440> version[rstp stp] txholdcount<value 1-10> fdpdu [enabled disabled]
enable stp	
disable stp	

Command	Parameters
show stp	
show stp ports	<portlist>

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

config stp ports

Purpose	Used to set up STP on the port level.
Syntax	config stp ports <portlist> {cost [auto <value 1-200000000>] priority <value 0-240> migrate [yes no] edge [true false] p2p [true false auto] state [enabled disabled]}
Description	This command is used to set up the Spanning Tree Protocol (STP) on the port level.
Parameters	<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

config stp ports

sub-commands listed below.

cost <value> – This defines a metric that indicates the relative cost of forwarding packets to the specified port list. The default cost for a 1000 Mbps port is 20,000, a 100 Mbps port is 200,000, and for a 10 Mbps port the default cost is 2,000,000.

auto – This instructs the switch to automatically detect the path cost based on the link speed of the port.

<value 1-2000000000> – This defines a metric that indicates the relative cost of forwarding packets to the specified port list.

priority <value 0-240> – This numeric value is between 0 and 240 and must also be divisible by 16. It is used in determining the root and designated port in an STP port list. The default is 128, with 0 indicating the highest priority.

migrate [yes|no] – yes will enable the port to migrate from 802.1d STP status to 802.1w RSTP status. RSTP can coexist with standard STP, however the benefits of RSTP are not realized on a port where an 802.1d network connects to an 802.1w enabled network. Migration should be enabled (yes) on ports connected to network stations or segments that will be upgraded to 802.1w RSTP on all or some portion of the segment.

config stp ports

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

p2p [true|false] – true indicates a point-to-point (p2p) shared link. These are similar to edge ports however they are restricted in that a p2p port must operate in full-duplex. Like edge ports, p2p ports transition to a forwarding state rapidly thus benefiting from RSTP.

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

Restrictions Only administrator-level users can issue this command.

Example Usage:

To config STP ports 5 to 10:

```
local>config stp ports 5-10 state enabled
Command: config stp ports 5-10 state enabled

Success.

local>
```


config stp

Purpose	Used to set up STP on the switch level.
Syntax	config stp {maxage <value 6-40> hellotime <value 1-10>forwarddelay <value 4-30> priority <value 0-61440> version [rstp stp] txholdcount <value 1-10> fbpdu [enabled disabled]}
Description	This command is used to set up the Spanning Tree Protocol (STP) on the switch level.
Parameters	<p>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.</p> <p>hellotime <value 1-10> – The time interval between transmission of configuration messages by the device. The default is 2 seconds.</p> <p>forwarddelay <value 4-30> – The maximum amount of time (in seconds) that the device will wait before changing states. The default is 15 seconds.</p> <p>priority <value 0-61440> – A numerical value between 0 and 61,440 that is used in determining the root device, root port, and designated port. The device with the highest priority becomes the root device. The lower the numerical value, the higher</p>

config stp

the priority. The default is 32,768.

version [rstp|stp] – Select the Spanning Tree Protocol version used for the switch. For IEEE 802.1d STP select STP. Select RSTP for IEEE 802.1w Rapid STP.

txholdcount <value 1-10> – The maximum number of Hello packets transmitted per interval. Default value = 3.

fdpdu [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 configure STP with maxage 18 and hellotime 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.
---------	--

enable stp

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

Example Usage:

To enable STP 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.

disable stp

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              : 20
Hello Time           : 2
Forward Delay        : 15
Priority              : 32768
STP Version          : STP compatible
TX Hold Count        : 3
Forwarding BPDU      : Disabled

Designated Root Bridge : 00-00-00-12-00-00
Root Priority           : 32768
Cost to Root           : 17
Root Port              : 33
Last Topology Change   : 106sec
Topology Changes Count : 11
Protocol Specification : 3
Max Age                : 20
Hello Time             : 2
Forward Delay          : 15
Hold Time              : 3

local>
```

Status 2: STP Disabled

```
local>show stp
Command: show stp

STP Status           : Disabled
Max Age              : 20
Hello Time           : 2
Forward Delay        : 15
```

```
Priority          : 32768
STP Version       : STP compatible
TX Hold Count    : 3
Forwarding BPDU   : Enabled

local>
```

show stp ports

Purpose	Used to display the switch's current per-port group STP configuration.
Syntax	show stp ports <portlist>
Description	This command displays the switch's current per-port group STP configuration.
Parameters	<portlist> – Specifies a range of ports to be configured. The port list is specified by listing the 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 STP state of port 1-9:

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

Port	Designated Bridge	State	Cost	Pri	Edge	P2P	Status	Role
1	N/A	Yes	*200000	128	No	Yes	Forwarding	NonStp
2	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
3	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
4	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
5	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
6	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
7	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
8	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
9	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled

10

FORWARDING DATABASE COMMANDS

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

Command	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

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

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

create fdb

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] <portlist>
Description	This command configures the multicast MAC address forwarding table.
Parameters	<vlan_name 32> – The name of the VLAN on which the MAC address resides. <macaddr> – The MAC address that will be added to the forwarding table. [add delete] – Add will add the MAC

config multicast_fdb

address to the forwarding table, delete will remove the MAC address from the forwarding table.

<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

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	<p><vlan_name 32> – The name of the VLAN on which the MAC address resides.</p> <p><macaddr> – The MAC address that will be added to the forwarding table.</p>
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
---------	---

clear fdb

addresses. You can enter a VLAN name and MAC address to delete a specific entry, or skip the MAC address parameter and delete all the entries belonging to a specified VLAN.

Syntax	clear fdb [vlan <vlan_name 32>{mac_address <macaddr>} port <port> all]
Description	This command is used to clear dynamically learned entries from the switch's forwarding database.
Parameters	<p><vlan_name 32> – The name of the VLAN on which the MAC address resides.</p> <p><macaddr> – Enter the MAC address of the entry to be deleted.</p> <p><port> – The port number corresponding to the MAC destination address. The switch will always forward traffic to the specified device through this port.</p> <p>all – Clears all dynamic entries to the switch's forwarding database.</p>
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	<p><vlan_name 32> – The name of the VLAN on which the MAC address resides.</p> <p><macaddr> – The MAC address that will be added to the forwarding table.</p>
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 switch.

config fdb aging_time

Parameters	<sec> – The aging time for the MAC address forwarding database value.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To set the fdb aging time:

```
Local>config fdb aging_time 25
Command: config fdb aging_time 25
```

Success.

```
local>
```

show fdb

Purpose	Used to display the current unicast MAC address forwarding database.
Syntax	show fdb {port <port> vlan <vlan_name 32> mac_address <macaddr> static aging_time}
Description	This command will display the current contents of the switch's forwarding database.
Parameters	<port> – The port number corresponding to the MAC destination address. The switch

show fdb

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>

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	<p><storm_grouplist 1-8> – Used to specify a broadcast storm control group.</p> <p>all – Specifies all broadcast storm control groups on the switch.</p> <p>broadcast [enabled disabled] – Enables or disables broadcast storm control.</p> <p>multicast [enabled disabled] – Enables or disables multicast storm control.</p> <p>dlf [enabled disabled] – Enables or disables dlf traffic control.</p> <p>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.</p>
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure traffic control and state:

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

Success.

local>
```

show traffic control

Purpose	Used to display current traffic control settings.
Syntax	show traffic control { group_list <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.
Restrictions	none.

Example Usage:

To display traffic control setting:

```
local>show traffic control
```

Command: show traffic control

Traffic Control

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

Total Entries: 8

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> {max_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	<p>The switch contains four hardware priority queues. Incoming packets must be mapped to one of these four queues. This command is used to specify the rotation by which these four hardware priority queues are emptied.</p> <p>The switch's default (if the config scheduling command is not used, or if the config scheduling command is entered with both</p>

config scheduling

max_packet and max_latency parameters are set to 0) is to empty the four hardware priority queues in order – from the highest priority queue (hardware queue 3) to the lowest priority queue (hardware queue 0). Each hardware queue will transmit all of the packets in its buffer before allowing the next lower priority queue to transmit its packets. When the lowest hardware priority queue has finished transmitting all of its packets, the highest hardware priority queue can again transmit any packets it may have received.

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 three packets – then the next lowest hardware priority queue (number 2) will be allowed to transmit three packets, and so on, until all of the queues have transmitted three 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

config scheduling

specified. This number is then multiplied by 16 ms to determine the maximum latency. For example, if 3 is specified, the maximum latency allowed will be $3 \times 16 = 48$ 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

config scheduling

the total allowed time for the queue to transmit packets. For example, a value of 3 specifies $3 \times 16 = 48$ 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

show scheduling

switch.

Parameters none.

Restrictions none.

Example Usage:

```
Local> show scheduling
Command: show scheduling
```

QOS Output Scheduling

	MAX. Packets	MAX. Latency
	-----	-----
Class-0	100	150
Class-1	99	100
Class-2	91	101
Class-3	21	201

local>

config 802.1p user_priority

Purpose Used to map the 802.1p user priority of an incoming packet to one of the four hardware queues available on the switch.

Syntax **config 802.1p user_priority <priority 0-7>**
<class_id 0-3>

config 802.1p user_priority**Description**

This command allows you to configure the way the switch will map an incoming packet, based on its 802.1p user priority, to one of the four available hardware priority queues on the switch.

The switch's default is to map the following incoming 802.1p user priority values to the four hardware priority queues:

802.1p	Hardware Queue	Remark
0	1	Mid-low
1	0	Lowest
2	0	Lowest
3	1	Mid-low
4	2	Mid-high
5	2	Mid-high
6	3	Highest
7	3	Highest.

This mapping scheme is based upon recommendations contained in IEEE 802.1D.

You can change this mapping by specifying the 802.1p user priority you want to go to the <class_id 0-3> (the number of the hardware queue).

config 802.1p user_priority

<priority 0-7> – The 802.1p user priority you want to associate with the <class_id 0-3> (the number of the hardware queue) with.

<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_priority

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

config 802.1p default_priority

settings on the switch. If an untagged packet is received by the switch, the priority configured with this command will be written to the packet's priority field.

Syntax	config 802.1p default_priority [<portlist> all] <priority 0-7>
Description	This command allows you to specify default priority handling of untagged packets received by the switch. The priority value entered with this command will be used to determine which of the four hardware priority queues the packet is forwarded to.
Parameters	<p><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.</p> <p>all – Specifies that the command applies to all ports on the switch (or in the switch stack).</p> <p><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.</p>
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 [all] <portlist>]
Description	This command is used to display the current default priority settings on the switch.
Parameters	<p>all – Specifies that the command applies to all ports on the switch (or in the switch stack).</p> <p><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</p>

show 802.1p default_priority

specifies all of the ports between port 3 and port 4 – in numerical order.

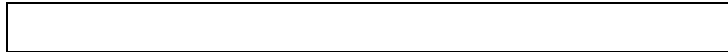
Restrictions None.

Example Usage:

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

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

```
CTRL+C [ESC] q QUIT SPACE n Next Page Enter Next Entry a All
```



config traffic_segmentation

Purpose	Used to configure traffic segmentation on the switch.
Syntax	config traffic_segmentation <portlist> forward_list [null <portlist>]
Description	The config traffic_segmentation command is used to configure traffic segmentation on the switch.
Parameters	<p><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.</p> <p>forward_list – Specifies a range of ports that will receive forwarded frames from the ports specified in the portlist above.</p> <p> null – Specifies that packets cannot be forwarded to any ports.</p> <p> <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</p>

config traffic_segmentation

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

show traffic_segmentation

segmentation configuration on the switch.

Parameters <portlist> – Specifies a range of ports for which the current traffic segmentation configuration on the switch will be displayed. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.

Restrictions None.

Example Usage:

To display the current traffic segmentation configuration on the switch:

```
local> show traffic_segmentation
Command: show traffic_segmentation
```

Traffic Segmentation Table

Port	Forward Portlist
------	------------------

1	9-15
2	9-15
3	9-15
4	9-15
5	9-15
6	9-15

7 9-15
8 9-15
9 9-15
10 9-15
11 1-26
12 1-26
13 1-26
14 1-26
15 1-26
16 1-26
17 1-26
18 1-26

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

config bandwidth_control

Purpose	Used to configure bandwidth control on a by-port basis.
Syntax	config bandwidth_control <portlist> rx_rate [no_limit <value 1-1000>] tx_rate [no_limit <value 1-1000>]
Description	The config bandwidth_control command is used to configure bandwidth on a by-port basis.
Parameters	<portlist> – Specifies a range of ports to be configured. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.

config bandwidth_control

rx_rate – Specifies that one of the parameters below (**no_limit** or **<value 1-1000>**) will be applied to the rate at which the above specified ports will be allowed to receive packets

no_limit – Specifies that there will be no limit on the rate of packets received by the above specified ports.

<value 1-1000> – Specifies the limit, in Mbps, that the above ports will be allowed to receive packets.

tx_rate – Specifies that one of the parameters below (**no_limit** or **<value 1-1000>**) will be applied to the rate at which the above specified ports will be allowed to transmit packets.

no_limit – Specifies that there will be no limit on the rate of packets received by the above specified ports.

<value 1-1000> – Specifies the limit, in Mbps, that the above ports will be allowed to receive packets.

Restrictions

Only administrator-level users can issue this command.

Example Usage:

To configure bandwidth control:


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

Success.

```
local>
```

show bandwidth_control

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

Example Usage:

To show bandwidth control for ports 1 through 11:

```
local>show bandwidth_control 1-11
```

```
Command: show bandwidth_control 1-11
```

Bandwidth Control Table

Port	RX Rate (Mbit sec)	TX_RATE (Mbit sec)
----	-----	-----
1	no_limit	10
2	no_limit	10
3	no_limit	10
4	no_limit	10
5	no_limit	10
6	no_limit	10
7	no_limit	10
8	no_limit	10
9	no_limit	10
10	no_limit	10
11	no_limit	no_limit

```
local>
```

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 delete] source ports <portlist> [rx tx both]
Description	This command allows you to add or delete mirroring ports. It also allows a range of ports to have all of their traffic sent to a designated port – where a network sniffer or other device can monitor the network traffic. You can also specify that only traffic received by or sent by or both is mirrored to the Target port.
Parameters	<p><port> – This specifies the Target port (the port where mirrored packets will be sent).</p> <p><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.</p> <p>rx – Allows the mirroring of only packets received (flowing into) the port or ports in the port list.</p> <p>tx – Allows the mirroring of only packets sent (flowing out of) the port or ports in the</p>

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

Success.

```
local>
```

enable mirror

Purpose Used to enable a previously entered port mirroring configuration.

Syntax **enable mirror**

Description This command, combined with the disable mirror command below, allows you to enter a port mirroring configuration into the switch, and then turn the port mirroring on and off without having to modify the port mirroring configuration.

enable mirror

Parameters	none.
Restrictions	none.

Example Usage:

To enable mirroring configurations:

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

disable mirror

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

Example Usage:

To disable mirroring configurations:

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

show mirror

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

Example Usage:

To display mirroring configuration:

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


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	<p><vlan_name 32> – The name of the VLAN to be created.</p> <p><vlanid> – The VLAN ID of the VLAN to be created.</p> <p>advertisement – Specifies the VLAN as able to join GVRP. If this parameter is not set, the VLAN cannot be configured to have forbidden ports.</p>
Restrictions	Each VLAN name can be up to 32 characters. 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	<p><vlan_name 32> – The name of the VLAN you want to add ports to.</p> <p>tagged – Specifies the additional ports as tagged.</p> <p>untagged – Specifies the additional ports as untagged.</p> <p>forbidden – Specifies the additional ports as forbidden.</p> <p><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</p>

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 32> advertisement [enabled disabled]
--------	--

config vlan advertisement

Description	This command is used to enable or disable GVRP on the specified VLAN.
Parameters	<p><vlan_name 32> – The name of the VLAN on which you want to enable or disable GVRP.</p> <p>enabled – Enables GVRP on the specified VLAN.</p> <p>disabled – Disables GVRP on the specified VLAN.</p>
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	<p><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.</p> <p>all – Specifies all of the ports on the switch.</p> <p>state [enabled disabled] – Enabled or disables GVRP for the ports specified in the port list.</p> <p>ingress_checking [enabled disabled] – Enables or disables ingress checking for the specified port list.</p>
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

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	<p>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.</p>
Parameters	<p><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</p>

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 <group_id 1-6> {type [lacp static]}
delete link_aggregation	group_id <group_id 1-6>
config link_aggregation	group_id <group_id 1-6> {master_port <port> ports <portlist> state [enabled disabled]}
config link_aggregation algorithm	mac_source mac_destination mac_source_dest ip_source ip_destination ip_source_dest
config lacp_port	<portlist> mode [active passive]

Command	Parameters
show link_aggregation	{group_id <group_id 1-6> algorithm}
show lacp_port	<portlist>

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

create link_aggregation group_id

Purpose	Used to create a link aggregation group on the switch.
Syntax	create link_aggregation group_id <group_id 1-6> {type [lacp static]}
Description	This command will create a link aggregation group.
Parameters	<p><group_id 1-6> – Specifies the group id. The switch allows up to six link aggregation groups to be configured. The group number identifies each of the groups.</p> <p>type [lacp static] – Specifies the type of group ID.</p>
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To create a link aggregation group:


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

Success.

local>
```

delete link_aggregation group_id

Purpose	Used to delete a previously configured link aggregation group.
Syntax	delete link_aggregation group_id <group_id 1-6>
Description	This command is used to delete a previously configured link aggregation group.
Parameters	<group_id 1-6> – Specifies the group id. The switch allows up to six 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 4
Command: delete link_aggregation group_id 4

Success.
```

```
local>
```

config link_aggregation

Purpose	Used to configure a previously created link aggregation group.
Syntax	config link_aggregation group_id <group_id 1-6> {master_port <port> ports <portlist> state [enabled disabled]}
Description	This command allows you to configure a link aggregation group that was created with the create link_aggregation command above.
Parameters	<p><group_id 1-6> – Specifies the group id. The switch allows up to six link aggregation groups to be configured. The group number identifies each of the groups.</p> <p><port> – Master port ID. Specifies which port (by port number) of the link aggregation group will be the master port.</p> <p><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</p>

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 7 ports 5-10
Command: config link_aggregation group_id 1 master_port 7
ports 5-10
```

Success.

```
local>
```

config link_aggregation algc rithm

Purpose Used to configure the link aggregation algorithm.

Syntax **config link_aggregation algorithm**
 [mac_source | mac_destination | mac_source_d
 est |
 ip_source | ip_destination | ip_source_dest]

config link_aggregation algc rithm

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	<p>mac_source – Indicates that the switch should examine the MAC source address.</p> <p>mac_destination – Indicates that the switch should examine the MAC destination address.</p> <p>mac_source_dest – Indicates that the switch should examine the MAC source and destination addresses</p> <p>ip_source – Indicates that the switch should examine the IP source address.</p> <p>ip_destination – Indicates that the switch should examine the IP destination address.</p> <p>ip_source_dest – Indicates that the switch should examine the IP source address and the destination address.</p>
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>
```

config lacp_port

Purpose	Used to configure the current mode of the Link Aggregation Control Protocol port.
Syntax	config lacp_port <portlist> mode [active passive]
Description	This command is used to configure LACP mode on a per port basis.
Parameters	portlist – Specifies a range of ports to be configured. mode [active passive] – This setting can be either active or passive.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure port LACP mode:

```
local>config lacp_port 1-12 mode active
Command: config lacp_port 1-12 mode active
```

Success.

local>

show link_aggregation

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

Example Usage:

To show link aggregation:

local>show link_aggregation

Command: show link_aggregation

Link Aggregation Algorithm = MAC-source

```
Group ID      : 5
Type          : TRUNK
Master Port   : 0
Member Port   :
Active Port   :
Status        : Disabled
Flooding Port : 0

local>
```

show lacp_port

Purpose	Used to show the current mode of the Link Aggregation Control Protocol port.
Syntax	show lacp_port <portlist>
Description	This command displays LACP mode on a per port basis.
Parameters	portlist – Specifies a range of ports to be configured.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To show the LACP ports:

```
local>show lacp_port
Command: config lacp_port

Port      Activity
-----

```

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

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	<ipif_name 12> vlan <vlan_name 32> ipaddress <network_address> state [enabled disabled] bootp dhcp
create ipif	<ipif_name 12> <network_address> <vlan_name 32> {state [enabled disabled]}
delete ipif	<ipif_name 12> all
enable ipif	<ipif_name 12> all
disable ipif	<ipif_name 12> all

Command	Parameters
show ipif	<ipif_name 12>

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

config ipif

Purpose	Used to configure an IP interface created with the create ipif command.
Syntax	config ipif <ipif_name 12> [{ipaddress <network_address> vlan <vlan_name 32> state [enabled disabled]} bootp dhcp}]
Description	This command is used to configure a previously created IP interface on the switch.
Parameters	<p><ipif_name 12> – The name of the IP interface.</p> <p><vlan_name 32> – The name of the VLAN corresponding to the System IP interface.</p> <p><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).</p> <p>state [enabled disabled] – Allows you to enable or disable the IP interface.</p> <p>bootp – Allows the selection of the BOOTP</p>

config ipif

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 named “sublime”:

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

Success.

```
local>
```

create ipif

Purpose Used to create an IP interface on the switch.

Syntax **create ipif <ipif_name 12> <network address> <vlan_name 32> {state [enabled | disabled]}**

Description This command creates an IP interface on the switch.

create ipif

Parameters	<p><ipif_name 12> – The name of the IP interface can be up to 12 alphanumeric characters.</p> <p><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).</p> <p><vlan_name 32> – The name of the VLAN corresponding to the System IP interface.</p> <p>state [enabled disabled] – Allows you to enable or disable the IP interface.</p>
Restrictions	none.

Example Usage:

To create an IP interface named “Tiberius”:

```
local>create ipif Tiberius 10.1.1.1/8 dog
Command: create ipif Tiberius 10.1.1.1/8 dog

Success.

local>
```

delete ipif

delete ipif

Purpose	Used to delete an IP interface on the switch.
Syntax	delete ipif {<ipif_name 12> all}
Description	This command will delete an IP interface on the switch.
Parameters	<ipif_name 12> – The name of the IP interface can be up to 12 alphanumeric characters. all – Specifies all IP interface names on the switch.
Restrictions	none.

Example Usage:

To delete an IP interface named “Tiberius”:

```
local>delete ipif Tiberius
Command: delete ipif Tiberius

Success.

local>
```

enable ipif

Purpose	Used to enable an IP interface on the switch.
---------	---

enable ipif

Syntax	enable ipif {<ipif_name 12> all}
Description	This command will enable an IP interface on the switch.
Parameters	<p><ipif_name 12> – The name of the IP interface can be up to 12 alphaneumeric characters.</p> <p>all – Specifies all IP interface names on the switch.</p>
Restrictions	none.

Example Usage:

To enable an IP interface named “Hal”:

```
local>enable ipif Hal
Command: enable ipif Hal

Success.

local>
```

disable ipif

Purpose	Used to disable an IP interface on the switch.
Syntax	disable ipif {<ipif_name 12> all}

disable ipif

Description	This command will disable an IP interface on the switch.
Parameters	<p><ipif_name 12> – The name of the IP interface can be up to 12 alphanumeric characters.</p> <p>all – Specifies all IP interface names on the switch.</p>
Restrictions	none.

Example Usage:

To disable an IP interface named Hal:

```
local>disable ipif Hal
Command: disable ipif Hal

Success.

local>
```

show ipif

Purpose	Used to display the configuration of an IP interface on the switch.
Syntax	show ipif {<ipif_name 12>}
Description	This command will display the configuration of an IP interface on the

show ipif

switch.

Parameters <ipif_name 12> - The name of the IP interface can be up to 12 alphanumeric characters.

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
Link Status    : Link UP
Member Ports   : 1-50

Total Entries   : 1
local>
```


17

ARP COMMANDS

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

Command	Parameters
create arpentry	<ipaddr> <macaddr>
delete arpentry	<ipaddr> all
config arp_aging	time <value 0-65535>
config arpentry	<ipaddr> <macaddr>
show arpentry	ipif <ipif_name 12> ipaddress <ipaddr> static
clear arptable	

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

create arpentry

Purpose	Used to make a static entry into the ARP table.
Syntax	create arpentry <ipaddr> <macaddr>
Description	This command is used to enter an IP address into the switch's ARP table.
Parameters	<p><ipaddr> – The IP address of the end node or station.</p> <p><macaddr> – The MAC address corresponding to the IP address above.</p>
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To create a static ARP entry for the IP address 10.48.74.121 and MAC address 00:50:BA:00:07:36:

```
local> create arpentry 10.48.74.121 00-50-BA-00-07-36
Command: create arpentry 10.48.74.121 00-50-BA-00-07-36
```

Success.

```
local>
```

delete arpentry

Purpose	Used to delete a static entry into the ARP table.
Syntax	delete arpentry {<ipaddr> all}
Description	This command is used to delete a static ARP entry, made using the create arpentry command above, by specifying either the IP address of the entry or all. Specifying all clears the switch's ARP table.
Parameters	<ipaddr> – The IP address of the end node or station. all – deletes all ARP entries.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

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

```
local>delete arpentry 10.48.74.121  
Command: delete arpentry 10.48.74.121
```

Success.

```
local>
```

config arp_aging

Purpose	Used to configure the age-out timer for ARP table entries on the switch.
Syntax	config arp_aging time <value 0-65535>
Description	This command sets the maximum amount of time, in seconds, that an ARP entry can remain in the switch's ARP table, without being accessed, before it is dropped from the table.
Parameters	time <value 0-65535> – The ARP age-out time, in seconds. The default is 20.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure ARP aging time:

```
local>config arp_aging time 30
Command: config arp_aging time 30

Success.

local>
```

config arpentry

Purpose	Used to configure ARP table entries on the switch.
---------	--

config arpentry

Syntax	config arpentry <ipaddr> <macaddr>
Description	This command configures ARP entries in the switch's ARP table.
Parameters	<ipaddr> – The IP address of the end node or station. <macaddr> – The MAC address corresponding to the IP address above.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure an ARP Table entry:

```
local>config arpentry 10.1.1.1 00-50-BA-00-07-36  
Command: config arpentry 10.1.1.1 00-50-BA-00-07-36
```

Success.

```
local>
```

show arpentry

Purpose	Used to display the ARP table.
Syntax	show arpentry {ipif <ipif_name 12> ipaddress <ipaddr> static}

show arpentry

Description	This command is used to display the current contents of the switch's ARP table.
Parameters	<p><ipif_name 12> – The name of the IP interface the end node or station for which the ARP table entry was made, resides on.</p> <p><ipaddr> – The IP address of the end node or station.</p> <p>static – Displays the static entries to the ARP table.</p>
Restrictions	none.

Example Usage:

To display the ARP table:

local>show arpentry			
Command: show arpentry			
ARP Aging Time : 30			
Interface	IP Address	MAC Address	Type
-----	-----	-----	-----
System	10.0.0.0	FF-FF-FF-FF-FF-FF	Local Broadcast
System	10.1.1.169	00-50-BA-70-E4-4E	Dynamic
System	10.1.1.254	00-01-30-FA-5F-00	Dynamic
System	10.9.68.1	00-A0-C9-A4-22-5B	Dynamic
System	10.9.68.4	00-80-C8-2E-C7-45	Dynamic
System	10.10.27.51	00-80-C8-48-DF-AB	Dynamic
System	10.11.22.145	00-80-C8-93-05-6B	Dynamic
System	10.11.94.10	00-10-83-F9-37-6E	Dynamic

System	10.14.82.24	00-50-BA-90-37-10	Dynamic
System	10.15.1.60	00-80-C8-17-42-55	Dynamic
System	10.17.42.153	00-80-C8-4D-4E-0A	Dynamic
System	10.19.72.100	00-50-BA-38-7D-5E	Dynamic
System	10.21.32.203	00-80-C8-40-C1-06	Dynamic
System	10.40.44.60	00-50-BA-6B-2A-1E	Dynamic
System	10.42.73.221	00-01-02-03-04-00	Dynamic
System	10.44.67.1	00-50-BA-DA-02-51	Dynamic
System	10.47.65.25	00-50-BA-DA-03-2B	Dynamic
System	10.50.8.7	00-E0-18-45-C7-28	Dynamic
System	10.90.90.90	00-01-02-03-04-00	Local
System	10.255.255.255	FF-FF-FF-FF-FF-FF	Local Broadcast

Total Entries = 20

local>

clear arptable

Purpose	Used to remove all dynamic ARP table entries.
Syntax	clear arptable
Description	This command is used to remove dynamic ARP table entries from the switch's ARP table. Static ARP table entries are not affected.
Parameters	none.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To remove dynamic entries in the ARP table:

```
local>clear arptable
Command: clear arptable

Success.

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 <network_address> <ipaddr> <metric 1-65535>
delete iproute	default <network_address>
show iproute	<network_address> static rip ospf

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

create iproute

Purpose	Used to create an IP route entry to the switch's IP routing table.
Syntax	create iproute [default <network_address>]<ipaddr> {<metric 1-65535>}
Description	This command is used to create an IP route entry to the switch's IP routing table.
Parameters	<p>default – Creates a default IP route entry.</p> <p><network_address> – IP address and netmask of the IP interface that is the destination of the route. 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).</p> <p><ipaddr> – The IP address for the next hop router.</p> <p><metric 1-65535> – The default setting is 1.</p>
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

Purpose	Used to delete an IP route entry from the switch's IP routing table.
Syntax	delete iproute [default <network_address>]
Description	This command will delete an existing entry from the switch's IP routing table.
Parameters	Default – Deletes a default IP route entry. <network_address> – IP address and netmask of the IP interface that is the destination of the route. 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).
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 {<network_address>} {static rip ospf}
Description	This command will display the switch's current IP routing table.
Parameters	<p><network_address> – IP address and netmask of the IP interface that is the destination of the route. 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).</p> <p>static – This displays the content of the IP routing table that is created by the user.</p> <p>rip – This displays the content of the IP routing table that is learned from the RIP protocol.</p> <p>ospf – This displays the content of the IP routing table that is learned from the OSPF protocol.</p>

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

ROUTE REDISTRIBUTION COMMANDS

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

Command	Parameters
create route redistribute dst ospf	src [static rip local] mettype [1 2] metric <value>
create route redistribute dst rip	src [static ospf{all internal external type_1 type_2}] metic <value>
config route redistribute dst ospf	src [static rip local] mettype [1 2] metric <value>
config route redistribute dst rip	src [static ospf {all internal external type_1 type_2} metric <value>
delete route redistribute	dst [rip ospf] src [rip static local ospf]
show route redistribute	dst [rip ospf] src [rip static local ospf]

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

create route redistribute dst ospf

Purpose	Used to add route redistribution settings for the exchange of RIP routes to OSPF routes on the switch.
Syntax	create route redistribute dst ospf src [static rip local] {mettype [1 2] metric <value>}
Description	This command will redistribute routing information between the OSPF and RIP routing protocols to all routers on the network that are running OSPF or RIP. Routing information entered into the Static Routing Table on the local DES-3350SR switch is also redistributed.
Parameters	<p>src [static rip local] – Allows for the selection of the protocol for the source device.</p> <p>dst – Allows for the selection of the protocol for the destination device.</p> <p>mettype [1 2] – Allows for the selection of one of two methods of calculating the metric value. Type-1 calculates (for RIP to OSPF) by adding the destination's interface cost to the metric entered in the Metric field. Type-2 uses the metric entered in the Metric field without change. This field applies only when the destination field is OSPF.</p>

create route redistribute dst ospf

<value> – Allows the entry of an OSPF interface cost. This is analogous to a Hop Count in the RIP routing protocol.

Restrictions Only administrator-level users can issue this command.

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

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

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

Example Usage:

To add route redistribution settings:


```
local>create route redistribute dst ospf src rip
Command: create route redistribute dst ospf src rip
```

Success.

```
local>
```

create route redistribute dst rip

Purpose	Used to add route redistribution settings for the exchange of OSPF routes to RIP routes on the switch.
Syntax	create route redistribute dst rip src [static ospf {all internal external type_1 type_2}] {metric <value>}
Description	This command will redistribute routing information between the OSPF and RIP routing protocols to all routers on the network that are running OSPF or RIP. Routing information entered into the Static Routing Table on the local DES-3350SR switch is also redistributed.
Parameters	<p>src [static ospf {all internal external type_1 type_2}] – Allows the selection of the protocol of the source device.</p> <p>dst – Allows the selection of the protocol of the destination device.</p> <p>metric <value> – Allows the entry of an</p>

create route redistribute dst rip

OSPF interface cost. This is analogous to a HOP Count in the RIP routing protocol.

Restrictions Only administrator-level users can issue this command.

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

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

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

Entering the metric 0 specifies transparency.

Example Usage:

To add route redistribution settings:

```
local>create route redistribute dst rip src ospf all metric 2
Command: create route redistribute dst rip src ospf all metric 2

Success.

local>
```

delete route redistribute

Purpose	Used to delete an existing route redistribute configuration on the switch.
Syntax	delete route redistribute [dst [rip ospf] src [rip static local ospf]]
Description	This command will delete the route redistribution settings on this switch.
Parameters	dst – Allows the selection of the protocol on the destination device. src – Allows the selection of the protocol on the source device.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete route redistribution settings:

```
local>delete route redistribute dst rip src ospf
```

Command: delete route redistribute dst rip src ospf

Success.

local>

config route redistribute dst ospf

Purpose	Used to configure route redistribution from RIP to OSPF.
Syntax	config route redistribute dst ospf src [static rip local] {mettype [1 2] metric <value>}
Description	Route redistribution allows routers on the network – that are running different routing protocols to exchange routing information. this is accomplished by comparing the routes stored in the various router's routing tables and assigning appropriate metrics. This information is then exchanged among the various routers according to the individual routers current routing protocol. The switch can redistribute routing information between the OSPF and RIP routing protocols to all routers on the network that are running OSPF or RIP. Routing information entered into the Static Routing Table on the local switch is also redistributed.
Parameters	src – Allows the selection of the protocol of the source device. dst – Allows the selection of the protocol of

config route redistribute dst ospf

the destination device.

mettype – allows the selection of one of the methods for calculating the metric value. Type-1 calculates the metric (for RIP to OSPF) by adding the destination's interface cost to the metric entered in the Metric field. Type-2 uses the metric entered in the Metric field without change. This field applies only when the destination field is OSPF.

metric <value> – Allows the entry of an OSPF interface cost. This is analogous to a Hop Count in the RIP routing protocol.

Restrictions Only administrator-level users can issue this command.

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

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

Local	0 to 16777214	mettype 1 mettype 2
-------	---------------	------------------------

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

Example Usage:

To configure route redistributions:

```
local>config route redistribute dst rip src ospf all metric 2
Command: config route redistribute dst rip src ospf all 1 metric 2
```

Success.

```
local>
```

config route redistribute dst rip

Purpose	Used to configure route redistribution from OSPF to RIP.
Syntax	config route redistribute dst rip src [static ospf {all internal external type_1 type_2}] {metric <value>}
Description	Route redistribution allows routers on the network – that are running different routing protocols to exchange routing information. this is accomplished by comparing the routes stored in the various router's routing tables and assigning appropriate metrics. this information is then exchanged among

config route redistribute dst rip

the various routers according to the individual routers current routing protocol. The switch can redistribute routing information between the OSPF and RIP routing protocols to all routers on the network that are running OSPF or RIP. Routing information entered into the Static Routing Table on the local switch is also redistributed.

Parameters	src – Allows the selection of the routing protocol on the source device.
	dst – Allows the selection of the routing protocol on the destination device.
	<value> – Allows the entry of an OSPF interface cost. This is analogous to a Hop Count in the RIP routing protocol.
Restrictions	Only administrator-level users can issue this command.

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

Route Source	Metric	Type
--------------	--------	------

OSPF	0 to 16	all type_1 type_2 internal type_1 internal type_2 external internal
Static	0 to 16	not applicable

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

Entering the metric 0 specifies transparency.

Example Usage:

To configure route redistributions:

```
local>config route redistribute dst ospf src rip mettype type_1  
metric 2
```

```
Command: config route redistribute dst ospf src rip mettype  
type_1 metric 2
```

Success.

```
local>
```

```
show route redistribute
```


show route redistribute

Purpose	Used to display the route redistribution on the switch.
Syntax	show route redistribute {dst [rip ospf] src [rip static local ospf]}
Description	Displays the current route redistribution settings on the switch.
Parameters	src – Allows the selection of the routing protocol on the source device. dst – Allows the selection of the routing protocol on the destination device.
Restrictions	none.

Example Usage:

To display route redistributions:

```
local>show route redistribute
Command: show route redistribute

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

Total Entries : 2

local>
```

20

IGMP 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	ipif <ipif_name 12> all version <value 1-2> query_interval <sec 1-65535> max_response_time <sec 0-25> robustness_variable <value 1-255> last_member_query_interval <sec 0-25> state [enabled disabled]
show igmp	ipif <ipif_name 12>
show igmp group	group <group> ipif <ipif_name 12>

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

config igmp

Purpose	Used to configure IGMP on the switch.
Syntax	config igmp [ipif<ipif_name 12> all] {version <value 1-2> query_interval <sec 1-65535> max_response_time <sec 0- 25> robustness_variable <value 1- 255> last_member_query_interval <sec 0- 25> state [enabled disabled]}]
Description	This command is used to configure IGMP on the switch.
Parameters	<p><ipif_name 12> – The name of the IP interface for which you want to configure IGMP.</p> <p>all – Specifies all the IP interfaces on the switch.</p> <p>version <value 1-2> – The IGMP version number.</p> <p>query_interval <sec 1-65535> – The time in seconds between general query transmissions, in seconds.</p> <p>max_response_time <sec 0-25> – The maximum time in seconds that the switch will wait for reports from members.</p> <p>robustness_variable <value 1-255> – The permitted packet loss that guarantees IGMP.</p> <p>last_member_query_interval <sec 0-25> – the Max Response Time inserted into Group-Specific Queries sent in response to Leave Group messages, and is also the amount of time between Group-Specific Query messages.</p>

config igmp

The default is 1 second.

state [enabled|disabled] – Enables or disables IGMP for the specified IP interface.

Restrictions Only administrator-level users can issue this command.

Example Usage:

To configure the IGMP for the IP interface System:

```
local>config igmp all version 1 state enabled
Command: config igmp all version 1 state enabled
```

Success.

```
local>
```

show igmp

Purpose Used to display the IGMP configuration for the switch or for a specified IP interface.

Syntax **show igmp {ipif <ipif_name 12>}**

Description This command will display the IGMP configuration for the switch if no IP interface name is specified. If an IP interface name is specified, the command will display the IGMP configuration for that IP interface.

Parameters <ipif_name 12> – The name of the IP interface for which the IGMP configuration

show igmp

will be displayed.

Restrictions none.

Example Usage:

To display IGMP configurations:

```
local>show igmp
```

Command: show igmp

IGMP Interface Configurations

Interface	IP Address	Ver-	Query	Maximum	Robust-	Last Member	State
		sion		Response	ness	Query	
				Time	Value	Interval	
System	10.90.90.90	1	125	10	2	1	Enabled
Develop	20.1.1.1	1	125	10	2	1	Enabled

Total Entries: 2

```
local>
```

show igmp group

Purpose Used to display the switch's IGMP group table.

Syntax **show igmp group {group <group>} {ipif <ipif_name 12>}**

show igmp group

Description	This command will display the IGMP group configuration.
Parameters	group <group> – The multicast group ID. <ipif_name 12> – The name of the IP interface the IGMP group is part of.
Restrictions	none.

Example Usage:

To display IGMP group table:

```
local>show igmp group
```

Command: show igmp group

Interface	Multicast Group	Last Reporter	IP Querier	IP Expire
System	224.0.0.2	10.42.73.111	SELF	260
System	224.0.0.9	10.20.53.1	SELF	260

Total Entries: 2

```
local>
```

21

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>
show igmp_snooping group	vlan <vlan_name 32>
show router_ports	vlan <vlan_name 32> static dynamic

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

config igmp_snooping

Purpose	Used to configure IGMP snooping on the switch.
Syntax	config igmp_snooping [<vlan_name 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	<p><vlan_name 32> – The name of the VLAN for which IGMP snooping is to be configured.</p> <p>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.</p>

config igmp_snooping

The default is 260 seconds.

`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 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	<p><vlan_name 32> – The name of the VLAN for which IGMP snooping querier is to be configured.</p> <p>query_interval <sec 1-65535> – Specifies the amount of time in seconds between general query transmissions. The default setting is 125 seconds.</p> <p>max_response_time <sec 1-25> – Specifies the maximum time in seconds to wait for reports from members. The default setting is 10 seconds.</p> <p>robustness_variable <value 1-255> – Provides fine-tuning to allow for expected packet loss on a subnet. The value of the robustness variable is used in calculating the following IGMP message intervals:</p> <ul style="list-style-type: none"> • Group member interval—Amount of time that must pass before a multicast router decides there are no

config igmp_snooping querier

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 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-

config igmp_snooping querier

querier.

Restrictions Only administrator-level users can issue this command.

Example Usage:

To configure the IGMP snooping:

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

Command: config igmp_snooping querier default query_interval 125 state enabled

Success.

```
local>
```

config router_ports

Purpose Used to configure ports as router ports.

Syntax **config router_ports <vlan_name 32>**
[add | delete] <portlist>

config router_ports

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	<p><vlan_name 32> – The name of the VLAN on which the router port resides.</p> <p><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 26 would be entered as 1-3, 26. Additional ports can be individually entered by their port number, separated by commas.</p>
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 : Disabled
Multicast router Only      : Disabled
VLAN Name                  : default
Query Interval             : 125
Max Response Time          : 10
Robustness Value           : 2
Last Member Query Interval : 1
Host Timeout               : 260
Route Timeout              : 260
Leave Timer                 : 2
Querier State              : Disabled
Querier Router Behavior    : Non-Querier
State                      : Disabled

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

Total Entries: 2

local>
```

```
show igmp_snooping group
```

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

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

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

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

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

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

Total Entries : 6
local>
```

show router_ports

Purpose	Used to display the currently configured router ports on the switch.
Syntax	show router_ports {vlan <vlan_name 32>} {static dynamic}
Description	This command will display the router ports currently configured on the switch.

show router_ports

Parameters	<p><vlan_name 32> – The name of the VLAN on which the router port resides.</p> <p>static – Displays router ports that have been statically configured.</p> <p>dynamic – Displays router ports that have been dynamically configured.</p>
Restrictions	none.

Example Usage:

To display the router ports:

```
local>show router_ports
Command: show router_ports
```

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

```
VLAN Name       : vlan2
Static router port :
Dynamic router port :
```

```
Total Entries: 2
```

```
local>
```


22

802.1X COMMANDS

The DES-3350SR implements the server-side of the IEEE 802.1x Port-based Network Access Control. This mechanism is intended to allow only authorized users, or other network devices, access to network resources by establishing criteria for each port on the switch that a user or network device must meet before allowing that port to forward or receive frames.

Command	Parameters
enable 802.1x	
disable 802.1x	
show 802.1x auth_configuration	ports <portlist>
show 802.1x auth_state	ports <portlist>
config 802.1x capability	ports <portlist> all authenticator none
config 802.1x auth_parameter	ports <portlist> all default direction [both in] port_control [force_unauth auto force_auth] quiet_period <sec 0-65535> tx_period <sec 1-65535> supp_timeout <sec 1-65535>

Command	Parameters
	server_timeout <sec 1-65535> max_req <value 1-10> reauth_period <sec 1-65535> enable_reauth [enabled disabled]
config 802.1x init	port_based ports [<portlist> all] mac_based ports [<portlist> all] {mac_address <macaddr>}
config 802.1x reauth	port_based ports [<portlist> all] mac_based ports [<portlist> all] {mac_address <macaddr>}
config 802.1x auth_mode	[port_based mac_based]
config radius add	<server_index 1-3> <server_ip> key <passwd 32> default auth_port <udp_port_number> acct_port <udp_port_number>
config radius delete	<server_index 1-3>
config radius	<server_index 1-3> ipaddress <server_ip> key <passwd 32> auth_port <udp_port_number> acct_port <udp_port_number>
show radius	

enable 802.1x

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

Example Usage:

To enable 802.1x switch-wide:

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

Success.

```
local>
```

disable 802.1x

Purpose	Used to disable the 802.1x server on the switch.
Syntax	disable 802.1x

disable 802.1x

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

Example Usage:

To disable 802.1x on the switch:

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

Success.

local>
```

show 802.1x auth_configuration

Purpose	Used to display the current authenticated configuration of the 802.1x server on the switch.
Syntax	show 802.1x auth_configuration {ports <portlist>}
Description	The show 802.1x auth_configuration command is used to display the current authenticated configuration of the 802.1x

show 802.1x auth_configuration

Port-based Network Access Control server application on the switch.

Parameters

ports <portlist> – Specifies a range of ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.

The following details what is displayed:

802.1x Enabled|Disabled – Shows the current status of 802.1x functions on the switch.

Authentication Mode: Port_based|Mac_based|None – Shows the current authentication mode.

Authentication Protocol: Radius_Eap – Shows the authentication protocol suite in use between the switch and a Radius server.

Port number – Shows the physical port number on the switch.

Capability: Authentication|None – Shows the capability of 802.1x functions on the

show 802.1x auth_configuration

port number displayed above. There are two 802.1x capabilities that can be set on the switch: Authentication and None.

AdminCtrlDir: Both|In – Shows whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction.

OpenCtrlDir: Both|In – Shows whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction.

Port Control:

ForceAuth|ForceUnauth|Auto – Shows the administrative control over the port's authorization status. ForceAuth forces the Authenticator of the port to become Authorized. ForceUnauth forces the port to become Unauthorized.

QuietPeriod – Shows the time interval between authentication failure and the start of a new authentication attempt.

TxPeriod – Shows the time to wait for a response from a supplicant (user) to send EAP Request|Identity packets.

SuppTimeout – Shows the time to wait for a response from a supplicant (user) for all EAP packets, except for the

show 802.1x auth_configuration

Request | Identity packets.

ServerTimeout – Shows the length of time to wait for a response from a Radius server.

MaxReq – Shows the maximum number of times to retry sending packets to the supplicant.

ReAuthPeriod – shows the time interval between successive re-authentications.

ReAuthenticate: Enabled | Disabled – Shows whether or not to re-authenticate.

Restrictions Only administrator-level users can issue this command.

Example Usage:

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

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

```
802.1X           : Disabled
Authentication Mode : None
Authentication Protocol : Radius_Eap
```

```
Port number      : 1
Capability        : None
AdminCrI Dir     : Both
OpenCrI Dir      : Both
Port Control     : Auto
QuietPeriod      : 60 sec
```

```
TxPeriod      : 30  sec
SuppTimeout   : 30  sec
ServerTimeout : 30  sec
MaxReq        : 2   times
ReAuthPeriod  : 3600 sec
ReAuthenticate : Disabled
```

show 802.1x auth_state

Purpose Used to display the current authentication state of the 802.1x server on the switch.

Syntax **show 802.1x auth_state {ports <portlist>}**

Description The show 802.1x auth_state command is used to display the current authentication state of the 802.1x Port-based Network Access Control server application on the switch.

Parameters ports <portlist> – Specifies a range of ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.

The following details what is displayed:

show 802.1x auth_state

Port number – Shows the physical port number on the switch.

Auth PAE State:

Initialize | Disconnected | Connecting |
Authenticating | Authenticated | Held
| ForceAuth | ForceUnauth – Shows the
current state of the Authenticator PAE.

Backend State: Request | Response | Fail |
Idle | Initialize | Success | Timeout – Shows
the current state of the Backend
Authenticator.

Port Status: Authorized | Unauthorized –
Shows the result of the authentication
process. Authorized means that the user
was authenticated, and can access the
network. Unauthorized means that the
user was not authenticated, and cannot
access the network.

Restrictions Only administrator-level users can issue
this command.

Example Usage:

To display the 802.1x authentication state:

local>show 802.1x auth_state				
Command: show 802.1x auth_state				
Port	Auth	PAE State	Backend State	Port Status
-----	-----	-----	-----	-----
1	ForceAuth	Success	Success	Authorized

2	ForceAuth	Success	Authorized
3	ForceAuth	Success	Authorized
4	ForceAuth	Success	Authorized
5	ForceAuth	Success	Authorized
6	ForceAuth	Success	Authorized
7	ForceAuth	Success	Authorized
8	ForceAuth	Success	Authorized
9	ForceAuth	Success	Authorized
10	ForceAuth	Success	Authorized
11	ForceAuth	Success	Authorized
12	ForceAuth	Success	Authorized
13	ForceAuth	Success	Authorized
14	ForceAuth	Success	Authorized
15	ForceAuth	Success	Authorized
16	ForceAuth	Success	Authorized
17	ForceAuth	Success	Authorized
18	ForceAuth	Success	Authorized
19	ForceAuth	Success	Authorized
20	ForceAuth	Success	Authorized
CTRL+C ESC q Quit SPACE n Next Page Enter Next Entry a All local>			

config 802.1x capability

Purpose	Used to configure the 802.1x capability of a range of ports on the switch.
Syntax	config 802.1x capability ports [<portlist> all] [authenticator none]
Description	The config 802.1x command has two capabilities that can be set for each port: Authenticator and None.
Parameters	<portlist> – Specifies a range of ports. The port list is specified by listing the lowest switch number and the beginning port

config 802.1x capability

number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.

all – Specifies all of the ports on the switch.

authenticator – A user must pass the authentication process to gain access to the network.

none – The port is not controlled by the 802.1x functions.

Restrictions Only administrator-level users can issue this command.

Example Usage:

To configure 802.1x capability on ports 1-10:

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

Success.

```
local>
```

config 802.1x auth_parameter

Purpose Used to configure the 802.1x

config 802.1x auth_parameter

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

config 802.1x auth_parameter

direction [both|in] – Determines whether a controlled port blocks communication in both the receiving and transmitting directions, or just the receiving direction.

port_control – Configures the administrative control over the authentication process for the range of ports.

force_auth – Forces the Authenticator for the port to become authorized. Network access is allowed.

auto – Allows the port's status to reflect the outcome of the authentication process.

force_unauth – Forces the Authenticator for the port to become unauthorized. Network access will be blocked.

quiet_period <sec 0-65535> – Configures the time interval between authentication failure and the start of a new authentication attempt.

max_req <value 1-10> – Configures the number of times to retry sending packets to a supplicant (user).

reauth_period <sec 1-65535> – Configures the time interval between successive re-authentications.

enable_reauth [enabled|disabled] – Determines whether or not the switch will re-authenticate. Enabled causes re-authentication of users at the time interval specified in the Re-

config 802.1x auth_parameter

authentication Period field, above.

Restrictions Only administrator-level users can issue this command.

Example Usage:

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

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

Success.

```
local>
```

config 802.1x init

Purpose Used to initialize the 802.1x functions on a range of ports.

Syntax **config 802.1x init port_based ports**
 [**<portlist> | all**] | **mac_based ports**
 [**<portlist> | all**] | {**mac_address**
 <macaddr>}

Description The config 802.1x init command is used to immediately initialize the 802.1x functions on a range of ports.

Parameters port_based|mac_based ports – The switch allows you to configure 802.1x by either port or MAC address.

config 802.1x init

<portlist> – Specifies a range of ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.

all – Specifies all of the ports on the switch.

Restrictions Only administrator-level users can issue this command.

Example Usage:

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

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

Success.

```
local>
```

config 802.1x reauth

Purpose Used to configure the 802.1x re-

config 802.1x reauth

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

Example Usage:

To configure 802.1x reauthentication for ports 1-15:

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

Success.
local>

config 802.1x auth_mode

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

Example Usage:

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

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

Success.
local>
```

config radius add

Purpose	Used to configure the settings the switch will use to communicate with a Radius server.
Syntax	config radius add <server_index 1-3> <server_ip> key <passwd 32> [default {auth_port <udp_port_number> acct_port <udp_port_number>}]
Description	The config radius add command is used to configure the settings the switch will use to communicate with a Radius server.
Parameters	<p><server_index 1-3> – Assigns a number to the current set of Radius server settings. Up to three groups of Radius server settings can be entered on the switch.</p> <p><server_ip> – The IP address of the Radius server.</p> <p>key – Specifies that a password and encryption key will be used between the switch and the Radius server.</p>

config radius add

<passwd 32> – The shared-secret key used by the Radius server and the switch. Up to 32 characters can be used.

default – Returns all of the ports in the range to their default Radius settings.

auth_port <udp_port_number> – The UDP port number for authentication requests. The default is 1812.

acct_port <udp_port_number> – The UDP port number for accounting requests. The default is 1813.

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

Example Usage:

To configure Radius server communication settings:

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

Success.

```
local>
```

config radius delete

Purpose	Used to delete a previously entered Radius server configuration.
---------	--

config radius delete

Syntax	config radius delete <server_index 1-3>
Description	The config radius delete command is used to delete a previously entered Radius server configuration.
Parameters	<server_index 1-3> – Assigns a number to the current set of Radius server settings. Up to three groups of Radius server settings can be entered on the switch.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete previously configured Radius server communication settings:

```
local>config radius delete 1
Command: config radius delete 1

Success.

local>
```

config radius

Purpose	Used to configure the switch's Radius settings.
Syntax	config radius <server_index 1-3> {ipaddress <server_ip> {ipaddress <server_ip> key <passwd 32> auth_port

config radius

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

Example Usage:

To configure Radius settings:

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

Success.

local>

show radius

Purpose	Used to display the current Radius configurations on the switch.
Syntax	show radius
Description	The show radius command is used to display the current Radius configurations on the switch.
Parameters	None.
Restrictions	None.

Example Usage:

To display Radius settings on the switch:

local>show radius

Command: show radius

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

Total Entries : 3

```
local>
```

23

ACCESS CONTROL LIST
(ACL) COMMANDS

The DES-3350SR implements Access Control Lists that enable the switch to deny network access to specific devices or device groups based on IP settings or MAC address.

Command	Parameters
create access_profile	ethernet vlan source_mac <macmask> destination_mac <macmask> 802.1p ethernet_type ip vlan source_ip_mask <netmask> destination_ip_mask <netmask> dscp icmp type code igmp type tcp src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xffff>

Command	Parameters
	udp src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xffff> protocol_id user_mask <hex 0x0-0xffffffff> packet_content_mask offset_0-15 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> offset_16-31 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> offset_32-47 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> offset_48-63 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> offset_64-79 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> port <portlist> all profile_id <value 1-255>
delete access_profile	profile_id <value 1-255>
config access_profile	profile_id <value 1-255> add access_id <value 1-255> ethernet vlan <vlan_name 32> source_mac <macaddr> destination_mac <macaddr> 802.1p <value 0-7> ethernet_type <hex 0x0-0xffff> ip

Command	Parameters
	vlan <vlan_name 32> source_ip <ipaddr> destination_ip <ipaddr> dscp <value> icmp type <value 0-255> code <value 0-255> igmp type <value 0-255> tcp src_port <value 0-65535> dst_prot <value 0-65535> udp src_port <value 0-65535> dst_port <value 0-65535> protocol_id <value 0-255> user_define <hex 0x0-0xffffffff> packet_content offset_0-15 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> offset_16-31 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> offset_32-47 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> offset_48-63 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> offset_64-79 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> delete access_id <value 1-255> permit deny

Command	Parameters
	priority <value 0-7> replace_priority replace_dscp <value 0-63>
show access_profile	profile_id <value1-255>

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

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

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

create access_profile ip source_ip_mask 255.255.255.0 profile_id 1

Here we have created an access profile that will examine the IP field of each frame received by the switch. Each source IP address the switch finds will be combined with the **source_ip_mask** with a logical AND operation. The **profile_id** parameter is used to give the access profile an identifying number – in this case, **1**.

Now that an access profile has been created, you must add the criteria the switch will use to decide if a given frame should be

forwarded or filtered. Here, we want to filter any packets that have an IP source address between 10.42.73.0 and 10.42.73.255:

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

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

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

The **deny** parameter instructs the switch to filter any frames that meet the criteria – in this case, when a logical AND operation between an IP address specified in the next step and the **ip_source_mask** match.

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

create access_profile

Purpose Used to create an access profile on the switch and to define which parts of each incoming frame's header the switch will examine. Masks can be entered that will be combined with the values the switch finds in the specified frame header fields. Specific values for the rules are entered using the config access_profile command, below.

Syntax

```

create access_profile
Ethernet
    {vlan|source_mac
    <macmask>|destination_mac
    <macmask>|802.1p|ethernet_type}
ip
    {vlan|source_ip_mask
    <netmask>|destination_ip_mask
    <netmask>|dscp|icmp
    {type|code}|igmp {type}|tcp
    {src_port_mask <hex 0x0-0xffff>|dst_port_mask <hex 0x0-0xffff>}|udp {src_port_mask <hex 0x0-0xffff>|dst_port_mask <hex 0x0-0xffff>}|protocol_id {user_mask <hex 0x0-0xffffffff>}}}]
packet_content_mask
    offset_0-15 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff>
    offset_16-31 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff>
    offset_32-47 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff>
  
```

create access_profile

```

0xffffffff><hex 0x0-0xffffffff><hex 0x0-
0xffffffff>
offset_48-63 <hex 0x0-0xffffffff><hex 0x0-
0xffffffff><hex 0x0-0xffffffff><hex 0x0-
0xffffffff>
offset_64-79 <hex 0x0-0xffffffff><hex 0x0-
0xffffffff><hex 0x0-0xffffffff><hex 0x0-
0xffffffff>

```

```
port
```

```
<portlist>
```

```
all
```

```
{profile_id <value 1-255>}
```

Description

The create access_profile command is used to create an access profile on the switch and to define which parts of each incoming frame's header the switch will examine. Masks can be entered that will be combined with the values the switch finds in the specified frame header fields. Specific values for the rules are entered using the config access_profile command, below.

Parameters

ethernet – Specifies that the switch will examine the layer 2 part of each packet header.

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

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

destination_mac <macmask> – Specifies

create access_profile

a MAC address mask for the destination MAC address.

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

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

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

vlan – Specifies a VLAN mask.

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

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

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

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

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

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

igmp – Specifies that the switch will

create access_profile

examine each frame's Internet Group Management Protocol (IGMP) field.

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

tcp – Specifies that the switch will examine each frames Transport Control Protocol (TCP) field.

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

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

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

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

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

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

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

packet_content_mask- Specifies that the

create access_profile

switch will examine the packet_content in each frame

offset_0-15 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> Specifies the packet_content_mask for the packet_content in offset_0-15

offset_16-31 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> Specifies the packet_content_mask for the packet_content in offset_16-31

offset_32-47 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> Specifies the packet_content_mask for the packet_content in offset_32-47

offset_48-63 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> Specifies the packet_content_mask for the packet_content in offset_48-63

offset_64-79 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff>-- Specifies the packet_content_mask for the packet_content in offset_64-79

profile_id <value 1-255> - Specifies an index number that will identify the access

create access_profile

	profile being created with this command.
	port <portlist> all – specifies a port or range of ports
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To create an access list rules:

```
local>create access_profile ip vlan source_ip_mask 20.0.0.0
destination_ip_mask
10.0.0.0 dscp icmp type code port 6 profile_id 4
Command: create access_profile ip vlan source_ip_mask
20.0.0.0 destination_ip_ma
sk 10.0.0.0 dscp icmp type code port 6 profile_id 4

Success.

local>
```

delete access_profile

Purpose	Used to delete a previously created access profile.
Syntax	delete access_profile [profile_id <value 1-255>]
Description	The delete access_profile command is used to delete a previously created access profile on the switch.

delete access_profile

Parameters	profile_id <value 1-255> – an integer between 1 and 255 that is used to identify the access profile that will be deleted with this command. This value is assigned to the access profile when it is created with the create access_profile command.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

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

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

Success.

local>
```

config access_profile

Purpose	Used to configure an access profile on the switch and to define specific values that will be used to by the switch to determine if a given packet should be forwarded or filtered. Masks entered using the create access_profile command will be
---------	--

config access_profile

Syntax

combined, using a logical AND operation, with the values the switch finds in the specified frame header fields. Specific values for the rules are entered using the config access_profile command, below.

```
config access_profile profile_id <value 1-255> [add access_id <value 1-255>][delete <value 1-255>] [ethernet {vlan <vlan_name 32>|source_mac <macaddr>|destination_mac <macaddr>|802.1 <value 0-7>|ethernet_type <hex 0x0-0xffff>|permit { priority <value 0-7>|replace_priority} |deny]
```

```
ip{vlan <vlan_name>|source_ip <ipaddr>|destination_ip <ipaddr>|dscp <value 0-63>|[icmp {type <value 0-65535> code <value 0-255>}|igmp {type <value 0-255>}|tcp {src_port <value 0-65535>|dst_port <value 0-65535>}|udp {src_port <value 0-65535>|dst_port <value 0-65535>}|protocol_id <value 0-255>|user_define <hex 0x0-0xffffffff>}}|permit { priority <value 0-7>|replace_priority|replace_dscp<value 0-63>} |deny}]
```

```
packet_content  
{offset_0-15 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff>  
offset_16-31 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff>  
offset_32-47 <hex 0x0-0xffffffff><hex
```



config access_profile

```

0x0-0xffffffff><hex 0x0-0xffffffff><hex
0x0-0xffffffff>
offset_48-63 <hex 0x0-0xffffffff><hex
0x0-0xffffffff><hex 0x0-0xffffffff><hex
0x0-0xffffffff>
offset_64-79 <hex 0x0-0xffffffff><hex
0x0-0xffffffff><hex 0x0-0xffffffff><hex
0x0-0xffffffff>
| permit | deny}]

```

Description	The config access_profile command is used to configure an access profile on the switch and to enter specific values that will be combined, using a logical AND operation, with masks entered with the create access_profile command, above.
Parameters	<p>profile_id <value 1-255> –</p> <p>add access_id <value 1-255> – Adds an additional rule to the above specified access profile. The value specifies the relative priority of the additional rule. A lower access ID, the higher the priority the rule will be given.</p> <p>ethernet – Specifies that the switch will look only into the layer 2 part of each packet.</p> <p>vlan <vlan_name 32> – Specifies that the access profile will apply to only to this VLAN.</p> <p>source_mac <macaddr> – Specifies that the access profile will apply to only packets with this source MAC address.</p>

config access_profile

destination_mac <macaddr> – Specifies that the access profile will apply to only packets with this destination MAC address.

802.1p <value 0-7> – Specifies that the access profile will apply only to packets with this 802.1p priority value.

ethernet_type <hex 0x0-0xffff> – Specifies that the access profile will apply only to packets with this hexadecimal 802.1Q Ethernet type value in the packet header.

ip – Specifies that the switch will look into the IP fields in each packet.

vlan <vlan_name 32> – Specifies that the access profile will apply to only to this VLAN.

source_ip <ipaddr> – Specifies that the access profile will apply to only packets with this source IP address.

destination_id <value 0-255> – Specifies that the access profile will apply to only packets with this destination IP address.

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

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

config access_profile

packet.

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

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

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

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

tcp – Specifies that the switch will examine the Transmission Control Protocol (TCP) field within each packet.

src_port <value 0-65535> – Specifies that the access profile will apply only to packets that have this TCP source port in their TCP header.

dst_port <value 0-65535> – Specifies that the access profile will apply only to packets that have this TCP destination port in their TCP header.

udp – Specifies that the switch will examine the Universal Datagram Protocol (UDP) field in each packet.

src_port <value 0-65535> –

config access_profile

Specifies that the access profile will apply only to packets that have this UDP source port in their header.

dst_port <value 0-65535> – Specifies that the access profile will apply only to packets that have this UDP destination port in their header.

protocol_id <value 0-255> – Specifies that the switch will examine the Protocol field in each packet and if this field contains the value entered here, apply the following rules.

user_define <hex 0x0-0xffffffff> – Specifies a mask to be combined with the value found in the frame header using a logical AND operation.

packet_content- Specifies that the switch will examine the packet_content in each frame

offset_0-15 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff>- Specifies the packet_content in offset_0-15

offset_16-31 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff>- Specifies the packet_content in offset_16-31

offset_32-47 <hex 0x0-0xffffffff><hex

config access_profile

0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff>-Specifies the packet_content in offset_32-47

offset_48-63 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff>-Specifies the packet_content in offset_48-63

offset_64-79 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff>-Specifies the packet_content in offset_64-79

deny - instructs the switch to filter any frames that meet the criteria

permit - default for an access profile on the switch is to permit traffic flow.

priority <value 0-7>- This parameter is specified if you want to assign the 802.1p user priority of a packet that meets the specified criteria. Otherwise, a packet will have its incoming 802.1p user priority rewritten to its original value before being transmitted from the switch.

replace_priority - This parameter is used to change the assigned user priority of a packet.

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

config access_profile

write the value in the DSCP field of the packet.

delete <value 1-255> – Specifies that the access ID of a rule you want to delete.

Restrictions Only administrator-level users can issue this command.

Example Usage:

To configure the access profile with the profile ID of 1 to filter frames that have IP addresses in the range between 10.42.72.1 to 10.42.72.15:

```
local>config access_profile profile_id 1 add access_id 1 ip
source_ip 10.42.72.1
destination_ip 10.42.72.15 udp src_port 1 dst_port 2 permit
Command: config access_profile profile_id 1 add access_id 1 ip
source_ip 10.42.7
2.1 destination_ip 10.42.72.15 udp src_port 1 dst_port 2 permit

Success.

local>
```

show access_profile

Purpose Used to display the currently configured access profiles on the switch.

Syntax **show access_profile**

show access_profile

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

Example Usage:

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

```
local>show access_profile
Command: show access_profile

Access Profile Table

Access Profile ID : 1
Type   : IP Frame Filter - ICMP
Ports  : 9
Masks  : VLAN          Source IP Addr  Dest. IP Addr  DSCP
ICMP TYPE CODE

      -----
                20.0.0.0    10.0.0.0
ID Mode
      -----

Total Entries : 0
local>
```


24

BOOTP RELAY COMMANDS

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

Command	Parameters
config bootp_relay	hops <value 1-16> time <sec 0-65535>
config bootp_relay add	ipif <ipif_name 12> <ipaddr>
config bootp_relay delete	ipif <ipif_name 12> <ipaddr>
enable bootp_relay	
disable bootp_relay	
show bootp_relay	ipif <ipif_name 12>

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

config bootp_relay

Purpose	Used to configure the BOOTP relay feature of the switch.
Syntax	config bootp_relay {hops <value 1-16>}{time <sec 0-65535>}
Description	This command is used to configure the BOOTP relay feature.
Parameters	<p>hops <value 1-16> – Specifies the maximum number of router hops that the BOOTP packets can cross.</p> <p>time <sec 0-65535> – The minimum time in seconds within which the switch must relay the BOOTP request. If this time is exceeded, the switch will drop the BOOTP packet.</p>
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure BOOTP relay status:

```
local>config bootp_relay hops 4 time 2
Command: config bootp_relay hops 4 time 2
```

Success.

```
local>
```

config bootp_relay add

Purpose	Used to add an IP destination address to the switch's BOOTP relay table.
Syntax	config bootp_relay add ipif <ipif_name 12> <ipaddr>
Description	This command adds an IP address as a destination to forward (relay) BOOTP packets to.
Parameters	<p><ipif_name 12> – The name of the IP interface which contains the IP address below.</p> <p><ipaddr> – The IP interface that is trying to add the BOOTP protocol packet.</p>
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To add a BOOTP relay:

```
local>config bootp_relay add ipif System 10.43.21.12
Command: config bootp_relay add ipif System 10.43.21.12
```

Success.

```
local>
```

config bootp_relay delete

Purpose	Used to delete one or all IP destination addresses from the switch's BOOTP relay table.
Syntax	config bootp_relay delete ipif <ipif_name 12> <ipaddr>
Description	This command is used to delete one or all of the IP destination addresses in the switch's BOOTP relay table.
Parameters	<p><ipif_name 12> – The name of the IP interface that contains the IP address below.</p> <p><ipaddr> – The IP interface that is trying to delete the BOOTP protocol packet.</p>
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete a BOOTP relay:

```
local>config bootp_relay delete ipif System 10.43.21.12
Command: config bootp_relay delete ipif System 10.43.21.12

Success.

local>
```

enable bootp_relay

Purpose	Used to enable the BOOTP relay function on the switch.
Syntax	enable bootp_relay
Description	This command, in combination with the disable bootp_relay command below, is used to enable and disable the BOOTP relay function on the switch.
Parameters	none.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable the BOOTP relay function:

```
local>enable bootp_relay
Command: enable bootp_relay

Success.

local>
```

disable bootp_relay

Purpose	Used to disable the BOOTP relay function on the switch.
Syntax	disable bootp_relay
Description	This command, in combination with the enable bootp_relay command above, is used to enable and disable the BOOTP relay function on the switch.
Parameters	none.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To disable the BOOTP relay function:

```
local>disable bootp_relay
Command: disable bootp_relay
```

Success.

```
local>
```

show bootp_relay

Purpose	Used to display the current BOOTP relay configuration.
Syntax	show bootp_relay {ipif <ipif_name 12>}

show bootp_relay

Description	This command will display the current BOOTP relay configuration for the switch, or if an IP interface name is specified, the BOOTP relay configuration for that IP interface.
Parameters	<ipif_name 12> – The name of the IP interface for which you want to display the current BOOTP relay configuration.
Restrictions	none.

Example Usage:

To display BOOTP relay status:

```
local>show bootp_relay
Command: show bootp_relay

Bootp Relay Status      :Disabled
Bootp Hops Count Limit  :4
bootp Relay Time Threshold :0
Interface    Server 1    Server 2    Server 3    Server 4
-----
local>
```

25

DNS RELAY COMMANDS

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

Command	Parameters
config dnsr	primary secondary nameserver <ipaddr>
config dnsr	add delete static <domain_name 32> <ipaddr>
enable dnsr	
disable dnsr	
enable dnsr cache	
disable dnsr cache	
enable dnsr static	
disable dnsr static	
show dnsr	static

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

config dnsr

Purpose	Used to configure the DNS relay function.
Syntax	config dnsr [primary secondary] nameserver <ipaddr>
Description	This command is used to configure the DNS relay function on the switch.
Parameters	<p>primary – Indicates that the IP address below is the address of the primary DNS server.</p> <p>secondary – Indicates that the IP address below is the address of the secondary DNS server.</p> <p>nameserver <ipaddr> – The IP address of the DNS nameserver.</p>
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To set IP address 10.43.21.12 of primary.

```
local>config dnsr primary nameserver 10.43.21.12  
Command: config dnsr primary nameserver 10.43.21.12
```

Success

```
local>
```

config dnsr [add | delete] static

Purpose	Used to add or delete a static entry into the switch's DNS resolution table.
Syntax	config dnsr [add delete] static <domain_name 32> <ipaddr>
Description	This command allows you to add or delete entries into the switch's DNS cache.
Parameters	<domain_name 32> – The domain name of the entry. <ipaddr> – The IP address of the entry.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

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

```
local>config dnsr add static dns1 10.43.21.12  
Command: config dnsr add static dns1 10.43.21.12  
  
Success.
```

```
local>
```

Example Usage:

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

```
local>config dnsr delete static dns1 10.43.21.12  
Command: config dnsr delete static dns1 10.43.21.12
```

Success.

```
local>
```

enable dnsr

Purpose	Used to enable DNS relay.
Syntax	enable dnsr
Description	This command is used, in combination with the disable dnsr command below, to enable and disable DNS Relay on the switch.
Parameters	none.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable status of DNS relay:

```
local>enable dnsr
Command: enable dnsr
```

Success.

```
local>
```

disable dnsr

Purpose	Used to disable DNS relay on the switch.
Syntax	disable dnsr
Description	This command is used, in combination with the enable dnsr command above, to enable and disable DNS Relay on the switch.
Parameters	none.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To disable status of DNS relay:

```
local>disable dnsr
Command: disable dnsr
```

Success.

```
local>
```

enable dnsr cache

Purpose	Used to enable the DNS relay cache.
Syntax	enable dnsr cache
Description	This command is used, in combination with the disable dnsr cache command below, to enable and disable the DNS relay cache.
Parameters	none.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable cache lookup for DNS relay:

```
local>enable dnsr cache  
Command: enable dnsr cache
```

Success.

```
local>
```

disable dnsr cache

Purpose	Used to disable the DNS relay cache.
Syntax	disable dnsr cache
Description	This command is used, in combination with the enable dnsr cache command above, to

disable dnsr cache

enable and disable the DNS relay cache.

Parameters none.

Restrictions Only administrator-level users can issue this command.

Example Usage:

To disable cache lookup for DNS relay:

```
local>disable dnsr cache
Command: disable dnsr cache
```

Success.

```
local>
```

enable dnsr static

Purpose Used to enable the DNS relay static table.

Syntax **enable dnsr static**

Description This command, in combination with the disable dnsr static command below, is used to enable or disable the DNS relay static forwarding table.

Parameters none.

Restrictions Only administrator-level users can issue this command.

enable dnsr static

this command.

Example Usage:

To enable static table lookup for DNS relay:

```
local>enable dnsr static  
Command: enable dnsr static
```

Success.

```
local>
```

disable dnsr static

Purpose	Used to disable the DNS relay static table.
Syntax	disable dnsr static
Description	This command, in combination with the disable dnsr static command below, is used to enable or disable the DNS relay static forwarding table.
Parameters	none.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To disable static table lookup for DNS relay:

```
local>disable dnsr static
Command: disable dnsr static
```

Success.

```
local>
```

show dnsr

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

Example Usage:

To display the current DNS status:


```
local>show dnsr
```

```
Command: show dnsr
```

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

```
DNSR Relay Static Table
```

Domain Name	IP Address
-----	-----

```
Total Entries: 0
```

```
local>
```

26

RIP COMMANDS

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

Command	Parameters
config rip ipif	<ipif_name 12> authentication [enabled <password 1-16> disabled] tx_mode [disabled v1_only v1_compatible v2_only] rx_mode [v1_only v2_only v1_or_v2 disabled] state [enabled disabled]
config rip all	authentication [enabled <password 1-16> disabled] tx_mode [disabled v1_only v1_compatible v2_only] rx_mode [v1_only v2_only v1_or_v2 disabled] state [enabled disabled]
enable rip	
disable rip	

Command	Parameters
show rip	ipif <ipif_name 12>

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

config rip ipif

Purpose	Used to configure RIP on the IP interface named “ipif” on the switch.
Syntax	config rip ipif <ipif_name 12> {authentication [enabled<password 1-16> disabled] tx_mode [disabled v1_only v1_compatible v2_only] rx_mode [v1_only v2_only v1_or_v2 disabled] state [enabled disabled]}
Description	This command is used to configure RIP settings on the IP interface named “ipif” on the switch.
Parameters	<ipif_name 12> – The name of the IP interface. authentication [enabled disabled] – Enables or disables authentication for RIP on the specified interfaces on the switch. <password 1-16> – Allows the specification of a case-sensitive password. tx_mode – This entry specifies which version of the RIP protocol will be used to transmit RIP packets. It determines how transmitted RIP packets will be interpreted—as RIP version v1 only, v2 only, or v1 compatible.

config rip ipif

The disabled entry prevents the transmission of RIP packets.

disabled – Prevents the transmission of RIP packets.

v1_only – Specifies that only RIP v1 packets will be transmitted.

v2_only – Specifies that only RIP v2 packets will be transmitted.

v1_compatible – Specifies that RIP v1-compatible packets will be transmitted.

rx_mode – This entry specifies which version of the RIP protocol will be used to receive RIP packets. Determines how received RIP packets will be interpreted – as RIP version v1 only, v2 only, or v1 or v2. The disabled entry prevents the reception of RIP packets.

disabled – Prevents the reception of RIP packets.

v1_only – Specifies that only RIP v1 packets will be accepted.

v2_only – Specifies that only RIP v2 packets will be accepted.

v1_or_v2 – Specifies that RIP v1 or v2 packets will be accepted.

state [enabled|disabled] – Allows RIP to be enabled and disabled on an IP interface on the switch.

Restrictions

Only administrator-level users can issue this command.

Example Usage:

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

```
local>config rip ipif System rx_mode v1_only
Command: config rip ipif System rx_mode v1_only

Success.

local>
```

config rip all

Purpose	Used to configure RIP on all the IP interfaces on the switch.
Syntax	config rip all {authentication [enabled<password 1-16> disabled] tx_mode [disabled v1_only v1_compatible v2_only] rx_mode [v1_only v2_only v1_or_v2 disabled] state [enabled disabled]}
Description	This command is used to configure RIP settings on all the IP interfaces on the switch.
Parameters	authentication [enabled disabled] – Enables or disables authentication for RIP on the specified interfaces on the switch. <password 1-16> – Allows the specification of a case-sensitive password. tx_mode – This entry specifies which version of the RIP protocol will be used to transmit

config rip all

RIP packets. It determines how transmitted RIP packets will be interpreted—as RIP version v1 only, v2 only, or v1 compatible. The disabled entry prevents the transmission of RIP packets.

disabled – Prevents the transmission of RIP packets.

v1_only – Specifies that only RIP v1 packets will be transmitted.

v2_only – Specifies that only RIP v2 packets will be transmitted.

v1_compatible – Specifies that RIP v1-compatible packets will be transmitted.

rx_mode – This entry specifies which version of the RIP protocol will be used to receive RIP packets. Determines how received RIP packets will be interpreted – as RIP version v1 only, v2 only, or v1 or v2. The disabled entry prevents the reception of RIP packets.

disabled – Prevents the reception of RIP packets.

v1_only – Specifies that only RIP v1 packets will be accepted.

v2_only – Specifies that only RIP v2 packets will be accepted.

v1_or_v2 – Specifies that RIP v1 or v2 packets will be accepted.

state [enabled|disabled] – Allows RIP to be enabled and disabled on an IP interface on the switch.

Restrictions

Only administrator-level users can issue this command.

config rip all

this command.

Example Usage:

To change the RIP state to enabled for all the IP interfaces on the switch:

```
local>config rip all state enabled
Command: config rip all state enabled

Success.

local>
```

enable rip

Purpose	Used to enable RIP.
Syntax	enable rip
Description	This command is used, along with the disable RIP command below, to enable or disable RIP on the switch.
Parameters	none.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable RIP:

```
local>enable rip
Command: enable rip

Success.

local>
```

disable rip

Purpose	Used to disable RIP.
Syntax	disable rip
Description	This command is used, along with the enable RIP command below, to enable or disable RIP on the switch.
Parameters	none.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To disable RIP:

```
local>disable rip
Command: disable rip

Success.

local>
```


show rip

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

Example Usage:

To show RIP:

```
local>show rip
```

```
Command: show rip
```

RIP Interface Settings

RIP Global State : Disabled

Interface	IP Address	TX Mode	RX Mode	Authen- tication	State
-----	-----	-----	-----	-----	-----
System	10.48.74.122	V2 Only	V1 Only	Disabled	Disabled
if20	20.48.74.121	Disabled	Disabled	Disabled	Disabled

Total Entries: 2

27

DVMRP 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 dvmrp	ipif <ipif_name 12> all metric <value 1-31> probe <sec 1-65535> neighbor_timeout <sec 1-65535> state [enabled disabled]
enable dvmrp	
disable dvmrp	
show dvmrp routing_table	ipaddress <network_address>
show dvmrp neighbor	ipif <ipif_name 12> ipaddress <ipaddr>
show dvmrp nexthop	ipif <ipif_name 12> ipaddress <network_address>
show dvmrp	ipif <ipif_name 12>

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

config dvmrp

Purpose	Used to configure DVMRP on the switch.
Syntax	config dvmrp [ipif <ipif_name 12> all] {metric <value 1-31> probe <second 1-65535> neighbor_timeout <second 1-65535> state [enabled disabled]}
Description	This command is used to configure DVMRP on the switch.
Parameters	<p><ipif_name 12> – The name of the IP interface for which DVMRP is to be configured.</p> <p>all – Specifies that DVMRP is to be configured for all IP interfaces on the switch.</p> <p>metric <value 1-31> – Allows the assignment of a DVMRP route cost to the above IP interface. A DVMRP route cost is a relative number that represents the real cost of using this route in the construction of a multicast delivery tree. It is similar to, but not defined as, the hop count in RIP. The default is 1.</p> <p>probe <second 1-65535> – This setting is the Probe Interval. The switch will send probe packets every Probe Interval. The DVMRP Router uses probe packets to discover DVMRP neighbor routers.</p> <p>neighbor_timeout <second 1-65535> – The time period for which DVMRP will hold Neighbor Router reports before issuing poison route messages. The default value is 35 seconds.</p>

config dvmrp

	state [enabled disabled] – Allows DVMRP to be enabled or disabled on this interface.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure DVMRP configurations of IP interface
System:

```
local>config dvmrp ipif System neighbor_timeout 30 metric 1  
probe 5  
Command: config dvmrp ipif System neighbor_timeout 30 metric  
1 probe 5  
  
Success  
  
local>
```

enable dvmrp

Purpose	Used to enable DVMRP.
Syntax	enable dvmrp
Description	This command, in combination with the disable dvmrp below, to enable and disable DVMRP on the switch.
Parameters	None.

enable dvmrp

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

Example Usage:

To enable DVMRP:

```
local>enable dvmrp
Command: enable dvmrp
```

Success.

```
local>
```

disable dvmrp

Purpose	Used to disable DVMRP.
Syntax	disable dvmrp
Description	This command, in combination with the enable dvmrp above, to enable and disable DVMRP on the switch.
Parameters	none.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To disable DVMRP:

```
local>disable dvmrp
Command: disable dvmrp
```

Success.

```
local>
```

show dvmrp routing_table

Purpose	Used to display the current DVMRP routing table.
Syntax	show dvmrp routing_table {ipaddress <network_address>}
Description	The command is used to display the current DVMRP routing table.
Parameters	ipaddress <network_address> – The IP address and netmask of the destination. You can specify the IP address and netmask information using the traditional format or the CIDR format. For example, 10.1.2.3/255.255.0.0 or 10.2.3.4/16.
Restrictions	none.

Example Usage:

To display DVMRP routing table:

```
local>show dvmrp routing_table
Command: show dvmrp routing_table
```

DVMRP Routing Table

Source Address	Source Mask	Upstream Neighbor	Metric	Learned	Interface	Expire
10.0.0.0	255.0.0.0	10.90.90.90	2	Local	System	-
20.0.0.0	255.0.0.0	20.1.1.1	2	Local	if11	-
30.0.0.0	255.0.0.0	30.1.1.1	2	Local	ip3	-

Total Entries: 3

local>

show dvmrp neighbor

Purpose Used to display the DVMRP neighbor table.

Syntax **show dvmrp neighbor {ipif <ipif_name 12> | ipaddress <ipaddr>}**

Description This command will display the current DVMRP neighbor table.

Parameters <ipif_name 12> – The name of the IP interface for which you want to display the DVMRP neighbor table.

ipaddress <ipaddr> – The IP address of the destination. You can specify the IP address information using the traditional format or the CIDR format. For example, 10.1.2.3/255.255.0.0 or 10.2.3.4/16.

Restrictions none.

Example Usage:

To display DVMRP neighbor table:

local>show dvmrp neighbor Command: show dvmrp neighbor			
DVMRP Neighbor Address Table			
Interface	Neighbor Address	Generation ID	Expire Time
-----	-----	-----	-----
System	10.2.1.123	2	250
Total Entries: 1			

show dvmrp nexthop

Purpose	Used to display the current DVMRP routing next hop table.
Syntax	show dvmrp nexthop {ipaddress <network_address> ipif <ipif_name 12>}
Description	This command will display the DVMRP routing next hop table.
Parameters	<p><ipif_name 12> – The name of the IP interface for which you want to display the current DVMRP routing next hop table.</p> <p>ipaddress <network_address> – The IP address and netmask of the destination. You can specify the IP address and netmask information using the traditional format or the CIDR format. For example, 10.1.2.3/255.255.0.0 or 10.2.3.4/16.</p>

show dvmrp nexthop

Restrictions none.

Example Usage:

To display DVMRP routing next hop table:

```
local>show dvmrp nexthop
```

Command: show dvmrp nexthop

Source IP Address	Source Mask	Interface Name	Type
10.0.0.0	255.0.0.0	ip2	Leaf
10.0.0.0	255.0.0.0	ip3	Leaf
20.0.0.0	255.0.0.0	System	Leaf
20.0.0.0	255.0.0.0	ip3	Leaf
30.0.0.0	255.0.0.0	System	Leaf
30.0.0.0	255.0.0.0	ip2	Leaf

Total Entries: 6

```
local>
```

show dvmrp

Purpose Used to display the current DVMRP status.

Syntax **show dvmrp {<ipif_name 12>}**

Description The command will display the current DVMRP status.

Parameters <ipif_name 12> – The name of the IP interface for which you want to display the

show dvmrp

interface for which you want to display the DVMRP status.

Restrictions none.

Example Usage:

To show DVMRP configurations:

```
local>show dvmrp
```

```
Command: show dvmrp
```

DVMRP Global State : Disabled

Interface	IP Address	Neighbor Timeout	Probe	Metric	State
System	10.90.90.90	35	10	1	Disabled

Total Entries: 1

```
local>
```

28

PIM COMMANDS

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

Command	Parameters
config pim	ipif <ipif_name 12> all hello <sec 1-18724> jp_interval <sec 1-18724> state [enabled/disabled]
enable pim	
disable pim	
show pim neighbor	ipif <ipif_name 12> ipaddress <ipaddr>
show pim	ipif <ipif_name 12>

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

config pim

Purpose	Used to configure PIM on the switch.
Syntax	config pim [ipif <ipif_name 12>/all {hello <sec 1-18724>/jp_interval <sec 1-18724>/state [enabled/disabled]}
Description	This command is used to configure PIM on the switch.
Parameters	<p><ipif_name 12> – The name of the IP interface for which you want to configure PIM.</p> <p>all – Specifies that PIM will be configured for all IP interfaces on the switch.</p> <p>hello <sec 1-18724> – The time, in seconds, between issuing hello packets to find neighboring routers.</p> <p>jp_interval <sec 1-18724> – The join prune interval is the time to wait before updating a peer's forwarding state.</p> <p>state – Allows PIM to be disabled or enabled for the above IP interface. The default is disabled.</p>
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure PIM:

```
local>config pim ipif System hello 35 jp_interval 70 state enabled
Command: config pim ipif System hello 35 jp_interval 70 state
enabled
```

Success.

```
local>
```

enable pim

Purpose	Used to enable PIM on the switch.
Syntax	enable pim
Description	This command, in combination with the disable pim command below, is used to enable or disable PIM on the switch.
Parameters	none.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable PIM:

```
local>enable pim
Command: enable pim
```

Success.

```
local>
```

disable pim

Purpose	Used to disable PIM on the switch.
Syntax	disable pim
Description	This command, in combination with the enable pim command above, is used to enable or disable PIM on the switch.
Parameters	none.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To disable PIM:

```
local>disable pim
Command: disable pim

Success.

local>
```

show pim neighbor

Purpose	Used to display the current PIM neighbor router table.
---------	--

show pim neighbor

Syntax	show pim neighbor {ipif <ipif_name 12>/ipaddress <ipaddr>}
Description	This command will display the current PIM neighbor router table.
Parameters	<p><ipif_name 12> – The name of the IP interface for which you want to display the current PIM neighbor routing table.</p> <p>ipaddress <ipaddr> – The IP address and netmask of the destination. You can specify the IP address and netmask information using the traditional format or the CIDR format. For example, 10.1.2.3/255.255.0.0 or 10.2.3.4/16.</p>
Restrictions	none.

Example Usage:

To show PIM neighbor:

```
local>show pim neighbor
Command: show pim neighbor

PIM Neighbor Address Table

Interface Name  Neighbor Address  Expire Time
-----
      System      10.48.74.122      5
Total Entries: 1
```


show pim

Purpose	Used to display the current PIM configuration.
Syntax	show pim {ipif <ipif_name 12>}
Description	This command will display the current PIM configuration.
Parameters	<ipif_name 12> – The name of the IP interface for which you want to display the PIM configuration for.
Restrictions	none.

Example Usage:

To display the current PIM configuration:

```
local>show pim
Command: show pim

PIM Global State : Disabled

PIM-DM Interface Table

```

Interface	IP Address	Hello Interval	Join/Prune Interval	State
System	10.90.90.90	35	0	Enabled

```
Total Entries: 1
```

```
local>
```

29

IP MULTICASTING COMMANDS

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

Command	Parameters
show ipmc cache	group <group> ipaddress <network_address>
show ipmc	ipif {ipif <ipif_name 12> protocol [dvmrp pim]}

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

show ipmc cache	
Purpose	Used to display the current IP multicast forwarding cache.
Syntax	show ipmc cache {group <group>} {ipaddress <network_address>}

show ipmc cache

Description	This command will display the current IP multicast forwarding cache.
Parameters	<p>group <group> – The multicast group ID.</p> <p>ipaddress <network_address> – The IP address and netmask of the destination. You can specify the IP address and netmask information using the traditional format or the CIDR format. For example, 10.1.2.3/255.255.0.0 or 10.2.3.4/16.</p>
Restrictions	none.

Usage Example:

To display the current IP multicast forwarding cache:

local>show ipmc cache					
Command: show ipmc cache					
Multicast Group	Source IP Address	Source IP Mask	Upstream Neighbor	Expire Time	Routing Protocol
224.1.1.1	10.48.74.121	255.0.0.0	10.48.75.63	30	dvmrp
224.1.1.1	20.48.74.25	255.0.0.0	20.48.75.25	20	pim-dm
224.1.2.3	10.48.75.3	255.0.0.0	10.48.76.6	30	dvmrp
Total Entries: 3					
local>					

show ipmc

Purpose	Used to display the IP multicast interface table.
Syntax	show ipmc {ipif <ipif_name 12> protocol [dvmrp pim]}
Description	This command will display the current IP multicast interface table.
Parameters	<p><ipif_name 12> – The name of the IP interface for which you want to display the IP multicast interface table for.</p> <p>protocol [dvmrp pim] – Allows you to specify either the DVMRP or PIM protocol to be used in displaying the IP multicast interface table. For example, if DVMRP is specified, the table will display only those entries that are related to the DVMRP protocol.</p>
Restrictions	none.

Usage Example

To display the current IP multicast interface table:

```
local>show ipmc
```

```
Command: show ipmc
```

<u>Interface</u>	<u>IP Address</u>	<u>Multicast Routing</u>
System	10.90.90.90	INACT

```
Total Entries: 1
```

```
local>
```

MD5 CONFIGURATION COMMANDS

The MD5 configuration commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
config md5	key <key_id 1-255> <password 16>
create md5	key <key_id 1-255> <password 16>
delete md5	key <key_id 1-255>
show md5	key <key_id 1-255>

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

config md5

Purpose	Used to enter configure an MD5 key and password.
Syntax	config md5 <key_id 1-255> <password 16>
Description	This command is used to configure an MD5 key and password.
Parameters	<key_id 1-255> – The MD5 key ID. <password 16> – An MD5 password of up to 16 bytes.
Restrictions	Only administrator-level users can issue this command.

Usage Example

To configure an MD5 Key and Password:

```
local>config md5 key 1 dlink
Command: config md5 key 1 dlink

Success.

local>
```


create md5

Purpose	Used to create an MD5 key table.
Syntax	create md5 key <key_id 1-255> <password 16>
Description	This command is used to create an MD5 key table.
Parameters	<key_id 1-255> – The MD5 key ID. <password 16> – An MD5 password of up to 16 bytes.
Restrictions	Only administrator-level users can issue this command.

Usage Example

To create an MD5 key table:

```
local> create md5 key 1 dlink
Command: create md5 key 1 dlink

Success.

local>
```

delete md5

Purpose	Used to delete an MD5 key table.
Syntax	delete md5 key <key_id 1-255>
Description	This command is used to delete an MD5 key table.
Parameters	<key_id 1-255> – The MD5 key ID.
Restrictions	Only administrator-level users can issue this command.

Usage Example

The delete an MD5 key table:

```
local> delete md5 key 1  
Command: delete md5 key 1
```

Success.

```
local>
```

show md5

Purpose	Used to display an MD5 key table.
Syntax	show md5 {key <key_id 1-255>}
Description	This command will display the current MD5 key table.
Parameters	<key_id 1-255> – The MD5 key ID.

show md5

Restrictions none.

Usage Example

To display the current MD5 key:

```
local>show md5  
Command: show md5
```

MD5 Key Table

Key-ID	Key
----	-----
1	dlink
2	develop
3	fireball
4	intelligent

Total Entries: 4

```
local>
```

31

OSPF CONFIGURATION COMMANDS

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

Command	Parameters
config ospf router_id	<ipaddr>
enable ospf	
disable ospf	
show ospf	
create ospf area	<area_id> type [normal stub] stub_summary [enabled disabled] metric <value 0-16777215>
delete ospf area	<area_id>
config ospf area	<area_id> type [normal stub] stub_summary [enabled disabled] metric <value 0-16777215>
show ospf area	<area_id>

Command	Parameters
create ospf host_route	<ipaddr> area <area_id> metric <value 1-65535>
delete ospf host_route	<ipaddr>
config ospf host_route	<ipaddr> area <area_id> metric <value>
show ospf host_route	<ipaddr>
create ospf aggregation	<area_id> <network_address> lsdb_type [summary] advertise [enabled disabled]
delete ospf aggregation	<area_id> <network_address> lsdb_type [summary]
config ospf aggregation	<area_id> <network_address> lsdb_type [summary] advertise [enabled disabled]
show ospf aggregation	<area_id>
show ospf lsdb	area_id <area_id> advertise_router <ipaddr> type [rtrlink netlink summary assummary asextl ink]
show ospf neighbor	<ipaddr>
show ospf virtual_neighbor	<area_id> <neighbor_id>
config ospf	ipif <ipif_name 12> all

Command	Parameters
	area <area_id> priority <value> hello_interval <sec 1-65535> dead_interval <sec 1-65535> authentication [none simple <password> md5 <key_id 1-255>] metric <value 1-65535> state [enabled disabled]
show ospf ipif	<ipif_name 12>
show ospf all	
create ospf virtual_link	<area_id> <neighbor_id> hello_interval <sec 1-65535> dead_interval <sec 1-65535> authentication [simple <password 8> md5 <key_id 1-255> none]
config ospf virtual_link	<area_id> <neighbor_id> hello_interval <sec 1-65535> dead_interval <sec 1-65535> authentication [simple <password 8> md5 <key_id 1-255> none]
delete ospf virtual_link	<area_id> <neighbor_id>
show ospf virtual_link	<area_id> <neighbor_id>

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

config ospf

config ospf

Purpose	Used to configure the OSPF router ID.
Syntax	config ospf router_id <ipaddr>
Description	This command is used to configure the OSPF router ID.
Parameters	<ipaddr> – The OSPF router ID.
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To configure the OSPF router ID:

```
local>config ospf router_id 10.48.74.122
Command: config ospf router_id 10.48.74.122
Success.
local>
```

enable ospf

Purpose	Used to enable OSPF on the switch.
Syntax	enable ospf
Description	This command, in combination with the disable ospf command below, is used to enable and disable OSPF on the switch.
Parameters	none.
Restrictions	Only administrator-level users can issue this command.

enable ospf

this command.

Usage Example

To enable OSPF on the switch:

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

disable ospf

Purpose	Used to disable OSPF on the switch.
Syntax	disable ospf
Description	This command, in combination with the enable ospf command above, is used to enable and disable OSPF on the switch.
Parameters	none.
Restrictions	Only administrator-level users can issue this command.

Usage Example

To disable OSPF on the switch:

```
local>disable ospf
Command: disable ospf
```



```
local>
```

show ospf

Purpose	Used to display the current OSPF state on the switch.
Syntax	show ospf
Description	<p>This command will display the current state of OSPF on the switch, divided into the following categories:</p> <ul style="list-style-type: none">General OSPF settingsInterface OSPF settingsArea OSPF settingsVirtual Interface settingsArea Aggregation settingsHost Route settings
Parameters	none.
Restrictions	none.

Usage Example:

To show OSPF state:

```
local>show ospf  
Command: show ospf
```

OSPF Router ID : 10.1.1.2

State : Enabled

OSPF Interface Settings

Interface	IP Address	Area ID	State	Link Status	Metric
-----	-----	-----	-----	-----	-----
System	10.90.90.90 8	0.0.0.0	Disabled	Link DOWN	1
ip2	20.1.1.1 8	0.0.0.0	Disabled	Link DOWN	1
ip3	30.1.1.1 8	0.0.0.0	Disabled	Link DOWN	1

Total Entries : 3

OSPF Area Settings

Area ID	Type	Stub Import Summary	LSA Stub Default Cost
-----	-----	-----	-----
0.0.0.0	Normal	None	None
10.0.0.0	Normal	None	None
10.1.1.1	Normal	None	None
20.1.1.1	Stub	Enabled	1

Total Entries : 4

Virtual Interface Configuration

Transit Area ID	Virtual Neighbor Router	Hello Interval	Dead Interval	Authentication	Link Status
-----	-----	-----	-----	-----	-----
10.0.0.0	20.0.0.0	10	60	None	DOWN
10.1.1.1	20.1.1.1	10	60	None	DOWN

Total Entries : 2

OSPF Area Aggregation Settings

Area ID	Aggregated Network Address	LSDB Type	Advertise
-----	-----	-----	-----

Total Entries : 0

OSPF Host Route Settings

Host Address	Metric	Area ID	TOS
-----	-----	-----	---
10.3.3.3	1	10.1.1.1	0

Total Entries : 1

local>

create ospf area

Purpose	Used to configure OSPF area settings.
Syntax	create ospf area <area_id> type [normal stub] {stub_summary [enabled disabled] metric <value 0-16777215>}
Description	This command is used to create an OSPF area and configure its settings.
Parameters	<area_id> – The OSPF area ID. type – The OSPF area mode of operation –

create ospf area

stub or normal.

stub_summary – Enables or disables the OSPF area to import summary LSA advertisements.

metric <value 0-16777215> – The OSPF area cost between 0 and 16,777,215. The default is 1.

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

Usage Example:

To create an OSPF area:

```
local>create ospf area 10.48.74.122 type normal
Command: create ospf area 10.48.74.122 type normal
```

Success.

```
local>
```

delete ospf area

Purpose	Used to delete an OSPF area.
---------	------------------------------

Syntax	delete ospf area <area_id>
--------	---

Description	This command is used to delete an OSPF area.
-------------	--

delete ospf area

Parameters	<area_id> – <area_id> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To delete an OSPF area:

```
local>delete ospf area 10.48.74.122
Command: delete ospf area 10.48.74.122

Success.

local>
```

config ospf area

Purpose	Used to configure an OSPF area's settings.
Syntax	config ospf area <area_id> type [normal stub {stub_summary [enabled disabled] metric <value 0-16777215>}]
Description	This command is used to configure an OSPF area's settings.
Parameters	<area_id> – The OSPF area ID.

config ospf area

type – Allows the specification of the OSPF mode of operation – stub or normal.

stub_summary [enabled|disabled] – Allows the OSPF area import of LSA advertisements to be enabled or disabled.

metric <value 0-16777215> – The OSPF area cost between 0 and 16,777,215. The default is 0.

Restrictions Only administrator-level users can issue this command.

Usage Example

To configure an OSPF area's settings:

```
local>config ospf area 10.48.74.122 type stub stub_summary
enabled metric 1
Command: config ospf area 10.48.74.122 type stub stub_summary
enabled metric 1
```

Success.

```
local>
```

show ospf

Purpose Used to display an OSPF area's configuration.

Syntax **show ospf <area_id>**

show ospf

Description	This command will display the current OSPF area configuration.
Parameters	<area_id> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.
Restrictions	none.

Usage Example:

To display an OSPF area's settings:

```
local>show ospf area
Command: show ospf area
  Area_id    Type  Stub Import Summary LSA Stub Default Cost
-----
   0.0.0.0   Normal          None          None
10.48.74.122 Stub          Enabled         1

Total Entries: 2

local>
```

create ospf host_route

Purpose	Used to configure OSPF host route settings.
Syntax	create ospf host_route <ipaddr> {area <area_id> metric <value 1-65535>}

create ospf host_route

Description	This command is used to configure the OSPF host route settings.
Parameters	<p><ipaddr> – The host's IP address.</p> <p>area <area_id> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.</p> <p>metric <value 1-65535> – A metric between 1 and 65535, which will be advertised.</p>
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To configure the OSPF host route settings:

```
local>create ospf host_route 10.48.74.122 area 10.1.1.1 metric 2
Command: create ospf host_route 10.48.74.122 area 10.1.1.1 metric
2
Success.
local>
```

delete ospf host_route

Purpose	Used to delete an OSPF host route.
---------	------------------------------------

delete ospf host_route

Syntax	delete ospf host_route <ipaddr>
Description	This command is used to delete an OSPF host route.
Parameters	<ipaddr> – The IP address of the OSPF host.
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To delete an OSPF host route:

```
local>delete ospf host_route 10.48.74.122
Command: delete ospf host_route 10.48.74.122

Success.

local>
```

config ospf host_route

Purpose	Used to configure OSPF host route settings.
Syntax	config ospf host_route <ipaddr> {area <area_id> metric <value 1-65535>}
Description	This command is used to configure an OSPF host route settings.
Parameters	<ipaddr> – The IP address of the host.

config ospf host_route

<area_id> – **<area_id>** – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.

metric <value 1-65535> – A metric between 1 and 65,535, which will be advertised.

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

Usage Example:

To configure an OSPF host route:

```
local>config ospf host_route 10.48.74.122 area 10.1.1.1 metric 2
Command: config ospf host_route 10.48.74.122 area 10.1.1.1
metric 2
Success.
local>
```

show ospf host_route

Purpose	Used to display the current OSPF host route table.
---------	--

Syntax	show ospf host_route {<ipaddr>}
--------	--

Description	This command will display the current OSPF host route table.
-------------	--

show ospf host_route

Parameters <ipaddr> – The IP address of the host.

Restrictions none.

Usage Example:

To display the current OSPF host route table:

```
local>show ospf host_route
```

Command: show ospf host_route

Host Address	Metric	Area_ID	TOS
10.48.73.21	2	10.1.1.1	0
10.48.74.122	1	10.1.1.1	0

Total Entries: 2

```
local>
```

create ospf aggregation

Purpose Used to configure OSPF area aggregation settings.

Syntax **create ospf aggregation <area_id>**
 <network_address> lsdb_type [summary]
 {advertise [enabled | disabled]}

create ospf aggregation

Description	This command is used to create an OSPF area aggregation.
Parameters	<p><area_id> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.</p> <p><network_address> – The 32-bit number in the form of an IP address that uniquely identifies the network that corresponds to the OSPF Area.</p> <p>lsdb_type [summary] – The type of address aggregation.</p> <p>advertise [enabled disabled] – Allows for the advertisement trigger to be enabled or disabled.</p>
Restrictions	Only administrator-level users can issue this command.

Usage Example

To create an OSPF area aggregation:

```
local>create ospf aggregation 10.1.1.1 10.48.76.122/16 lsdb_type
summary advertise enabled
Command: create ospf aggregation 10.1.1.1 10.48.76.122/16
lsdb_type summary advertise enabled

Success.
```

local>

delete ospf aggregation

Purpose	Used to delete an OSPF area aggregation configuration.
Syntax	delete ospf aggregation <area_id> <network_address> lsdb_type [summary]
Description	This command is used to delete an OSPF area aggregation configuration.
Parameters	<p><area_id> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.</p> <p><network_address> – The 32-bit number in the form of an IP address that uniquely identifies the network that corresponds to the OSPF Area.</p> <p>lsdb_type [summary] – Specifies the type of address aggregation.</p>
Restrictions	Only administrator-level users can issue this command.

Usage Example

To configure the OSPF area aggregation settings:

```
local>delete ospf aggregation 10.1.1.1 10.48.76.122/16 lsdb_type  
summary  
Command: delete ospf aggregation 10.1.1.1 10.48.76.122/16  
lsdb_type summary
```

Success.

local>

config ospf aggregation

Purpose	Used to configure the OSPF area aggregation settings.
Syntax	config ospf aggregation <area_id> <network_address> lsdb_type [summary] advertise [enabled disabled]
Description	This command is used to configure the OSPF area aggregation settings.
Parameters	<p><area_id> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.</p> <p><network_address> – The 32-bit number in the form of an IP address that uniquely identifies the network that corresponds to the OSPF Area.</p> <p>lsdb_type [summary] – Specifies the type of address aggregation.</p> <p>advertise [enabled disabled] – Allows for the advertisement trigger to be enabled or disabled.</p>
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To configure the OSPF area aggregation settings:

```
local>config ospf aggregation 10.1.1.1 10.48.76.122/16 lsdb_type
summary advertise enabled
Command: config ospf aggregation 10.1.1.1 10.48.76.122/16
lsdb_type summary advertise enabled
```

Success.

```
local>
```

show ospf aggregation

Purpose	Used to display the current OSPF area aggregation settings.
Syntax	show ospf aggregation {<area_id>}
Description	This command will display the current OSPF area aggregation settings.
Parameters	<area_id> – The OSPF area ID.
Restrictions	none.

Usage Example:

To display OSPF area aggregation settings:

```
local>show ospf aggregation
Command: show ospf aggregation
```


OSPF Area Aggregation Settings

Area ID	Aggregated Network Address	LSDB Type	Advertise
10.1.1.1	10.0.0.0/8	Summary	Enabled
10.1.1.1	20.2.0.0/16	Summary	Enabled

Total Entries: 2

local>

show ospf lsdb

Purpose Used to display the OSPF Link State Database (LSDB).

Syntax **show ospf lsdb {area_id <area_id> | advertise_router <ipaddr> | type [rtrlink | netlink | summary | assummary | asextlink]}**

Description This command will display the current OSPF Link State Database (LSDB).

Parameters area_id <area_id> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.

advertise_router <ipaddr> – The router ID of the advertising router.

type
[rtrlink | netlink | summary | assummary | asextlink]
] – The type of link.

show ospf lsdb

Restrictions none.

Note: When this command displays a “*” (a star symbol) in the OSPF LSDB table for the Area_id or the Cost, this is interpreted as “no area ID” for external LSAs, and as “no cost given” for the advertised link.

Usage Example:

To display the link state database of OSPF:

```
local>show ospf lsdb
```

Command: show ospf lsdb

Area ID	LSDB Type	Advertising Router ID	Link State ID	Cost	Sequence Number
0.0.0.0	RTRLink	50.48.75.73	50.48.75.73	*	0x80000002
0.0.0.0	Summary	50.48.75.73	10.0.0.0 8	1	0x80000001
1.0.0.0	RTRLink	50.48.75.73	50.48.75.73	*	0x80000001
1.0.0.0	Summary	50.48.75.73	40.0.0.0 8	1	0x80000001
1.0.0.0	Summary	50.48.75.73	50.0.0.0 8	1	0x80000001
*	ASExtLink	50.48.75.73	1.2.0.0 16	20	0x80000001

Total Entries: 5

```
local>
```

show ospf neighbor

Purpose Used to display the current OSPF neighbor router table

show ospf neighbor

router table.

Syntax	show ospf neighbor {<ipaddr>}
Description	This command will display the current OSPF neighbor router table.
Parameters	<ipaddr> – The IP address of the neighbor router.
Restrictions	none.

Usage Example:

To display the current OSPF neighbor router table:

```
local>show ospf neighbor
Command: show ospf neighbor
```

IP Address of Neighbor	Router ID of Neighbor	Neighbor Priority	Neighbor State
10.48.74.122	10.2.2.2	1	Initial

```
local>
```

show ospf virtual_neighbor

Purpose Used to display the current OSPF virtual neighbor router table.

Syntax **show ospf virtual_neighbor** {<area_id>
<neighbor_id>}

show ospf virtual_neighbor**<neighbor_id>}**

Description	This command will display the current OSPF virtual neighbor router table.
Parameters	<p><area_id> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.</p> <p><neighbor_id> – The OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router.</p>
Restrictions	none.

Usage Example:

To display the current OSPF virtual neighbor table:

local>show ospf virtual_neighbor**Command: show ospf virtual_neighbor**

Transit Area ID	Router ID of Virtual Neighbor	IP Address of Virtual Neighbor	Virtual Neighbor State
10.1.1.1	10.2.3.4	10.48.74.111	Exchange

local>

config ospf ipif

Purpose	Used to configure the OSPF interface settings.
Syntax	config ospf [ipif <ipif_name 12>/all {area <area_id> priority <value> hello_interval <sec 1-65535> dead_interval <sec 1-65535> authentication [none simple <password 8> md5 <key_id 1-255>]} metric <value> state [enabled disabled]}
Description	This command is used to configure the OSPF interface settings.
Parameters	<p><ipif_name 12> – The name of the IP interface.</p> <p>priority <value> – The priority used in the election of the Designated Router (DR). A number between 0 and 255.</p> <p>metric <value 1-65535> – The interface metric (1 to 65535). Entering a 0 will allow automatic calculation of the metric.</p> <p>hello_interval <sec 1-65535> – Allows the specification of the interval between the transmission of OSPF Hello packets, in seconds. Between 1 and 65535 seconds can be specified. The Hello Interval, Dead Interval, Authorization Type, and Authorization Key should be the same for all routers on the same network.</p> <p>dead_interval <sec 1-65535> – Allows the specification of the length of time between</p>

config ospf ipif

the receipt of Hello packets from a neighbor router before the selected area declares that router down. An interval between 1 and 65535 seconds can be specified. The Dead Interval must be evenly divisible by the Hello Interval.

<password 8> – A case-sensitive password.

<key_id 1-255> – A previously configured MD5 key ID (1 to 255).

metric <value 1-65535> – This field allows the entry of a number between 1 and 65,535 that is representative of the OSPF cost of reaching the selected OSPF interface. The default metric is 0.

Restrictions Only administrator-level users can issue this command.

Usage Example:

To configure OSPF:

```
local>config ospf ipif System priority 2 hello_interval 15 metric 2
state enabled
Command: config ospf ipif System priority 2 metric 2 state enabled
hello_interval 15

Success.

local>
```

show ospf ipif

Purpose	Used to display the current OSPF interface settings for the specified interface name.
Syntax	show ospf ipif {<ipif_name 12>}
Description	This command will display the current OSPF interface settings for the specified interface name.
Parameters	<ipif_name 12> – The IP interface name for which you want to display the current OSPF interface settings.
Restrictions	none.

Usage Example:

To display the current OSPF interface settings, for a specific OSPF interface:

```
local>show ospf ipif2
Command: show ospf ipif2

Interface Name: ipif2          IP Address: 123.234.12.34/24
(Link Up)
Network Medium Type: BROADCAST Metric: 1
Area ID: 1.0.0.0              Administrative State: Enabled
Priority: 1                    DR State: DR
DR Address: 123.234.12.34      Backup DR Address: None
Hello Interval: 10            Dead Interval: 40
Transmit Delay: 1             Retransmit Time: 5
Authentication: None

Total Entries: 1
```

```
local>
```

show ospf all

Purpose	Used to display the current OSPF settings of all the OSPF interfaces on the switch.
Syntax	show ospf all
Description	This command will display the current OSPF settings for all OSPF interfaces on the switch.
Parameters	none.
Restrictions	none.

Usage Example:

To display the current OSPF interface settings, for all OSPF interfaces on the switch:

```
local>show ospf all
Command: show ospf all

Interface Name: System          IP Address: 10.42.73.10|8
Link Up)
Network Medium Type: BROADCAST Metric: 1
Area ID: 0.0.0.0               Administrative State: Enabled
Priority: 1                     DR State: DR
DR Address: 10.42.73.10         Backup DR Address: None
Hello Interval: 10              Dead Interval: 40
Transmit Delay: 1               Retransmit Time: 5
Authentication: None
```


Interface Name: ipif2	IP Address: 123.234.12.34/24
(Link Up)	
Network Medium Type: BROADCAST	Metric: 1
Area ID: 1.0.0.0	Administrative State: Enabled
Priority: 1	DR State: DR
DR Address: 123.234.12.34	Backup DR Address: None
Hello Interval: 10	Dead Interval: 40
Transmit Delay: 1	Retransmit Time: 5
Authentication: None	

Total Entries: 2

local>

config ospf virtual_link

Purpose	Used to configure the OSPF virtual interface settings.
---------	--

Syntax	config ospf virtual_link <area_id> <neighbor_id> {hello_interval <sec 1-65535> dead_interval <sec 1-65535> authentication [simple <password 8> md5 <key_id 1-255> none]}
--------	---

Description	This command is used to configure the OSPF virtual interface settings.
-------------	--

config ospf virtual_link

Parameters	<p><area_id> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.</p> <p><neighbor_id> – The OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router.</p> <p>hello_interval <sec 1-65535> – Allows the specification of the interval between the transmission of OSPF Hello packets, in seconds. Between 1 and 65,535 seconds can be specified. The Hello Interval, Dead Interval, Authorization Type, and Authorization Key should be the same for all routers on the same network.</p> <p>dead_interval <sec 1-65535> – Allows the specification of the length of time between the receipt of Hello packets from a neighbor router before the selected area declares that router down. An interval between 1 and 65,535 seconds can be specified. The Dead Interval must be evenly divisible by the Hello Interval.</p> <p><password 8> – A case-sensitive password.</p> <p><key_id 1-255> – A previously configured MD5 key. A value between 1 and 255 seconds can be entered.</p>
------------	---

config ospf virtual_link

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

Usage Example:

To configure the OSPF virtual interface settings:

```
local>config ospf virtual_link 10.1.1.2 20.1.1.1 hello_interval 10
Command: config ospf virtual_link 10.1.1.2 20.1.1.1 hello_interval
10

Success.

local>
```

create ospf virtual_link

Purpose	Used to create an OSPF virtual interface.
Syntax	create ospf virtual_link <area_id> <neighbor_id> {hello_interval <sec 1- 65535> dead_interval <sec 1- 65535> authentication [none simple <password 8> md5 <key_id 1-255>}]}
Description	This command is used to create an OSPF virtual interface.

create ospf virtual_link

Parameters	<p><area_id> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.</p> <p><neighbor_id> – The OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router. The router ID of the neighbor router.</p> <p>hello_interval <sec 1-65535> – Allows the specification of the interval between the transmission of OSPF Hello packets, in seconds. Between 1 and 65,535 seconds can be specified. The Hello Interval, Dead Interval, Authorization Type, and Authorization Key should be the same for all routers on the same network.</p> <p>dead_interval <sec 1-65535> – Allows the specification of the length of time between the receipt of Hello packets from a neighbor router before the selected area declares that router down. An interval between 1 and 65,535 seconds can be specified. The Dead Interval must be evenly divisible by the Hello Interval.</p> <p><password 8> – A case-sensitive password.</p> <p><key_id 1-255> – A previously configured MD5 key ID (1 to 255).</p>
------------	---

create ospf virtual_link

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

Usage Example:

To create an OSPF virtual interface:

```
local>create ospf virtual_link 10.1.12 20.1.1.1 hello_interval 10
Command: create ospf virtual_link 10.1.12 20.1.1.1 hello_interval 10

Success.

local>
```

delete ospf virtual_link

Purpose	Used to delete an OSPF virtual interface.
Syntax	delete ospf virtual_link <area_id> <neighbor_id>
Description	This command will delete an OSPF virtual interface from the switch.
Parameters	<area_id> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain. <neighbor_id> – The OSPF router ID for

delete ospf virtual_link

the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router. The router ID of the neighbor router.

Restrictions Only administrator-level users can issue this command.

Usage Example:

To delete an OSPF virtual interface from the switch:

```
local>delete ospf virtual_link 10.1.12 20.1.1.1
Command: delete ospf virtual_link 10.1.12 20.1.1.1
```

Success.

```
local>
```

show ospf virtual_link

Purpose Used to display the current OSPF virtual interface configuration.

Syntax **show ospf virtual_link {<area_id> <neighbor_id>}**

Description This command will display the current OSPF virtual interface configuration.

Parameters <area_id> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the

show ospf virtual_link

OSPF domain.

<neighbor_id> – The OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router. This is the router ID of the neighbor router.

Restrictions none.

Usage Example:

To display the current OSPF virtual interface configuration:

```
local>show ospf virtual_link
```

Transit Area ID	Virtual Neighbor Router	Hello Interval	Dead Interval	Authentication	Link Status
10.0.0.0	20.0.0.0	10	60	None	DOWN

Total Entries: 1

```
local>
```

32

SNTP COMMANDS

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

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

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

config sntp

Purpose	Used to configure SNTP on the switch.
---------	---------------------------------------

config sntp

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

Example Usage:

To configure SNTP for the primary server for a switch:

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

Success.

```
local>
```

enable sntp

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

Example Usage:

To enable SNTP on the switch:

```
local>enable sntp  
Command: enable sntp
```

Success.

```
local>
```

disable sntp

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

Example Usage:

To disable SNTP on the switch:

```
local>disable sntp
Command: disable sntp

Success.

local>
```

show sntp

Purpose	Used to show SNTP on the switch.
Syntax	show sntp
Description	This command will show SNTP on the switch.

Parameters	None.
Restrictions	None.

Example Usage:

To show SNTP on the switch:

```
local>show sntp
Command: show sntp

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

local>
```

33

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 arptable  
clear counters  
clear fdb  
clear log  
config 802.1p default_priority  
config 802.1p user_priority  
config 802.1x auth_mode  
config 802.1x auth_parameter ports  
config 802.1x capability ports  
config 802.1x init  
config 802.1x reauth  
config access_profile profile_id  
config account  
config aggport  
config aggport_actor_admin_state  
config aggport_partner_admin_state  
config aggregator
```

```
config arp_aging time
config arpentry
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 802.1x auth_mode
config 802.1x auth_parameter ports
config 802.1x capability ports
config 802.1x init
config 802.1x reauth
config access_profile profile_id
config account
config aggport
config aggport_actor_admin_state
config aggport_partner_admin_state
config aggregator
config arp_aging time
config arprentry
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>
```



TECHNICAL SPECIFICATIONS

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

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

Physical and Environmental	
AC input & External Redundant power Supply:	100 – 120; 200 - 240 VAC, 50 60 Hz (internal universal power supply)
Power Consumption:	30 watts maximum
DC fans:	2 built-in 40 x 40 x 10 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

<i>NO.</i>	<i>Message</i>	<i>Remark</i>
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!"	

<i>Variable Name</i>	<i>Maximum Length</i>	<i>Type</i>
<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](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, Allee 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 4 th 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?



TO:

Three vertical lines for an address.

D-Link®