



DES-3350SR

48 10/100Mbps plus 2 Gigabit Ports

Layer 3 Stackable Switch

Command Line Interface Reference Manual

Release 3

Information in this document is subject to change without notice.

© 2005 D-Link Computer Corporation. All rights reserved.

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

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

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

March 2005 P/N 651SR3350035

Table of Contents

Introduction.....	1
Using the Console CLI.....	4
Command Syntax	9
Basic Switch Commands.....	12
Switch Port Commands	24
Port Security Commands.....	27
Network Management (SNMP) Commands	30
Switch Utility Commands	54
Network Monitoring Commands.....	58
Spanning Tree Commands	63
Forwarding Database Commands.....	71
Broadcast Storm Control Commands.....	79
QoS Commands	82
Port Mirroring Commands	92
VLAN Commands.....	96
Link Aggregation Commands	103
IP-MAC Binding.....	110
Basic IP Commands	115
IGMP Commands.....	120
IGMP Snooping Commands	123
802.1X Commands.....	134
Access Control List (ACL) Commands.....	148
Traffic Segmentation Commands.....	157
Time and SNTP Commands.....	160
ARP Commands.....	165
Routing Table Commands.....	170

Route Redistribution Commands	174
BOOTP Relay Commands	181
DNS Relay Commands	185
RIP Commands	190
DVMRP Commands	194
PIM Commands	200
IP Multicasting Commands	205
MD5 Configuration Commands	207
OSPF Configuration Commands	210
Command History List.....	234
Technical Specifications	237

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.

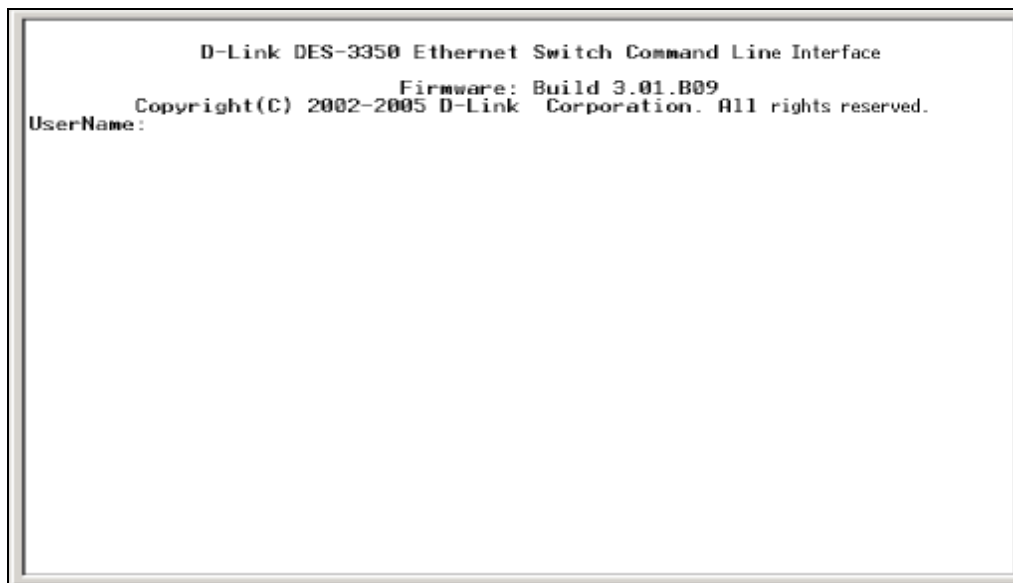
Accessing the Switch via the Serial Port

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.



```
D-Link DES-3350 Ethernet Switch Command Line Interface
Firmware: Build 3.01.B09
Copyright(C) 2002-2005 D-Link Corporation. All rights reserved.
UserName:
```

Figure 1-1. Initial CLI screen

There is no initial username or password. Just press the **Enter** key twice to display the CLI input cursor – **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 on the initial boot console screen – shown below.



```
Boot Procedure 1.00.002
-----
Power On Self Test ..... 100 %
MAC Address   : 00-01-02-03-04-00
H/W Version   : 0A1
Please wait, loading Runtime image ..... 100 %
```

Figure 1-2. Boot Screen

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

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

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

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

```
local>config ipif System ipaddress 10.58.44.221/8
Command: config ipif System ipaddress 10.58.44.221/8
Success.
local>
```

Figure 1-3. Assigning an IP Address

In the above example, the switch was assigned an IP address of 10.53.13.144/8 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.

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.



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

Connecting to the Switch

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

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

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

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

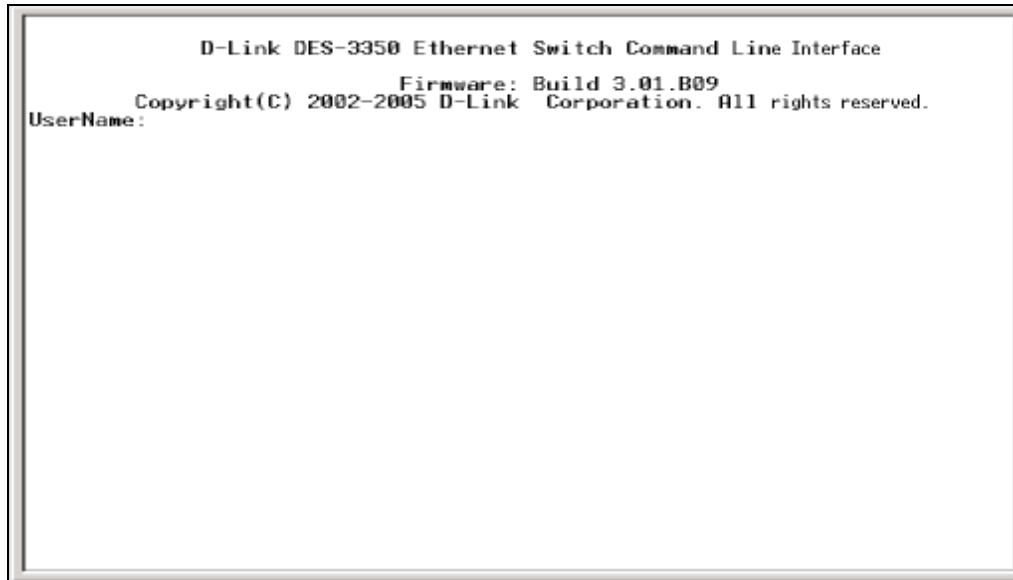


Figure 2-1. Initial Console Screen

Commands are entered at the command prompt, **local>** There are a number of helpful features included in the CLI. Entering the **?** command will display a list of all of the top-level commands.

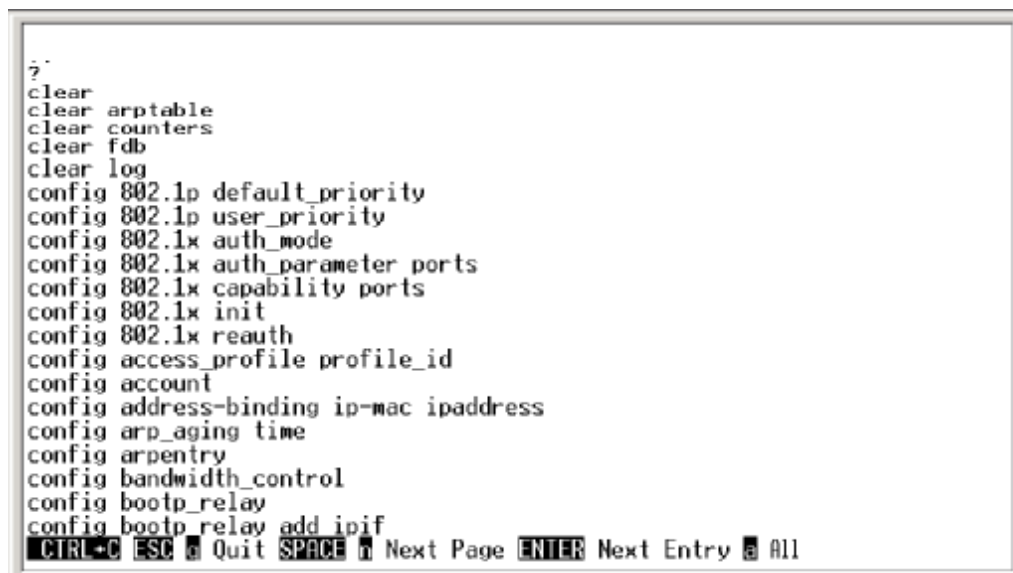


Figure 2-2. The ? Command

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

```
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.

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

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

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

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

Figure 2-5. The Next Available Commands Prompt

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

For example, if 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 address-binding arprentry bandwidth_
control bootp_relay command_history config dnsr dump error fdb garp igmp igmp_s
nooping ipfdb ipif ipmc iproute lacp_port link_aggregation log md5 mirror multic
ast_fdb ospf
  packet pim port_security ports power radius rip route router_ports sched
uling serial_port session snmp snmp stp switch time traffic traffic_segmentation
trusted_host utilization vlan
local>
```

Figure 2-6. Show Command

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

COMMAND SYNTAX

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



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

<angle brackets>	
Purpose	Encloses a variable or value that must be specified.
Syntax	create ipif <ipif_name> vlan <vlan_name 32> ipaddress <network_address>
Description	In the above syntax example, you must supply an IP interface name in the <ipif_name> space, a VLAN name in the <vlan_name 32> space, and the network address in the <network_address> space. Do not type the angle brackets.
Example Command	create ipif Engineering vlan Design ipaddress 10.24.22.5/255.0.0.0

[square brackets]	
Purpose	Encloses a required value or set of required arguments. One value or argument 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	show snmp [community detail]
Description	In the above syntax example, you must specify either community , or detail . Do not type the backslash.
Example Command	show snmp community

{braces}	
-----------------	--

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

Line Editing Key Usage	
Delete	Deletes the character under the cursor and then shifts the remaining characters in the line to the left.
Backspace	Deletes the character to the left of the cursor and shifts the remaining characters in the line to the left.
Left Arrow	Moves the cursor to the left.
Right Arrow	Moves the cursor to the right.
Up Arrow	Repeat the previously entered command. Each time the up arrow is pressed, the command previous to that displayed appears. This way it is possible to review the command history for the current session. Use the down arrow to progress sequentially forward through the command history list.
Down Arrow	The down arrow will display the next command in the command history entered in the current session. This displays each command sequentially as it was entered. Use the up arrow to review previous commands.
Tab	Shifts the cursor to the next field to the left.

Multiple Page Display Control Keys	
Space	Displays the next page.
CTRL+c	Stops the display of remaining pages when multiple pages are to be displayed.
ESC	Stops the display of remaining pages when multiple pages are to be displayed.
n	Displays the next page.
p	Displays the previous page.
q	Stops the display of remaining pages when multiple pages are to be displayed.
r	Refreshes the pages currently displayed.
a	Displays the remaining pages without pausing between pages.

Enter	Displays the next line or table entry.
-------	--

BASIC SWITCH COMMANDS

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

Command	Parameters
create account	[admin user] <username 15>
config account	<username>
show account	
delete account	<username>
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>
disable web	
save	
reboot	
reset	{{config system}}
login	
logout	

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

create account	
Purpose	Used to create user accounts
Syntax	create [admin user] <username 15>
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	<i>Admin <username></i> <i>User <username></i>

create account

Restrictions	Only Administrator-level users can issue this command.
	Usernames can be between 1 and 15 characters.
	Passwords can be between 0 and 15 characters.

Example usage:

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

```

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

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

Success.

local>

```

config account

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

Example usage:

To configure the user password of “dlink” account:

```

local>config account dlink
Command: config account dlink

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

local>

```

show account

Purpose	Used to display user accounts
Syntax	show account
Description	Displays all user accounts created on the switch. Up to 8 user accounts can exist on the switch at one time.
Parameters	None.
Restrictions	None.

Example usage:

To display the accounts that 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.

delete account

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 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       : 10.58.44.222 (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 3.01.B09
Hardware Version  : 0A1
System Up Time   : 0 days 00:49:27
Time             : Unknown
Time Source      : System Clock
System Name      :
System Location  :
System Contact   :
Spanning Tree    : Enabled
GVRP             : Disabled
IGMP Snooping    : Enabled
RIP              : Enabled
DVMRP           : Enabled
PIM-DM          : Enabled
OSPF            : Enabled
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.
Parameters	<p><i>baud_rate</i> [9600 19200 38400 115200] – The serial bit rate that will be used to communicate with the management host.</p> <p><i>auto logout</i> – This parameter will set the time that the switch will wait before logging out automatically, if left idle. The choices that accompany this parameter are:</p> <ul style="list-style-type: none"> § <i>never</i> – No time limit on the length of time the console can be open with no user input. § <i>2_minutes</i> – The console will log out the current user if there is no user input for 2 minutes. § <i>5_minutes</i> – The console will log out the current user if there is no user input for 5 minutes. § <i>10_minutes</i> – The console will log out the current user if there is no user input for 10 minutes. § <i>15_minutes</i> – The console will log out the current user if there is no user input for 15 minutes.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure baud rate:

```

local>config serial_port baud_rate 9600
Command: config serial_port baud_rate 9600

Success.

local>

```

enable clipaging

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

Example usage:

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

```

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 displays 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	<i><tcp_port_number 1-65535></i> - The TCP port number. TCP ports are numbered between 1 and 65535. The “well-known” TCP port for the Telnet protocol is 23.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable Telnet and configure port number:

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

Success.

local>
```

disable telnet

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

Example usage:

To disable the Telnet protocol on the switch:

```
local>disable telnet
Command: disable telnet

Success.

local>
```

enable web	
Purpose	Used to enable the HTTP-based management software on the switch.
Syntax	enable web <tcp_port_number 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	<i><tcp_port_number 1-65535></i> – The TCP port number. TCP ports are numbered between 1 and 65535. The “well-known” port for the Web-based management software is 80.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable HTTP and configure port number:

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

Success.

local>
```

disable web	
Purpose	Used to disable the HTTP-based management software on the switch.
Syntax	disable web
Description	This command disables the Web-based management software on the switch.
Parameters	None.

disable web

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

Example usage:

To disable HTTP:

```
local>disable web
Command: disable web

Success.

local>
```

save

Purpose	Used to save changes in the switch's configuration to non-volatile RAM.
Syntax	save
Description	This command is used to enter the current switch configuration into non-volatile RAM. The saved switch configuration will be loaded into the switch's memory each time the switch is restarted.
Parameters	Entering just the save command will save the switch configuration to NV-Ram
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 configurations to NV-RAM... Done

local>
```

reboot

Purpose	Used to restart the switch.
Syntax	reboot
Description	This command is used to restart the switch.

reboot

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><i>config</i> – If the keyword 'config' is specified, all of the factory default settings are restored on the switch including the IP address, user accounts, and the switch history log. The switch will not save or reboot.</p> <p><i>system</i> – If the keyword 'system' is specified all of the factory default settings are restored on the switch. The switch will save and reboot after the settings are changed to default. Rebooting will clear all entries in the Forwarding Data Base.</p> <p>If no parameter is specified, the switch's current IP address, user accounts, and the switch history log are not changed. All other parameters are restored to the factory default settings. The switch will not save or reboot.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
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
```

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 <desc 32> }
show ports	[all <portlist>] {description}

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



NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

config ports	
Purpose	Used to configure the Switch's Ethernet port settings.
Syntax	[<portlist> all] { speed [auto 10_half 10_full 100_half 100_full 1000_half 1000_full] state [enabled disabled] description <desc 32> }
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><portlist> – Specifies a port or range of ports to be configured.</p> <p><i>all</i> – Configure all ports on the switch.</p> <p><i>auto</i> – 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 [enable disable] – Enables or disables the specified range of ports.</p> <p>description <desc 32> - Enter an alphanumeric string of no more than 32 characters to describe a selected port interface.</p>
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 enable:

```
local>config ports 1-3 speed auto state enabled
Command: config ports 1-3 speed auto state enabled

Success.

local>
```

show ports

Purpose	Used to display the current configuration of a range of ports.
Syntax	show ports [all <portlist>] {description}
Description	This command is used to display the current configuration of a range of ports.
Parameters	<i>all</i> - specifies all the ports. <i><portlist></i> – Specifies a port or range of ports to be configured. <i>description</i> – Enter this parameter to view the description of the port previously set in the config ports command.
Restrictions	None.

Example usage:

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

```

local>Port Port  Settings  Connection
      State  Speed/Duplex 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      100M/Full
 6  Enabled  Auto      Link Down
 7  Enabled  Auto      Link Down
 8  Enabled  Auto      Link Down
 9  Enabled  Auto      Link Down
10  Enabled  Auto      Link Down
11  Enabled  Auto      Link Down
12  Enabled  Auto      Link Down
13  Enabled  Auto      Link Down
14  Enabled  Auto      Link Down
15  Enabled  Auto      100M/Full
16  Enabled  Auto      Link Down
17  Enabled  Auto      Link Down
18  Enabled  Auto      Link Down
19  Enabled  Auto      Link Down
20  Enabled  Auto      Link Down

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

```

Example usage:

To view port 1:1 with description

```

local> show ports 1-4 description
Command: show ports 1-4 description

Port Port  Settings  Connection
      State  Speed/Duplex Speed/Duplex
-----
 1  Enabled  Auto      Link Down
    Desc:
 2  Enabled  Auto      Link Down
    Desc:
 3  Enabled  Auto      Link Down
    Desc:
 4  Enabled  Auto      Link Down
    Desc:

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

```

PORT SECURITY COMMANDS

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

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

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



NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

config port_security ports	
Purpose	Used to configure port security settings.
Syntax	[<portlist> all] { admin_state [enabled disabled] max_learning_addr <max_lock_no 0-10> lock_address_mode [DeleteOnTimeout DeleteOnReset]}
Description	This command allows for the configuration of the port security feature. Only the ports listed in the <portlist> are effected.
Parameters	<p><portlist> – Specifies a port or range of ports to be configured.</p> <p>all – Configure port security for all ports on the switch.</p> <p>admin_state [enable disable] – Enables or disables port security for the listed ports.</p> <p>max_learning_addr <max_lock_no 0-10> - Use this to limit the number of MAC addresses dynamically listed in the FDB for the ports.</p> <p>lock_address_mode [DeleteOnTimeout DeleteOnReset] – Delete FDB dynamic entries for the ports on timeout of the FDB (see Forwarding Database Commands). Specify DeleteOnReset to delete all FDB entries, including static entries upon system reset or rebooting.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the port security:

```

local>config port_security ports 1-3 admin_state enabled
max_learning_addr 1 lock_address_mode DeleteOnTimeout

Command: config port_security ports 1-3 admin_state enabled
max_learning_addr 1lock_address_mode DeleteOnTimeout

Success.

local>

```

show port_security

Purpose	Used to display the current port security configuration.
Syntax	show port_security {ports <portlist>}
Description	This command is used to display port security information of the switch ports. The information displayed includes port security admin state, maximum number of learning address and lock mode.
Parameters	<portlist> – Specifies a port or range of ports to be viewed.
Restrictions	Only administrator-level can use this command.

Example usage:

To display the port security configuration:

```

local>show port_security ports
Command: show port_security ports

Port#  Admin State  Max. Learning Addr.  Lock Address Mode
----  -
15:1   Disabled        1                     DeleteOnReset
15:2   Disabled        1                     DeleteOnReset
15:3   Disabled        1                     DeleteOnReset
15:4   Disabled        1                     DeleteOnReset
15:5   Disabled        1                     DeleteOnReset
15:6   Disabled        1                     DeleteOnReset
15:7   Enabled         10                    DeleteOnReset
15:8   Disabled        1                     DeleteOnReset
15:9   Disabled        1                     DeleteOnReset
15:10  Disabled        1                     DeleteOnReset
15:11  Disabled        1                     DeleteOnReset
15:12  Disabled        1                     DeleteOnReset

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

```


NETWORK MANAGEMENT (SNMP) COMMANDS

The DES-3350SR supports the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. You can specify which version of the SNMP you want to use to monitor and control the switch. The three versions of SNMP vary in the level of security provided between the management station and the network device. The following table lists the security features of the three SNMP versions:

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

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

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

Command	Parameters
create snmp user	<username 32> <groupname 32> {encrypted [by_password auth [md5 <auth_password 8-16> sha <auth_password 8-20 >] priv [none des <priv_password 8-16>] by_key auth [md5 <auth_key 32-32> sha <auth_key 40-40>] priv [none des <priv_key 32-32>]}]}
delete snmp user	<username 32>
show snmp user	
create snmp view	<view_name 32> <oid> view_type [included excluded]
delete snmp view	<view_name 32> [all oid]
show snmp view	{<view_name 32>}
create snmp community	<community_string 32> view <view_name 32> [read_only read_write]
delete snmp community	<community_string 32>
show snmp community	{<community_string 32>}
config snmp engineID	<snmp_engineID>
show snmp engineID	

Command	Parameters
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>
show snmp groups	
create snmp host	<ipaddr> {v1 v2c v3 [noauth_nopriv auth_nopriv auth_priv]} <auth_string 32>
delete snmp host	<ipaddr>
show snmp host	{<ipaddr>}
create trusted_host	<ipaddr>
delete trusted_host	<ipaddr>
show trusted_host	{<ipaddr>}
enable snmp traps	
enable snmp authenticate traps	
disable snmp traps	
disable snmp authenticate traps	
config snmp system_contact	<sw_contact>
config snmp system_location	<sw_location>
config snmp system_name	<sw_name>
enable rmon	
disable rmon	

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

create snmp user

Purpose	Used to create a new SNMP user and adds the user to an SNMP group that is also created by this command.
Syntax	create snmp user <username 32> <groupname 32> {encrypted [by_password auth [md5 <auth_password 8-16> sha <auth_password 8-20>] priv [none des <priv_password 8-16>] by_key auth [md5 <auth_key 32-32> sha <auth_key 40-40>] priv [none des <priv_key 32-32>]}]}

create snmp user

Description	<p>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. SNMP ensures:</p> <p>Message integrity – Ensures that packets have not been tampered with during transit.</p> <p>Authentication – Determines if an SNMP message is from a valid source.</p> <p>Encryption – Scrambles the contents of messages to prevent it being viewed by an unauthorized source.</p>
Parameters	<p><i><username 32></i> – An alphanumeric name of up to 32 characters that will identify the new SNMP user.</p> <p><i><groupname 32></i> – An alphanumeric name of up to 32 characters that will identify the SNMP group the new SNMP user will be associated with.</p> <p><i>by_password</i> – Requires the SNMP user to enter a password for authentication and privacy. The password is defined by specifying the <i>auth_password</i> below. This method is recommended.</p> <p><i>by_key</i> - Requires the SNMP user to enter a encryption key for authentication and privacy. The key is defined by specifying the <i>priv_password</i> below. This method is not recommended.</p> <p><i>encrypted</i> – Specifies that the password will be in an encrypted format.</p> <p><i>auth [md5 sha]</i> – Initiate an authentication-level setting session.</p> <p> § <i>md5</i> – Specifies that the HMAC-MD5-96 authentication level will be used.</p> <p> § <i>sha</i> – Specifies that the HMAC-SHA-96 authentication level will be used.</p> <p><i><auth_password 8-20></i> – An alphanumeric string of between 8 and 20 characters that will be used to authorize the agent to receive packets for the host.</p> <p><i>des <priv_password 8-16></i> – 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.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create an SNMP user on the switch:

```

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

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

Success.

local>

```

delete snmp user

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

Example usage:

To delete a previously entered SNMP user on the switch:

```

local>delete snmp user dlink

Command: delete snmp user dlink

Success.

local>

```

show snmp user

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

Example usage:

To display the SNMP users currently configured on the switch:

```

local>show snmp user
Command: show snmp user

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

Total Entries: 1

local>

```

create snmp view

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

Example usage:

To delete a previously configured SNMP view from the switch:

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

Success.

local>
```

show snmp view

Purpose	Used to display an SNMP view previously created on the switch.
Syntax	show snmp view {<view_name 32>}
Description	The show snmp view command displays an SNMP view previously created on the switch.
Parameters	<i><view_name 32></i> – An alphanumeric string of up to 32 characters that identifies the SNMP view that will be displayed.
Restrictions	Only administrator-level users can use this command.

Example usage:

To display SNMP view configuration:

```

local>show snmp view
Command: show snmp view

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

Total Entries: 11

local>

```

create snmp community

Purpose	<p>Used to create an SNMP community string to define the relationship between the SNMP manager and an agent. The community string acts like a password to permit access to the agent on the switch. One or more of the following characteristics can be associated with the community string:</p> <ul style="list-style-type: none"> An Access List of IP addresses of SNMP managers that are permitted to use the community string to gain access to the switch's SNMP agent. An MIB view that defines the subset of all MIB objects that will be accessible to the SNMP community. Read write or read-only level permission for the MIB objects accessible to the SNMP community.
Syntax	<pre>create snmp community <community_string 32> view <view_name 32> [read_only read_write]</pre>
Description	<p>The create snmp community command is used to create an SNMP community string and to assign access-limiting characteristics to this community string.</p>

create snmp community

Parameters	<p><i><community_string 32></i> – An alphanumeric string of up to 32 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the switch's SNMP agent.</p> <p><i><view_name 32></i> – An alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the switch.</p> <p><i>read_only</i> – Specifies that SNMP community members using the community string created with this command can only read the contents of the MIBs on the switch.</p> <p><i>read_write</i> – Specifies that SNMP community members using the community string created with this command can read from and write to the contents of the MIBs on the switch.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create the SNMP community string “dlink:”

```

local>create snmp community dlink view ReadView read_write
Command: create snmp community dlink view ReadView read_write

Success.

local>

```

delete snmp community

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

Example usage:

To delete the SNMP community string “dlink:”

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

Success.

local>
```

show snmp community

Purpose	Used to display SNMP community strings configured on the switch.
Syntax	show snmp community {<community_string 32>}
Description	The show snmp community command is used to display SNMP community strings that are configured on the switch.
Parameters	<i><community_string 32></i> – An alphanumeric string of up to 32 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the switch’s SNMP agent.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To display the currently entered SNMP community strings:

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

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

Total Entries: 3

local>
```

config snmp engineID

config snmp engineID

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

Example usage:

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

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

Success.

local>
```

show snmp engineID

Purpose	Used to display the identification of the SNMP engine on the switch.
Syntax	show snmp engineID
Description	The show snmp engineID command displays the identification of the SNMP engine on the switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

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

SNMP Engine ID : 0035636666

local>
```

create snmp group

Purpose	Used to create a new SNMP group, or a table that maps SNMP users to SNMP views.
Syntax	create snmp group <groupname 32> [v1 v2c v3 [noauth_nopriv auth_nopriv auth_priv]] {read_view <view_name 32> write_view <view_name 32> notify_view <view_name 32>}
Description	The create snmp group command creates a new SNMP group, or a table that maps SNMP users to SNMP views.

create snmp group

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

Example usage:

To create an SNMP group named “sg1:”

```
local>create snmp group sg1 v3 noauth_nopriv read_view v1
write_view v1 notify_view v1
Command: create snmp group sg1 v3 noauth_nopriv read_view v1
write_view v1 notify_view v1

Success.

local>
```

delete snmp group

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

Example usage:

To delete the SNMP group named “sg1”.

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

Success.

local>
```

show snmp groups

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

show snmp groups

Restrictions Only administrator-level can use this command.

Example usage:

To display the currently configured SNMP groups on the switch:

```
local>show snmp groups
Command: show snmp groups

Vacm Access Table Settings

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

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

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

Total Entries: 10

local>
```

create snmp host

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

Example usage:

To create an SNMP host to receive SNMP messages:

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

Success.

local>
```

delete snmp host

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

Example usage:

To delete an SNMP host entry:

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

Success.

local>
```

show snmp host

Purpose	Used to display the recipient of SNMP traps generated by the switch's SNMP agent.
Syntax	show snmp host {<ipaddr>}
Description	The show snmp host command is used to display the IP addresses and configuration information of remote SNMP managers that are designated as recipients of SNMP traps that are generated by the switch's SNMP agent.
Parameters	<ipaddr> – The IP address of a remote SNMP manager that will receive SNMP traps generated by the switch's SNMP agent.

show snmp host

Restrictions	Only administrator-level can use this command.
--------------	--

Example usage:

To display the currently configured SNMP hosts on the switch:

```

local>show snmp host
Command: show snmp host

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

Total Entries: 2

local>

```

create trusted_host

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

Example usage:

To create the trusted host:

```

local>create trusted_host 10.48.74.121
Command: create trusted_host 10.48.74.121

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 {<ipaddr>}
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	Only administrator-level can use this command.

Example Usage:

To display the list of trust hosts:

```

local>show trusted_host
Command: show trusted_host

Management Stations

IP Address
-----
10.53.13.94

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.

delete trusted_host

Parameters	<ipaddr> – The IP address of the trusted host.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete a trusted host with an IP address 10.48.74.121:

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

Success.

local>
```

enable snmp traps

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

Example usage:

To enable SNMP trap support on the switch:

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

Success.

local>
```

enable snmp authenticate_traps

Purpose	Used to enable SNMP authentication trap support.
Syntax	enable snmp authenticate_traps
Description	This command is used to enable SNMP authentication trap support on the Switch.

enable snmp authenticate_traps

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 traps

Purpose	Used to disable SNMP trap support on the switch.
Syntax	disable 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>
```

disable snmp authenticate_traps

Purpose	Used to disable SNMP authentication trap support.
Syntax	disable snmp authenticate_traps

disable snmp authenticate_traps

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

Example Usage:

To disable the SNMP authentication trap support:

```
local>disable snmp authenticate_traps
Command: disable snmp authenticate_traps

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	The config snmp system_contact command is used to enter the name and/or other information to identify a contact person who is responsible for the switch. A maximum of 255 character can be used.
Parameters	<sw_contact> - A maximum of 255 characters is allowed. A NULL string is accepted if there is no contact.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
local>config snmp system_contact MIS Department II
Command: config snmp system_contact MIS Department II

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	The config snmp system_location 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 maximum of 255 characters is allowed. A NULL string is accepted if there is no location desired.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
local>config snmp system_location HQ 5F
Command: config snmp system_location HQ 5F

Success.

local>
```

config snmp system_name

Purpose	Used to configure the name for the switch.
Syntax	config snmp system_name <sw_name>
Description	The config snmp system_name command configures the name of the switch.
Parameters	<sw_name> - A maximum of 255 characters is allowed. A NULL string is accepted if no name is desired.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
local>config snmp system_name DES-3350SR Stackable Switch
Command: config snmp system_name DES-3350SR Stackable Switch

Success.

local>
```

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

Example Usage:

To enable RMON:

```
local>enable rmon
Command: enable rmon

Success.

local>
```

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

Example Usage:

To disable RMON:


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

SWITCH UTILITY COMMANDS

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

Command	Parameters
download	[firmware <ipaddr> <path_filename 127> configuration <ipaddr> <path_filename 127> {increment}]
upload	[configuration log] <ipaddr> <path_filename 127>
ping	<ipaddr> {times <value 1-255>} {timeout <sec 1-99>}
tracert	<ipaddr> {ttl <value 1-60> port <value 30000-64900> timeout <sec 1-65535> probe <value <1-9>

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	[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><i>firmware</i> – Download and install new firmware on the switch from a TFTP server.</p> <p><i>configuration</i> - Download a switch configuration file from a TFTP server.</p> <p><i><ipaddr></i> – The IP address of the TFTP server.</p> <p><i><path_filename></i> – The DOS path and filename of the firmware or switch configuration file on a TFTP server. For example, C:\3226S.had.</p> <p><i>increment</i> – 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-level users can issue this command.

Example usage:

To download a configuration file:

```

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	[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><i>configuration</i> – Specifies that the switch's current settings will be uploaded to the TFTP server.</p> <p><i>log</i> – Specifies that the switch's current log will be uploaded to the TFTP server.</p> <p><i><ipaddr></i> – The IP address of the TFTP server. The TFTP server must be on the same IP subnet as the switch.</p> <p><i><path_filename 127></i> – Specifies the location of the switch configuration file on the TFTP server. This file will be replaced by the uploaded file from the switch.</p>
Restrictions	The TFTP server must be on the same IP subnet as the switch. Only administrator-level users can issue this command.

Example usage:

To upload a configuration file:

```

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>

```

ping

Purpose	Used to test the connectivity between network devices.
---------	--

ping

Syntax	ping <ipaddr> {times <value 1-255>} {timeout <sec 1-99>}
Description	The ping command sends Internet Control Message Protocol (ICMP) echo messages to a remote IP address. The remote IP address will then “echo” or return the message. This is used to confirm connectivity between the switch and the remote device.
Parameters	<p><i><ipaddr></i> - Specifies the IP address of the host.</p> <p><i>times <value 1-255></i> - The number of individual ICMP echo messages to be sent. The maximum value is 255. The default is 0.</p> <p><i>timeout <sec 1-99></i> - Defines the time-out period while waiting for a response from the remote device. A value of 1 to 99 seconds can be specified. The default is 1 second.</p> <p>Pinging an IP address without the <i>times</i> parameter will ping the target device an infinite amount of times.</p>
Restrictions	None.

Example usage:

To ping the IP address 10.48.74.121 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>

```

tracert

Purpose	Used to trace the routed path between the switch and a destination endstation.
Syntax	<ipaddr> {ttl <value 1-60> port <value 30000-64900> timeout <sec 1-65535> probe <value <1-9>
Description	The tracert command allows you to trace a route between the switch and a give host on the network.

traceroute

Parameters	<p><i><ipaddr></i> - Specifies the IP address of the host.</p> <p><i>tll <value 1-60></i> - 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.</p> <p><i>port <value 30000-64900></i> The port number. Must be above 1024. The value range is from 30000 to 64900 .</p> <p><i>timeout <sec 1-65535></i>- Defines the time-out period while waiting for a response from the remote device. The user may choose an entry between 1 and 65535 seconds.</p> <p><i>probe <value 1-9></i> - The probe value is the number of times the switch will send probe packets to the next hop on the intended traceroute path. The default is 1.</p>
Restrictions	None.

Example usage:

To 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 <10ms 10.254.254.251
 2 <10ms 10.55.25.35
 3 <10ms 10.22.35.1

local>
```

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}
clear counters	ports <portlist>
clear log	
show log	index <value>

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



NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

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

Example usage:

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

```
local>show packet port 2:7
```

```
Port number : 2:7
```

Frame Size	Frame Counts	Frames/sec	Frame Type	Total	Total/sec
-----	-----	-----	-----	-----	-----
64	3275	10	RX Bytes	408973	1657
65-127	755	10	RX Frames	4395	19
128-255	316	1			
256-511	145	0	TX Bytes	7918	178
512-1023	15	0	TX Frames	111	2
1024-1518	0	0			
Unicast RX	152	1			
Multicast RX	557	2			
Broadcast RX	3686	16			

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

show error ports

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

Example usage:

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

```
local>show errors port 1:3
```

```
Port number 1:3
```

Error Type	RX Frames	Error Type	TX Frames
CRC Error	19	Excessive Deferral	0
Undersize	0	CRC Error	0
Oversize	0	Late Collision	0
Fragment	0	Excessive Collision	0
Jabber	11	Single Collision	0
Drop Pkts	20837	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]
Description	This command will display the real-time port and cpu utilization statistics for the switch.
Parameters	<i>cpu</i> – Entering this parameter will display the current cpu utilization of the switch, as a percentage.
Restrictions	None.

To display the current cpu utilization:

```
local>show utilization cpu
```

```
Command: show utilization cpu
```

```
CPU utilization :
```

```
-----
```

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

```
local>
```

clear counters

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 port or range of ports to be configured.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To clear the counters:

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

Success.

local>
```

clear log

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

Example usage:

To clear the log information:

```
local>clear log
Command: clear log

Success.

local>
```

show log

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	<i>index <value></i> – Enter a value that corresponds to an entry made in the log. Multiple entries may be made in the form of x-x where x is the number of an entry in the log. The smallest number (and therefore the earlier entry) will be first.
Restrictions	None.

Example usage:

To display the switch history log:

```

local>show log index 1-4
Command: show log index 1-4

Index  Time      Log Text
-----  -
4      01:54:53  Port 1:13 link up, 100Mbps FULL duplex
3      01:54:53  Spanning Tree Protocol is enabled
2      01:54:53  Unit 1, System started up
1      06:06:09  Spanning Tree Protocol is disabled

local>

```

SPANNING TREE COMMANDS

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

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

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



NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

config stp

Purpose	Used to setup STP and RSTP on the switch.
Syntax	config stp {maxage <value 6-40> hellotime <value 1-10> forwarddelay <value 4-30> priority <value 0-61440> version [rstp stp] txholdcount <value 1-10> fbpdu [enable disable]}
Description	This command is used to setup the Spanning Tree Protocol (STP) for the entire switch.

config stp

Parameters	<p><i>maxage</i> <value 6-40> – The maximum amount of time (in seconds) that the switch will wait to receive a BPDU packet before reconfiguring STP. The user may choose a time between 6 and 40 seconds. The default is 20 seconds.</p> <p><i>hellotime</i> <value 1-10> – The time interval between transmission of configuration messages by the root device. The user may choose a time between 1 and 10 seconds. The default is 2 seconds.</p> <p><i>forwarddelay</i> <value 4-30> – The maximum amount of time (in seconds) that the root device will wait before changing states. The user may choose a time between 4 and 30 seconds. The default is 15 seconds.</p> <p><i>priority</i> <value 0-61440> – A numerical value between 0 and 61440 that is used in determining the root device, root port, and designated port. The device with the highest priority becomes the root device. The lower the numerical value, the higher the priority. The default is 32,768.</p> <p><i>version</i> [<i>rstp</i> <i>stp</i>] - Select the Spanning Tree Protocol version used for the switch.</p> <ul style="list-style-type: none"> • <i>stp</i> – Select this parameter for IEEE 802.1d STP and for IEEE 802.1w STP compatibility mode. • <i>rstp</i> - Select this parameter for IEEE 802.1w Rapid STP mode. <p><i>fbpdu</i> [<i>enable</i> <i>disable</i>] – Allows the forwarding of STP BPDU packets from other network devices when STP is disabled on the switch. The default is enabled.</p> <p><i>txholdcount</i> <1-10> - The maximum number of Hello packets transmitted per interval. Default value = 3.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure STP with maxage 18 and hellotime 4:

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

Success.

local>
```

config stp ports

config stp ports

Purpose	Used to setup STP on the port level.
Syntax	config stp ports <portlist> {cost [auto <value 1-200000000>] priority <value 0-240> migrate [yes no] edge [true false] p2p [true false auto] state [enable disable]}
Description	This command is used to create and configure STP for a group of ports.

config stp ports

Parameters	<p><i>cost</i> – This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set in the following two ways:</p> <p>§ <i>auto</i> – Setting this parameter for the cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. Default port cost: 100Mbps port = 200000. Gigabit port = 20000.</p> <p>§ <i><value 1-200000000></i> - Define a value between 1 and 200000000 to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets.</p> <p>Default port cost: 100Mbps port = 200000 Gigabit port = 20000</p> <p><i>priority <value 0-240></i> – Port Priority can be from 0 to 240. The lower the number, the greater the probability the port will be chosen as the Root Port. Default = 128.</p> <p><i><portlist></i> – Specifies a port or range of ports to be configured.</p> <p><i>migrate [yes no]</i> – <i>yes</i> 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 (<i>yes</i>) on ports connected to network stations or segments that will be upgraded to 802.1w RSTP on all or some portion of the segment.</p> <p><i>edge [true false]</i> – <i>true</i> 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. <i>false</i> indicates that the port does not have edge port status.</p> <p><i>p2p [true false auto]</i> – <i>true</i> indicates a point-to-point (P2P) shared link. P2P ports are similar to edge ports however they are restricted in that a P2P port must operate in full-duplex. Like edge ports, P2P ports transition to a forwarding state rapidly thus benefiting from RSTP. A <i>p2p</i> value of <i>false</i> indicates that the port cannot have <i>p2p</i> status. <i>auto</i> allows the port to have <i>p2p</i> status whenever possible and operate as if the <i>p2p</i> status were <i>true</i>. If the port cannot maintain this status (for example if the port is forced to half-duplex operation) the <i>p2p</i> status changes to operate as if the <i>p2p</i> value were <i>false</i>.</p> <p><i>state [enable disable]</i> – Allows STP to be enabled or disabled for the ports specified in the port list. The default is disabled.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure STP with path cost set at auto, priority 16, and state enabled for ports 1-5 of module 1.

```
local> config stp ports 1-4 cost auto state enabled
Command: config stp ports 1-4 cost auto state enabled

Success.

local>
```

enable stp

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

Example usage:

To enable STP, globally, on the switch:

```
local>enable stp
Command: enable stp

Success.

local>
```

disable stp

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

Example usage:

To disable STP on the switch:

```
local>disable stp
Command: disable stp

Success.

local>
```

show stp

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

Example usage:

To display the status of STP on the switch:

Status 1: STP enabled with STP compatible version


```
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: 00-01-02-03-04-00
Root Priority    : 32768
Cost to Root    : 0
Root Port       : None
Last Topology Change : 140sec
Topology Changes Count: 66
Protocol Specification : 3
Max Age         : 20
Hello Time      : 2
Forward Delay   : 15
Hold Time       : 3
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

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

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 port or range of ports to be configured.
Restrictions	None

Example usage:

To display STP state of ports 1-4:

```
local> local>show stp ports 1-4
Command: show stp ports 1-4
```

Port	Designated	Bridge	State	Cost	Pri	Edge	P2P	Status	Role
-----			---	-----	---	---	---	-----	-----
1	N/A		Yes	*200000	0	No	Yes	Disabled	Disabled
2	N/A		Yes	*200000	0	No	Yes	Disabled	Disabled
3	N/A		Yes	*200000	0	No	Yes	Disabled	Disabled
4	N/A		Yes	*200000	0	No	Yes	Disabled	Disabled

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

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>
config fdb aging_time	<sec 10-1000000>
delete fdb	<vlan_name 32> <macaddr>
clear fdb	[vlan <vlan_name 32> port <port> all]
show multicast_fdb	{vlan <vlan_name 32> mac_address <macaddr>}
show fdb	{port <port> vlan <vlan_name 32> mac_address <macaddr> static aging_time}
show ipfdb	<ipaddr>

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



NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

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

Example usage:

To create a unicast MAC FDB entry:

```
local>create fdb default 00-00-00-00-01-02 port 2:5
Command: create fdb default 00-00-00-00-01-02 port 2:5

Success.

local>
```

create multicast_fdb

Purpose	Used to create a static entry to the multicast MAC address forwarding table (database)
Syntax	create multicast_fdb <vlan_name 32> <macaddr>
Description	This command will make an entry into the switch's multicast MAC address forwarding database.
Parameters	<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 create multicast MAC forwarding:

```
local>create multicast_fdb default 01-00-00-00-00-01
Command: create multicast_fdb default 01-00-00-00-00-01

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.

config multicast_fdb

Parameters	<p><i><vlan_name 32></i> – The name of the VLAN on which the MAC address resides.</p> <p><i><macaddr></i> – The MAC address that will be added to the multicast forwarding table.</p> <p><i>[add delete]</i> – Add will add ports to the forwarding table. Delete will remove ports from the multicast forwarding table.</p> <p>§ <i><portlist></i> – Specifies a port or range of ports to be configured.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To add multicast MAC forwarding:

```

local>config multicast_fdb default 01-00-00-00-00-01 add 1:1-1:5
Command: config multicast_fdb default 01-00-00-00-00-01 add 1:1-1:5

Success.

local>

```

config fdb aging_time

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

Example usage:

To set the fdb aging time:

```
local>config fdb aging_time 300
Command: config fdb aging_time 300

Success.

local>
```

delete fdb

Purpose	Used to delete an entry to the switch's forwarding database.
Syntax	delete fdb <vlan_name 32> <macaddr>
Description	This command is used to delete a previous entry to the switch's MAC address forwarding database.
Parameters	<p><vlan_name 32> – The name of the VLAN on which the MAC address resides.</p> <p><macaddr> – The MAC address that will be deleted from 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>
```

Example usage:

To delete a multicast fdb entry:

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

Success.

local>
```

clear fdb

Purpose	Used to clear the switch's forwarding database of all dynamically learned MAC addresses.
Syntax	clear fdb [vlan <vlan_name 32> port <port> all]
Description	This command is used to clear dynamically learned entries to the switch's forwarding database.
Parameters	<p><i>vlan <vlan_name 32></i> – The name of the VLAN on which the MAC address resides.</p> <p><i>port <port></i> – The port number corresponding to the MAC destination address. The switch will always forward traffic to the specified device through this port.</p> <p><i>all</i> – 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><i><vlan_name 32></i> – The name of the VLAN on which the MAC address resides.</p> <p><i><macaddr></i> – The MAC address that is present in the forwarding database 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   : 1:1-1:5,1:12
Mode           : Static

Total Entries : 1

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	<p><i>port <port></i> – The port number corresponding to the MAC destination address. The switch will always forward traffic to the specified device through this port.</p> <p><i><vlan_name 32></i> – The name of the VLAN on which the MAC address resides.</p> <p><i><macaddr></i> – The MAC address that is present in the forwarding database table.</p> <p><i>static</i> – Displays the static MAC address entries.</p> <p><i>aging_time</i> – Displays the aging time for the MAC address forwarding database.</p>
Restrictions	None.

Example usage:

To display unicast MAC address table:


```

local>show fdb
Command: show fdb

Unicast MAC Address Aging Time = 300

VID  VLAN Name      MAC Address          Port    Type
---  -
1    default         00-00-39-34-66-9A   10      Dynamic
1    default         00-00-51-43-70-00   10      Dynamic
1    default         00-00-5E-00-01-01   10      Dynamic
1    default         00-00-74-60-72-2D   10      Dynamic
1    default         00-00-81-05-00-80   10      Dynamic
1    default         00-00-81-05-02-00   10      Dynamic
1    default         00-00-81-48-70-01   10      Dynamic
1    default         00-00-E2-4F-57-03   10      Dynamic
1    default         00-00-E2-61-53-18   10      Dynamic
1    default         00-00-E2-6B-BC-F6   10      Dynamic
1    default         00-00-E2-7F-6B-53   10      Dynamic
1    default         00-00-E2-82-7D-90   10      Dynamic
1    default         00-00-F8-7C-1C-29   10      Dynamic
1    default         00-01-02-03-04-00   CPU     Self
1    default         00-01-02-03-04-05   10      Dynamic
1    default         00-01-30-10-2C-C7   10      Dynamic
1    default         00-01-30-FA-5F-00   10      Dynamic
1    default         00-02-3F-63-DD-68   10      Dynamic
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All

```

show ipfdb

Purpose	Used to display the current IP address forwarding database table.
Syntax	show ipfdb <ipaddr>
Description	This command will display the current contents of the switch's IP forwarding database.
Parameters	<i>ip_address <ipaddr></i> - Use this parameter to view the table by an IP address entered here.
Restrictions	None.

Example usage:

To view the IP forwarding database table:

```
local>show ipfdb
```

```
Command: show ipfdb
```

```
Interface  IP Address  Port  Learned
```

```
-----  
System    10.0.0.178   15   Dynamic  
System    10.0.0.183   15   Dynamic  
System    10.0.25.1    15   Dynamic  
System    10.0.34.1    15   Dynamic  
System    10.0.46.1    15   Dynamic  
System    10.0.58.4    15   Dynamic  
System    10.1.1.1     15   Dynamic  
System    10.1.1.101   15   Dynamic  
System    10.1.1.151   15   Dynamic  
System    10.1.1.152   15   Dynamic  
System    10.1.1.157   15   Dynamic  
System    10.1.1.161   15   Dynamic  
System    10.1.1.164   15   Dynamic  
System    10.1.1.173   15   Dynamic  
System    10.1.1.191   15   Dynamic  
System    10.1.1.254   15   Dynamic  
System    10.1.49.1    15   Dynamic  
System    10.1.49.5    15   Dynamic  
System    10.1.49.9    15   Dynamic  
System    10.1.49.15   15   Dynamic
```

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

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 [enable disable] multicast [enable disable] dlf [enable disable] threshold <value 0-255> }
show traffic control	{group_list <storm_grouplist>}

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



NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

config traffic control

Purpose	Used to configure broadcast/multicast traffic control.
Syntax	config traffic control [<storm_grouplist> all] { broadcast [enable disable] multicast [enable disable] dlf [enable disable] threshold <value 0-255>}
Description	This command is used to configure broadcast storm control.
Parameters	<p><i><storm_grouplist></i> – Used to specify a broadcast storm control group. This is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the 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, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.</p> <p><i>all</i> – Specifies all broadcast storm control groups on the switch.</p> <p><i>broadcast</i> [enable disable] – Enables or disables broadcast storm control.</p> <p><i>multicast</i> [enable disable] – Enables or disables multicast storm control.</p> <p><i>dlf</i> [enable disable] – Enables or disables dlf traffic control.</p> <p><i>threshold</i> <value 0-255> – The upper threshold at which the specified traffic control is switched on. The <value> is the number of broadcast / multicast / dlf packets, in Kbps, received by the switch that will trigger the storm traffic control measures.</p>

config traffic control

Restrictions Only administrator-level users can issue this command.

Example usage:

To configure traffic control and enable broadcast storm control system wide:

```
local>config traffic control all broadcast enable
Command: config traffic control all broadcast enable

Success.

local>
```

show traffic control

Purpose	Used to display current traffic control settings.
Syntax	show traffic control {group_list <storm_grouplist>}
Description	This command displays the current storm traffic control configuration on the switch.
Parameters	<i>group_list <storm_grouplist></i> – Used to specify a broadcast storm control group. This is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the 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, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.
Restrictions	None.

Example usage:

To display traffic control setting:

```
local>show traffic control
Command: show traffic control
Traffic Control
                Broadcast Multicast Destination
Group [ports] Threshold Storm    Storm    Lookup Fail
-----
1 [ 1 - 8 ]    128     Disabled Disabled Disabled
2 [ 9 - 16]    128     Disabled Disabled Disabled
3 [17 - 24]    128     Disabled Disabled Disabled
4 [25 - 32]    128     Disabled Disabled Disabled
5 [33 - 40]    128     Disabled Disabled Disabled
6 [41 - 48]    128     Disabled Disabled Disabled
7 [ 49 ]       128     Disabled Disabled Disabled
8 [ 50 ]       128     Disabled Disabled Disabled

Total Entries: 8

local>
```

QoS COMMANDS

The DES-3350SR switch supports 802.1p priority queuing. The Switch has five hardware priority queues, one of which is internal and not configurable. These hardware priority queues are numbered from 7 (Class 7) — the highest hardware priority queue — to 0 (Class 0) — the lowest hardware priority queue. The eight priority tags specified in IEEE 802.1p (p0 to p7) are mapped to the switch's hardware priority queues as follows:

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

For strict priority-based scheduling, any packets residing in the higher priority queues are transmitted first. Multiple strict priority queues empty based on their priority tags. Only when these queues are empty, are packets of lower priority transmitted.

For round-robin queuing, the number of packets sent from each priority queue depends upon the assigned weight. For a configuration of 8 CoS queues, A~H with their respective weight value: 8~1, the packets are sent in the following sequence: A1, B1, C1, D1, E1, F1, G1, H1, A2, B2, C2, D2, E2, F2, G2, A3, B3, C3, D3, E3, F3, A4, B4, C4, D4, E4, A5, B5, C5, D5, A6, B6, C6, A7, B7, A8, A1, B1, C1, D1, E1, F1, G1, H1.

For round-robin queuing, if each CoS queue has the same weight value, then each CoS queue has an equal opportunity to send packets just like round-robin queuing.

For round-robin queuing, if the weight for a CoS is set to 0, then it will continue processing the packets from this CoS until there are no more packets for this CoS. The other CoS queues that have been given a nonzero value, and depending upon the weight, will follow a common round-robin scheme.

Remember that the switch has 4 priority queues (and eight Classes of Service) for each port on the Switch.

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



NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

Command	Parameters
config bandwidth_control	<portlist>{rx_rate [no_limit <value 1-1000>] tx_rate [no_limit <value 1-1000>]}

Command	Parameters
show bandwidth_control	{<portlist>}
config 802.1p user_priority	{<priority 0-7> <class_id 0-3>}
show 802.1p user_priority	
config 802.1p default_priority	[<portlist> all] <priority 0-7>
show 802.1p default_priority	{<portlist> all}
show scheduling	show scheduling
config scheduling	<class_id 0-3> { max_packet <value 0-255> max_latency <value 0-255> }

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

config bandwidth_control	
Purpose	Used to configure bandwidth control on a by-port basis.
Syntax	<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	<p><i><portlist></i> – Specifies a port or range of ports to be configured.</p> <p><i>all</i> – Choose this parameter to select all configurable ports.</p> <p><i>rx_rate</i> – Specifies that one of the parameters below (<i>no_limit</i> or <i><value 1-1000></i>) will be applied to the rate at which the above specified ports will be allowed to receive packets</p> <p>§ <i>no_limit</i> – Specifies that there will be no limit on the rate of packets received by the above specified ports.</p> <p>§ <i><value 1-1000></i> – Specifies the packet limit, in Mbps, that the above ports will be allowed to receive.</p> <p><i>tx_rate</i> – Specifies that one of the parameters below (<i>no_limit</i> or <i><value 1-1000></i>) will be applied to the rate at which the above specified ports will be allowed to transmit packets.</p> <p>§ <i>no_limit</i> – Specifies that there will be no limit on the rate of packets received by the above specified ports.</p> <p>§ <i><value 1-1000></i> – Specifies the packet limit, in Mbps, that the above ports will be allowed to receive.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure bandwidth control:

```
local> config bandwidth_control 1-4 rx_rate no_limit
Command: config bandwidth_control 1-4 rx_rate no_limit

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	<p><i><portlist></i> – Specifies a port or range of ports to be configured.</p> <p>Using this command without adding a portlist entry will show the bandwidth control for all ports in the switch stack.</p>
Restrictions	None.

Example usage:

To display bandwidth control settings:


```

local> show bandwidth_control
Command: show bandwidth_control

Bandwidth Control Table

Port  RX Rate (Mbit/sec) TX_RATE (Mbit/sec)
-----
1    no_limit           no_limit
2    no_limit           no_limit
3    no_limit           no_limit
4    no_limit           no_limit
5    no_limit           no_limit
6    no_limit           no_limit
7    no_limit           no_limit
8    no_limit           no_limit
9    no_limit           no_limit
10   no_limit           no_limit
11   no_limit           no_limit
12   no_limit           no_limit
13   no_limit           no_limit
14   no_limit           no_limit
15   no_limit           no_limit
16   no_limit           no_limit
17   no_limit           no_limit
18   no_limit           no_limit

local>

```

config 802.1p user_priority

Purpose Used to map the 802.1p user priority tags of an incoming packet to one of the eight 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 The **config 802.1p user_priority** command is used to configure the way the switch will map an incoming packet, based on its 802.1p user priority tag, to one of the eight hardware priority queues available on the switch. The switch's default is to map the incoming 802.1p priority values to the eight hardware priority queues according to the following chart:

802.1p Switch Hardware

Value Priority Queue

Value	Priority Queue
0	1
1	0
2	0
3	1
4	2
5	2
6	3
7	3

Parameters *<priority 0-7>* – Specifies which of the eight 802.1p priority tags (0 through 7) you want to map to one of the switch's hardware priority queues (*<class_id>*, 0 through 3).

<class_id 0-3> – Specifies which of the switch's hardware priority queues the 802.1p priority tags (specified above) will be mapped to.

Restrictions Only administrator-level users can issue this command.

Example usage:

To configure 802.1p user priority on the switch:

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

Success.

local>
```

show 802.1p user_priority

show 802.1p user_priority

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

Example usage:

To show 802.1p user priority:

```

local> show 802.1p user_priority
Command: show 802.1p user_priority

QOS Class of Traffic

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

local>

```

config 802.1p default_priority

Purpose	Used to specify default priority settings on the switch. Untagged packets that are received by the switch will be assigned a priority tag in its priority field using this command.
Syntax	config 802.1p default_priority [<portlist> all] <priority 0-7>
Description	The config 802.1p default_priority command allows you to specify the 802.1p priority value an untagged, incoming packet will be assigned before being forwarded to its destination.

config 802.1p default_priority

Parameters	<p><i><portlist></i> – Specifies a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the 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, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.</p> <p><i>all</i> – Specifies that the config 802.1p default_priority command will be applied to all ports on the switch.</p> <p><i><priority 0-7></i> – Specifies the 802.1p priority tag that an untagged, incoming packet will be given before being forwarded to its destination.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure 802.1p default priority on the switch:

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

Example usage:

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

```

local> 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

local>

```

show scheduling

show scheduling

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

Example Usage:

To show the scheduling:

```

local>show scheduling
Command: show scheduling

QOS Output Scheduling

      MAX. Packets MAX. Latency
      -----
Class-0  0           0
Class-1  0           0
Class-2  0           0
Class-3  0           0

local>

```

config scheduling

Purpose	Used to configure QOS output scheduling.
Syntax	config scheduling <class_id 0-3> { max_packet <value 0-255> max_latency <value 0-255> }
Description	This command will config QOS output scheduling in use on the switch.
Parameters	None.
Restrictions	None.

Example Usage:

To show the scheduling:

```
local> config scheduling 0 max_packet 2 max_latency 3
Command: config scheduling 0 max_packet 2 max_latency 3

Success.

local>
```

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.



NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

config mirror port

Purpose	Used to configure a mirror port – source port pair on the switch.
Syntax	config mirror port <port> add source ports <portlist> [rx tx both]
Description	This command allows a range of ports to have all of their traffic also sent to a designated port, where a network sniffer or other device can monitor the network traffic. In addition, you can specify that only traffic received by or sent by one or both is mirrored to the Target port.
Parameters	<p><i>port <port></i> – This specifies the Target port (the port where mirrored packets will be sent).</p> <p><i>add source ports</i> – The port or ports being mirrored. This cannot include the Target port.</p> <p>§ <i><portlist></i> – This specifies a range of ports that will be mirrored. That is, the range of ports in which all traffic will be copied and sent to the Target port.</p> <p>§ <i>rx</i> – Allows the mirroring of only packets received by (flowing into) the port or ports in the port list.</p> <p><i>tx</i> – Allows the mirroring of only packets sent to (flowing out of) the port or ports in the port list.</p> <p><i>both</i> – Mirrors all the packets received or sent by the port or ports in the port list.</p>

config mirror port

Restrictions	The Target port cannot be listed as a source port. Only administrator-level users can issue this command.
--------------	---

Example usage:

To add the mirroring ports:

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

Success.

local>
```

config mirror delete

Purpose	Used to delete a port mirroring configuration.
Syntax	config mirror port <port> delete source port <portlist> [rx tx both]
Description	This command is used to delete a previously entered port mirroring configuration.
Parameters	<p><i>port <port></i> – This specifies the Target port (the port where mirrored packets will be sent).</p> <p><i>delete source port</i> – Adding this parameter will delete source ports according to ports entered using the <i><portlist></i>.</p> <p>§ <i><portlist></i> – This specifies a range of ports that will be mirrored. That is, the range of ports in which all traffic will be copied and sent to the Target port.</p> <p>§ <i>rx</i> – Allows the mirroring of only packets received by (flowing into) the port or ports in the port list.</p> <p><i>tx</i> – Allows the mirroring of only packets sent to (flowing out of) the port or ports in the port list.</p> <p><i>both</i> – Mirrors all the packets received or sent by the port or ports in the port list.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete the mirroring ports:

```

local>config mirror port 1:5 delete source port 1:1-1:5 both
Command: config mirror 1:5 delete source 1:1-1:5 both

Success.

local>

```

enable mirror

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

Example usage:

To enable mirroring configurations:

```

local>enable mirror
Command: enable mirror

Success.

local>

```

disable mirror

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

Example usage:

To disable mirroring configurations:

```
local>disable mirror
Command: disable mirror

Success.

local>
```

show mirror

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

Example usage:

To display mirroring configuration:

```
local>show mirror
Command: show mirror

Current Settings
Mirror Status: Enabled
Target Port : 1:9
Mirrored Port:
    RX:
    TX: 1:1-1:5

local>
```

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] delete] <portlist> advertisement [enable disable]}
config gvrp	[<portlist> all] {state [enable disable] ingress_checking [enable disable] acceptable_frame [tagged_only admit_all] pvid <vlanid 1-4094>}
enable gvrp	
disable gvrp	
show vlan	<vlan_name 32>
show gvrp	<portlist>

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



NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

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><i>tag <vlanid></i> - The VLAN ID of the VLAN to be created.</p> <p><i>advertisement</i> – Specifies that the VLAN is able to join GVRP. If this parameter is not set, the VLAN cannot be configured to have forbidden ports.</p>
Restrictions	Each VLAN name can be up to 32 characters. 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 the vlan “v1”:

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

Success.

local>
```

config vlan

Purpose	Used to add additional ports to a previously configured VLAN.
Syntax	config vlan <vlan_name 32> { [add [tagged untagged forbidden] delete] <portlist> advertisement [enable disable]}
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.

config vlan

Parameters	<p><vlan_name 32> – The name of the VLAN to be configured.</p> <p><i>add</i> – Used to add ports to the specified VLAN, in conjunction with the <i>portlist</i> parameter.</p> <p><i>tagged</i> – Specifies that the ports are to be VLAN tagged.</p> <p>untagged – Specifies the ports as untagged.</p> <p><i>forbidden</i> – Specifies the ports as forbidden ports.</p> <p><i>delete</i> – Used to delete ports from the specified VLAN, in conjunction with the <i>portlist</i> parameter.</p> <p><portlist> – A range of ports to add to the VLAN.</p> <p><i>advertisement [enable disable]</i> – Enables or disables GVRP on the specified VLAN.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To add 4 through 8 of module 2 as tagged ports to the VLAN v1:

```
local>config vlan v1 add tagged 2:4-2:8
Command: config vlan v1 add tagged 2:4-2:8

Success.

local>
```

config gvrp

Purpose	Used to configure GVRP on the switch.
Syntax	config gvrp [<portlist> all] {state [enable disable] ingress_checking [enable disable] acceptable_frame [tagged_only admit_all] pvid <vlanid 1-4094>}
Description	This command is used to configure the Group VLAN Registration Protocol on the switch. You can configure ingress checking, the sending and receiving of GVRP information, and the Port VLAN ID (PVID).

config gvrp

Parameters	<p><i><portlist></i> – A range of ports for which you want ingress checking.</p> <p><i>all</i> – Specifies all of the ports on the switch.</p> <p><i>state [enable disable]</i> – Enables or disables GVRP for the ports specified in the port list.</p> <p><i>ingress_checking [enable disable]</i> – Enables or disables ingress checking for the specified port list.</p> <p><i>acceptable_frame [tagged_only admit_all]</i> – This parameter states the frame type that will be accepted by the switch for this function. <i>tagged_only</i> implies that only VLAN tagged frames will be accepted, while <i>admit_all</i> implies tagged and untagged frames will be accepted by the switch.</p> <p><i>pvid <vlanid 1-4094></i> – Specifies the default VLAN associated with the port.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
local>config gvrp 1:1-1:4 state enable ingress_checking enable
acceptable_frame tagged_only pvid 2

Command: config gvrp 1:1-1:4 state enable ingress_checking enable
acceptable_frame tagged_only pvid 2

Success.

local>
```

enable gvrp

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

Example usage:

To enable the generic VLAN Registration Protocol (GVRP):

```

local>enable gvrp
Command: enable gvrp

Success.

local>

```

disable gvrp

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

Example usage:

To disable the Generic VLAN Registration Protocol (GVRP):

```

local>disable gvrp
Command: disable gvrp

Success.

local>

```

show vlan

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

Example usage:

To display the switch's current VLAN settings:

```

local>show vlan
Command: show vlan

VID          : 1          VLAN Name    : default
VLAN TYPE    : static    Advertisement : Enabled
Member ports : 1:1-1:11,2:1-2:11
Static ports : 1:1-1:11,2:1-2:11
Untagged ports : 1:1-1:11,2:1-2:11
Forbidden ports :

VID          : 2          VLAN Name    : v1
VLAN TYPE    : static    Advertisement : Disabled
Member ports : 1:12,2:12
Static ports : 1:12,2:12
Untagged ports :
Forbidden ports :

Total Entries : 2

local>

```

show gvrp

Purpose	Used to display the GVRP status for a port list on the switch.
Syntax	show gvrp {<portlist>}
Description	This command displays the GVRP status for a port list on the switch
Parameters	<portlist> – Specifies a range of ports for which the GVRP status is to be displayed.
Restrictions	None.

Example usage:

To display GVRP port status:

```
local>show gvrp
Command: show gvrp

Global GVRP : Disabled

Port   PVID   GVRP      Ingress Checking  Acceptable Frame Type
-----
1:1    1       Disabled   Enabled           All Frames
1:2    1       Disabled   Enabled           All Frames
1:3    1       Disabled   Enabled           All Frames
1:4    1       Disabled   Enabled           All Frames
1:5    1       Disabled   Enabled           All Frames
1:6    1       Disabled   Enabled           All Frames
1:7    1       Disabled   Enabled           All Frames
1:8    1       Disabled   Enabled           All Frames
1:9    1       Disabled   Enabled           All Frames
1:10   1       Disabled   Enabled           All Frames
1:11   1       Disabled   Enabled           All Frames
1:12   1       Disabled   Enabled           All Frames
2:1    1       Disabled   Enabled           All Frames
2:2    1       Disabled   Enabled           All Frames
2:3    1       Disabled   Enabled           All Frames
2:4    1       Disabled   Enabled           All Frames
2:5    1       Disabled   Enabled           All Frames
2:6    1       Disabled   Enabled           All Frames
2:7    1       Disabled   Enabled           All Frames
2:8    1       Disabled   Enabled           All Frames
2:9    1       Disabled   Enabled           All Frames
2:10   1       Disabled   Enabled           All Frames
2:11   1       Disabled   Enabled           All Frames
2:12   1       Disabled   Enabled           All Frames

Total Entries : 24

local>
```

LINK AGGREGATION COMMANDS

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

Command	Parameters
create link_aggregation	group_id <value 1-6> {type [lacp static]}
delete link_aggregation	group_id <value 1-6>
config link_aggregation	group_id <value 1-6> {master_port <port> ports <portlist> state [enable disable]}
config link_aggregation algorithm	[mac_source mac_destination mac_source_dest ip_source ip_destination ip_source_dest]
show link_aggregation	{group_id <value 1-6> algorithm}
config lacp_port	<portlist> mode [active passive]
show lacp_port	{<portlist>}

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



NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

create link_aggregation

Purpose	Used to create a link aggregation group on the switch.
Syntax	create link_aggregation group_id <value 1-6> {type [lacp static]}
Description	This command will create a link aggregation group with a unique identifier.

create link_aggregation

Parameters	<p><i><value 1-6></i> – Specifies the group ID. The switch allows up to 6 link aggregation groups to be configured. The group number identifies each of the groups.</p> <p><i>type</i> – Specify the type of link aggregation used for the group. If the type is not specified the default type is static.</p> <p>§ <i>lacp</i> – This designates the port group as LACP compliant. LACP allows dynamic adjustment to the aggregated port group. LACP compliant ports may be further configured (see config lacp_ports). LACP compliant must be connected to LACP compliant devices.</p> <p>§ <i>static</i> – This designates the aggregated port group as static. Static port groups can not be changed as easily as LACP compliant port groups since both linked devices must be manually configured if the configuration of the trunked group is changed. If static link aggregation is used, be sure that both ends of the connection are properly configured and that all ports have the same speed/duplex settings.</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 <value 1-6>
Description	This command is used to delete a previously configured link aggregation group.
Parameters	<i><value 1-6></i> – Specifies the group ID. The switch allows up to 6 link aggregation groups to be configured. The group number identifies each of the groups.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete link aggregation group:

```

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

Success.

local>

```

config link_aggregation

Purpose	Used to configure a previously created link aggregation group.
Syntax	config link_aggregation group_id <value 1-6> {master_port <port> ports <portlist> state [enable disable]}
Description	This command allows you to configure a link aggregation group that was created with the create link_aggregation command above. The DES-3350SR supports link aggregation cross box which specifies that link aggregation groups may be spread over multiple switches in the switching stack.
Parameters	<p><i>group_id <value 1-6></i> – Specifies the group ID. The switch allows up to 6 link aggregation groups to be configured. The group number identifies each of the groups.</p> <p><i>master_port<port></i> – Master port ID. Specifies which port (by port number) of the link aggregation group will be the master port. All of the ports in a link aggregation group will share the port configuration with the master port.</p> <p><i>ports <portlist></i> – Specifies a range of ports that will belong to the link aggregation group.</p> <p><i>state [enable disable]</i> – Allows you to enable or disable the specified link aggregation group.</p>
Restrictions	Only administrator-level users can issue this command. Link aggregation groups may not overlap.

Example usage:

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

```

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

Success.

local>

```

config link_aggregation algorithm

Purpose	Used to configure the link aggregation algorithm.
Syntax	config link_aggregation algorithm [mac_source mac_destination mac_source_dest ip_source ip_destination ip_source_dest]
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><i>mac_source</i> – Indicates that the switch should examine the MAC source address.</p> <p><i>mac_destination</i> – Indicates that the switch should examine the MAC destination address.</p> <p><i>mac_source_dest</i> – Indicates that the switch should examine the MAC source and destination addresses</p> <p><i>ip_source</i> – Indicates that the switch should examine the IP source address.</p> <p><i>ip_destination</i> – Indicates that the switch should examine the IP destination address.</p> <p><i>ip_source_dest</i> – 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>

```

show link_aggregation

Purpose	Used to display the current link aggregation configuration on the switch.
Syntax	show link_aggregation {group_id <value 1-6> algorithm}

show link_aggregation

Description	This command will display the current link aggregation configuration of the switch.
Parameters	<i>group_id</i> <value 1-6> – Specifies the group ID. The switch allows up to 6 link aggregation groups to be configured. The group number identifies each of the groups. <i>algorithm</i> – Allows you to specify the display of link aggregation by the algorithm in use by that group.
Restrictions	None.

Example usage:

To display Link Aggregation configuration:

```

local>show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = MAC-source-dest
Group ID      : 1
Master Port   : 2:10
Member Port   : 1:5-1:10,2:10
Active Port:
Status        : Disabled
Flooding Port : 1:5

DES-3350SR:4

```

config lacp_ports

Purpose	Used to configure settings for LACP compliant ports.
Syntax	config lacp_ports <portlist> mode [active passive]
Description	This command is used to configure ports that have been previously designated as LACP ports (see create link_aggregation).

config lacp_ports

Parameters	<p><i><portlist></i> – Specifies a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the 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, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.</p> <p><i>mode</i> – Select the mode to determine if LACP ports will process LACP control frames.</p> <p>§ <i>active</i> – Active LACP ports are capable of processing and sending LACP control frames. This allows LACP compliant devices to negotiate the aggregated link so the group may be changed dynamically as needs require. In order to utilize the ability to change an aggregated port group, that is, to add or subtract ports from the group, at least one of the participating devices must designate LACP ports as active. Both devices must support LACP.</p> <p>§ <i>passive</i> – LACP ports that are designated as passive cannot process LACP control frames. In order to allow the linked port group to negotiate adjustments and make changes dynamically, at one end of the connection must have “active” LACP ports (see above).</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure LACP port mode settings:

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

Success.

local>
```

show lacp_port

Purpose	Used to display current LACP port mode settings.
Syntax	show lacp_port {<portlist>}
Description	This command will display the LACP mode settings as they are currently configured.

show lacp_port

Parameters	<i><portlist></i> - Specifies a range of ports that will be viewed. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the 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, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To display LACP port mode settings:

```
local>show lacp_port 1:1-1:11
Command: show lacp_port 1:1-1:11

Port   Activity
-----
1:1    Active
1:2    Active
1:3    Active
1:4    Active
1:5    Active
1:6    Active
1:7    Active
1:8    Active
1:9    Active
1:10   Active
1:11   Active

local>
```

IP-MAC BINDING

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

Command	Parameters
create address_binding ip_mac ipaddress	<ipaddr> mac_address <macaddr>
config address_binding ip_mac ipaddress	<ipaddr> mac_address <macaddr>
config address_binding ip_mac ports	[<portlist> all] state [enable disable]
show address_binding	[ip_mac {ipaddress <ipaddr> mac_address <macaddr> } blocked {vlan_name <vlan_name> mac_address <macaddr> } ports]
delete address_binding	[ip_mac [ipaddress <ipaddr> {mac_address <macaddr>} all] blocked [all] vlan_name <vlan_name> mac_address <macaddr>]]

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

create address_binding ip_mac ipaddress	
Purpose	Used to create an IP-MAC Binding entry.
Syntax	<ipaddr> mac_address <macaddr>
Description	This command will create an IP-MAC Binding entry.
Parameters	<p><ipaddr> The IP address of the device where the IP-MAC binding is made.</p> <p><macaddr> The MAC address of the device where the IP-MAC binding is made.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create address binding on the switch:

```

local>create address_binding ip_mac ipaddress 10.1.1.3
mac_address 00-00-00-00-00-04

Command: create address_binding ip_mac ipaddress
10.1.1.3 mac_address 00-00-00-00-00-04

Success.
local>

```

config address_binding ip_mac ipaddress

Purpose	Used to Configure a IP-MAC Binding entry.
Syntax	<ipaddr> mac_address <macaddr>
Description	This command will configure an IP-MAC Binding entry.
Parameters	<p><i><ipaddr></i> The IP address of the device where the IP-MAC binding is made.</p> <p><i><macaddr></i> The MAC address of the device where the IP-MAC binding is made.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To config address binding on the switch:

```

local>config address_binding ip_mac ipaddress 10.1.1.3
mac_address 00-00-00-00-00-05

Command: config address_binding ip_mac ipaddress
10.1.1.3 mac_address 00-00-00-00-00-05

Success.

local>

```

config address_binding ip_mac ports

Purpose	Used to configure an IP-MAC state to enable or disable for specified ports.
Syntax	[<portlist> all] state [enable disable]
Description	This command will configure IP-MAC state to enable or disable for specified ports.
Parameters	<p><i><portlist></i> – Specifies a port or range of ports.</p> <p><i>all</i> – specifies all ports on the switch.</p> <p><i>state [enable disable]</i> – Enables or disables the specified range of ports.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To config address binding on the switch:

```

local>config address_binding ip_mac ports 2 state enable
Command: config address_binding ip_mac ports 2 state
enable

Success.
local>

```

show address_binding

Purpose	Used to display IP-MAC Binding entries.
Syntax	[ip_mac {ipaddress <ipaddr> mac_address<macaddr>} blocked {vlan_name <vlan_name> mac_address <macaddr>} ports]
Description	<p>This command will display IP-MAC Binding entries. Three different kinds of information can be viewed.</p> <ul style="list-style-type: none"> • <i>IP_MAC</i> –Address Binding enties can be viewed by entering the physical and IP addresses of the device. • <i>Blocked</i> – Blocked address binding entries (bindings between VLAN names and MAC addresses) can be viewed by entering the VLAN name and the physical address of the device. • <i>Ports</i> - The number of enabled ports on a device.
Parameters	<p><ipaddr> The IP address of the device where the IP-MAC binding is made.</p> <p><macaddr> The MAC address of the device where the IP-MAC binding is made.</p> <p><vlan_name> The VLAN name of the VLAN that is bound to a MAC address in order to block a specific device on a known VLAN.</p>
Restrictions	none

Example usage:

To show IP-MAC Binding on the switch:

```
local>show address_binding ip_mac ipaddress 10.1.1.8
mac_address 00-00-00-00-00-12
```

```
Command: show address_binding ip_mac ipaddress
10.1.1.8 mac_address 00-00-00-00-00-12
```

Enabled ports: 2

IP Address	MAC Address
-----	-----
10.1.1.8	00-00-00-00-00-12

Total entries : 1

```
local>
```

Delete address_binding

Purpose	Used to delete IP-MAC Binding entries.
Syntax	[ip_mac [ipaddress <ipaddr> {mac_address <macaddr>} [all] blocked [all] vlan_name <vlan_name> mac_address <macaddr>]]
Description	<p>This command will delete IP-MAC Binding entries. Two different kinds of information can be deleted.</p> <ul style="list-style-type: none"> • <i>IP_MAC</i> – Individual Address Binding entries can be deleted by entering the physical and IP addresses of the device. Toggling to <i>all</i> will delete all the Address Binding entries. • <i>Blocked</i> – Blocked address binding entries (bindings between VLAN names and MAC addresses) can be deleted by entering the VLAN name and the physical address of the device. To delete all the Blocked Address Binding entries, toggle <i>all</i>.
Parameters	<p><i><ipaddr></i> The IP address of the device where the IP-MAC binding is made.</p> <p><i><macaddr></i> The MAC address of the device where the IP-MAC binding is made.</p> <p><i><vlan_name></i> The VLAN name of the VLAN that is bound to a MAC address in order to block a specific device on a known VLAN.</p> <p><i>all</i> – For <i>IP_MAC</i> binding <i>all</i> specifies all the IP-MAC binding entries; for Blocked Address Binding entries <i>all</i> specifies all the blocked VLANs and their bound physical addresses.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete an IP-MAC Binding on the switch:

```
local>delete address_binding ip_mac ipaddress 10.1.1.1
mac_address 00-00-00-00-00-06

Command: delete address_binding ip_mac ipaddress
10.1.1.1 mac_address 00-00-00-00-00-06

Success.

local>
```

BASIC IP COMMANDS

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

Command	Parameters
enable ipif	{<ipif_name 12> all}
create ipif	<ipif_name12> <network_address> <vlan_name 32> {secondary state [enable disable]}
config ipif	<ipif_name12> [{ipaddress <network_address> {vlan <vlan_name 32> state [enable disable]} bootp dhcp}
show ipif	<ipif_name 12>
delete ipif	<ipif_name 12> all
disable ipif	<ipif_name 12> all

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

enable ipif	
Purpose	Used to enable an IP interface on the switch.
Syntax	enable ipif {<ipif_name 12> all}
Description	This command will enable the IP interface function on the switch.
Parameters	<p><i><ipif_name 12></i> – The name for the IP interface to be created. This name cannot exceed 12 characters.</p> <p><i>all</i> – Entering this parameter will delete all the IP interfaces currently configured on the switch.</p>
Restrictions	none

Example usage:

To enable the ipif function on the switch:

```

local>enable ipif s2
Command: enable ipif s2

Success.

local>

```

create ipif

create ipif

Purpose	Used to create an IP interface on the switch.
Syntax	create ipif <ipif_name12> <network_address> <vlan_name 32> {secondary state [enable disable]}
Description	This command will create an IP interface.
Parameters	<p><i><ipif_name 12></i> – The name for the IP interface to be created.</p> <p><i><network_address></i> – 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, 10.1.2.3/8).</p> <p><i><vlan_name 32></i> – The name of the VLAN that will be associated with the above IP interface.</p> <p><i>secondary</i> - Enter this parameter if this configured IP interface is to be a <i>secondary</i> IP interface of the VLAN previously specified. Secondary interfaces can only be configured if a primary interface is first configured.</p> <p><i>state [enable disable]</i> – Allows you to enable or disable the IP interface.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create an IP interface on the switch:

```

local>create ipif System ipaddress 10.48.74.122/8 v2 state enable
Command: create ipif System ipaddress 10.48.74.122/8 v2 state enable

Success.

local>

```

config ipif

Purpose	Used to configure the System IP interface.
Syntax	config ipif <ipif_name 12> [{ipaddress <network_address> {vlan <vlan_name 32> state [enable disable]} bootp dhcp]
Description	This command is used to configure the System IP interface on the switch.

config ipif

Parameters	<p><i><ipif_name 12></i> – The name for the IP interface previously created, that is to be configured.</p> <p><i>ipaddress <network_address></i> – IP address and netmask of the IP interface to be configured. 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, 10.1.2.3/8).</p> <p><i>vlan <vlan_name 32></i> – The name of the VLAN corresponding to the System IP interface.</p> <p><i>state [enable disable]</i> – Allows you to enable or disable the IP interface.</p> <p><i>bootp</i> – Allows the selection of the BOOTP protocol for the assignment of an IP address to the switch's System IP interface.</p> <p><i>dhcp</i> – Allows the selection of the DHCP protocol for the assignment of an IP address to the switch's System IP interface.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the IP interface System:

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

Success.

local>
```

show ipif

Purpose	Used to display the configuration of an IP interface on the switch.
Syntax	show ipif <ipif_name 12>
Description	This command will display the configuration of an IP interface on the switch.
Parameters	<i><ipif_name 12></i> – The name created for the IP interface to view.
Restrictions	None.

Example usage:

To display IP interface settings.

```

local>show ipif System
Command: show ipif System

IP Interface Settings

Interface Name   : System
IP Address      : 10.48.74.122 (MANUAL)
Subnet Mask     : 255.0.0.0
VLAN Name       : default
Admin. State    : Disabled
Link Status     : Link UP
Member Ports    : 1:1-1:12

local>

```

delete ipif

Purpose	Used to delete the configuration of an IP interface on the switch.
Syntax	delete ipif <ipif_name 12 all>
Description	This command will delete the configuration of an IP interface on the switch.
Parameters	<p><i><ipif_name></i> – The name created for the IP interface.</p> <p><i>all</i> – Entering this parameter will delete all the IP interfaces currently configured on the switch.</p>
Restrictions	None.

Example usage:

To delete the IP interface named s2:

```

local>delete ipif s2
Command: delete ipif s2

Success.

local>

```

disable ipif

Purpose	Used to disable the configuration of an IP interface on the switch.
---------	---

disable ipif

Syntax	disable ipif <ipif_name 12> all
Description	This command will disable the configuration of an IP interface on the switch.
Parameters	<i><ipif_name 12></i> – The name created for the IP interface. <i>all</i> – Entering this parameter will delete all the IP interfaces currently configured on the switch.
Restrictions	None.

Example usage:

To disable the IP interface named “s2”:

```
local>disable ipif s2
Command: disable ipif s2

Success.

local>
```

IGMP COMMANDS

The IGMP 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 1-25> robustness_variable <value 1-255> last_member_query_interval <sec 1-25> state [enable disable]}
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 1-25> max_response_time <sec 1-25> robustness_variable <value 1-255> last_member_query_interval <sec 1-25> state [enable disable]}
Description	This command allows you to configure IGMP snooping on the switch.
Parameters	<p><i><ipif_name 12></i> – The name of the IP interface for which you want to configure IGMP.</p> <p><i>all</i> – Specifies all the IP interfaces on the switch.</p> <p><i>version <value 1-2></i> – The IGMP version number.</p> <p><i>query_interval <sec 1-25></i> – The time in seconds between general query transmissions, in seconds.</p> <p><i>max_response_time <sec 1-25></i> – Enter the maximum time in seconds that the switch will wait for reports from members.</p> <p><i>robustness_variable <value 1-255></i> – This value states the permitted packet loss that guarantees IGMP.</p> <p><i>last_member_query_interval <value 1-25></i> – 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. The default is 1 second</p> <p><i>state [enable disable]</i> – Enables or disables IGMP for the specified IP interface.</p>
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 enable
Command: config igmp all version 1 state enable

Success.

local>
```

show igmp

Purpose	Used to display the IGMP configuration for the switch of 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 will be displayed.
Restrictions	None.

Example Usage:

To display IGMP configurations:

```
local>show igmp
Command: show igmp

IGMP Interface Configurations

Interface IP Address  Version Query Maximum Response Time Interval Robustness Value Last Member Query State
-----
System 10.58.44.222/8 2 125 10 2 1 Disabled

Total Entries: 1

local>
```

show igmp group

Purpose	Used to display the switch's IGMP group table.
Syntax	show igmp group {group <group>} {ipif <ipif_name 12>}
Description	This command will display the IGMP group configuration.
Parameters	<p><i>group <group></i> – The multicast group ID which the user wishes to display.</p> <p><i><ipif_name 12></i> – The name of the IP interface the IGMP group is part of.</p>
Restrictions	None.

Example Usage:

To display IGMP group table:

```

local>show igmp group
Command: show igmp group

Interface Name  Multicast Group  Last Reporter  IP Querier  IP Expire
-----
System          224.0.0.2           10.42.73.111    10.48.74.122  260
System          224.0.0.9           10.20.53.1     10.48.74.122  260
System          224.0.1.24         10.18.1.3      10.48.74.122  259
System          224.0.1.41         10.1.43.252    10.48.74.122  259
System          224.0.1.149        10.20.63.11    10.48.74.122  259

Total Entries: 5

local>

```

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 1-6711450> state [enable disable]}
config igmp_snooping querier	[<vlan_name 32> all] {query_interval <sec 1-65535> max_response_time <sec 1-25> robustness_variable <value 1-255> last_member_query_interval <sec 1-25> state [enable disable]}
enable igmp snooping	{forward_mcrouter_only}
disable igmp snooping	{forward_mcrouter_only}
config router_ports	{<vlan_name 32>} [add delete] <portlist>
show router_ports	{vlan <vlan_name 32>} {static dynamic}
show igmp_snooping	{vlan <vlan_name 32>}
show igmp_snooping group	{vlan <vlan_name 32>}
show igmp_snooping forwarding	{vlan <vlan_name 32>}

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



NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

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 [enable disable]}
Description	This command allows you to configure IGMP snooping on the switch.

config igmp_snooping

Parameters	<p><i><vlan_name 32></i> – The name of the VLAN for which IGMP snooping is to be configured.</p> <p><i>all</i> – Selecting this parameter will configure IGMP snooping for all VLANs on the switch.</p> <p><i>host_timeout <sec 1-16711450></i> – Specifies the maximum amount of time a host can be a member of a multicast group without the switch receiving a host membership report. The default is 260 seconds.</p> <p><i>router_timeout <sec 1-16711450></i> – Specifies the maximum amount of time a route can be a member of a multicast group without the switch receiving a host membership report. The default is 260 seconds.</p> <p><i>leave_timer <sec 1-16711450></i> – Leave timer. The default is 2 seconds.</p> <p><i>state [enable disable]</i> – Allows you to enable or disable IGMP snooping for the specified VLAN.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the igmp snooping:

```

local>config igmp_snooping default host_timeout 250 state enable
Command: config igmp_snooping default host_timeout 250 state enable

Success.

local>

```

config igmp_snooping querier

Purpose	This command configures IGMP snooping querier.
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 1-25> state [enable disable]}
Description	Used to configure the time in seconds between general query transmissions, the maximum time in seconds to wait for reports from members and the permitted packet loss that guarantees IGMP snooping.

config igmp_snooping querier

Parameters	<p><i><vlan_name 32></i> – The name of the VLAN for which IGMP snooping querier is to be configured.</p> <p><i>all</i> – Selecting this parameter will configure the IGMP snooping querier for all VLANs on the switch.</p> <p><i>query_interval <sec 1-65535></i> – Specifies the amount of time in seconds between general query transmissions. The default setting is 125 seconds.</p> <p><i>max_response_time <sec 1-25></i> – Specifies the maximum time in seconds to wait for reports from members. The default setting is 10 seconds.</p> <p><i>robustness_variable <value 1-255></i> – 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 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. <p><i>last_member_query_interval <sec 1-25></i> – 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.</p> <p><i>state [enable disable]</i> – Allows the switch to be specified as an IGMP Querier or Non-querier.</p>
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
enable
Command: config igmp_snooping querier default query_interval 125
state enable

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 <i>forward_mcrouter_only</i> is specified, the switch will only forward all multicast traffic to the multicast router, only. Otherwise, the switch forwards all multicast traffic to any IP router.
Parameters	<i>forward_mcrouter_only</i> – Specifies that the switch should only forward all multicast traffic to a multicast-enabled router. Otherwise, the switch will forward all multicast traffic to any IP router.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable IGMP snooping on the switch:

```

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 {forward_mcrouter_only}

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. If <i>forward_mrouter_only</i> is specified, the switch will discontinue forwarding all multicast traffic to the multicast router.
Parameters	<i>forward_mrouter_only</i> – Specifies that the switch will discontinue forwarding all multicast traffic to a multicast-enabled router.
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>
```

config router_ports

Purpose	Used to configure ports as router ports.
Syntax	config router_ports <vlan_name 32> [add delete] <portlist>
Description	This command allows you to designate a range of ports as being connected to multicast-enabled routers. This will ensure that all packets with such a router as its destination will reach the multicast-enabled router – regardless of protocol, etc.
Parameters	<p><i><vlan_name 32></i> – The name of the VLAN on which the router port resides.</p> <p><i>[add delete]</i> – Specify if you wish to add or delete the following ports as router ports.</p> <p><i><portlist></i> – Specifies a port or range of ports that will be configured as router ports.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To set up static router ports:

```

local>config router_ports default add 2:1-2:10
Command: config router_ports default add 2:1-2:10

Success.

local>

```

show router_ports

Purpose	Used to display the currently configured router ports on the switch.
Syntax	show router_ports {vlan <vlan_name 32>} {static dynamic}
Description	This command will display the router ports currently configured on the switch.
Parameters	<p><i><vlan_name 32></i> – The name of the VLAN on which the router port resides.</p> <p><i>static</i> – Displays router ports that have been statically configured.</p> <p><i>dynamic</i> – Displays router ports that have been dynamically configured.</p>
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>

```

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

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.

show igmp_snooping group

Parameters	<i>vlan <vlan_name 32></i> – 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  : 1:2,2:7

VLAN Name   : default
Multicast group: 224.0.0.9
MAC address  : 01-00-5E-00-00-09
Reports     : 1
Port Member  : 1:5,2:4

VLAN Name   : default
Multicast group: 234.5.6.7
MAC address  : 01-00-5E-05-06-07
Reports     : 1
Port Member  : 1:6,2:9

VLAN Name   : default
Multicast group: 236.54.63.75
MAC address  : 01-00-5E-36-3F-4B
Reports     : 1
Port Member  : 1:10,2:2

VLAN Name   : default
Multicast group: 239.255.255.250
MAC address  : 01-00-5E-7F-FF-FA
Reports     : 2
Port Member  : 1:8,2:4

VLAN Name   : default
Multicast group: 239.255.255.254
MAC address  : 01-00-5E-7F-FF-FE
Reports     : 1
Port Member  : 1:5,2:5

Total Entries : 6

local>
```


show igmp_snooping forwarding

Purpose	Used to display the IGMP snooping forwarding table entries on the switch.
Syntax	show igmp_snooping forwarding {vlan <vlan_name 32>}
Description	This command will display the current IGMP snooping forwarding table entries currently configured on the switch.
Parameters	<vlan_name 32> – The name of the VLAN for which you want to view IGMP snooping forwarding table information.
Restrictions	None.

Example usage:

To view the IGMP snooping forwarding table for VLAN “Trinity”:

```
local>show igmp_snooping forwarding vlan Trinity
Command: show igmp_snooping forwarding vlan Trinity

VLAN Name      : Trinity
Multicast group : 224.0.0.2
MAC address     : 01-00-5E-00-00-02
Port Member    : 1:11

Total Entries: 1

local>
```

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.

The 802.1X commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

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

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



NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

enable 802.1x

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

Example usage:

To enable 802.1x switch wide:

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

Success.

local>
```

disable 802.1x

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

Example usage:

To disable 802.1x on the switch:

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

Success.

local>
```

show 802.1x auth_configuration

Purpose	Used to display the current configuration of the 802.1x server on the switch.
Syntax	show 802.1x auth_configuration {ports [<portlist>}
Description	The show 802.1x command is used to display the current configuration of the 802.1x Port-based Network Access Control server application on the switch.

show 802.1x auth_configuration

Parameters	<p><i>ports <portlist></i> – Specifies a port or range of ports.</p> <p>The following details what is displayed:</p> <p>802.1x Enabled/Disabled – Shows the current status of 802.1x functions on the switch.</p> <p>Authentication Protocol: Radius_Eap – Shows the authentication protocol suite in use between the switch and a Radius server.</p> <p>Port number – Shows the physical port number on the switch.</p> <p>Capability: Authenticator/None – Shows the capability of 802.1x functions on the port number displayed above. There are two 802.1x capabilities that can be set on the switch: Authenticator and None.</p> <p>AdminCtlDir: 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.</p> <p>OpenCtlDir: Both/In – Shows whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction.</p> <p>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.</p> <p>QuietPeriod – Shows the time interval between authentication failure and the start of a new authentication attempt.</p> <p>TxPeriod – Shows the time to wait for a response from a supplicant (user) to send EAP Request/Identity packets.</p> <p>SuppTimeout – Shows the time to wait for a response from a supplicant (user) for all EAP packets, except for the Request/Identity packets.</p> <p>ServerTimeout – Shows the length of time to wait for a response from a RADIUS server.</p> <p>MaxReq – Shows the maximum number of times to retry sending packets to the supplicant.</p> <p>ReAuthPeriod – Shows the time interval between successive re-authentications.</p> <p>ReAuthenticate: Enabled/Disabled – Shows whether or not to re-authenticate.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To display the 802.1x authentication states:

```

local>show 802.1x auth_configuration ports 1
Command: show 802.1x auth_configuration ports 1

802.1X           : Enabled
Authentication Mode   : None
Authentication Protocol : Radius_EAP

Port number       : 1:1
Capability        : None
AdminCrIDir      : Both
OpenCrIDir       : Both
Port Control      : Auto
QuietPeriod       : 60  sec
TxPeriod          : 30  sec
SuppTimeout       : 30  sec
ServerTimeout     : 30  sec
MaxReq            : 2   times
ReAuthPeriod      : 3600 sec
ReAuthenticate    : Disabled

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

```

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.

show 802.1x auth_state

Parameters	<i>ports <portlist></i> – Specifies a port or range of ports. The following details what is displayed: Port number – Shows the physical port number on the switch. Auth PAE State: Initialize / Disconnected / Connecting / Authenticating / Authenticated / Held / ForceAuth / ForceUnauth – Shows the current state of the Authenticator PAE. Backend State: Request / Response / Fail / Idle / Initialize / Success / Timeout – Shows the current state of the Backend Authenticator. Port Status: Authorized / Unauthorized – Shows the result of the authentication process. Authorized means that the user was authenticated, and can access the network. Unauthorized means that the user was not authenticated, and cannot access the network.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To display the 802.1x auth state for ports 1-4:

```
local> show 802.1x auth_state ports 1-4
Command: show 802.1x auth_state ports 1-4

Port  Auth PAE State  Backend State  Port Status
-----
1    ForceAuth         Success        Authorized
2    ForceAuth         Success        Authorized
3    ForceAuth         Success        Authorized
4    ForceAuth         Success        Authorized

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

config 802.1x auth_mode

Purpose	Used to configure the 802.1x authentication mode on the switch.
Syntax	config 802.1x auth_mode [port_based mac_based]
Description	The config 802.1x auth_mode command is used to enable either the port-based or MAC-based 802.1x authentication feature on the switch.

config 802.1x auth_mode

Parameters	<i>[port_based mac_based ports]</i> – The switch allows you to authenticate 802.1x by either port or MAC address.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure 802.1x authentication by MAC address:

```
local>config 802.1x auth_mode mac_based
Command: config 802.1x auth_mode mac_based

Success.

local>
```

config 802.1x capability ports

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 capability ports command has four capabilities that can be set for each port. Authenticator, Supplicant, Authenticator and Supplicant, and None.
Parameters	<p><i><portlist></i> – Specifies a range of ports.</p> <p><i>all</i> – Specifies all of the ports on the switch.</p> <p><i>authenticator</i> – A user must pass the authentication process to gain access to the network.</p> <p><i>none</i> – The port is not controlled by the 802.1x functions.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure 802.1x capability on ports 1-10 on switch 1:


```
local> local>config 802.1x capability ports all authenticator
```

```
Command: config 802.1x capability ports all authenticator
```

```
Success.
```

```
local>
```

```
local>
```

config 802.1x auth_parameter

Purpose	Used to configure the 802.1x Authentication parameters on a range of ports. The default parameter will return all ports in the specified range to their default 802.1x settings.
Syntax	config 802.1x auth_parameter ports [<portlist> all] [default {direction [both in] port_control [force_unauth auto force_auth] quiet_period <sec 0-65535> tx_period <sec 1-65535> supp_timeout <sec 1-65535> server_timeout <sec 1-65535> max_req <value 1-10> reauth_period <sec 1-65535> enable_reauth [enable disable]]]
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.

config 802.1x auth_parameter

Parameters	<p><i><portlist></i> – Specifies a port or range of ports.</p> <p><i>all</i> – Specifies all of the ports on the switch.</p> <p><i>default</i> – Returns all of the ports in the specified range to their 802.1x default settings.</p> <p><i>direction [both in]</i> – Determines whether a controlled port blocks communication in both the receiving and transmitting directions, or just the receiving direction.</p> <p><i>port_control</i> – Configures the administrative control over the authentication process for the range of ports. The user has the following authentication options:</p> <ul style="list-style-type: none"> • <i>force_auth</i> – Forces the Authenticator for the port to become authorized. Network access is allowed. • <i>auto</i> – Allows the port's status to reflect the outcome of the authentication process. • <i>force_unauth</i> – Forces the Authenticator for the port to become unauthorized. Network access will be blocked. <p><i>quiet_period <sec 0-65535></i> – Configures the time interval between authentication failure and the start of a new authentication attempt.</p> <p><i>tx_period <sec 1-65535></i> – Configures the time to wait for a response from a supplicant (user) to send EAP Request/Identity packets.</p> <p><i>supp_timeout <sec 1-65535></i> – Configures the time to wait for a response from a supplicant (user) for all EAP packets, except for the Request/Identity packets.</p> <p><i>server_timeout <sec 1-65535></i> – Configure the length of time to wait for a response from a RADIUS server.</p> <p><i>max_req <value 1-10></i> – Configures the number of times to retry sending packets to a supplicant (user).</p> <p><i>reauth_period <sec 1-65535></i> – Configures the time interval between successive re-authentications.</p> <p><i>enable_reauth [enable disable]</i> – Determines whether or not the switch will re-authenticate. Enabled causes re-authentication of users at the time interval specified in the Re-authentication Period field, above.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure 802.1x authentication parameters for ports 1 – 20 of switch 1:

```

local>config 802.1x auth_parameter ports 1-4 direction both
Command: config 802.1x auth_parameter ports 1-4 direction both

Success.

local>

```

config 802.1x init

Purpose	Used to initialize the 802.1x function 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 specified range of ports or for specified MAC addresses operating from a specified range of ports.
Parameters	<p><i>port_based</i> – This instructs the switch to initialize 802.1x functions based only on the port number. Ports approved for initialization can then be specified.</p> <p>§ <portlist> – Specifies a port or range of ports.</p> <p>§ all – Specifies all of the ports on the switch.</p> <p><i>mac_based</i> - This instructs the switch to initialize 802.1x functions based on the MAC address of a device on a specific port or range of ports. MAC address approved for initialization can then be specified.</p> <p>§ <portlist> – Specifies a port or range of ports.</p> <p>§ all – Specifies all of the ports on the switch.</p> <p><i>mac_address <macaddr></i> - Specifies the MAC address of the client the user wishes to add.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To initialize the authentication state machine of some or all:

```

local> config 802.1x init port_based ports all
Command: config 802.1x init port_based ports all

Success.

local>

```

config 802.1x reauth ports

Purpose	Used to configure the 802.1x re-authentication feature of the switch.
Syntax	config 802.1x reauth [port_based ports [<portlist all>] mac_based [ports] [<portlist> all] {mac_address <macaddr>}]
Description	The config 802.1x reauth command is used to re-authenticate a previously authenticated device based on port number or MAC address.
Parameters	<p><i>port_based</i> – This instructs the switch to re-authorize 802.1x function based only on the port number. Ports approved for re-authorization can then be specified.</p> <p> § <i>ports</i> <portlist> – Specifies a port or range of ports.</p> <p> § <i>all</i> – Specifies all of the ports on the switch.</p> <p><i>mac-based</i> - This instructs the switch to re-authorize 802.1x function based on a specific MAC address. Ports approved for re-authorization can then be specified.</p> <p> § <portlist> – Specifies a port or range of ports.</p> <p> § <i>all</i> – Specifies all of the ports on the switch.</p> <p><i>mac_address</i> <macaddr> - Specifies the MAC address of the client the user wishes to add.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure 802.1x reauthentication for ports 1-10:

```
local>config 802.1x reauth port_based ports 1-8
Command: config 802.1x reauth port_based ports 1-8

Success.

local>
```

config radius add

Purpose	Used to add a new RADIUS server.
Syntax	config radius add <server_index 1-3> <server_ip> key <passwd 32> [default {auth_port <udp_port_number 1-65535> acct_port <udp_port_number 1-65535>}]

config radius add

Description	The config radius add command is used to add RADIUS servers to the switch.
Parameters	<p><i><server_index 1-3></i> – Assigns a number to the current set of RADIUS server settings. Up to 3 groups of RADIUS server settings can be entered on the switch. The lowest index number will have a higher authenticative priority</p> <p><i><server_ip></i> – The IP address of the RADIUS server.</p> <p><i>key</i> – Specifies that a password and encryption key will be used between the switch and the RADIUS server.</p> <p>§ <i><passwd 32></i> – The shared-secret key used by the RADIUS server and the switch. Up to 32 characters can be used.</p> <p><i>default</i> – Uses the default udp port number in both the “auth_port” and “acct_port” settings.</p> <p><i>auth_port <udp_port_number></i> – The UDP port number for authentication requests. The default is 1812.</p> <p><i>acct_port <udp_port_number></i> – 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 the RADIUS server communication settings:

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

Success.

local>
```

config radius delete

Purpose	Used to delete a previously entered RADIUS server configuration.
Syntax	config radius delete <server_index 1-3>
Description	The config radius delete command is used to delete a previously entered RADIUS server configuration.
Parameters	<i><server_index 1-3></i> – A number identifying the current set of RADIUS server settings the user wishes to delete. Up to 3 groups of RADIUS server settings can be entered on the switch.

config radius delete

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> key <passwd 32> auth_port <udp_port_number 1-65535> acct_port <udp_port_number 1-65535>}
Description	The config radius command is used to configure the switch's RADIUS settings.
Parameters	<p><i><server_index 1-3></i> – Assigns a number to the current set of RADIUS server settings. Up to 3 groups of RADIUS server settings can be entered on the switch.</p> <p><i>ipaddress <server_ip></i> – The IP address of the RADIUS server.</p> <p><i>key</i> – Specifies that a password and encryption key will be used between the switch and the RADIUS server.</p> <p> § <i><passwd 32></i> – The shared-secret key used by the RADIUS server and the switch. Up to 32 characters can be used.</p> <p><i>auth_port <udp_port_number></i> – The UDP port number for authentication requests. The default is 1812.</p> <p><i>acct_port <udp_port_number></i> – 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 the RADIUS settings:

```

local>config radius 1 10.48.74.121 key dlink default
Command: config radius 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 Acct-Port Status  Key
      Number      Number
-----
1  10.1.1.1      1812     1813   Active  kizzel
2  10.1.1.2      1812     1813   Active  mynizzel
Total Entries:2

local>

```

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

Command	Parameters
create access_profile	[ethernet {vlan source_mac <macmask> destination_mac <macmask> 802.1p ethernet_type} ip {vlan source_ip_mask <netmask> destination_ip_mask <netmask> dscp [icmp {type code } igmp {type } tcp {src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xffff> flag_mask [all {urg ack psh rst syn fin}]} 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 {vlan <vlan_name 32> source_ip <ipaddr> destination_ip <ipaddr> dscp <value 0-63> [icmp {type <value 0-255> code <value 0-255>} igmp {type <value 0-255>} tcp {src_port <value 0-65535> dst_port <value 0-65535> flag_mask [all {urg ack psh rst syn fin}]} udp {src_port <value 0-65535> dst_port <value 0-65535>} protocol_id <value 0 - 255> {user_define <hex 0x0-0xffffffff>}}] 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>} permit {priority <value 0-7> {replace_priority} replace_dscp_with <value 0-63> } deny] delete access_id <value 1-255>]
show access_profile	{profile_id <value 1-255>}

Access profiles allow you to establish criteria to determine whether or not 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:

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

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

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

config access_profile profile_id 1 add access_id 1 ip source_ip 10.42.73.1 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.

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.

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



NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

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.
---------	--

create access_profile

Syntax	<pre>[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> flag_mask [all {urg ack psh rst syn fin}]} 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 <hex0x0-0xffffffff> <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>]</pre>
Description	<p>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.</p>

create access_profile

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 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 examine each frame's Internet Group Management Protocol (IGMP) field.
 - *type* – Specifies that the switch will examine each frame's IGMP Type field.
- *tcp* – Specifies that the switch will examine each frames Transport Control Protocol (TCP) field.
 - *src_port_mask <hex 0x0-0xffff>* – Specifies a TCP port mask for the source port.
 - *dst_port_mask <hex 0x0-0xffff>* – Specifies a TCP port mask for the destination port.
 - *flag_mask [all | {urg | ack | psh | rst | syn | fin}]* – Enter the appropriate flag_mask parameter. All incoming packets have TCP port numbers contained in them as the forwarding

create access_profile

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

Example usage:

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

```

local>create access_profile ip vlan source_ip_mask 20.0.0.0
destination_ip_mask 10.0.0.0 dscp icmp type code permit profile_id 101
Command: create access_profile ip vlan source_ip_mask 20.0.0.0
destination_ip_mask 10.0.0.0 dscp icmp type code permit profile_id 101

Success.

DES-3350SR

```

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.
Parameters	<i>profile_id <value 1-255></i> – Enter 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

config access_profile

Purpose	Used to configure an access profile on the switch and to define specific values that will be used to by the switch to determine if a given packet should be forwarded or filtered. Masks entered using the create access_profile command will be combined, using a logical AND operation, with the values the switch finds in the specified frame header fields. Specific values for the rules are entered using the config access_profile command, below.
Syntax	<pre> config access_profile <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 {vlan <vlan_name 32> source_ip <ipaddr> destination_ip <ipaddr> dscp <value 0-63> [icmp {type <value 0-255> code <value 0-255>} igmp {type <value 0-255>} tcp {src_port <value 0-65535> dst_port <value 0-65535> flag_mask [all {urg ack psh rst syn fin}}] udp {src_port <value 0- 65535> dst_port <value 0-65535>} protocol_id <value 0 - 255> {user_define <hex 0x0-0xffffffff>}] 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>}] [permit {replace_priority_with <value 0-7> replace_dscp_with <value 0-63> } deny] delete access_id <value 1-255>] </pre>
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.

config access_profile

Parameters

profile_id <value 1-255> – Enter 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.

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. The lower access ID, the higher the priority the rule will be given.

ethernet – Specifies that the switch will look only into the layer 2 part of each packet.

- *vlan* <vlan_name 32> – Specifies that the access profile will apply to only to this VLAN.
- *source_mac* <macaddr> – Specifies that the access profile will apply to only packets with this source MAC address.
- *destination_mac* <macaddr> – Specifies that the access profile will apply to only packets with this destination MAC address.
- *802.1p* <value 0-7> – Specifies that the access profile will apply only to packets with this 802.1p priority value.
- *ethernet_type* <hex 0x0-0xffff> – Specifies that the access profile will apply only to packets with this 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_ip* <ipaddr> – Specifies that the access profile will apply to only packets with this destination IP address.
- *dscp* <value 0-63> – Specifies that the access profile will apply only to packets that have this value in their Type-of-Service (DiffServ code point, DSCP) field in their IP packet header.
- *icmp* – Specifies that the switch will examine the Internet Control Message Protocol (ICMP) field within each packet.
 - *type* <value 0-255> – 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.

config access_profile

Restrictions Only administrator-level users can issue this command.

Example usage:

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

```
local> config access_profile profile_id 2 add access_id 1 ip source_ip
10.42.73.1 deny
Command: config access_profile profile_id 1 add access_id 1 ip source_ip
10.42.73.1 deny

Success.

local>
```

show access_profile

Purpose	Used to display the currently configured access profiles on the switch.
Syntax	show access_profile {profile_id <value 1-255>}
Description	The show access_profile command is used to display the currently configured access profiles
Parameters	<i>profile_id <value 1-255></i> - Enter this parameter, along with the appropriate value between 1 and 255, to view a specific access profile. Entering this command without a parameter will display all access profiles currently set on the switch.
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: 2

TYPE : Ethernet Frame Filter

Ports:1

Masks : VLAN 802.1P

ID	Mode
3	Permit 0 0-x

```
local>
```


TRAFFIC SEGMENTATION COMMANDS

Traffic segmentation allows you to further sub-divide VLANs into smaller groups of ports that will help to reduce traffic on the VLAN. The VLAN rules take precedence, and then the traffic segmentation rules are applied. The traffic segmentation commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
config traffic_segmentation	<portlist> forward_list [null <portlist>]
show traffic_segmentation	{<portlist>}

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



NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

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><i><portlist></i> – Specifies a range of ports that will be configured for traffic segmentation.</p> <p><i>forward_list</i> – Specifies a range of ports that will receive forwarded frames from the ports specified in the portlist, above.</p> <p><i>null</i> – no ports are specified</p> <p><i><portlist></i> – Specifies a range of ports for the forwarding list. This list must be on the same switch previously specified for traffic segmentation (i.e. following the <i><portlist></i> specified above for config traffic_segmentation).</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure ports 1 through 9 to be able to forward frames to port 10 through 12:

```
local> config traffic_segmentation 1-9 forward_list 10-12
Command: config traffic_segmentation 1-9 forward_list 1-12

Success.

local>
```

show traffic_segmentation

Purpose	Used to display the current traffic segmentation configuration on the switch.
Syntax	show traffic_segmentation <portlist>
Description	The show traffic_segmentation command is used to display the current traffic segmentation configuration on the switch.
Parameters	<i><portlist></i> – Specifies a port or range of ports for which the current traffic segmentation configuration on the switch will be displayed.
Restrictions	The port lists for segmentation and the forward list must be on the same switch.

Example usage:

To display the current traffic segmentation configuration on the switch.

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

Traffic Segmentation Table

Port Forward Portlist

```
-----  
1  1-50  
2  1-50  
3  1-50  
4  1-50  
5  1-50  
6  1-50  
7  1-50  
8  1-50  
9  1-50  
10 1-50  
11 1-50  
12 1-50  
13 1-50  
14 1-50  
15 1-50  
16 1-50  
17 1-50  
18 1-50
```

```
local>
```

TIME AND SNTP COMMANDS

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

Command	Parameters
config sntp	{primary <ipaddr> secondary <ipaddr> poll-interval <int 30-99999>}
show sntp	
enable sntp	
disable sntp	
config time	{time <time hh:mm:ss> date <date ddmmyyyy> time-zone {operator [+ -] hour <gmt_hour 0-13> min <minute 0-59>} dst [disable repeating {s-which <start_which 1-4,last> s-day <start_day sun-sat> s-mth <start_mth 1-12> s-time <start_time hh:mm> e-which<end_which 1-4,last> e-day <end_day sun-sat> e-mth<end_mth 1-12> e-time <end_time hh:mm> offset [30 60]} annual {s-date <start_date 1-31> s-mth <start_mth 1-12> s-time <start_time hh:mm> e-date <end_date 1-31> e-mth <end_mth 1-12> e-time <end_time hh:mm> offset [30 60]}}
show time	

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

config sntp	
Purpose	Used to setup SNTP service.
Syntax	config sntp {primary <ipaddr> secondary <ipaddr> poll-interval <int 30-99999>}
Description	Use this command to configure SNTP service from an SNTP server. SNTP must be enabled for this command to function (See enable sntp).
Parameters	<p><i>primary</i> – This is the primary server the SNTP information will be taken from.</p> <p>§ <ipaddr> – The IP address of the primary server.</p> <p><i>secondary</i> – This is the secondary server the SNTP information will be taken from in the event the primary server is unavailable.</p> <p>§ <ipaddr> – The IP address for the secondary server.</p> <p><i>poll-interval <int 30-99999></i> – This is the interval between requests for updated SNTP information. The polling interval ranges from 30 to 99,999 seconds.</p>
Restrictions	Only administrator-level users can issue this command. SNTP service must be enabled for this command to function (enable sntp).

Example usage:

To configure SNTP settings:

```
local>config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 30
Command: config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 30

Success.

local>
```

show sntp

Purpose	Used to display the SNTP information.
Syntax	show sntp
Description	This command will display SNTP settings information including the source IP address, time and poll interval.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To display SNTP configuration information:

```
local>show sntp
Command: show sntp

Current Time Source : System Clock
SNTP : Disabled
SNTP Primary Server   : 10.1.1.1
SNTP Secondary Server : 10.1.1.2
SNTP Poll Interval   : 720 sec

local>
```

enable sntp

Purpose	Enables SNTP server support.
Syntax	enable sntp
Description	This will enable SNTP support. SNTP service must be separately configured (see config sntp).Enabling and configuring SNTP support will override any manually configured system time settings.

enable sntp

Parameters	None.
Restrictions	Only administrator-level users can issue this command. SNTP settings must be configured for SNTP to function (config sntp).

Example usage:

To enable the SNTP function:

```
local>enable sntp
Command: enable sntp

Success.

local>
```

disable sntp

Purpose	Disables SNTP server support.
Syntax	disable sntp
Description	This will disable SNTP support. SNTP service must be separately configured (see config sntp).
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example:

To stop SNTP support:

```
local>disable sntp
Command: disable sntp

Success.

local>
```

config time

Purpose	Used to manually configure system time and date settings.
---------	---

config time

Syntax	{time <time hh:mm:ss> date <date ddmmyyyy> time-zone {operator [+ -] hour <gmt_hour 0-13> min <minute 0-59>} dst [disable repeating {s-which <start_which 1-4,last> s-day <start_day sun-sat> s-mth <start_mth 1-12> s-time <start_time hh:mm> e-which<end_which 1-4,last> e-day <end_day sun-sat> e-mth<end_mth 1-12> e-time <end_time hh:mm> offset [30 60]} annual {s-date <start_date 1-31> s-mth <start_mth 1-12> s-time <start_time hh:mm> e-date <end_date 1-31> e-mth <end_mth 1-12> e-time <end_time hh:mm> offset [30 60]}}
Description	This will configure the system time and date settings. These will be overridden if SNTP is configured and enabled.
Parameters	<p><i>date</i> – Express the date using two numerical characters for the day of the month, three alphabetical characters for the name of the month, and four numerical characters for the year.</p> <p><i>time</i> – Express the system time using the format hh:mm:ss, that is, two numerical characters each for the hour using a 24-hour clock, the minute and second. For example: 19:42:30.</p>
Restrictions	Only administrator-level users can issue this command. Manually configured system time and date settings are overridden if SNTP support is enabled.

Example usage:

To manually set system time and date settings:

```

local>config time 17012005 17:28:30
Command: config time 17jan2005 17:28:30

Success.

local>

```

show time

Purpose	Used to display the current time settings and status.
Syntax	show time
Description	This will display system time and date configuration as well as display current system time.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To show the time currently set on the switch's System clock:

```
local>show time
Command: show time

Current Time Source : System Clock
Boot Time   : 0 Days 00:00:00
Current Time : 0 Days 01:16:47
Time zone   : GMT -06:00
Daylight Saving Time : Disabled
Offset in minutes : 60
Repeating   From : Apr 1st Sun 02:00
           To   : Oct last Sun 02:00
Annual     From : 29 Apr 02:00
           To   : 12 Oct 02:00

local>
```


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>
config arpentry	<ipaddr> <macaddr>
delete arpentry	[<ipaddr> all]
show arpentry	{ipif <ipif_name 12> ipaddress <ipaddr> static local}
config arp_aging time	<value 0-65535>
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 and the corresponding MAC 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>
```

config arpentry

Purpose	Used to configure a static entry in the ARP table.
---------	--

config arpentry

Syntax	config arpentry <ipaddr> <macaddr>
Description	This command is used to configure a static entry in the ARP Table. The user may specify the IP address and the corresponding MAC address of an entry in the switch's ARP table.
Parameters	<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 configure a static ARP entry for the IP address 10.48.74.12 and MAC address 00:50:BA:00:07:36:

```
local>config arpentry 10.48.74.12 00-50-BA-00-07-36
Command: config arpentry 10.48.74.12 00-50-BA-00-07-36

Success.

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 <i>all</i> clears the switch's ARP table.
Parameters	<p><ipaddr> – The IP address of the end node or station.</p> <p><i>all</i> – Deletes all ARP entries.</p>
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 minutes, that an ARP entry can remain in the switch's ARP table, without being accessed, before it is dropped from the table.
Parameters	<i>time <value 0-65535></i> – The ARP age-out time, in minutes. The value may be set in the range of 0-65535 minutes with a default setting of 20 minutes.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure ARP aging time:

```

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

Success.

local>

```

show arpentry

Purpose	Used to display the ARP table.
Syntax	show arpentry {ipif <ipif_name 12> ipaddress <ipaddr> static local}
Description	This command is used to display the current contents of the switch's ARP table.

show arpentry

Parameters	<p><i><ipif_name 12></i> – The name of the IP interface the end node or station for which the ARP table entry was made, resides on.</p> <p><i><ipaddr></i> – The network address corresponding to the IP interface name above.</p> <p><i>static</i> – Displays the static entries of the ARP table.</p> <p><i>local</i> – Displays the local entries of 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

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>
```

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	<network_address> <ipaddr> {<metric 1-65535>} {[primary backup]}
create iproute default	<ipaddr> {<metric 1-65535>}
delete iproute default	
delete iproute	<network_address> <ipaddr> {[primary backup]}
show iproute	{<network_address>} {[static rip ospf]}

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

create iproute	
Purpose	Used to create IP route entries to the switch's IP routing table.
Syntax	create iproute <network_address> <ipaddr> {<metric 1-65535>} {[primary backup]}
Description	This command is used to create a primary and backup IP route entry to the switch's 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, 10.1.2.3/8).</p> <p><ipaddr> – The gateway IP address for the next hop router.</p> <p><metric 1-65535> – Allows the entry of a routing protocol metric entry, representing the number of routers between the Switch and the IP address above. The default setting is 1.</p> <p>[primary backup] - The user may choose between <i>Primary</i> and <i>Backup</i>. If the Primary Static/Default Route fails, the Backup Route will support the entry. Please take note that the Primary and Backup entries cannot have the same Gateway.</p>
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To add a single static address 10.48.74.121, mask 255.0.0.0 and gateway 10.1.1.254 to the routing table:

```

local>create iproute 10.48.74.121/255.0.0.0 10.1.1.254 1
Command: create iproute 10.48.74.121/8 10.1.1.254 1

Success.

local>

```

create iproute default

Purpose	Used to create IP route entries to the switch's IP routing table.
Syntax	create iproute default <ipaddr> {<metric>}
Description	This command is used to create a default static IP route entry to the switch's IP routing table.
Parameters	<p><i><ipaddr></i> – The gateway IP address for the next hop router.</p> <p><i><metric></i> – Allows the entry of a routing protocol metric entry representing the number of routers between the Switch and the IP address above. The default setting is 1.</p>
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To add the default static address 10.48.74.121, with a metric setting of 1, to the routing table:

```

local>create iproute default 10.48.74.121 1
Command: create iproute default 10.48.74.121 1

Success.

local>

```

delete iproute

Purpose	Used to delete an IP route entry from the switch's IP routing table.
Syntax	delete iproute <network_address> <ipaddr> {[primary backup]}
Description	This command will delete an existing entry from the switch's IP routing table.

delete iproute

Parameters	<p><i><network_address></i> – 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, 10.1.2.3/8).</p> <p><i><ipaddr></i> – The gateway IP address for the next hop router.</p> <p><i>[primary backup]</i> – The user may choose between <i>Primary</i> and <i>Backup</i>. If the Primary Static/Default Route fails, the Backup Route will support the entry. Please take note that the Primary and Backup entries cannot have the same Gateway.</p>
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete a backup static address 10.48.75.121, mask 255.0.0.0 and gateway (ipaddr) entry of 10.1.1.254 from the routing table:

```
local>delete iproute 10.48.74.121/8 10.1.1.254
Command: delete iproute 10.48.74.121/8 10.1.1.254

Success.

local>
```

delete iproute default

Purpose	Used to delete a default IP route entry from the switch's IP routing table.
Syntax	delete iproute default
Description	This command will delete an existing default entry from the switch's IP routing table.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete the default IP route 10.53.13.254:


```

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><i><network_address></i> – 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, 10.1.2.3/8).</p> <p><i>static</i> – Use this parameter to display static iproute entries.</p> <p><i>rip</i> – Use this parameter to display RIP iproute entries.</p> <p><i>ospf</i> – Use this parameter to display OSPF iproute entries.</p>
Restrictions	None.

Example Usage:

To display the contents of the IP routing table:

```

local>show iproute
Command: show iproute

IP Address/Netmask Gateway Interface Hops Protocol
-----
0.0.0.0 10.1.1.254 System 1 Default
10.0.0.0 10.48.74.122 System 1 Local

Total Entries: 2

local>

```

ROUTE REDISTRIBUTION COMMANDS

The route redistribution 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	[local static ospf {all internal external type_1 type_2 inter+e1 inter+e2}] {metric <value>}
config route redistribute dst ospf src	[static rip local] {mettype [1 2] metric <value>}
config route redistribute dst rip src	[local static ospf {all internal external type_1 type_2 inter+e1 inter+e2}] {metric <value>}
delete route redistribute	{dst [rip ospf] src [rip local static 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 src

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><i>src [static rip local]</i> – Allows for the selection of the protocol for the source device.</p> <p><i>mettype [1 2]</i> – 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> <p><i>metric <value></i> – Allows the entry of an OSPF interface cost. This is analogous to a Hop Count in the RIP routing protocol.</p>
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 src

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 {all internal external type_1 type_2 inter+e1 inter+e2}] {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	<i>src</i> {all internal external type_1 type_2 inter+e1 inter+e2} – Allows the selection of the protocol of the source device. <i>metric <value></i> – 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 inter+e1 inter+e2 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>

```

config route redistribute dst ospf src

Purpose	Used configure route redistribution settings for the exchange of RIP routes to OSPF routes on the switch.
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.

config route redistribute dst ospf src

Parameters	<p><i>src</i> [<i>static</i> <i>rip</i> <i>local</i>] – Allows the selection of the protocol of the source device.</p> <p><i>mettype</i> – 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.</p> <p><i>metric</i> <<i>value</i>> – Allows the entry of an OSPF interface cost. This is analogous to a Hop Count in the RIP routing protocol.</p>
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 ospf src all metric 2
Command: config route redistribute dst ospf src all metric 2

Success.

local>
```

config route redistribute dst rip src

Purpose	Used configure route redistribution settings for the exchange of RIP routes to OSPF routes on the switch.
---------	---

config route redistribute dst rip src

Syntax	config route redistribute dst rip src [local static ospf [all internal external type_1 type_2 inter+e1 inter+e2]] {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	<i>src {all internal external type_1 type_2 inter+e1 inter+e2}</i> – Allows the selection of the protocol of the source device. <i>metric <value></i> – 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.

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>

```

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	<i>dst [rip ospf]</i> – Allows the selection of the protocol on the destination device. <i>src [rip static local ospf]</i> – Allows the selection of the protocol on the source device.

delete route redistribute

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>
```

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	<i>src [rip static local ospf]</i> – Allows the selection of the routing protocol on the source device. <i>dst [rip ospf]</i> – 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 Protocol  Destination Protocol  Type      Metric
-----
STATIC  RIP              All       1
LOCAL   OSPF             Type-2    20

Total Entries : 2

local>
```


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><i>hops <value 1-16></i> – Specifies the maximum number of relay agent hops that the BOOTP packets can cross.</p> <p><i>time <sec 0-65535></i> – If this time is exceeded, the switch will relay 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 in which BOOTP relay is to be enabled.</p> <p><ipaddr> – The BOOTP server IP address.</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 an 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 an 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 BOOTP server IP address.</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>}
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
-----
System    10.48.74.122  10.23.12.34  10.12.34.12  10.48.75.121

Total Entries: 1

local>

```

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> [add delete] static <domain_name 32> <ipaddr>}
enable dnsr	{cache static}
disable dnsr	{cache 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> [add delete] static <domain_name 32> <ipaddr>}
Description	This command is used to configure the DNS relay function on the switch.
Parameters	<p><i>primary</i> – Indicates that the IP address below is the address of the primary DNS server.</p> <p><i>secondary</i> – Indicates that the IP address below is the address of the secondary DNS server.</p> <p><i>nameserver <ipaddr></i> – The IP address of the DNS nameserver.</p> <p><i>[add delete]</i> – Indicates if the user wishes to add or delete the DNS relay function.</p> <p><i><domain_name 32></i> – The domain name of the entry.</p> <p><i><ipaddr></i> – The IP address of the entry.</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 10.43.21.12
Command: config dnsr primary 10.43.21.12

Success

local>

```

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 {cache static}
Description	This command is used, in combination with the disable dnsr command below, to enable and disable DNS Relay on the switch.
Parameters	<p><i>cache</i> - This parameter will allow the user to enable the cache lookup for the DNS rely on the switch.</p> <p><i>static</i> - This parameter will allow the user to enable the static table lookup for the DNS rely on the switch.</p>
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>

```

Example Usage:

To enable cache lookup for DNS relay.

```

local>enable dnsr cache
Command: enable dnsr cache

Success.

local>

```

Example Usage:

To enable static table lookup for DNS relay.

```

local>enable dnsr static
Command: enable dnsr static

Success.

local>

```

disable dnsr

Purpose	Used to disable DNS relay on the switch.
Syntax	disable dnsr {cache static}
Description	This command is used, in combination with the enable dnsr command above, to enable and disable DNS Relay on the switch.
Parameters	<p><i>cache</i> – This parameter will allow the user to disable the cache lookup for the DNS rely on the switch.</p> <p><i>static</i> - This parameter will allow the user to disable the static table lookup for the DNS rely on the switch.</p>
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>

```

Example Usage:

To disable cache lookup for DNS relay.

```

local>disable dnsr cache
Command: disable dnsr cache

Success.

local>

```

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	<i>static</i> – 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 DNS relay 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 Cache Table Status : Disabled

DNS Relay Static Table

Domain Name           IP Address
-----
www.123.com.tw        10.12.12.123
bbs.ntu.edu.tw        140.112.1.23

Total Entries: 2

local>
```

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> all] {authentication [enable <password 16> disable] tx_mode [disable v1_only v1_compatible v2_only] rx_mode [v1_only v2_only v1_or_v2 disable] state [enable disable]}
enable rip	
disable rip	
show rip	ipif <ipif_name 12>

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

config rip	
Purpose	Used to configure RIP on the switch.
Syntax	config rip [ipif <ipif_name 12> all] {authentication [enable <password 16> disable] tx_mode [disable v1_only v1_compatible v2_only] rx_mode [v1_only v2_only v1_or_v2 disable] state [enable disable]}
Description	This command is used to configure RIP on the switch.

config rip

Parameters	<p><i><ipif_name 12></i> – The name of the IP interface.</p> <p><i>all</i> – To configure all RIP receiving mode for all IP interfaces.</p> <p><i>authentication [enable disable]</i> – Enables or disables authentication for RIP on the switch.</p> <p>§ <i><password 16></i> – Allows the specification of a case-sensitive password.</p> <p><i>tx_mode</i> – Determines how received RIP packets will be interpreted – as RIP version V1 only, V2 Only, or V1 Compatible (V1 and V2). This entry specifies which version of the RIP protocol will be used to transfer RIP packets. The Disabled entry prevents the reception of RIP packets.</p> <p>§ <i>disable</i> – Prevents the transmission of RIP packets.</p> <p>§ <i>v1_only</i> – Specifies that only RIP v1 packets will be transmitted.</p> <p>§ <i>v1_compatible</i> – Specifies that only RIP v1 compatible packets will be transmitted.</p> <p>§ <i>v2_only</i> - Specifies that only RIP v2 packets will be transmitted.</p> <p><i>rx_mode</i> – Determines how received RIP packets will be interpreted – as RIP version V1 only, V2 Only, or V1 or V2. This entry specifies which version of the RIP protocol will be used to receive RIP packets. The Disabled entry prevents the reception of RIP packets.</p> <p>§ <i>v1_only</i> – Specifies that only RIP v1 packets will be transmitted.</p> <p>§ <i>v2_only</i> - Specifies that only RIP v2 packets will be transmitted.</p> <p>§ <i>v1_or_v2</i> - Specifies that only RIP v1 or v2 packets will be transmitted.</p> <p><i>state [enable disable]</i> – Allows RIP to be enabled and disabled on the switch.</p>
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>

```

enable rip

Purpose	Used to enable RIP.
Syntax	enable rip
Description	This command is used to enable 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 to 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 and statistics for a given IP interface or for all IP interfaces.
Parameters	<i>ipif <ipif_name 12></i> – 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 display RIP configuration:

```

local>show rip
Command: show rip

RIP Global State : Disabled

RIP Interface Settings

Interface  IP Address      TX Mode  RX Mode  Authen-  State
-----  -
System    10.41.44.33/8  Disabled Disabled  Disabled Disabled

Total Entries : 1

local>

```

DVMRP COMMANDS

The DVMRP 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 [enable disable]}
enable dvmrp	
disable dvmrp	
show dvmrp neighbor	{ipif <ipif_name 12> ipaddress <network_address>}
show dvmrp nexthop	{ipaddress <network_address> ipif <ipif_name 12>}
show dvmrp routing_table	{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 <sec 1-65535> neighbor_timeout <sec 1-65535> state [enable disable]}
Description	This command is used to configure DVMRP on the switch.

config dvmrp

Parameters	<p><i><ipif_name 12></i> – The name of the IP interface for which DVMRP is to be configured.</p> <p><i>all</i> – Specifies that DVMRP is to be configured for all IP interfaces on the switch.</p> <p><i>metric <value 1-31></i> – 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><i>probe <second 1-65535></i> – DVMRP defined an extension to IGMP that allows routers to query other routers to determine if a DVMRP neighbor is present on a given subnetwork or not. This is referred to as a 'probe'. This entry will set an intermittent probe (in seconds) on the device that will transmit dvmrp messages, depending on the time specified. This probe is also used to "keep alive" the connection between DVMRP enabled devices. The default value is 10 seconds.</p> <p><i>neighbor_timeout <second 1-65535></i> – The time period for which DVMRP will hold Neighbor Router reports before issuing poison route messages. The default value is 35 seconds.</p> <p><i>state [enable disable]</i> – Allows DVMRP to be enabled or disabled.</p>
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.

show dvmrp routing_table

Parameters	<i>ipaddress <network_address></i> – 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/Netmask  Upstream Neighbor  Metric  Learned  Interface  Expire
-----
10.0.0.0/8              10.90.90.90        2       Local    System     -
20.0.0.0/8              20.1.1.1           2       Local    ip2        117
30.0.0.0/8              30.1.1.1           2       Dynamic  ip3        106

Total Entries: 3

local>
```

show dvmrp neighbor

Purpose	Used to display the DVMRP neighbor table.
Syntax	show dvmrp neighbor {ipif <ipif_name 12> ipaddress <network_address>}
Description	This command will display the current DVMRP neighbor table.
Parameters	<p><i><ipif_name 12></i> – The name of the IP interface for which you want to display the DVMRP neighbor table.</p> <p><i>ipaddress <network_address></i> – 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 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

local>

```

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><i><ipif_name 12></i> – The name of the IP interface for which you want to display the current DVMRP routing next hop table.</p> <p><i>ipaddress <network_address></i> – 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 display DVMRP routing next hop table:

```

local>show dvmrp nexthop
Command: show dvmrp nexthop

Source IP Address/Netmask Interface Name Type
-----
10.0.0.0/8                ip2                Leaf
10.0.0.0/8                ip3                Leaf
20.0.0.0/8                System             Leaf
20.0.0.0/8                ip3                Leaf
30.0.0.0/8                System             Leaf
30.0.0.0/8                ip2                Leaf

Total Entries: 6

local>

```

show dvmrp

Purpose	Used to display the current DVMRP routing table.
Syntax	show dvmrp {<ipif_name 12>}
Description	The command will display the current DVMRP routing table.
Parameters	<ipif_name 12> – The name of the IP interface for which you want to display the DVMRP routing table.
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   10.90.90.90/8    35                10    1    Disabled

Total Entries: 1

local>

```

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 [enable disable]}
enable pim	
disable pim	
show pim neighbor	{ipif <ipif_name 12> ipaddress <network_address>}
show pim	{ipif <ipif_name 12>}

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

config pim	
Purpose	Used to configure PIM settings for the switch or for specified IP interfaces.
Syntax	config pim [ipif <ipif_name 12> all] { hello <sec 1-18724> jp_interval <sec 1-18724> state [enable disable]}
Description	The config pim command is used to configure PIM settings and enable or disable PIM settings for specified IP interfaces. PIM must also be globally enabled to function (see enable pim).
Parameters	<p><i>ipif <ipif_name 12></i> – Name assigned to the specific IP interface being configured for PIM settings.</p> <p><i>all</i> – Used to configure PIM settings for all IP interfaces.</p> <p><i>hello <sec 1-18724></i> - The time, in seconds, between issuing hello packets to find neighboring routers.</p> <p><i>jp_interval <sec 1-18724></i> – The join/prune interval is the time value (seconds) between transmitting (flooding to all interfaces) multicast messages to downstream routers, and automatically ‘pruning’ a branch from the multicast delivery tree. The <i>jp_interval</i> is also the interval used by the router to automatically remove prune information from a branch of a multicast delivery tree and begin to flood multicast messages to all branches of that delivery tree. These two actions are equivalent. The range is between 1 and 18724 seconds. The default is 60 seconds.</p> <p><i>state [enable disable]</i> – This can enable or disable PIM for the specified IP interface. The default is disabled. Note that PIM settings must also be enabled globally for the switch with the enable pim described below for PIM to operate on any configured IP interfaces.</p>

config pim

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

Usage Example:

To configure PIM settings for IP interface “System”:

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

Success.

local>
```

enable pim

Purpose	Used to enable PIM function on the switch.
Syntax	enable pim
Description	This command will enable PIM for the switch. PIM settings must first be configured for specific IP interfaces using the config pim command.
Parameters	None.
Restrictions	Only administrator-level users can use this command.

Usage Example:

To enable PIM as previously configured on the switch:

```
local>enable pim
Command: enable pim

Success.

local>
```

disable pim

Purpose	Used to disable PIM function on the switch.
Syntax	disable pim
Description	This command will disable PIM for the switch. Any previously configured PIM settings will remain unchanged and may be enabled at a later time with the enable pim command.

disable pim

Parameters	None.
Restrictions	Only administrator-level users can use this command.

Usage Example:

To disable PIM on the switch:

```
local>disable pim
Command: disable pim

Success.

local>
```

show pim neighbor

Purpose	Used to display PIM neighbor router table entries.
Syntax	show pim neighbor {ipif <ipif_name 12> ipaddress <network_address>}
Description	This command will list current entries in the PIM neighbor table for a specified IP interface or destination router IP address.
Parameters	<p><i>ipif <ipif_name 12></i> – The name of an IP interface for which you want to view the PIM neighbor router table.</p> <p><i>ipaddress <network_address></i> The IP address and netmask of the destination routing device for which you want to view the neighbor router table. 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> <p>If no parameters are specified, all PIM neighbor router tables are displayed.</p>
Restrictions	None.

Example usage:

To display PIM settings as configured on the switch:

```

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

local>

```

show pim

Purpose	Used to display current PIM configuration.
Syntax	show pim {ipif <ipif_name 12>}
Description	This command will list current PIM configuration settings for a specified IP interface or all IP interfaces.
Parameters	<i>ipif <ipif_name 12></i> – The name of an IP interface for which PIM settings are listed. If no parameters are specified, all PIM settings are displayed for all interfaces.
Restrictions	None.

Usage Example:

To display PIM settings as configured on the switch:

```
local>show pim
Command: show pim

PIM Global State : Disabled

PIM-DM Interface Table

      Hello   Join/Prune
Interface  IP Address  Interval Interval  State
-----
System    10.90.90.90/8  35      60      Enabled

Total Entries : 1

local>
```


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_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>}
Description	This command will display the current IP multicast forwarding cache.
Parameters	<p><i><group></i> – The multicast group ID.</p> <p><i>ipaddress <network_address></i> – 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      Source Address/Netmask  Upstream   Expire   Routing
  Group          -----
  -----
  224.1.1.1      10.48.74.121/32        10.48.75.63  30      dvmrp
  224.1.1.1      20.48.74.25 /32        20.48.75.25  20      dvmrp
  224.1.2.3      10.48.75.3 /3         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><i><ipif_name 12></i> – The name of the IP interface for which you want to display the IP multicast interface table for.</p> <p><i>protocol [dvmrp pim]</i> – Allows the user to specify whether or not to use the DVMRP or PIM protocol to display 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 by DVMRP entry:

```

local>show ipmc ipif System protocol dvmrp
Command: show ipmc ipif System protocol dvmrp

Interface Name  IP Address  Multicast Routing
-----
System         10.90.90.90  DVMRP

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

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

create md5 key

Purpose	Used to create a new entry in the MD5 key table.
Syntax	create md5 key <key_id 1-255> <password 16>
Description	This command is used to create an entry for the MD5 key table.
Parameters	<p><key_id 1-255> – The MD5 key ID. The user may enter a key ranging from 1 to 255.</p> <p><password> – An MD5 password of up to 16 bytes.</p>
Restrictions	Only administrator-level users can issue this command.

Usage Example

To create an entry in the MD5 key table:

```

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

Success.

local>

```

config md5 key

Purpose	Used to enter configure the password for an MD5 key.
Syntax	config md5 key <key_id 1-255> <password 16>
Description	This command is used to configure an MD5 key and password.

config md5 key

Parameters	<p><i><key_id 1-255></i> – The previously defined MD5 key ID.</p> <p><i><password 16></i> – The user may change the MD5 password for the md5 key. A new password of up to 16 characters can be created.</p>
Restrictions	Only administrator-level users can issue this command.

Usage Example

To configure an MD5 Key password:

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

Success.

local>
```

delete md5 key

Purpose	Used to delete an entry in the MD5 key table.
Syntax	delete md5 key <key_id 1-255>
Description	This command is used to delete a specific entry in the MD5 key table.
Parameters	<i><key_id 1-255></i> – The MD5 key ID the user wishes to delete.
Restrictions	Only administrator-level users can issue this command.

Usage Example

The delete an entry in the 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.
---------	-----------------------------------

show md5

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.
Restrictions	None.

Usage Example

To display the current MD5 key:

```
local>show md5
Command: show md5

MD5 Key Table Configurations

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

Total Entries: 4

local>
```

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 [enable disable] metric <value 0-16777215>}]
delete ospf area	<area_id>
config ospf area	<area_id> type [normal stub {stub_summary [enable disable] metric <value 0-16777215>}]
show ospf area	{<area_id>}
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 1-65535>}
show ospf host_route	<ipaddr>
create ospf aggregation	<area_id> <network_address> lsdb_type summary {advertise [enable disable]}
delete ospf aggregation	<area_id> <network_address> lsdb_type summary
config ospf aggregation	<area_id> <network_address> lsdb_type summary {advertise [enable disable]}
show ospf aggregation	<area_id>
show ospf lsdb	{area <area_id> advertise_router <ipaddr> type [rtrlink netlink summary assummary asexmlink]}
show ospf neighbor	<ipaddr>
show ospf virtual_neighbor	{<area_id> <neighbor_id>}
config ospf ipif	<ipif_name 12> {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 1-65535> state [enable disable]}
config ospf all	{area <area_id> priority <value> hello_interval <1-65535 sec> dead_interval <1-65535 sec> authentication [none simple <password 8> md5 <key_id 1-255>] metric <value 1-65535> state [enable disable]}
show ospf ipif	<ipif_name 12>
show ospf all	

Command	Parameters
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>]}
config 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>]}
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 router_id	
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 IP address of the OSPF router.
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.

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

Success.

local>
```

show ospf

Purpose	Used to display the current OSPF state on the switch.
Syntax	show ospf

show ospf

Description	This command will display the current state of OSPF on the switch, divided into the following categories: General OSPF settings OSPF Interface settings OSPF Area settings OSPF Virtual Interface settings OSPF Area Aggregation settings OSPF Host 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
		2/4	

create ospf area

Purpose	Used to configure OSPF area settings.
Syntax	create ospf area <area_id> type [normal stub {stub_summary [enable disable] metric <value 0-16777215>}]
Description	This command is used to create an OSPF area and configure its settings.
Parameters	<p><i><area_id></i> – The OSPF area ID. The user may enter 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><i>type [normal stub]</i> – The OSPF area mode of operation – stub or normal.</p> <p><i>stub_summary [enable disable]</i> – Enables or disables the OSPF area to import summary LSA advertisements.</p> <p><i>metric <value 0-16777215></i> – The OSPF area cost between 0 and 16777215. 0 denotes that the value will be automatically assigned. The default setting is 0.</p>
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.
Parameters	<i><area_id></i> – 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 [enable disable] metric <value 0-16777215>}]
Description	This command is used to configure an OSPF area's settings.
Parameters	<p><i><area_id></i> – The OSPF area ID. The user may enter 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><i>type [normal stub]</i> – Allows the specification of the OSPF mode of operation – stub or normal.</p> <p><i>stub_summary [enable disable]</i> – Allows the OSPF area import of LSA advertisements to be enabled or disabled.</p> <p><i>metric <value 0-16777215></i> – The OSPF area stub default cost.</p>
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 enable metric 1
Command: config ospf area 10.48.74.122 type stub stub_summary enable
metric 1

Success.

local>
```

show ospf area	
Purpose	Used to display an OSPF area's configuration.

show ospf area

Syntax	show ospf area {<area_id>}
Description	This command will display the current OSPF area configuration.
Parameters	<i><area_id></i> – 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      None
10.48.74.122 Stub       Enabled                               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>}
Description	This command is used to configure the OSPF host route settings.
Parameters	<i><ipaddr></i> – The host's IP address. <i><area_id></i> – 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. <i>metric <value 1-65535></i> – A metric between 1 and 65535, which will be advertised.
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.
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>}
Description	This command is used to configure an OSPF host route settings.
Parameters	<p><ipaddr> – The IP address of the host.</p> <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><value> – A metric value between 1 and 65535 that will be advertised for the route.</p>
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.
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
10.48.74.122 1           10.1.1.1

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 [enable disable]}
Description	This command is used to create an OSPF area aggregation.

create ospf 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 [enable disable] – 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 enable
Command: create ospf aggregation 10.1.1.1 10.48.76.122/16
lsdb_type summary advertise enable

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 [enable disable]}
Description	This command is used to configure the OSPF area aggregation settings.
Parameters	<p><i><area_id></i> – 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><i><network_address></i> – The 32-bit number in the form of an IP address that uniquely identifies the network that corresponds to the OSPF Area.</p> <p><i>lsdb_type summary</i> – Specifies the type of address aggregation.</p> <p><i>advertise [enable disable]</i> – 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 enable
Command: config ospf aggregation 10.1.1.1 10.48.76.122/16 lsdb_type
summary advertise enable

Success.

local>

```

show ospf aggregation

Purpose	Used to display the current OSPF area aggregation settings.
---------	---

show ospf aggregation

Syntax	show ospf aggregation {<area_id>}
Description	This command will display the current OSPF area aggregation settings.
Parameters	<i><area_id></i> – Enter this parameter if you wish to view this table by a specific 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<br>Network Address | LSDB<br>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	<p><i>area_id <area_id></i> – 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><i>advertise_router <ipaddr></i> – The router ID of the advertising router.</p> <p><i>type [rtrlink netlink summary assummary asextlink]</i> – The type of link.</p>

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.
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>}
Description	This command will display the current OSPF virtual neighbor router table.
Parameters	<p><i><area_id></i> – 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><i><neighbor_id></i> – The OSPF router ID for the neighbor. 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

Total Entries : 1

local>

```

config ospf ipif

config ospf ipif

Purpose	Used to configure the OSPF interface settings.
Syntax	config ospf ipif <ipif_name 12> {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 1-65535> state [enable disable]}
Description	This command is used to configure the OSPF interface settings.
Parameters	<p><i><ipif_name 12></i> – The name of the IP interface.</p> <p><i>area <area_id></i> - 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><i>priority <value></i> – The priority used in the election of the Designated Router (DR). A number between 0 and 255.</p> <p><i>hello_interval <sec 1-65535></i> – 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><i>dead_interval <sec 1-65535></i> – 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 65535 seconds can be specified. The <i>dead interval</i> must be evenly divisible by the Hello Interval.</p> <p><i>metric <value 1-65535 ></i> – The interface metric (1 to 65535). Entering a 0 will allow automatic calculation of the metric.</p> <p><i>authentication</i> – Enter the type of authentication preferred. The user may choose between:</p> <ul style="list-style-type: none"> § <i>none</i> – Choosing this parameter will require no authentication. § <i>simple <password 8></i> – Choosing this parameter will set a simple authentication which includes a case-sensitive password of no more than 8 characters. § <i>md5 <key_id 1-255></i> – Choosing this parameter will set authentication based on md5 encryption. A previously configured MD5 key ID (1 to 255) is required. <p><i>metric <value 1-65535></i> – 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 1.</p> <p><i>state [enable disable]</i> – Used to enable or disable this function.</p>
Restrictions	Only administrator-level users can issue this command.

Usage Example

To configure OSPF interface settings:

```

local>config ospf ipif System priority 2 hello_interval 15 metric 2
state enable

Command: config ospf ipif System priority 2 hello_interval 15
metric 2 state enable

Success.

local>

```

config ospf all

Purpose	Used to configure all of the OSPF interfaces on the switch at one time.
Syntax	config ospf 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 1-65535> state [enable disable]}
Description	This command is used to configure all of the OSPF interfaces on the switch, using a single group of parameters, at one time.

config ospf all

Parameters	<p><i>area</i> <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><i>priority</i> <value> – The priority used in the election of the Designated Router (DR). A number between 0 and 255.</p> <p><i>hello_interval</i> <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><i>dead_interval</i> <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 65535 seconds can be specified. The Dead Interval must be evenly divisible by the Hello Interval.</p> <p><i>metric</i> <value 1-65535 > – The interface metric (1 to 65535). Entering a 0 will allow automatic calculation of the metric.</p> <p><i>authentication</i> – Enter the type of authentication preferred. The user may choose between:</p> <ul style="list-style-type: none"> § <i>none</i> – Choosing this parameter will require no authentication. § <i>simple</i> <password 8> – Choosing this parameter will set a simple authentication which includes a case-sensitive password of no more than 8 characters. § <i>md5</i> <key_id 1-255> – Choosing this parameter will set authentication based on md5 encryption. A previously configured MD5 key ID (1 to 255) is required. <p><i>metric</i> <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 1.</p> <p><i>state</i> [<i>enable</i> <i>disable</i>] – Used to enable or disable this function.</p>
Restrictions	Only administrator-level users can issue this command.

Usage Example

To configure all of the OSPF interfaces on the switch with a single group of parameters:

```

local>config ospf all state enable
Command: config ospf all state enable

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> all}
Description	This command will display the current OSPF interface settings for the specified interface name.
Parameters	<i><ipif_name 12></i> – The IP interface name for which you want to display the current OSPF interface settings. <i>all</i> – Entering this parameter will display all ospf Interface settings.
Restrictions	None.

Usage Example

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


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

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>
```

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.
Parameters	<p><i><area_id></i> – 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><i><neighbor_id></i> – 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><i>hello_interval <sec 1-65535></i> – 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><i>dead_interval <sec 1-65535></i> – 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 65535 seconds can be specified. The Dead Interval must be evenly divisible by the Hello Interval.</p> <p><i>authentication</i> – Enter the type of authentication preferred. The user may choose between:</p> <ul style="list-style-type: none"> § <i>none</i> – Choosing this parameter will require no authentication. § <i>simple <password 8></i> – Choosing this parameter will set a simple authentication which includes a case-sensitive password of no more than 8 characters. § <i>md5 <key_id 1-255></i> – Choosing this parameter will set authentication based on md5 encryption. A previously configured MD5 key ID (1 to 255) is required.
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>

```

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 [none simple <password 8> md5 <key_id 1-255>]}
Description	This command is used to configure the OSPF virtual interface settings.
Parameters	<p><i><area_id></i> – 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><i><neighbor_id></i> – 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><i>hello_interval <sec 1-65535></i> – 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><i>dead_interval <sec 1-65535></i> – 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 65535 seconds can be specified. The Dead Interval must be evenly divisible by the Hello Interval.</p> <p><i>authentication</i> – Enter the type of authentication preferred. The user may choose between:</p> <ul style="list-style-type: none"> § <i>none</i> – Choosing this parameter will require no authentication. § <i>simple <password 8></i> – Choosing this parameter will set a simple authentication which includes a case-sensitive password of no more than 8 characters. § <i>md5 <key_id 1-255></i> – Choosing this parameter will set authentication based on md5 encryption. A previously configured MD5 key ID (1 to 255) is required.

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>
```

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	<p><i><area_id></i> – 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><i><neighbor_id></i> – 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>
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.
---------	---

show ospf virtual_link

Syntax	show ospf virtual_link {<area_id> <neighbor_id>}
Description	This command will display the current OSPF virtual interface configuration.
Parameters	<p><i><area_id></i> – 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><i><neighbor_id></i> – 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.</p>
Restrictions	None.

Usage Example:

To display the current OSPF virtual interface configuration:

```

local>show ospf virtual_link

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

Total Entries: 1

local>

```

COMMAND HISTORY LIST

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

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

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

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

Example usage

To display all of the commands in the CLI:

```

local>?
..
?
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 auth_protocol
config 802.1x capability ports
config 802.1x init
config 802.1x reauth
config access profile profile_id
config account
config admin local_enable
config all_boxes_id
config arp_aging time
config authen_application
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All

```

show command_history

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

Example usage

To display the command history:

```

local>show command_history
Command: show command_history

?
? show
show vlan
config router_ports vlan2 add 1:1-1:10
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>

```

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> – The number of previously executed commands maintained in the buffer. Up to 40 of the latest executed commands may be viewed.
Restrictions	None.

Example usage

To configure the command history:

```

local>config command_history 20
Command: config command_history 20

Success.

local>

```


TECHNICAL SPECIFICATIONS

Physical and Environmental	
AC Input & External Redundant power Supply:	100 – 120; 200 - 240 VAC, 50/60 Hz (internal universal power supply)
Power Consumption:	90 watts maximum
DC Fans:	2 built-in 40 x 40 x10 mm fans
Operating Temperature:	0 to 40 degrees Celsius
Storage Temperature:	-25 to 55 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
Weight:	3.15 kg
EMC:	FCC Class A , CE Mark, C-Tick
Safety:	CSA International

General	
Standards:	IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.1 P/Q VLAN IEEE 802.3x Full-duplex Flow Control IEEE 802.3 Nway auto-negotiation IEEE 802.3z SFP ports IEEE 802.1D/w/s Spanning trees. IEEE 802.1p QoS (Priority Bits) IEEE 802.1X Access Control
Protocols:	CSMA/CD

General	
Data Transfer Rates:	Half-duplex Full-duplex
Ethernet	10 Mbps 20Mbps
Fast Ethernet	100Mbps 200Mbps
Gigabit Ethernet	n/a 2000Mbps
Fiber Optic	SFP (Mini GBIC) Support IEEE 802.3z 1000BASE-LX (DEM-310GT transceiver) IEEE 802.3z 1000BASE-SX (DEM-311GT transceiver) IEEE 802.3z 1000BASE-LH (DEM-314GT transceiver) IEEE 802.3z 1000BASE-ZX (DEM-315GT transceiver)
Network Cables:	
10BASE-T:	UTP Cat.5, Cat.5 Enhanced for 1000Mbps UTP Cat.5 for 100Mbps UTP Cat.3, 4, 5 for 10Mbps
100BASE-TX:	EIA/TIA-568 100-ohm screened twisted-pair (STP)(100m)
Number of Ports:	48 10/100 + 2 Gigabit Ethernet ports

Performance	
Transmission Method:	Store-and-forward
RAM Buffer:	1 MB per device
Filtering Address Table:	16K MAC address per device
Packet Filtering/Forwarding Rate:	Full-wire speed for all connections. 148,810 pps per port (for 100Mbps) 1,488,100 pps per port (for 1000Mbps)
MAC Address Learning:	Automatic update.
Forwarding Table Age Time:	Max age: 10 - 1000000 seconds. Default = 300.



DES-3350SR

48 10/100Mbps plus 2 Gigabit Ports

Layer 3 Stackable Switch

Command Line Interface Reference Manual

Release 3

Information in this document is subject to change without notice.

© 2005 D-Link Computer Corporation. All rights reserved.

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

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

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

March 2005 P/N 651SR3350035

Table of Contents

Introduction.....	1
Using the Console CLI.....	4
Command Syntax	9
Basic Switch Commands.....	12
Switch Port Commands	24
Port Security Commands.....	27
Network Management (SNMP) Commands	30
Switch Utility Commands	54
Network Monitoring Commands.....	58
Spanning Tree Commands	63
Forwarding Database Commands.....	71
Broadcast Storm Control Commands.....	79
QoS Commands	82
Port Mirroring Commands	92
VLAN Commands.....	96
Link Aggregation Commands	103
IP-MAC Binding.....	110
Basic IP Commands	115
IGMP Commands.....	120
IGMP Snooping Commands	123
802.1X Commands.....	134
Access Control List (ACL) Commands.....	148
Traffic Segmentation Commands.....	157
Time and SNTP Commands.....	160
ARP Commands.....	165
Routing Table Commands.....	170

Route Redistribution Commands	174
BOOTP Relay Commands	181
DNS Relay Commands	185
RIP Commands	190
DVMRP Commands	194
PIM Commands	200
IP Multicasting Commands	205
MD5 Configuration Commands	207
OSPF Configuration Commands	210
Command History List.....	234
Technical Specifications	237

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.

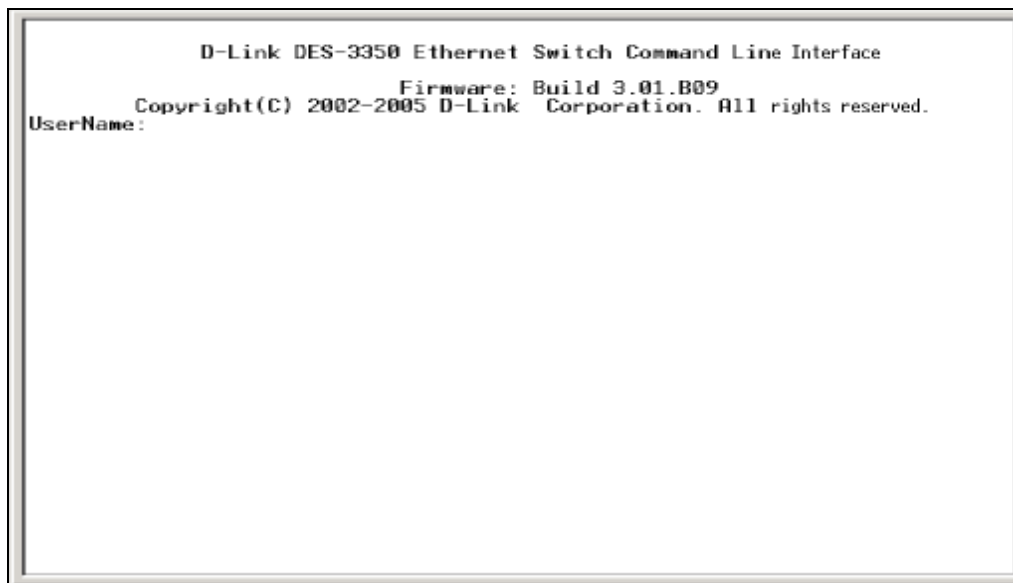
Accessing the Switch via the Serial Port

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.



```
D-Link DES-3350 Ethernet Switch Command Line Interface
Firmware: Build 3.01.B09
Copyright(C) 2002-2005 D-Link Corporation. All rights reserved.
UserName:

```

Figure 1-1. Initial CLI screen

There is no initial username or password. Just press the **Enter** key twice to display the CLI input cursor – **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 on the initial boot console screen – shown below.



```
Boot Procedure 1.00.002
-----
Power On Self Test ..... 100 %
MAC Address   : 00-01-02-03-04-00
H/W Version   : 0A1
Please wait, loading Runtime image ..... 100 %
```

Figure 1-2. Boot Screen

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

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

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

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

```
local>config ipif System ipaddress 10.58.44.221/8
Command: config ipif System ipaddress 10.58.44.221/8
Success.
local>
```

Figure 1-3. Assigning an IP Address

In the above example, the switch was assigned an IP address of 10.53.13.144/8 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.

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.



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

Connecting to the Switch

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

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

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

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

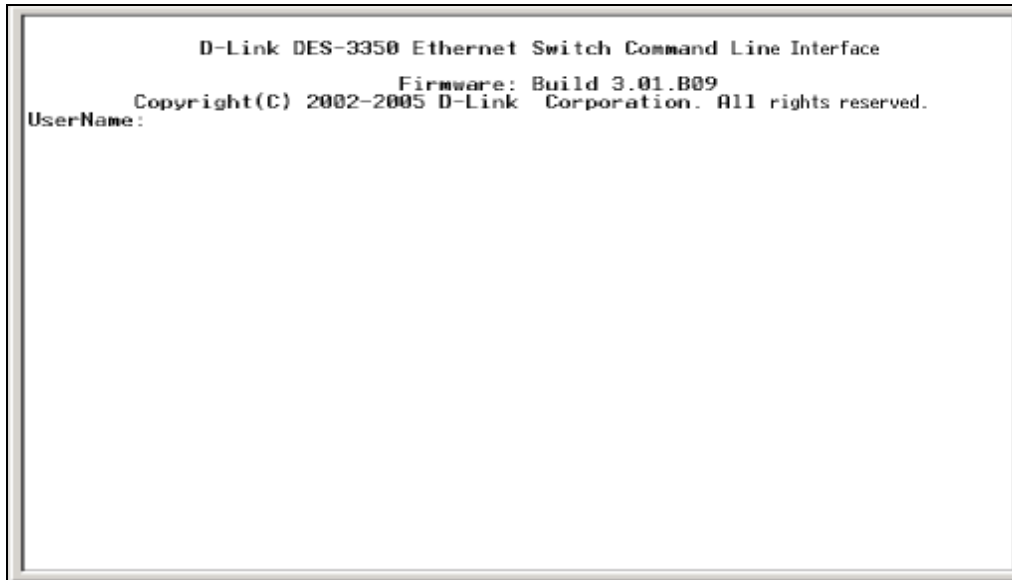


Figure 2-1. Initial Console Screen

Commands are entered at the command prompt, **local>** There are a number of helpful features included in the CLI. Entering the **?** command will display a list of all of the top-level commands.

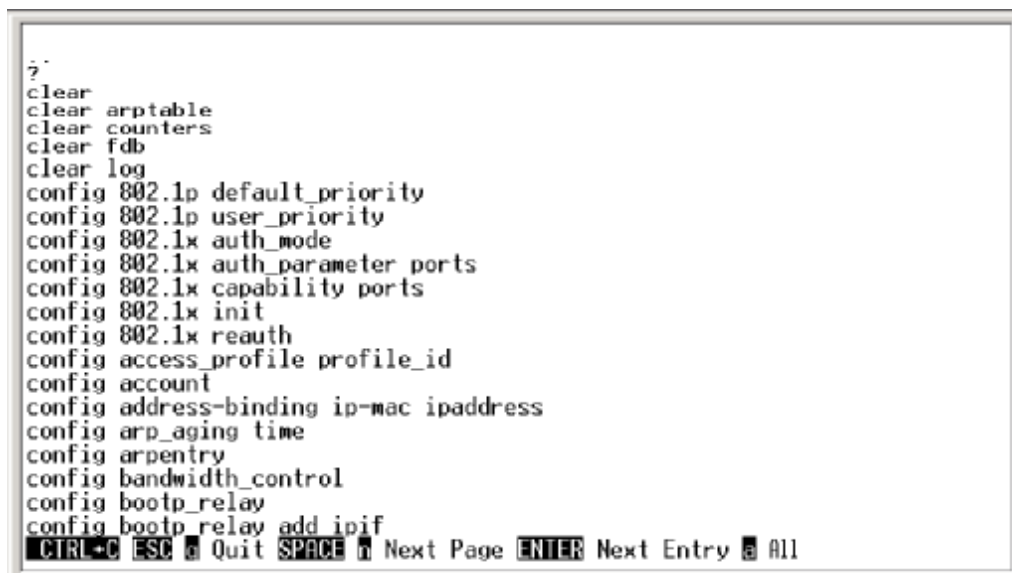


Figure 2-2. The ? Command

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

```
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.

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

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

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

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

Figure 2-5. The Next Available Commands Prompt

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

For example, if 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.lp 802.lx access_profile account address-binding arpentry bandwidth_
control bootp_relay command_history config dnsr dump error fdb garp igmp igmp_s
nooping ipfdb ipif ipmc iproute lacp_port link_aggregation log md5 mirror multic
ast_fdb ospf
  packet pim port_security ports power radius rip route router_ports sched
uling serial_port session snmp sntp stp switch time traffic traffic_segmentation
trusted_host utilization vlan
local>
```

Figure 2-6. Show Command

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

COMMAND SYNTAX

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



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

<angle brackets>	
Purpose	Encloses a variable or value that must be specified.
Syntax	create ipif <ipif_name> vlan <vlan_name 32> ipaddress <network_address>
Description	In the above syntax example, you must supply an IP interface name in the <ipif_name> space, a VLAN name in the <vlan_name 32> space, and the network address in the <network_address> space. Do not type the angle brackets.
Example Command	create ipif Engineering vlan Design ipaddress 10.24.22.5/255.0.0.0

[square brackets]	
Purpose	Encloses a required value or set of required arguments. One value or argument 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	show snmp [community detail]
Description	In the above syntax example, you must specify either community , or detail . Do not type the backslash.
Example Command	show snmp community

{braces}

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

Line Editing Key Usage	
Delete	Deletes the character under the cursor and then shifts the remaining characters in the line to the left.
Backspace	Deletes the character to the left of the cursor and shifts the remaining characters in the line to the left.
Left Arrow	Moves the cursor to the left.
Right Arrow	Moves the cursor to the right.
Up Arrow	Repeat the previously entered command. Each time the up arrow is pressed, the command previous to that displayed appears. This way it is possible to review the command history for the current session. Use the down arrow to progress sequentially forward through the command history list.
Down Arrow	The down arrow will display the next command in the command history entered in the current session. This displays each command sequentially as it was entered. Use the up arrow to review previous commands.
Tab	Shifts the cursor to the next field to the left.

Multiple Page Display Control Keys	
Space	Displays the next page.
CTRL+c	Stops the display of remaining pages when multiple pages are to be displayed.
ESC	Stops the display of remaining pages when multiple pages are to be displayed.
n	Displays the next page.
p	Displays the previous page.
q	Stops the display of remaining pages when multiple pages are to be displayed.
r	Refreshes the pages currently displayed.
a	Displays the remaining pages without pausing between pages.

Enter	Displays the next line or table entry.
-------	--

BASIC SWITCH COMMANDS

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

Command	Parameters
create account	[admin user] <username 15>
config account	<username>
show account	
delete account	<username>
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>
disable web	
save	
reboot	
reset	{{[config system]}}
login	
logout	

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

create account	
Purpose	Used to create user accounts
Syntax	create [admin user] <username 15>
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	<i>Admin <username></i> <i>User <username></i>

create account

Restrictions	Only Administrator-level users can issue this command. Usernames can be between 1 and 15 characters. Passwords can be between 0 and 15 characters.
---------------------	--

Example usage:

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

```

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

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

Success.

local>

```

config account

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

delete account

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 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       : 10.58.44.222 (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 3.01.B09
Hardware Version  : 0A1
System Up Time   : 0 days 00:49:27
Time             : Unknown
Time Source      : System Clock
System Name      :
System Location   :
System Contact    :
Spanning Tree    : Enabled
GVRP             : Disabled
IGMP Snooping    : Enabled
RIP              : Enabled
DVMRP           : Enabled
PIM-DM          : Enabled
OSPF            : Enabled
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.
Parameters	<p><i>baud_rate</i> [9600 19200 38400 115200] – The serial bit rate that will be used to communicate with the management host.</p> <p><i>auto logout</i> – This parameter will set the time that the switch will wait before logging out automatically, if left idle. The choices that accompany this parameter are:</p> <ul style="list-style-type: none"> § <i>never</i> – No time limit on the length of time the console can be open with no user input. § <i>2_minutes</i> – The console will log out the current user if there is no user input for 2 minutes. § <i>5_minutes</i> – The console will log out the current user if there is no user input for 5 minutes. § <i>10_minutes</i> – The console will log out the current user if there is no user input for 10 minutes. § <i>15_minutes</i> – The console will log out the current user if there is no user input for 15 minutes.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure baud rate:

```

local>config serial_port baud_rate 9600
Command: config serial_port baud_rate 9600

Success.

local>

```

enable clipaging

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

Example usage:

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

```

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 displays 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	<i><tcp_port_number 1-65535></i> - The TCP port number. TCP ports are numbered between 1 and 65535. The “well-known” TCP port for the Telnet protocol is 23.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable Telnet and configure port number:

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

Success.

local>
```

disable telnet

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

Example usage:

To disable the Telnet protocol on the switch:

```
local>disable telnet
Command: disable telnet

Success.

local>
```

enable web	
Purpose	Used to enable the HTTP-based management software on the switch.
Syntax	enable web <tcp_port_number 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	
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.

disable web

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

Example usage:

To disable HTTP:

```
local>disable web
Command: disable web

Success.

local>
```

save

Purpose	Used to save changes in the switch's configuration to non-volatile RAM.
Syntax	save
Description	This command is used to enter the current switch configuration into non-volatile RAM. The saved switch configuration will be loaded into the switch's memory each time the switch is restarted.
Parameters	Entering just the save command will save the switch configuration to NV-Ram
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 configurations to NV-RAM... Done

local>
```

reboot

Purpose	Used to restart the switch.
Syntax	reboot
Description	This command is used to restart the switch.

reboot

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><i>config</i> – If the keyword 'config' is specified, all of the factory default settings are restored on the switch including the IP address, user accounts, and the switch history log. The switch will not save or reboot.</p> <p><i>system</i> – If the keyword 'system' is specified all of the factory default settings are restored on the switch. The switch will save and reboot after the settings are changed to default. Rebooting will clear all entries in the Forwarding Data Base.</p> <p>If no parameter is specified, the switch's current IP address, user accounts, and the switch history log are not changed. All other parameters are restored to the factory default settings. The switch will not save or reboot.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
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
```

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 <desc 32> }
show ports	[all <portlist>] {description}

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



NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

config ports	
Purpose	Used to configure the Switch's Ethernet port settings.
Syntax	[<portlist> all] { speed [auto 10_half 10_full 100_half 100_full 1000_half 1000_full] state [enabled disabled] description <desc 32> }
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><portlist> – Specifies a port or range of ports to be configured.</p> <p><i>all</i> – Configure all ports on the switch.</p> <p><i>auto</i> – 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 [enable disable] – Enables or disables the specified range of ports.</p> <p>description <desc 32> - Enter an alphanumeric string of no more than 32 characters to describe a selected port interface.</p>
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 enable:

```
local>config ports 1-3 speed auto state enabled
Command: config ports 1-3 speed auto state enabled

Success.

local>
```

show ports

Purpose	Used to display the current configuration of a range of ports.
Syntax	show ports [all <portlist>] {description}
Description	This command is used to display the current configuration of a range of ports.
Parameters	<i>all</i> - specifies all the ports. <i><portlist></i> – Specifies a port or range of ports to be configured. <i>description</i> – Enter this parameter to view the description of the port previously set in the config ports command.
Restrictions	None.

Example usage:

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

```

local>Port Port  Settings  Connection
      State  Speed/Duplex 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      100M/Full
 6  Enabled  Auto      Link Down
 7  Enabled  Auto      Link Down
 8  Enabled  Auto      Link Down
 9  Enabled  Auto      Link Down
10  Enabled  Auto      Link Down
11  Enabled  Auto      Link Down
12  Enabled  Auto      Link Down
13  Enabled  Auto      Link Down
14  Enabled  Auto      Link Down
15  Enabled  Auto      100M/Full
16  Enabled  Auto      Link Down
17  Enabled  Auto      Link Down
18  Enabled  Auto      Link Down
19  Enabled  Auto      Link Down
20  Enabled  Auto      Link Down

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

```

Example usage:

To view port 1:1 with description

```

local> show ports 1-4 description
Command: show ports 1-4 description

Port Port  Settings  Connection
      State  Speed/Duplex Speed/Duplex
-----
 1  Enabled  Auto      Link Down
    Desc:
 2  Enabled  Auto      Link Down
    Desc:
 3  Enabled  Auto      Link Down
    Desc:
 4  Enabled  Auto      Link Down
    Desc:

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

```

PORT SECURITY COMMANDS

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

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

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



NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

config port_security ports	
Purpose	Used to configure port security settings.
Syntax	[<portlist> all] { admin_state [enabled disabled] max_learning_addr <max_lock_no 0-10> lock_address_mode [DeleteOnTimeout DeleteOnReset]}
Description	This command allows for the configuration of the port security feature. Only the ports listed in the <portlist> are effected.
Parameters	<p><portlist> – Specifies a port or range of ports to be configured.</p> <p>all – Configure port security for all ports on the switch.</p> <p>admin_state [enable disable] – Enables or disables port security for the listed ports.</p> <p>max_learning_addr <max_lock_no 0-10> - Use this to limit the number of MAC addresses dynamically listed in the FDB for the ports.</p> <p>lock_address_mode [DeleteOnTimeout DeleteOnReset] – Delete FDB dynamic entries for the ports on timeout of the FDB (see Forwarding Database Commands). Specify DeleteOnReset to delete all FDB entries, including static entries upon system reset or rebooting.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the port security:

```

local>config port_security ports 1-3 admin_state enabled
max_learning_addr 1 lock_address_mode DeleteOnTimeout

Command: config port_security ports 1-3 admin_state enabled
max_learning_addr 1lock_address_mode DeleteOnTimeout

Success.

local>

```

show port_security

Purpose	Used to display the current port security configuration.
Syntax	show port_security {ports <portlist>}
Description	This command is used to display port security information of the switch ports. The information displayed includes port security admin state, maximum number of learning address and lock mode.
Parameters	<portlist> – Specifies a port or range of ports to be viewed.
Restrictions	Only administrator-level can use this command.

Example usage:

To display the port security configuration:

```

local>show port_security ports
Command: show port_security ports

Port#  Admin State  Max. Learning Addr.  Lock Address Mode
----  -
15:1   Disabled      1                    DeleteOnReset
15:2   Disabled      1                    DeleteOnReset
15:3   Disabled      1                    DeleteOnReset
15:4   Disabled      1                    DeleteOnReset
15:5   Disabled      1                    DeleteOnReset
15:6   Disabled      1                    DeleteOnReset
15:7   Enabled       10                   DeleteOnReset
15:8   Disabled      1                    DeleteOnReset
15:9   Disabled      1                    DeleteOnReset
15:10  Disabled      1                    DeleteOnReset
15:11  Disabled      1                    DeleteOnReset
15:12  Disabled      1                    DeleteOnReset

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

```


NETWORK MANAGEMENT (SNMP) COMMANDS

The DES-3350SR supports the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. You can specify which version of the SNMP you want to use to monitor and control the switch. The three versions of SNMP vary in the level of security provided between the management station and the network device. The following table lists the security features of the three SNMP versions:

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

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

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

Command	Parameters
create snmp user	<username 32> <groupname 32> {encrypted [by_password auth [md5 <auth_password 8-16> sha <auth_password 8-20 >] priv [none des <priv_password 8-16>] by_key auth [md5 <auth_key 32-32> sha <auth_key 40-40>] priv [none des <priv_key 32-32>]}]}
delete snmp user	<username 32>
show snmp user	
create snmp view	<view_name 32> <oid> view_type [included excluded]
delete snmp view	<view_name 32> [all oid]
show snmp view	{<view_name 32>}
create snmp community	<community_string 32> view <view_name 32> [read_only read_write]
delete snmp community	<community_string 32>
show snmp community	{<community_string 32>}
config snmp engineID	<snmp_engineID>
show snmp engineID	

Command	Parameters
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>
show snmp groups	
create snmp host	<ipaddr> {v1 v2c v3 [noauth_nopriv auth_nopriv auth_priv]} <auth_string 32>
delete snmp host	<ipaddr>
show snmp host	{<ipaddr>}
create trusted_host	<ipaddr>
delete trusted_host	<ipaddr>
show trusted_host	{<ipaddr>}
enable snmp traps	
enable snmp authenticate traps	
disable snmp traps	
disable snmp authenticate traps	
config snmp system_contact	<sw_contact>
config snmp system_location	<sw_location>
config snmp system_name	<sw_name>
enable rmon	
disable rmon	

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

create snmp user

Purpose	Used to create a new SNMP user and adds the user to an SNMP group that is also created by this command.
Syntax	create snmp user <username 32> <groupname 32> {encrypted [by_password auth [md5 <auth_password 8-16> sha <auth_password 8-20>] priv [none des <priv_password 8-16>] by_key auth [md5 <auth_key 32-32> sha <auth_key 40-40>] priv [none des <priv_key 32-32>]}]}

create snmp user

Description	<p>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. SNMP ensures:</p> <p>Message integrity – Ensures that packets have not been tampered with during transit.</p> <p>Authentication – Determines if an SNMP message is from a valid source.</p> <p>Encryption – Scrambles the contents of messages to prevent it being viewed by an unauthorized source.</p>
Parameters	<p><i><username 32></i> – An alphanumeric name of up to 32 characters that will identify the new SNMP user.</p> <p><i><groupname 32></i> – An alphanumeric name of up to 32 characters that will identify the SNMP group the new SNMP user will be associated with.</p> <p><i>by_password</i> – Requires the SNMP user to enter a password for authentication and privacy. The password is defined by specifying the <i>auth_password</i> below. This method is recommended.</p> <p><i>by_key</i> - Requires the SNMP user to enter a encryption key for authentication and privacy. The key is defined by specifying the <i>priv_password</i> below. This method is not recommended.</p> <p><i>encrypted</i> – Specifies that the password will be in an encrypted format.</p> <p><i>auth [md5 sha]</i> – Initiate an authentication-level setting session.</p> <p> § <i>md5</i> – Specifies that the HMAC-MD5-96 authentication level will be used.</p> <p> § <i>sha</i> – Specifies that the HMAC-SHA-96 authentication level will be used.</p> <p><i><auth_password 8-20></i> – An alphanumeric string of between 8 and 20 characters that will be used to authorize the agent to receive packets for the host.</p> <p><i>des <priv_password 8-16></i> – 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.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create an SNMP user on the switch:


```

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

Success.

local>

```

delete snmp user

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

Example usage:

To delete a previously entered SNMP user on the switch:

```

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

Success.

local>

```

show snmp user

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

Example usage:

To display the SNMP users currently configured on the switch:

```

local>show snmp user
Command: show snmp user

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

Total Entries: 1

local>

```

create snmp view

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

Example usage:

To delete a previously configured SNMP view from the switch:

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

Success.

local>
```

show snmp view

Purpose	Used to display an SNMP view previously created on the switch.
Syntax	show snmp view {<view_name 32>}
Description	The show snmp view command displays an SNMP view previously created on the switch.
Parameters	<i><view_name 32></i> – An alphanumeric string of up to 32 characters that identifies the SNMP view that will be displayed.
Restrictions	Only administrator-level users can use this command.

Example usage:

To display SNMP view configuration:

```

local>show snmp view
Command: show snmp view

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

Total Entries: 11

local>

```

create snmp community

Purpose	<p>Used to create an SNMP community string to define the relationship between the SNMP manager and an agent. The community string acts like a password to permit access to the agent on the switch. One or more of the following characteristics can be associated with the community string:</p> <ul style="list-style-type: none"> An Access List of IP addresses of SNMP managers that are permitted to use the community string to gain access to the switch's SNMP agent. An MIB view that defines the subset of all MIB objects that will be accessible to the SNMP community. Read write or read-only level permission for the MIB objects accessible to the SNMP community.
Syntax	<pre>create snmp community <community_string 32> view <view_name 32> [read_only read_write]</pre>
Description	<p>The create snmp community command is used to create an SNMP community string and to assign access-limiting characteristics to this community string.</p>

create snmp community

Parameters	<p><i><community_string 32></i> – An alphanumeric string of up to 32 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the switch's SNMP agent.</p> <p><i><view_name 32></i> – An alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the switch.</p> <p><i>read_only</i> – Specifies that SNMP community members using the community string created with this command can only read the contents of the MIBs on the switch.</p> <p><i>read_write</i> – Specifies that SNMP community members using the community string created with this command can read from and write to the contents of the MIBs on the switch.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create the SNMP community string “dlink:”

```

local>create snmp community dlink view ReadView read_write
Command: create snmp community dlink view ReadView read_write

Success.

local>

```

delete snmp community

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

Example usage:

To delete the SNMP community string “dlink:”

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

Success.

local>
```

show snmp community

Purpose	Used to display SNMP community strings configured on the switch.
Syntax	show snmp community {<community_string 32>}
Description	The show snmp community command is used to display SNMP community strings that are configured on the switch.
Parameters	<i><community_string 32></i> – An alphanumeric string of up to 32 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the switch’s SNMP agent.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To display the currently entered SNMP community strings:

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

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

Total Entries: 3

local>
```

config snmp engineID

config snmp engineID

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

Example usage:

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

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

Success.

local>
```

show snmp engineID

Purpose	Used to display the identification of the SNMP engine on the switch.
Syntax	show snmp engineID
Description	The show snmp engineID command displays the identification of the SNMP engine on the switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

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

SNMP Engine ID : 0035636666

local>
```

create snmp group

Purpose	Used to create a new SNMP group, or a table that maps SNMP users to SNMP views.
Syntax	create snmp group <groupname 32> [v1 v2c v3 [noauth_nopriv auth_nopriv auth_priv]] {read_view <view_name 32> write_view <view_name 32> notify_view <view_name 32>}
Description	The create snmp group command creates a new SNMP group, or a table that maps SNMP users to SNMP views.

create snmp group

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

Example usage:

To create an SNMP group named “sg1:”

```

local>create snmp group sg1 v3 noauth_nopriv read_view v1
write_view v1 notify_view v1

Command: create snmp group sg1 v3 noauth_nopriv read_view v1
write_view v1 notify_view v1

Success.

local>

```

delete snmp group

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

Example usage:

To delete the SNMP group named “sg1”.

```

local>delete snmp group sg1

Command: delete snmp group sg1

Success.

local>

```

show snmp groups

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

show snmp groups

Restrictions Only administrator-level can use this command.

Example usage:

To display the currently configured SNMP groups on the switch:

```
local>show snmp groups
Command: show snmp groups

Vacm Access Table Settings

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

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

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

Total Entries: 10

local>
```

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

Example usage:

To create an SNMP host to receive SNMP messages:

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

Success.

local>
```

delete snmp host

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

Example usage:

To delete an SNMP host entry:

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

Success.

local>
```

show snmp host

Purpose	Used to display the recipient of SNMP traps generated by the switch's SNMP agent.
Syntax	show snmp host {<ipaddr>}
Description	The show snmp host command is used to display the IP addresses and configuration information of remote SNMP managers that are designated as recipients of SNMP traps that are generated by the switch's SNMP agent.
Parameters	<i><ipaddr></i> – The IP address of a remote SNMP manager that will receive SNMP traps generated by the switch's SNMP agent.

show snmp host

Restrictions	Only administrator-level can use this command.
--------------	--

Example usage:

To display the currently configured SNMP hosts on the switch:

```

local>show snmp host
Command: show snmp host

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

Total Entries: 2

local>

```

create trusted_host

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

Example usage:

To create the trusted host:

```

local>create trusted_host 10.48.74.121
Command: create trusted_host 10.48.74.121

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 {<ipaddr>}
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	Only administrator-level can use this command.

Example Usage:

To display the list of trust hosts:

```

local>show trusted_host
Command: show trusted_host

Management Stations

IP Address
-----
10.53.13.94

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.

delete trusted_host

Parameters	<i><ipaddr></i> – The IP address of the trusted host.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete a trusted host with an IP address 10.48.74.121:

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

Success.

local>
```

enable snmp traps

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

Example usage:

To enable SNMP trap support on the switch:

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

Success.

local>
```

enable snmp authenticate_traps

Purpose	Used to enable SNMP authentication trap support.
Syntax	enable snmp authenticate_traps
Description	This command is used to enable SNMP authentication trap support on the Switch.

enable snmp authenticate_traps

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 traps

Purpose	Used to disable SNMP trap support on the switch.
Syntax	disable 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>
```

disable snmp authenticate_traps

Purpose	Used to disable SNMP authentication trap support.
Syntax	disable snmp authenticate_traps

disable snmp authenticate_traps

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

Example Usage:

To disable the SNMP authentication trap support:

```
local>disable snmp authenticate_traps
Command: disable snmp authenticate_traps

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	The config snmp system_contact command is used to enter the name and/or other information to identify a contact person who is responsible for the switch. A maximum of 255 character can be used.
Parameters	<sw_contact> - A maximum of 255 characters is allowed. A NULL string is accepted if there is no contact.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
local>config snmp system_contact MIS Department II
Command: config snmp system_contact MIS Department II

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	The config snmp system_location 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 maximum of 255 characters is allowed. A NULL string is accepted if there is no location desired.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
local>config snmp system_location HQ 5F
Command: config snmp system_location HQ 5F

Success.

local>
```

config snmp system_name

Purpose	Used to configure the name for the switch.
Syntax	config snmp system_name <sw_name>
Description	The config snmp system_name command configures the name of the switch.
Parameters	<sw_name> - A maximum of 255 characters is allowed. A NULL string is accepted if no name is desired.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
local>config snmp system_name DES-3350SR Stackable Switch
Command: config snmp system_name DES-3350SR Stackable Switch

Success.

local>
```

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

Example Usage:

To enable RMON:

```
local>enable rmon
Command: enable rmon

Success.

local>
```

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

Example Usage:

To disable RMON:

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

SWITCH UTILITY COMMANDS

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

Command	Parameters
download	[firmware <ipaddr> <path_filename 127> configuration <ipaddr> <path_filename 127> {increment}]
upload	[configuration log] <ipaddr> <path_filename 127>
ping	<ipaddr> {times <value 1-255>} {timeout <sec 1-99>}
tracert	<ipaddr> {ttl <value 1-60> port <value 30000-64900> timeout <sec 1-65535> probe <value <1-9>

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	[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><i>firmware</i> – Download and install new firmware on the switch from a TFTP server.</p> <p><i>configuration</i> - Download a switch configuration file from a TFTP server.</p> <p><i><ipaddr></i> – The IP address of the TFTP server.</p> <p><i><path_filename></i> – The DOS path and filename of the firmware or switch configuration file on a TFTP server. For example, C:\3226S.had.</p> <p><i>increment</i> – 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-level users can issue this command.

Example usage:

To download a configuration file:

```

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	[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><i>configuration</i> – Specifies that the switch's current settings will be uploaded to the TFTP server.</p> <p><i>log</i> – Specifies that the switch's current log will be uploaded to the TFTP server.</p> <p><i><ipaddr></i> – The IP address of the TFTP server. The TFTP server must be on the same IP subnet as the switch.</p> <p><i><path_filename 127></i> – Specifies the location of the switch configuration file on the TFTP server. This file will be replaced by the uploaded file from the switch.</p>
Restrictions	The TFTP server must be on the same IP subnet as the switch. Only administrator-level users can issue this command.

Example usage:

To upload a configuration file:

```

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>

```

ping

Purpose	Used to test the connectivity between network devices.
---------	--

ping

Syntax	ping <ipaddr> {times <value 1-255>} {timeout <sec 1-99>}
Description	The ping command sends Internet Control Message Protocol (ICMP) echo messages to a remote IP address. The remote IP address will then “echo” or return the message. This is used to confirm connectivity between the switch and the remote device.
Parameters	<p><i><ipaddr></i> - Specifies the IP address of the host.</p> <p><i>times <value 1-255></i> - The number of individual ICMP echo messages to be sent. The maximum value is 255. The default is 0.</p> <p><i>timeout <sec 1-99></i> - Defines the time-out period while waiting for a response from the remote device. A value of 1 to 99 seconds can be specified. The default is 1 second.</p> <p>Pinging an IP address without the <i>times</i> parameter will ping the target device an infinite amount of times.</p>
Restrictions	None.

Example usage:

To ping the IP address 10.48.74.121 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>

```

tracert

Purpose	Used to trace the routed path between the switch and a destination endstation.
Syntax	<ipaddr> {ttl <value 1-60> port <value 30000-64900> timeout <sec 1-65535> probe <value <1-9>
Description	The tracert command allows you to trace a route between the switch and a give host on the network.

traceroute

Parameters	<p><i><ipaddr></i> - Specifies the IP address of the host.</p> <p><i>tll <value 1-60></i> - 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.</p> <p><i>port <value 30000-64900></i> The port number. Must be above 1024. The value range is from 30000 to 64900 .</p> <p><i>timeout <sec 1-65535></i>- Defines the time-out period while waiting for a response from the remote device. The user may choose an entry between 1 and 65535 seconds.</p> <p><i>probe <value 1-9></i> - The probe value is the number of times the switch will send probe packets to the next hop on the intended traceroute path. The default is 1.</p>
Restrictions	None.

Example usage:

To 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 <10ms 10.254.254.251
 2 <10ms 10.55.25.35
 3 <10ms 10.22.35.1

local>
```

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}
clear counters	ports <portlist>
clear log	
show log	index <value>

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



NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

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

Example usage:

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

```
local>show packet port 2:7
```

```
Port number : 2:7
```

Frame Size	Frame Counts	Frames/sec	Frame Type	Total	Total/sec
-----	-----	-----	-----	-----	-----
64	3275	10	RX Bytes	408973	1657
65-127	755	10	RX Frames	4395	19
128-255	316	1			
256-511	145	0	TX Bytes	7918	178
512-1023	15	0	TX Frames	111	2
1024-1518	0	0			
Unicast RX	152	1			
Multicast RX	557	2			
Broadcast RX	3686	16			

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

show error ports

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

Example usage:

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

```
local>show errors port 1:3
```

```
Port number 1:3
```

Error Type	RX Frames	Error Type	TX Frames
CRC Error	19	Excessive Deferral	0
Undersize	0	CRC Error	0
Oversize	0	Late Collision	0
Fragment	0	Excessive Collision	0
Jabber	11	Single Collision	0
Drop Pkts	20837	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]
Description	This command will display the real-time port and cpu utilization statistics for the switch.
Parameters	<i>cpu</i> – Entering this parameter will display the current cpu utilization of the switch, as a percentage.
Restrictions	None.

To display the current cpu utilization:

```
local>show utilization cpu
```

```
Command: show utilization cpu
```

```
CPU utilization :
```

```
-----
```

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

```
local>
```

clear counters

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 port or range of ports to be configured.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To clear the counters:

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

Success.

local>
```

clear log

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

Example usage:

To clear the log information:

```
local>clear log
Command: clear log

Success.

local>
```

show log

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	<i>index <value></i> – Enter a value that corresponds to an entry made in the log. Multiple entries may be made in the form of x-x where x is the number of an entry in the log. The smallest number (and therefore the earlier entry) will be first.
Restrictions	None.

Example usage:

To display the switch history log:

```

local>show log index 1-4
Command: show log index 1-4

Index  Time      Log Text
-----  -
4      01:54:53  Port 1:13 link up, 100Mbps FULL duplex
3      01:54:53  Spanning Tree Protocol is enabled
2      01:54:53  Unit 1, System started up
1      06:06:09  Spanning Tree Protocol is disabled

local>

```

SPANNING TREE COMMANDS

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

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

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



NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

config stp

Purpose	Used to setup STP and RSTP on the switch.
Syntax	config stp {maxage <value 6-40> hellotime <value 1-10> forwarddelay <value 4-30> priority <value 0-61440> version [rstp stp] txholdcount <value 1-10> fbpdu [enable disable]}
Description	This command is used to setup the Spanning Tree Protocol (STP) for the entire switch.

config stp

Parameters	<p><i>maxage</i> <value 6-40> – The maximum amount of time (in seconds) that the switch will wait to receive a BPDU packet before reconfiguring STP. The user may choose a time between 6 and 40 seconds. The default is 20 seconds.</p> <p><i>hellotime</i> <value 1-10> – The time interval between transmission of configuration messages by the root device. The user may choose a time between 1 and 10 seconds. The default is 2 seconds.</p> <p><i>forwarddelay</i> <value 4-30> – The maximum amount of time (in seconds) that the root device will wait before changing states. The user may choose a time between 4 and 30 seconds. The default is 15 seconds.</p> <p><i>priority</i> <value 0-61440> – A numerical value between 0 and 61440 that is used in determining the root device, root port, and designated port. The device with the highest priority becomes the root device. The lower the numerical value, the higher the priority. The default is 32,768.</p> <p><i>version</i> [<i>rstp</i> <i>stp</i>] - Select the Spanning Tree Protocol version used for the switch.</p> <ul style="list-style-type: none"> • <i>stp</i> – Select this parameter for IEEE 802.1d STP and for IEEE 802.1w STP compatibility mode. • <i>rstp</i> - Select this parameter for IEEE 802.1w Rapid STP mode. <p><i>fbpdu</i> [<i>enable</i> <i>disable</i>] – Allows the forwarding of STP BPDU packets from other network devices when STP is disabled on the switch. The default is enabled.</p> <p><i>txholdcount</i> <1-10> - The maximum number of Hello packets transmitted per interval. Default value = 3.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure STP with maxage 18 and hellotime 4:

```

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

Success.

local>

```

config stp ports

config stp ports

Purpose	Used to setup STP on the port level.
Syntax	config stp ports <portlist> {cost [auto <value 1-200000000>] priority <value 0-240> migrate [yes no] edge [true false] p2p [true false auto] state [enable disable]}
Description	This command is used to create and configure STP for a group of ports.

config stp ports

Parameters	<p><i>cost</i> – This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set in the following two ways:</p> <p>§ <i>auto</i> – Setting this parameter for the cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. Default port cost: 100Mbps port = 200000. Gigabit port = 20000.</p> <p>§ <i><value 1-200000000></i> - Define a value between 1 and 200000000 to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets.</p> <p>Default port cost: 100Mbps port = 200000 Gigabit port = 20000</p> <p><i>priority <value 0-240></i> – Port Priority can be from 0 to 240. The lower the number, the greater the probability the port will be chosen as the Root Port. Default = 128.</p> <p><i><portlist></i> – Specifies a port or range of ports to be configured.</p> <p><i>migrate [yes no]</i> – <i>yes</i> 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 (<i>yes</i>) on ports connected to network stations or segments that will be upgraded to 802.1w RSTP on all or some portion of the segment.</p> <p><i>edge [true false]</i> – <i>true</i> 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. <i>false</i> indicates that the port does not have edge port status.</p> <p><i>p2p [true false auto]</i> – <i>true</i> indicates a point-to-point (P2P) shared link. P2P ports are similar to edge ports however they are restricted in that a P2P port must operate in full-duplex. Like edge ports, P2P ports transition to a forwarding state rapidly thus benefiting from RSTP. A <i>p2p</i> value of <i>false</i> indicates that the port cannot have <i>p2p</i> status. <i>auto</i> allows the port to have <i>p2p</i> status whenever possible and operate as if the <i>p2p</i> status were <i>true</i>. If the port cannot maintain this status (for example if the port is forced to half-duplex operation) the <i>p2p</i> status changes to operate as if the <i>p2p</i> value were <i>false</i>.</p> <p><i>state [enable disable]</i> – Allows STP to be enabled or disabled for the ports specified in the port list. The default is disabled.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure STP with path cost set at auto, priority 16, and state enabled for ports 1-5 of module 1.

```

local> config stp ports 1-4 cost auto state enabled
Command: config stp ports 1-4 cost auto state enabled

Success.

local>

```

enable stp

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

Example usage:

To enable STP, globally, on the switch:

```

local>enable stp
Command: enable stp

Success.

local>

```

disable stp

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

Example usage:

To disable STP on the switch:

```
local>disable stp
Command: disable stp

Success.

local>
```

show stp

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

Example usage:

To display the status of STP on the switch:

Status 1: STP enabled with STP compatible version

```
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: 00-01-02-03-04-00
Root Priority    : 32768
Cost to Root    : 0
Root Port       : None
Last Topology Change : 140sec
Topology Changes Count: 66
Protocol Specification : 3
Max Age         : 20
Hello Time      : 2
Forward Delay   : 15
Hold Time       : 3
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

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

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 port or range of ports to be configured.
Restrictions	None

Example usage:

To display STP state of ports 1-4:

```
local> local>show stp ports 1-4
Command: show stp ports 1-4
```

Port	Designated	Bridge	State	Cost	Pri	Edge	P2P	Status	Role
-----	-----	-----	---	-----	---	---	---	-----	-----
1	N/A		Yes	*200000	0	No	Yes	Disabled	Disabled
2	N/A		Yes	*200000	0	No	Yes	Disabled	Disabled
3	N/A		Yes	*200000	0	No	Yes	Disabled	Disabled
4	N/A		Yes	*200000	0	No	Yes	Disabled	Disabled

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

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>
config fdb aging_time	<sec 10-1000000>
delete fdb	<vlan_name 32> <macaddr>
clear fdb	[vlan <vlan_name 32> port <port> all]
show multicast_fdb	{vlan <vlan_name 32> mac_address <macaddr>}
show fdb	{port <port> vlan <vlan_name 32> mac_address <macaddr> static aging_time}
show ipfdb	<ipaddr>

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



NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

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

Example usage:

To create a unicast MAC FDB entry:

```
local>create fdb default 00-00-00-00-01-02 port 2:5
Command: create fdb default 00-00-00-00-01-02 port 2:5

Success.

local>
```

create multicast_fdb

Purpose	Used to create a static entry to the multicast MAC address forwarding table (database)
Syntax	create multicast_fdb <vlan_name 32> <macaddr>
Description	This command will make an entry into the switch's multicast MAC address forwarding database.
Parameters	<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 create multicast MAC forwarding:

```
local>create multicast_fdb default 01-00-00-00-00-01
Command: create multicast_fdb default 01-00-00-00-00-01

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.

config multicast_fdb

Parameters	<p><i><vlan_name 32></i> – The name of the VLAN on which the MAC address resides.</p> <p><i><macaddr></i> – The MAC address that will be added to the multicast forwarding table.</p> <p><i>[add delete]</i> – Add will add ports to the forwarding table. Delete will remove ports from the multicast forwarding table.</p> <p>§ <i><portlist></i> – Specifies a port or range of ports to be configured.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To add multicast MAC forwarding:

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

Success.

local>
```

config fdb aging_time

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

Example usage:

To set the fdb aging time:

```
local>config fdb aging_time 300
Command: config fdb aging_time 300

Success.

local>
```

delete fdb

Purpose	Used to delete an entry to the switch's forwarding database.
Syntax	delete fdb <vlan_name 32> <macaddr>
Description	This command is used to delete a previous entry to the switch's MAC address forwarding database.
Parameters	<p><vlan_name 32> – The name of the VLAN on which the MAC address resides.</p> <p><macaddr> – The MAC address that will be deleted from 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>
```

Example usage:

To delete a multicast fdb entry:

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

Success.

local>
```

clear fdb

Purpose	Used to clear the switch's forwarding database of all dynamically learned MAC addresses.
Syntax	clear fdb [vlan <vlan_name 32> port <port> all]
Description	This command is used to clear dynamically learned entries to the switch's forwarding database.
Parameters	<p><i>vlan <vlan_name 32></i> – The name of the VLAN on which the MAC address resides.</p> <p><i>port <port></i> – The port number corresponding to the MAC destination address. The switch will always forward traffic to the specified device through this port.</p> <p><i>all</i> – 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><i><vlan_name 32></i> – The name of the VLAN on which the MAC address resides.</p> <p><i><macaddr></i> – The MAC address that is present in the forwarding database 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   : 1:1-1:5,1:12
Mode           : Static

Total Entries  : 1

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	<p><i>port <port></i> – The port number corresponding to the MAC destination address. The switch will always forward traffic to the specified device through this port.</p> <p><i><vlan_name 32></i> – The name of the VLAN on which the MAC address resides.</p> <p><i><macaddr></i> – The MAC address that is present in the forwarding database table.</p> <p><i>static</i> – Displays the static MAC address entries.</p> <p><i>aging_time</i> – Displays the aging time for the MAC address forwarding database.</p>
Restrictions	None.

Example usage:

To display unicast MAC address table:

```

local>show fdb
Command: show fdb

Unicast MAC Address Aging Time = 300

VID  VLAN Name      MAC Address          Port    Type
---  -
1    default        00-00-39-34-66-9A   10     Dynamic
1    default        00-00-51-43-70-00   10     Dynamic
1    default        00-00-5E-00-01-01   10     Dynamic
1    default        00-00-74-60-72-2D   10     Dynamic
1    default        00-00-81-05-00-80   10     Dynamic
1    default        00-00-81-05-02-00   10     Dynamic
1    default        00-00-81-48-70-01   10     Dynamic
1    default        00-00-E2-4F-57-03   10     Dynamic
1    default        00-00-E2-61-53-18   10     Dynamic
1    default        00-00-E2-6B-BC-F6   10     Dynamic
1    default        00-00-E2-7F-6B-53   10     Dynamic
1    default        00-00-E2-82-7D-90   10     Dynamic
1    default        00-00-F8-7C-1C-29   10     Dynamic
1    default        00-01-02-03-04-00   CPU    Self
1    default        00-01-02-03-04-05   10     Dynamic
1    default        00-01-30-10-2C-C7   10     Dynamic
1    default        00-01-30-FA-5F-00   10     Dynamic
1    default        00-02-3F-63-DD-68   10     Dynamic
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All

```

show ipfdb

Purpose	Used to display the current IP address forwarding database table.
Syntax	show ipfdb <ipaddr>
Description	This command will display the current contents of the switch's IP forwarding database.
Parameters	<i>ip_address <ipaddr></i> - Use this parameter to view the table by an IP address entered here.
Restrictions	None.

Example usage:

To view the IP forwarding database table:

```
local>show ipfdb
```

```
Command: show ipfdb
```

```
Interface  IP Address  Port  Learned
```

```
-----  
System    10.0.0.178   15   Dynamic  
System    10.0.0.183   15   Dynamic  
System    10.0.25.1    15   Dynamic  
System    10.0.34.1    15   Dynamic  
System    10.0.46.1    15   Dynamic  
System    10.0.58.4    15   Dynamic  
System    10.1.1.1     15   Dynamic  
System    10.1.1.101   15   Dynamic  
System    10.1.1.151   15   Dynamic  
System    10.1.1.152   15   Dynamic  
System    10.1.1.157   15   Dynamic  
System    10.1.1.161   15   Dynamic  
System    10.1.1.164   15   Dynamic  
System    10.1.1.173   15   Dynamic  
System    10.1.1.191   15   Dynamic  
System    10.1.1.254   15   Dynamic  
System    10.1.49.1    15   Dynamic  
System    10.1.49.5    15   Dynamic  
System    10.1.49.9    15   Dynamic  
System    10.1.49.15   15   Dynamic
```

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

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 [enable disable] multicast [enable disable] dlf [enable disable] threshold <value 0-255> }
show traffic control	{group_list <storm_grouplist>}

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



NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

config traffic control

Purpose	Used to configure broadcast/multicast traffic control.
Syntax	config traffic control [<storm_grouplist> all] { broadcast [enable disable] multicast [enable disable] dlf [enable disable] threshold <value 0-255>}
Description	This command is used to configure broadcast storm control.
Parameters	<p><i><storm_grouplist></i> – Used to specify a broadcast storm control group. This is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the 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, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.</p> <p><i>all</i> – Specifies all broadcast storm control groups on the switch.</p> <p><i>broadcast</i> [enable disable] – Enables or disables broadcast storm control.</p> <p><i>multicast</i> [enable disable] – Enables or disables multicast storm control.</p> <p><i>dlf</i> [enable disable] – Enables or disables dlf traffic control.</p> <p><i>threshold</i> <value 0-255> – The upper threshold at which the specified traffic control is switched on. The <value> is the number of broadcast / multicast / dlf packets, in Kbps, received by the switch that will trigger the storm traffic control measures.</p>

config traffic control

Restrictions Only administrator-level users can issue this command.

Example usage:

To configure traffic control and enable broadcast storm control system wide:

```
local>config traffic control all broadcast enable
Command: config traffic control all broadcast enable

Success.

local>
```

show traffic control

Purpose	Used to display current traffic control settings.
Syntax	show traffic control {group_list <storm_grouplist>}
Description	This command displays the current storm traffic control configuration on the switch.
Parameters	<i>group_list <storm_grouplist></i> – Used to specify a broadcast storm control group. This is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the 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, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.
Restrictions	None.

Example usage:

To display traffic control setting:


```
local>show traffic control
Command: show traffic control
Traffic Control
                Broadcast Multicast Destination
Group [ports] Threshold Storm    Storm    Lookup Fail
-----
1 [ 1 - 8 ]    128      Disabled Disabled Disabled
2 [ 9 - 16]    128      Disabled Disabled Disabled
3 [17 - 24]    128      Disabled Disabled Disabled
4 [25 - 32]    128      Disabled Disabled Disabled
5 [33 - 40]    128      Disabled Disabled Disabled
6 [41 - 48]    128      Disabled Disabled Disabled
7 [ 49  ]     128      Disabled Disabled Disabled
8 [ 50  ]     128      Disabled Disabled Disabled

Total Entries: 8

local>
```

QoS COMMANDS

The DES-3350SR switch supports 802.1p priority queuing. The Switch has five hardware priority queues, one of which is internal and not configurable. These hardware priority queues are numbered from 7 (Class 7) — the highest hardware priority queue — to 0 (Class 0) — the lowest hardware priority queue. The eight priority tags specified in IEEE 802.1p (p0 to p7) are mapped to the switch's hardware priority queues as follows:

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

For strict priority-based scheduling, any packets residing in the higher priority queues are transmitted first. Multiple strict priority queues empty based on their priority tags. Only when these queues are empty, are packets of lower priority transmitted.

For round-robin queuing, the number of packets sent from each priority queue depends upon the assigned weight. For a configuration of 8 CoS queues, A~H with their respective weight value: 8~1, the packets are sent in the following sequence: A1, B1, C1, D1, E1, F1, G1, H1, A2, B2, C2, D2, E2, F2, G2, A3, B3, C3, D3, E3, F3, A4, B4, C4, D4, E4, A5, B5, C5, D5, A6, B6, C6, A7, B7, A8, A1, B1, C1, D1, E1, F1, G1, H1.

For round-robin queuing, if each CoS queue has the same weight value, then each CoS queue has an equal opportunity to send packets just like round-robin queuing.

For round-robin queuing, if the weight for a CoS is set to 0, then it will continue processing the packets from this CoS until there are no more packets for this CoS. The other CoS queues that have been given a nonzero value, and depending upon the weight, will follow a common round-robin scheme.

Remember that the switch has 4 priority queues (and eight Classes of Service) for each port on the Switch.

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



NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

Command	Parameters
config bandwidth_control	<portlist>{rx_rate [no_limit <value 1-1000>] tx_rate [no_limit <value 1-1000>]}

Command	Parameters
show bandwidth_control	{<portlist>}
config 802.1p user_priority	{<priority 0-7> <class_id 0-3>}
show 802.1p user_priority	
config 802.1p default_priority	[<portlist> all] <priority 0-7>
show 802.1p default_priority	{<portlist> all}
show scheduling	show scheduling
config scheduling	<class_id 0-3> { max_packet <value 0-255> max_latency <value 0-255> }

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

config bandwidth_control	
Purpose	Used to configure bandwidth control on a by-port basis.
Syntax	<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	<p><i><portlist></i> – Specifies a port or range of ports to be configured.</p> <p><i>all</i> – Choose this parameter to select all configurable ports.</p> <p><i>rx_rate</i> – Specifies that one of the parameters below (<i>no_limit</i> or <i><value 1-1000></i>) will be applied to the rate at which the above specified ports will be allowed to receive packets</p> <p>§ <i>no_limit</i> – Specifies that there will be no limit on the rate of packets received by the above specified ports.</p> <p>§ <i><value 1-1000></i> – Specifies the packet limit, in Mbps, that the above ports will be allowed to receive.</p> <p><i>tx_rate</i> – Specifies that one of the parameters below (<i>no_limit</i> or <i><value 1-1000></i>) will be applied to the rate at which the above specified ports will be allowed to transmit packets.</p> <p>§ <i>no_limit</i> – Specifies that there will be no limit on the rate of packets received by the above specified ports.</p> <p>§ <i><value 1-1000></i> – Specifies the packet limit, in Mbps, that the above ports will be allowed to receive.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure bandwidth control:

```
local> config bandwidth_control 1-4 rx_rate no_limit
Command: config bandwidth_control 1-4 rx_rate no_limit

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	<p><i><portlist></i> – Specifies a port or range of ports to be configured.</p> <p>Using this command without adding a portlist entry will show the bandwidth control for all ports in the switch stack.</p>
Restrictions	None.

Example usage:

To display bandwidth control settings:

```

local> show bandwidth_control
Command: show bandwidth_control

Bandwidth Control Table

Port  RX Rate (Mbit/sec) TX_RATE (Mbit/sec)
-----
1    no_limit           no_limit
2    no_limit           no_limit
3    no_limit           no_limit
4    no_limit           no_limit
5    no_limit           no_limit
6    no_limit           no_limit
7    no_limit           no_limit
8    no_limit           no_limit
9    no_limit           no_limit
10   no_limit           no_limit
11   no_limit           no_limit
12   no_limit           no_limit
13   no_limit           no_limit
14   no_limit           no_limit
15   no_limit           no_limit
16   no_limit           no_limit
17   no_limit           no_limit
18   no_limit           no_limit

local>

```

config 802.1p user_priority

Purpose Used to map the 802.1p user priority tags of an incoming packet to one of the eight 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 The **config 802.1p user_priority** command is used to configure the way the switch will map an incoming packet, based on its 802.1p user priority tag, to one of the eight hardware priority queues available on the switch. The switch's default is to map the incoming 802.1p priority values to the eight hardware priority queues according to the following chart:

802.1p Switch Hardware

Value Priority Queue

-----	-----
0	1
1	0
2	0
3	1
4	2
5	2
6	3
7	3

Parameters *<priority 0-7>* – Specifies which of the eight 802.1p priority tags (0 through 7) you want to map to one of the switch's hardware priority queues (*<class_id>*, 0 through 3).

<class_id 0-3> – Specifies which of the switch's hardware priority queues the 802.1p priority tags (specified above) will be mapped to.

Restrictions Only administrator-level users can issue this command.

Example usage:

To configure 802.1p user priority on the switch:

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

Success.

local>
```

show 802.1p user_priority

show 802.1p user_priority

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

Example usage:

To show 802.1p user priority:

```

local> show 802.1p user_priority
Command: show 802.1p user_priority

QOS Class of Traffic

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

local>

```

config 802.1p default_priority

Purpose	Used to specify default priority settings on the switch. Untagged packets that are received by the switch will be assigned a priority tag in its priority field using this command.
Syntax	config 802.1p default_priority [<portlist> all] <priority 0-7>
Description	The config 802.1p default_priority command allows you to specify the 802.1p priority value an untagged, incoming packet will be assigned before being forwarded to its destination.

config 802.1p default_priority

Parameters	<p><i><portlist></i> – Specifies a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the 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, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.</p> <p><i>all</i> – Specifies that the config 802.1p default_priority command will be applied to all ports on the switch.</p> <p><i><priority 0-7></i> – Specifies the 802.1p priority tag that an untagged, incoming packet will be given before being forwarded to its destination.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure 802.1p default priority on the switch:

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

Example usage:

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

```

local> 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

local>

```

show scheduling

show scheduling

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

Example Usage:

To show the scheduling:

```

local>show scheduling
Command: show scheduling

QOS Output Scheduling

      MAX. Packets MAX. Latency
      -----
Class-0  0           0
Class-1  0           0
Class-2  0           0
Class-3  0           0

local>

```

config scheduling

Purpose	Used to configure QOS output scheduling.
Syntax	config scheduling <class_id 0-3> { max_packet <value 0-255> max_latency <value 0-255> }
Description	This command will config QOS output scheduling in use on the switch.
Parameters	None.
Restrictions	None.

Example Usage:

To show the scheduling:

```
local> config scheduling 0 max_packet 2 max_latency 3
Command: config scheduling 0 max_packet 2 max_latency 3

Success.

local>
```

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.



NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

config mirror port

Purpose	Used to configure a mirror port – source port pair on the switch.
Syntax	config mirror port <port> add source ports <portlist> [rx tx both]
Description	This command allows a range of ports to have all of their traffic also sent to a designated port, where a network sniffer or other device can monitor the network traffic. In addition, you can specify that only traffic received by or sent by one or both is mirrored to the Target port.
Parameters	<p><i>port <port></i> – This specifies the Target port (the port where mirrored packets will be sent).</p> <p><i>add source ports</i> – The port or ports being mirrored. This cannot include the Target port.</p> <p>§ <i><portlist></i> – This specifies a range of ports that will be mirrored. That is, the range of ports in which all traffic will be copied and sent to the Target port.</p> <p>§ <i>rx</i> – Allows the mirroring of only packets received by (flowing into) the port or ports in the port list.</p> <p><i>tx</i> – Allows the mirroring of only packets sent to (flowing out of) the port or ports in the port list.</p> <p><i>both</i> – Mirrors all the packets received or sent by the port or ports in the port list.</p>

config mirror port

Restrictions	The Target port cannot be listed as a source port. Only administrator-level users can issue this command.
--------------	---

Example usage:

To add the mirroring ports:

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

Success.

local>
```

config mirror delete

Purpose	Used to delete a port mirroring configuration.
Syntax	config mirror port <port> delete source port <portlist> [rx tx both]
Description	This command is used to delete a previously entered port mirroring configuration.
Parameters	<p><i>port <port></i> – This specifies the Target port (the port where mirrored packets will be sent).</p> <p><i>delete source port</i> – Adding this parameter will delete source ports according to ports entered using the <i><portlist></i>.</p> <p>§ <i><portlist></i> – This specifies a range of ports that will be mirrored. That is, the range of ports in which all traffic will be copied and sent to the Target port.</p> <p>§ <i>rx</i> – Allows the mirroring of only packets received by (flowing into) the port or ports in the port list.</p> <p><i>tx</i> – Allows the mirroring of only packets sent to (flowing out of) the port or ports in the port list.</p> <p><i>both</i> – Mirrors all the packets received or sent by the port or ports in the port list.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete the mirroring ports:

```

local>config mirror port 1:5 delete source port 1:1-1:5 both
Command: config mirror 1:5 delete source 1:1-1:5 both

Success.

local>

```

enable mirror

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

Example usage:

To enable mirroring configurations:

```

local>enable mirror
Command: enable mirror

Success.

local>

```

disable mirror

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

Example usage:

To disable mirroring configurations:

```
local>disable mirror
Command: disable mirror

Success.

local>
```

show mirror

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

Example usage:

To display mirroring configuration:

```
local>show mirror
Command: show mirror

Current Settings
Mirror Status: Enabled
Target Port : 1:9
Mirrored Port:
    RX:
    TX: 1:1-1:5

local>
```

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] delete] <portlist> advertisement [enable disable]}
config gvrp	[<portlist> all] {state [enable disable] ingress_checking [enable disable] acceptable_frame [tagged_only admit_all] pvid <vlanid 1-4094>}
enable gvrp	
disable gvrp	
show vlan	<vlan_name 32>
show gvrp	<portlist>

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



NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

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><i>tag <vlanid></i> - The VLAN ID of the VLAN to be created.</p> <p><i>advertisement</i> – Specifies that the VLAN is able to join GVRP. If this parameter is not set, the VLAN cannot be configured to have forbidden ports.</p>
Restrictions	Each VLAN name can be up to 32 characters. 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 the vlan “v1”:

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

Success.

local>
```

config vlan

Purpose	Used to add additional ports to a previously configured VLAN.
Syntax	config vlan <vlan_name 32> { [add [tagged untagged forbidden] delete] <portlist> advertisement [enable disable]}
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.

config vlan

Parameters	<p><i><vlan_name 32></i> – The name of the VLAN to be configured.</p> <p><i>add</i> – Used to add ports to the specified VLAN, in conjunction with the <i>portlist</i> parameter.</p> <p><i>tagged</i> – Specifies that the ports are to be VLAN tagged.</p> <p><i>untagged</i> – Specifies the ports as untagged.</p> <p><i>forbidden</i> – Specifies the ports as forbidden ports.</p> <p><i>delete</i> – Used to delete ports from the specified VLAN, in conjunction with the <i>portlist</i> parameter.</p> <p><i><portlist></i> – A range of ports to add to the VLAN.</p> <p><i>advertisement [enable disable]</i> – Enables or disables GVRP on the specified VLAN.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To add 4 through 8 of module 2 as tagged ports to the VLAN v1:

```
local>config vlan v1 add tagged 2:4-2:8
Command: config vlan v1 add tagged 2:4-2:8

Success.

local>
```

config gvrp

Purpose	Used to configure GVRP on the switch.
Syntax	config gvrp [<portlist> all] {state [enable disable] ingress_checking [enable disable] acceptable_frame [tagged_only admit_all] pvid <vlanid 1-4094>}
Description	This command is used to configure the Group VLAN Registration Protocol on the switch. You can configure ingress checking, the sending and receiving of GVRP information, and the Port VLAN ID (PVID).

config gvrp

Parameters	<p><i><portlist></i> – A range of ports for which you want ingress checking.</p> <p><i>all</i> – Specifies all of the ports on the switch.</p> <p><i>state [enable disable]</i> – Enables or disables GVRP for the ports specified in the port list.</p> <p><i>ingress_checking [enable disable]</i> – Enables or disables ingress checking for the specified port list.</p> <p><i>acceptable_frame [tagged_only admit_all]</i> – This parameter states the frame type that will be accepted by the switch for this function. <i>tagged_only</i> implies that only VLAN tagged frames will be accepted, while <i>admit_all</i> implies tagged and untagged frames will be accepted by the switch.</p> <p><i>pvid <vlanid 1-4094></i> – Specifies the default VLAN associated with the port.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
local>config gvrp 1:1-1:4 state enable ingress_checking enable
acceptable_frame tagged_only pvid 2

Command: config gvrp 1:1-1:4 state enable ingress_checking enable
acceptable_frame tagged_only pvid 2

Success.

local>
```

enable gvrp

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

Example usage:

To enable the generic VLAN Registration Protocol (GVRP):

```

local>enable gvrp
Command: enable gvrp

Success.

local>

```

disable gvrp

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

Example usage:

To disable the Generic VLAN Registration Protocol (GVRP):

```

local>disable gvrp
Command: disable gvrp

Success.

local>

```

show vlan

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

Example usage:

To display the switch's current VLAN settings:

```

local>show vlan
Command: show vlan

VID          : 1          VLAN Name     : default
VLAN TYPE    : static     Advertisement : Enabled
Member ports : 1:1-1:11,2:1-2:11
Static ports : 1:1-1:11,2:1-2:11
Untagged ports : 1:1-1:11,2:1-2:11
Forbidden ports :

VID          : 2          VLAN Name     : v1
VLAN TYPE    : static     Advertisement : Disabled
Member ports : 1:12,2:12
Static ports : 1:12,2:12
Untagged ports :
Forbidden ports :

Total Entries : 2

local>

```

show gvrp

Purpose	Used to display the GVRP status for a port list on the switch.
Syntax	show gvrp {<portlist>}
Description	This command displays the GVRP status for a port list on the switch
Parameters	<portlist> – Specifies a range of ports for which the GVRP status is to be displayed.
Restrictions	None.

Example usage:

To display GVRP port status:

```
local>show gvrp
Command: show gvrp

Global GVRP : Disabled

Port   PVID   GVRP      Ingress Checking  Acceptable Frame Type
-----
1:1    1       Disabled  Enabled           All Frames
1:2    1       Disabled  Enabled           All Frames
1:3    1       Disabled  Enabled           All Frames
1:4    1       Disabled  Enabled           All Frames
1:5    1       Disabled  Enabled           All Frames
1:6    1       Disabled  Enabled           All Frames
1:7    1       Disabled  Enabled           All Frames
1:8    1       Disabled  Enabled           All Frames
1:9    1       Disabled  Enabled           All Frames
1:10   1       Disabled  Enabled           All Frames
1:11   1       Disabled  Enabled           All Frames
1:12   1       Disabled  Enabled           All Frames
2:1    1       Disabled  Enabled           All Frames
2:2    1       Disabled  Enabled           All Frames
2:3    1       Disabled  Enabled           All Frames
2:4    1       Disabled  Enabled           All Frames
2:5    1       Disabled  Enabled           All Frames
2:6    1       Disabled  Enabled           All Frames
2:7    1       Disabled  Enabled           All Frames
2:8    1       Disabled  Enabled           All Frames
2:9    1       Disabled  Enabled           All Frames
2:10   1       Disabled  Enabled           All Frames
2:11   1       Disabled  Enabled           All Frames
2:12   1       Disabled  Enabled           All Frames

Total Entries : 24

local>
```

LINK AGGREGATION COMMANDS

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

Command	Parameters
create link_aggregation	group_id <value 1-6> {type [lacp static]}
delete link_aggregation	group_id <value 1-6>
config link_aggregation	group_id <value 1-6> {master_port <port> ports <portlist> state [enable disable]}
config link_aggregation algorithm	[mac_source mac_destination mac_source_dest ip_source ip_destination ip_source_dest]
show link_aggregation	{group_id <value 1-6> algorithm}
config lacp_port	<portlist> mode [active passive]
show lacp_port	{<portlist>}

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



NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

create link_aggregation

Purpose	Used to create a link aggregation group on the switch.
Syntax	create link_aggregation group_id <value 1-6> {type [lacp static]}
Description	This command will create a link aggregation group with a unique identifier.

create link_aggregation

Parameters	<p><i><value 1-6></i> – Specifies the group ID. The switch allows up to 6 link aggregation groups to be configured. The group number identifies each of the groups.</p> <p><i>type</i> – Specify the type of link aggregation used for the group. If the type is not specified the default type is static.</p> <p>§ <i>lacp</i> – This designates the port group as LACP compliant. LACP allows dynamic adjustment to the aggregated port group. LACP compliant ports may be further configured (see config lacp_ports). LACP compliant must be connected to LACP compliant devices.</p> <p>§ <i>static</i> – This designates the aggregated port group as static. Static port groups can not be changed as easily as LACP compliant port groups since both linked devices must be manually configured if the configuration of the trunked group is changed. If static link aggregation is used, be sure that both ends of the connection are properly configured and that all ports have the same speed/duplex settings.</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 <value 1-6>
Description	This command is used to delete a previously configured link aggregation group.
Parameters	<i><value 1-6></i> – Specifies the group ID. The switch allows up to 6 link aggregation groups to be configured. The group number identifies each of the groups.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete link aggregation group:


```

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

Success.

local>

```

config link_aggregation

Purpose	Used to configure a previously created link aggregation group.
Syntax	config link_aggregation group_id <value 1-6> {master_port <port> ports <portlist> state [enable disable]}
Description	This command allows you to configure a link aggregation group that was created with the create link_aggregation command above. The DES-3350SR supports link aggregation cross box which specifies that link aggregation groups may be spread over multiple switches in the switching stack.
Parameters	<p><i>group_id <value 1-6></i> – Specifies the group ID. The switch allows up to 6 link aggregation groups to be configured. The group number identifies each of the groups.</p> <p><i>master_port<port></i> – Master port ID. Specifies which port (by port number) of the link aggregation group will be the master port. All of the ports in a link aggregation group will share the port configuration with the master port.</p> <p><i>ports <portlist></i> – Specifies a range of ports that will belong to the link aggregation group.</p> <p><i>state [enable disable]</i> – Allows you to enable or disable the specified link aggregation group.</p>
Restrictions	Only administrator-level users can issue this command. Link aggregation groups may not overlap.

Example usage:

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

```

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

Success.

local>

```

config link_aggregation algorithm

Purpose	Used to configure the link aggregation algorithm.
Syntax	config link_aggregation algorithm [mac_source mac_destination mac_source_dest ip_source ip_destination ip_source_dest]
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><i>mac_source</i> – Indicates that the switch should examine the MAC source address.</p> <p><i>mac_destination</i> – Indicates that the switch should examine the MAC destination address.</p> <p><i>mac_source_dest</i> – Indicates that the switch should examine the MAC source and destination addresses</p> <p><i>ip_source</i> – Indicates that the switch should examine the IP source address.</p> <p><i>ip_destination</i> – Indicates that the switch should examine the IP destination address.</p> <p><i>ip_source_dest</i> – 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>
```

show link_aggregation

Purpose	Used to display the current link aggregation configuration on the switch.
Syntax	show link_aggregation {group_id <value 1-6> algorithm}

show link_aggregation

Description	This command will display the current link aggregation configuration of the switch.
Parameters	<p><i>group_id</i> <value 1-6> – Specifies the group ID. The switch allows up to 6 link aggregation groups to be configured. The group number identifies each of the groups.</p> <p><i>algorithm</i> – Allows you to specify the display of link aggregation by the algorithm in use by that group.</p>
Restrictions	None.

Example usage:

To display Link Aggregation configuration:

```

local>show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = MAC-source-dest
Group ID      : 1
Master Port   : 2:10
Member Port   : 1:5-1:10,2:10
Active Port:
Status        : Disabled
Flooding Port : 1:5

DES-3350SR:4

```

config lacp_ports

Purpose	Used to configure settings for LACP compliant ports.
Syntax	config lacp_ports <portlist> mode [active passive]
Description	This command is used to configure ports that have been previously designated as LACP ports (see create link_aggregation).

config lacp_ports

Parameters	<p><i><portlist></i> – Specifies a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the 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, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.</p> <p><i>mode</i> – Select the mode to determine if LACP ports will process LACP control frames.</p> <p>§ <i>active</i> – Active LACP ports are capable of processing and sending LACP control frames. This allows LACP compliant devices to negotiate the aggregated link so the group may be changed dynamically as needs require. In order to utilize the ability to change an aggregated port group, that is, to add or subtract ports from the group, at least one of the participating devices must designate LACP ports as active. Both devices must support LACP.</p> <p>§ <i>passive</i> – LACP ports that are designated as passive cannot process LACP control frames. In order to allow the linked port group to negotiate adjustments and make changes dynamically, at one end of the connection must have “active” LACP ports (see above).</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure LACP port mode settings:

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

Success.

local>
```

show lacp_port

Purpose	Used to display current LACP port mode settings.
Syntax	show lacp_port {<portlist>}
Description	This command will display the LACP mode settings as they are currently configured.

show lacp_port

Parameters	<i><portlist></i> - Specifies a range of ports that will be viewed. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the 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, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To display LACP port mode settings:

```
local>show lacp_port 1:1-1:11
Command: show lacp_port 1:1-1:11

Port    Activity
-----  -
1:1     Active
1:2     Active
1:3     Active
1:4     Active
1:5     Active
1:6     Active
1:7     Active
1:8     Active
1:9     Active
1:10    Active
1:11    Active

local>
```

IP-MAC BINDING

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

Command	Parameters
create address_binding ip_mac ipaddress	<ipaddr> mac_address <macaddr>
config address_binding ip_mac ipaddress	<ipaddr> mac_address <macaddr>
config address_binding ip_mac ports	[<portlist> all] state [enable disable]
show address_binding	[ip_mac {ipaddress <ipaddr> mac_address <macaddr> } blocked {vlan_name <vlan_name> mac_address <macaddr> } ports]
delete address_binding	[ip_mac [ipaddress <ipaddr> {mac_address <macaddr>} all] blocked [all] vlan_name <vlan_name> mac_address <macaddr>]]

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

create address_binding ip_mac ipaddress	
Purpose	Used to create an IP-MAC Binding entry.
Syntax	<ipaddr> mac_address <macaddr>
Description	This command will create an IP-MAC Binding entry.
Parameters	<p><ipaddr> The IP address of the device where the IP-MAC binding is made.</p> <p><macaddr> The MAC address of the device where the IP-MAC binding is made.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create address binding on the switch:

```

local>create address_binding ip_mac ipaddress 10.1.1.3
mac_address 00-00-00-00-00-04

Command: create address_binding ip_mac ipaddress
10.1.1.3 mac_address 00-00-00-00-00-04

Success.
local>

```

config address_binding ip_mac ipaddress

Purpose	Used to Configure a IP-MAC Binding entry.
Syntax	<ipaddr> mac_address <macaddr>
Description	This command will configure an IP-MAC Binding entry.
Parameters	<p><i><ipaddr></i> The IP address of the device where the IP-MAC binding is made.</p> <p><i><macaddr></i> The MAC address of the device where the IP-MAC binding is made.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To config address binding on the switch:

```

local>config address_binding ip_mac ipaddress 10.1.1.3
mac_address 00-00-00-00-00-05

Command: config address_binding ip_mac ipaddress
10.1.1.3 mac_address 00-00-00-00-00-05

Success.

local>

```

config address_binding ip_mac ports

Purpose	Used to configure an IP-MAC state to enable or disable for specified ports.
Syntax	[<portlist> all] state [enable disable]
Description	This command will configure IP-MAC state to enable or disable for specified ports.
Parameters	<p><i><portlist></i> – Specifies a port or range of ports.</p> <p><i>all</i> – specifies all ports on the switch.</p> <p><i>state [enable disable]</i> – Enables or disables the specified range of ports.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To config address binding on the switch:

```
local>config address_binding ip_mac ports 2 state enable
```

```
Command: config address_binding ip_mac ports 2 state enable
```

```
Success.
```

```
local>
```

show address_binding

Purpose	Used to display IP-MAC Binding entries.
Syntax	[ip_mac {ipaddress <ipaddr> mac_address<macaddr>} blocked {vlan_name <vlan_name> mac_address <macaddr>} ports]
Description	This command will display IP-MAC Binding entries. Three different kinds of information can be viewed. <ul style="list-style-type: none"> • <i>IP_MAC</i> –Address Binding enties can be viewed by entering the physical and IP addresses of the device. • <i>Blocked</i> – Blocked address binding entries (bindings between VLAN names and MAC addresses) can be viewed by entering the VLAN name and the physical address of the device. • <i>Ports</i> - The number of enabled ports on a device.
Parameters	<p><ipaddr> The IP address of the device where the IP-MAC binding is made.</p> <p><macaddr> The MAC address of the device where the IP-MAC binding is made.</p> <p><vlan_name> The VLAN name of the VLAN that is bound to a MAC address in order to block a specific device on a known VLAN.</p>
Restrictions	none

Example usage:

To show IP-MAC Binding on the switch:


```
local>show address_binding ip_mac ipaddress 10.1.1.8
mac_address 00-00-00-00-00-12
```

```
Command: show address_binding ip_mac ipaddress
10.1.1.8 mac_address 00-00-00-00-00-12
```

Enabled ports: 2

IP Address	MAC Address
-----	-----
10.1.1.8	00-00-00-00-00-12

Total entries : 1

```
local>
```

Delete address_binding

Purpose	Used to delete IP-MAC Binding entries.
Syntax	[ip_mac [ipaddress <ipaddr> {mac_address <macaddr>} [all] blocked [all] vlan_name <vlan_name> mac_address <macaddr>]]
Description	<p>This command will delete IP-MAC Binding entries. Two different kinds of information can be deleted.</p> <ul style="list-style-type: none"> • <i>IP_MAC</i> – Individual Address Binding entries can be deleted by entering the physical and IP addresses of the device. Toggling to <i>all</i> will delete all the Address Binding entries. • <i>Blocked</i> – Blocked address binding entries (bindings between VLAN names and MAC addresses) can be deleted by entering the VLAN name and the physical address of the device. To delete all the Blocked Address Binding entries, toggle <i>all</i>.
Parameters	<p><ipaddr> The IP address of the device where the IP-MAC binding is made.</p> <p><macaddr> The MAC address of the device where the IP-MAC binding is made.</p> <p><vlan_name> The VLAN name of the VLAN that is bound to a MAC address in order to block a specific device on a known VLAN.</p> <p><i>all</i> – For <i>IP_MAC</i> binding <i>all</i> specifies all the IP-MAC binding entries; for Blocked Address Binding entries <i>all</i> specifies all the blocked VLANs and their bound physical addresses.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete an IP-MAC Binding on the switch:

```
local>delete address_binding ip_mac ipaddress 10.1.1.1
mac_address 00-00-00-00-00-06

Command: delete address_binding ip_mac ipaddress
10.1.1.1 mac_address 00-00-00-00-00-06

Success.

local>
```

BASIC IP COMMANDS

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

Command	Parameters
enable ipif	{<ipif_name 12> all}
create ipif	<ipif_name12> <network_address> <vlan_name 32> {secondary state [enable disable]}
config ipif	<ipif_name12> [{ipaddress <network_address> {vlan <vlan_name 32> state [enable disable]}] bootp dhcp}
show ipif	<ipif_name 12>
delete ipif	<ipif_name 12> all
disable ipif	<ipif_name 12> all

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

enable ipif	
Purpose	Used to enable an IP interface on the switch.
Syntax	enable ipif {<ipif_name 12> all}
Description	This command will enable the IP interface function on the switch.
Parameters	<p><i><ipif_name 12></i> – The name for the IP interface to be created. This name cannot exceed 12 characters.</p> <p><i>all</i> – Entering this parameter will delete all the IP interfaces currently configured on the switch.</p>
Restrictions	none

Example usage:

To enable the ipif function on the switch:

```

local>enable ipif s2
Command: enable ipif s2

Success.

local>

```

create ipif

create ipif

Purpose	Used to create an IP interface on the switch.
Syntax	create ipif <ipif_name12> <network_address> <vlan_name 32> {secondary state [enable disable]}
Description	This command will create an IP interface.
Parameters	<p><i><ipif_name 12></i> – The name for the IP interface to be created.</p> <p><i><network_address></i> – 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, 10.1.2.3/8).</p> <p><i><vlan_name 32></i> – The name of the VLAN that will be associated with the above IP interface.</p> <p><i>secondary</i> - Enter this parameter if this configured IP interface is to be a <i>secondary</i> IP interface of the VLAN previously specified. Secondary interfaces can only be configured if a primary interface is first configured.</p> <p><i>state [enable disable]</i> – Allows you to enable or disable the IP interface.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create an IP interface on the switch:

```

local>create ipif System ipaddress 10.48.74.122/8 v2 state enable
Command: create ipif System ipaddress 10.48.74.122/8 v2 state enable

Success.

local>

```

config ipif

Purpose	Used to configure the System IP interface.
Syntax	config ipif <ipif_name 12> [{ipaddress <network_address> {vlan <vlan_name 32> state [enable disable]} bootp dhcp]
Description	This command is used to configure the System IP interface on the switch.

config ipif

Parameters	<p><i><ipif_name 12></i> – The name for the IP interface previously created, that is to be configured.</p> <p><i>ipaddress <network_address></i> – IP address and netmask of the IP interface to be configured. 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, 10.1.2.3/8).</p> <p><i>vlan <vlan_name 32></i> – The name of the VLAN corresponding to the System IP interface.</p> <p><i>state [enable disable]</i> – Allows you to enable or disable the IP interface.</p> <p><i>bootp</i> – Allows the selection of the BOOTP protocol for the assignment of an IP address to the switch's System IP interface.</p> <p><i>dhcp</i> – Allows the selection of the DHCP protocol for the assignment of an IP address to the switch's System IP interface.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the IP interface System:

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

Success.

local>
```

show ipif

Purpose	Used to display the configuration of an IP interface on the switch.
Syntax	show ipif <ipif_name 12>
Description	This command will display the configuration of an IP interface on the switch.
Parameters	<i><ipif_name 12></i> – The name created for the IP interface to view.
Restrictions	None.

Example usage:

To display IP interface settings.

```

local>show ipif System
Command: show ipif System

IP Interface Settings

Interface Name   : System
IP Address      : 10.48.74.122  (MANUAL)
Subnet Mask     : 255.0.0.0
VLAN Name       : default
Admin. State    : Disabled
Link Status     : Link UP
Member Ports    : 1:1-1:12

local>

```

delete ipif

Purpose	Used to delete the configuration of an IP interface on the switch.
Syntax	delete ipif <ipif_name 12 all>
Description	This command will delete the configuration of an IP interface on the switch.
Parameters	<p><i><ipif_name></i> – The name created for the IP interface.</p> <p><i>all</i> – Entering this parameter will delete all the IP interfaces currently configured on the switch.</p>
Restrictions	None.

Example usage:

To delete the IP interface named s2:

```

local>delete ipif s2
Command: delete ipif s2

Success.

local>

```

disable ipif

Purpose	Used to disable the configuration of an IP interface on the switch.
---------	---

disable ipif

Syntax	disable ipif <ipif_name 12> all
Description	This command will disable the configuration of an IP interface on the switch.
Parameters	<i><ipif_name 12></i> – The name created for the IP interface. <i>all</i> – Entering this parameter will delete all the IP interfaces currently configured on the switch.
Restrictions	None.

Example usage:

To disable the IP interface named “s2”:

```
local>disable ipif s2
Command: disable ipif s2

Success.

local>
```

IGMP COMMANDS

The IGMP 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 1-25> robustness_variable <value 1-255> last_member_query_interval <sec 1-25> state [enable disable]}
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 1-25> max_response_time <sec 1-25> robustness_variable <value 1-255> last_member_query_interval <sec 1-25> state [enable disable]}
Description	This command allows you to configure IGMP snooping on the switch.
Parameters	<p><i><ipif_name 12></i> – The name of the IP interface for which you want to configure IGMP.</p> <p><i>all</i> – Specifies all the IP interfaces on the switch.</p> <p><i>version <value 1-2></i> – The IGMP version number.</p> <p><i>query_interval <sec 1-25></i> – The time in seconds between general query transmissions, in seconds.</p> <p><i>max_response_time <sec 1-25></i> – Enter the maximum time in seconds that the switch will wait for reports from members.</p> <p><i>robustness_variable <value 1-255></i> – This value states the permitted packet loss that guarantees IGMP.</p> <p><i>last_member_query_interval <value 1-25></i> – 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. The default is 1 second</p> <p><i>state [enable disable]</i> – Enables or disables IGMP for the specified IP interface.</p>
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 enable
Command: config igmp all version 1 state enable

Success.

local>
```

show igmp

Purpose	Used to display the IGMP configuration for the switch of 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 will be displayed.
Restrictions	None.

Example Usage:

To display IGMP configurations:

```
local>show igmp
Command: show igmp

IGMP Interface Configurations

Interface IP Address  Version Query Maximum Response Time Interval Robustness Value Last Member Query State
-----
System 10.58.44.222/8 2 125 10 2 1 Disabled

Total Entries: 1

local>
```

show igmp group

Purpose	Used to display the switch's IGMP group table.
Syntax	show igmp group {group <group>} {ipif <ipif_name 12>}
Description	This command will display the IGMP group configuration.
Parameters	<p><i>group <group></i> – The multicast group ID which the user wishes to display.</p> <p><i><ipif_name 12></i> – The name of the IP interface the IGMP group is part of.</p>
Restrictions	None.

Example Usage:

To display IGMP group table:

```

local>show igmp group
Command: show igmp group

Interface Name  Multicast Group  Last Reporter  IP Querier  IP Expire
-----
System          224.0.0.2           10.42.73.111    10.48.74.122  260
System          224.0.0.9           10.20.53.1     10.48.74.122  260
System          224.0.1.24         10.18.1.3      10.48.74.122  259
System          224.0.1.41         10.1.43.252    10.48.74.122  259
System          224.0.1.149        10.20.63.11    10.48.74.122  259

Total Entries: 5

local>

```

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 1-6711450> state [enable disable]}
config igmp_snooping querier	[<vlan_name 32> all] {query_interval <sec 1-65535> max_response_time <sec 1-25> robustness_variable <value 1-255> last_member_query_interval <sec 1-25> state [enable disable]}
enable igmp snooping	{forward_mcrouter_only}
disable igmp snooping	{forward_mcrouter_only}
config router_ports	{<vlan_name 32>} [add delete] <portlist>
show router_ports	{vlan <vlan_name 32>} {static dynamic}
show igmp_snooping	{vlan <vlan_name 32>}
show igmp_snooping group	{vlan <vlan_name 32>}
show igmp_snooping forwarding	{vlan <vlan_name 32>}

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



NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

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 [enable disable]}
Description	This command allows you to configure IGMP snooping on the switch.

config igmp_snooping

Parameters	<p><i><vlan_name 32></i> – The name of the VLAN for which IGMP snooping is to be configured.</p> <p><i>all</i> – Selecting this parameter will configure IGMP snooping for all VLANs on the switch.</p> <p><i>host_timeout <sec 1-16711450></i> – Specifies the maximum amount of time a host can be a member of a multicast group without the switch receiving a host membership report. The default is 260 seconds.</p> <p><i>router_timeout <sec 1-16711450></i> – Specifies the maximum amount of time a route can be a member of a multicast group without the switch receiving a host membership report. The default is 260 seconds.</p> <p><i>leave_timer <sec 1-16711450></i> – Leave timer. The default is 2 seconds.</p> <p><i>state [enable disable]</i> – Allows you to enable or disable IGMP snooping for the specified VLAN.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the igmp snooping:

```

local>config igmp_snooping default host_timeout 250 state enable
Command: config igmp_snooping default host_timeout 250 state enable

Success.

local>

```

config igmp_snooping querier

Purpose	This command configures IGMP snooping querier.
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 1-25> state [enable disable]}
Description	Used to configure the time in seconds between general query transmissions, the maximum time in seconds to wait for reports from members and the permitted packet loss that guarantees IGMP snooping.

config igmp_snooping querier

Parameters	<p><i><vlan_name 32></i> – The name of the VLAN for which IGMP snooping querier is to be configured.</p> <p><i>all</i> – Selecting this parameter will configure the IGMP snooping querier for all VLANs on the switch.</p> <p><i>query_interval <sec 1-65535></i> – Specifies the amount of time in seconds between general query transmissions. The default setting is 125 seconds.</p> <p><i>max_response_time <sec 1-25></i> – Specifies the maximum time in seconds to wait for reports from members. The default setting is 10 seconds.</p> <p><i>robustness_variable <value 1-255></i> – 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 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. <p><i>last_member_query_interval <sec 1-25></i> – 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.</p> <p><i>state [enable disable]</i> – Allows the switch to be specified as an IGMP Querier or Non-querier.</p>
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
enable
Command: config igmp_snooping querier default query_interval 125
state enable

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 <i>forward_mcrouter_only</i> is specified, the switch will only forward all multicast traffic to the multicast router, only. Otherwise, the switch forwards all multicast traffic to any IP router.
Parameters	<i>forward_mcrouter_only</i> – Specifies that the switch should only forward all multicast traffic to a multicast-enabled router. Otherwise, the switch will forward all multicast traffic to any IP router.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable IGMP snooping on the switch:

```

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 {forward_mcrouter_only}

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. If <i>forward_mcrouter_only</i> is specified, the switch will discontinue forwarding all multicast traffic to the multicast router.
Parameters	<i>forward_mcrouter_only</i> – Specifies that the switch will discontinue forwarding all multicast traffic to a multicast-enabled router.
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>
```

config router_ports

Purpose	Used to configure ports as router ports.
Syntax	config router_ports <vlan_name 32> [add delete] <portlist>
Description	This command allows you to designate a range of ports as being connected to multicast-enabled routers. This will ensure that all packets with such a router as its destination will reach the multicast-enabled router – regardless of protocol, etc.
Parameters	<p><i><vlan_name 32></i> – The name of the VLAN on which the router port resides.</p> <p><i>[add delete]</i> – Specify if you wish to add or delete the following ports as router ports.</p> <p><i><portlist></i> – Specifies a port or range of ports that will be configured as router ports.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To set up static router ports:

```

local>config router_ports default add 2:1-2:10
Command: config router_ports default add 2:1-2:10

Success.

local>

```

show router_ports

Purpose	Used to display the currently configured router ports on the switch.
Syntax	show router_ports {vlan <vlan_name 32>} {static dynamic}
Description	This command will display the router ports currently configured on the switch.
Parameters	<p><vlan_name 32> – The name of the VLAN on which the router port resides.</p> <p><i>static</i> – Displays router ports that have been statically configured.</p> <p><i>dynamic</i> – Displays router ports that have been dynamically configured.</p>
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>

```


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

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.

show igmp_snooping group

Parameters	<i>vlan <vlan_name 32></i> – 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  : 1:2,2:7

VLAN Name   : default
Multicast group: 224.0.0.9
MAC address  : 01-00-5E-00-00-09
Reports     : 1
Port Member  : 1:5,2:4

VLAN Name   : default
Multicast group: 234.5.6.7
MAC address  : 01-00-5E-05-06-07
Reports     : 1
Port Member  : 1:6,2:9

VLAN Name   : default
Multicast group: 236.54.63.75
MAC address  : 01-00-5E-36-3F-4B
Reports     : 1
Port Member  : 1:10,2:2

VLAN Name   : default
Multicast group: 239.255.255.250
MAC address  : 01-00-5E-7F-FF-FA
Reports     : 2
Port Member  : 1:8,2:4

VLAN Name   : default
Multicast group: 239.255.255.254
MAC address  : 01-00-5E-7F-FF-FE
Reports     : 1
Port Member  : 1:5,2:5

Total Entries : 6

local>
```

show igmp_snooping forwarding

Purpose	Used to display the IGMP snooping forwarding table entries on the switch.
Syntax	show igmp_snooping forwarding {vlan <vlan_name 32>}
Description	This command will display the current IGMP snooping forwarding table entries currently configured on the switch.
Parameters	<vlan_name 32> – The name of the VLAN for which you want to view IGMP snooping forwarding table information.
Restrictions	None.

Example usage:

To view the IGMP snooping forwarding table for VLAN “Trinity”:

```
local>show igmp_snooping forwarding vlan Trinity
Command: show igmp_snooping forwarding vlan Trinity

VLAN Name      : Trinity
Multicast group : 224.0.0.2
MAC address     : 01-00-5E-00-00-02
Port Member     : 1:11

Total Entries: 1

local>
```

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.

The 802.1X commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

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

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



NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

enable 802.1x

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

Example usage:

To enable 802.1x switch wide:

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

Success.

local>
```

disable 802.1x

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

Example usage:

To disable 802.1x on the switch:

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

Success.

local>
```

show 802.1x auth_configuration

Purpose	Used to display the current configuration of the 802.1x server on the switch.
Syntax	show 802.1x auth_configuration {ports [<portlist>}
Description	The show 802.1x command is used to display the current configuration of the 802.1x Port-based Network Access Control server application on the switch.

show 802.1x auth_configuration

Parameters	<p><i>ports <portlist></i> – Specifies a port or range of ports.</p> <p>The following details what is displayed:</p> <p>802.1x Enabled/Disabled – Shows the current status of 802.1x functions on the switch.</p> <p>Authentication Protocol: Radius_Eap – Shows the authentication protocol suite in use between the switch and a Radius server.</p> <p>Port number – Shows the physical port number on the switch.</p> <p>Capability: Authenticator/None – Shows the capability of 802.1x functions on the port number displayed above. There are two 802.1x capabilities that can be set on the switch: Authenticator and None.</p> <p>AdminCtlDir: 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.</p> <p>OpenCtlDir: Both/In – Shows whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction.</p> <p>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.</p> <p>QuietPeriod – Shows the time interval between authentication failure and the start of a new authentication attempt.</p> <p>TxPeriod – Shows the time to wait for a response from a supplicant (user) to send EAP Request/Identity packets.</p> <p>SuppTimeout – Shows the time to wait for a response from a supplicant (user) for all EAP packets, except for the Request/Identity packets.</p> <p>ServerTimeout – Shows the length of time to wait for a response from a RADIUS server.</p> <p>MaxReq – Shows the maximum number of times to retry sending packets to the supplicant.</p> <p>ReAuthPeriod – Shows the time interval between successive re-authentications.</p> <p>ReAuthenticate: Enabled/Disabled – Shows whether or not to re-authenticate.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To display the 802.1x authentication states:

```

local>show 802.1x auth_configuration ports 1
Command: show 802.1x auth_configuration ports 1

802.1X           : Enabled
Authentication Mode   : None
Authentication Protocol : Radius_EAP

Port number       : 1:1
Capability        : None
AdminCrIDir      : Both
OpenCrIDir       : Both
Port Control      : Auto
QuietPeriod      : 60  sec
TxPeriod         : 30  sec
SuppTimeout      : 30  sec
ServerTimeout    : 30  sec
MaxReq           : 2   times
ReAuthPeriod     : 3600 sec
ReAuthenticate    : Disabled

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

```

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.

show 802.1x auth_state

Parameters	<p><i>ports <portlist></i> – Specifies a port or range of ports.</p> <p>The following details what is displayed:</p> <p>Port number – Shows the physical port number on the switch.</p> <p>Auth PAE State: Initialize / Disconnected / Connecting / Authenticating / Authenticated / Held / ForceAuth / ForceUnauth – Shows the current state of the Authenticator PAE.</p> <p>Backend State: Request / Response / Fail / Idle / Initialize / Success / Timeout – Shows the current state of the Backend Authenticator.</p> <p>Port Status: Authorized / Unauthorized – Shows the result of the authentication process. Authorized means that the user was authenticated, and can access the network. Unauthorized means that the user was not authenticated, and cannot access the network.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To display the 802.1x auth state for ports 1-4:

```
local> show 802.1x auth_state ports 1-4
Command: show 802.1x auth_state ports 1-4

Port  Auth PAE State  Backend State  Port Status
-----
1    ForceAuth         Success        Authorized
2    ForceAuth         Success        Authorized
3    ForceAuth         Success        Authorized
4    ForceAuth         Success        Authorized

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

config 802.1x auth_mode

Purpose	Used to configure the 802.1x authentication mode on the switch.
Syntax	config 802.1x auth_mode [port_based mac_based]
Description	The config 802.1x auth_mode command is used to enable either the port-based or MAC-based 802.1x authentication feature on the switch.

config 802.1x auth_mode

Parameters	<i>[port_based mac_based ports]</i> – The switch allows you to authenticate 802.1x by either port or MAC address.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure 802.1x authentication by MAC address:

```
local>config 802.1x auth_mode mac_based
Command: config 802.1x auth_mode mac_based

Success.

local>
```

config 802.1x capability ports

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 capability ports command has four capabilities that can be set for each port. Authenticator, Supplicant, Authenticator and Supplicant, and None.
Parameters	<p><i><portlist></i> – Specifies a range of ports.</p> <p><i>all</i> – Specifies all of the ports on the switch.</p> <p><i>authenticator</i> – A user must pass the authentication process to gain access to the network.</p> <p><i>none</i> – The port is not controlled by the 802.1x functions.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure 802.1x capability on ports 1-10 on switch 1:

```
local> local>config 802.1x capability ports all authenticator
```

```
Command: config 802.1x capability ports all authenticator
```

```
Success.
```

```
local>
```

```
local>
```

config 802.1x auth_parameter

Purpose	Used to configure the 802.1x Authentication parameters on a range of ports. The default parameter will return all ports in the specified range to their default 802.1x settings.
Syntax	config 802.1x auth_parameter ports [<portlist> all] [default {direction [both in] port_control [force_unauth auto force_auth] quiet_period <sec 0-65535> tx_period <sec 1-65535> supp_timeout <sec 1-65535> server_timeout <sec 1-65535> max_req <value 1-10> reauth_period <sec 1-65535> enable_reauth [enable disable]]]
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.

config 802.1x auth_parameter

Parameters	<p><i><portlist></i> – Specifies a port or range of ports.</p> <p><i>all</i> – Specifies all of the ports on the switch.</p> <p><i>default</i> – Returns all of the ports in the specified range to their 802.1x default settings.</p> <p><i>direction [both in]</i> – Determines whether a controlled port blocks communication in both the receiving and transmitting directions, or just the receiving direction.</p> <p><i>port_control</i> – Configures the administrative control over the authentication process for the range of ports. The user has the following authentication options:</p> <ul style="list-style-type: none"> • <i>force_auth</i> – Forces the Authenticator for the port to become authorized. Network access is allowed. • <i>auto</i> – Allows the port's status to reflect the outcome of the authentication process. • <i>force_unauth</i> – Forces the Authenticator for the port to become unauthorized. Network access will be blocked. <p><i>quiet_period <sec 0-65535></i> – Configures the time interval between authentication failure and the start of a new authentication attempt.</p> <p><i>tx_period <sec 1-65535></i> – Configures the time to wait for a response from a supplicant (user) to send EAP Request/Identity packets.</p> <p><i>supp_timeout <sec 1-65535></i> – Configures the time to wait for a response from a supplicant (user) for all EAP packets, except for the Request/Identity packets.</p> <p><i>server_timeout <sec 1-65535></i> – Configure the length of time to wait for a response from a RADIUS server.</p> <p><i>max_req <value 1-10></i> – Configures the number of times to retry sending packets to a supplicant (user).</p> <p><i>reauth_period <sec 1-65535></i> – Configures the time interval between successive re-authentications.</p> <p><i>enable_reauth [enable disable]</i> – Determines whether or not the switch will re-authenticate. Enabled causes re-authentication of users at the time interval specified in the Re-authentication Period field, above.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure 802.1x authentication parameters for ports 1 – 20 of switch 1:

```

local>config 802.1x auth_parameter ports 1-4 direction both
Command: config 802.1x auth_parameter ports 1-4 direction both

Success.

local>

```

config 802.1x init

Purpose	Used to initialize the 802.1x function 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 specified range of ports or for specified MAC addresses operating from a specified range of ports.
Parameters	<p><i>port_based</i> – This instructs the switch to initialize 802.1x functions based only on the port number. Ports approved for initialization can then be specified.</p> <p>§ <portlist> – Specifies a port or range of ports.</p> <p>§ all – Specifies all of the ports on the switch.</p> <p><i>mac_based</i> - This instructs the switch to initialize 802.1x functions based on the MAC address of a device on a specific port or range of ports. MAC address approved for initialization can then be specified.</p> <p>§ <portlist> – Specifies a port or range of ports.</p> <p>§ all – Specifies all of the ports on the switch.</p> <p><i>mac_address <macaddr></i> - Specifies the MAC address of the client the user wishes to add.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To initialize the authentication state machine of some or all:

```

local> config 802.1x init port_based ports all
Command: config 802.1x init port_based ports all

Success.

local>

```

config 802.1x reauth ports

Purpose	Used to configure the 802.1x re-authentication feature of the switch.
Syntax	config 802.1x reauth [port_based ports [<portlist all>] mac_based [ports] [<portlist> all] {mac_address <macaddr>}]
Description	The config 802.1x reauth command is used to re-authenticate a previously authenticated device based on port number or MAC address.
Parameters	<p><i>port_based</i> – This instructs the switch to re-authorize 802.1x function based only on the port number. Ports approved for re-authorization can then be specified.</p> <p>§ <i>ports</i> <portlist> – Specifies a port or range of ports.</p> <p>§ <i>all</i> – Specifies all of the ports on the switch.</p> <p><i>mac-based</i> - This instructs the switch to re-authorize 802.1x function based on a specific MAC address. Ports approved for re-authorization can then be specified.</p> <p>§ <portlist> – Specifies a port or range of ports.</p> <p>§ <i>all</i> – Specifies all of the ports on the switch.</p> <p><i>mac_address</i> <macaddr> - Specifies the MAC address of the client the user wishes to add.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure 802.1x reauthentication for ports 1-10:

```
local>config 802.1x reauth port_based ports 1-8
Command: config 802.1x reauth port_based ports 1-8

Success.

local>
```

config radius add

Purpose	Used to add a new RADIUS server.
Syntax	config radius add <server_index 1-3> <server_ip> key <passwd 32> [default {auth_port <udp_port_number 1-65535> acct_port <udp_port_number 1-65535>}]

config radius add

Description	The config radius add command is used to add RADIUS servers to the switch.
Parameters	<p><i><server_index 1-3></i> – Assigns a number to the current set of RADIUS server settings. Up to 3 groups of RADIUS server settings can be entered on the switch. The lowest index number will have a higher authenticative priority</p> <p><i><server_ip></i> – The IP address of the RADIUS server.</p> <p><i>key</i> – Specifies that a password and encryption key will be used between the switch and the RADIUS server.</p> <p>§ <i><passwd 32></i> – The shared-secret key used by the RADIUS server and the switch. Up to 32 characters can be used.</p> <p><i>default</i> – Uses the default udp port number in both the “auth_port” and “acct_port” settings.</p> <p><i>auth_port <udp_port_number></i> – The UDP port number for authentication requests. The default is 1812.</p> <p><i>acct_port <udp_port_number></i> – 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 the RADIUS server communication settings:

```

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

Success.

local>

```

config radius delete

Purpose	Used to delete a previously entered RADIUS server configuration.
Syntax	config radius delete <server_index 1-3>
Description	The config radius delete command is used to delete a previously entered RADIUS server configuration.
Parameters	<i><server_index 1-3></i> – A number identifying the current set of RADIUS server settings the user wishes to delete. Up to 3 groups of RADIUS server settings can be entered on the switch.

config radius delete

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> key <passwd 32> auth_port <udp_port_number 1-65535> acct_port <udp_port_number 1-65535>}
Description	The config radius command is used to configure the switch's RADIUS settings.
Parameters	<p><i><server_index 1-3></i> – Assigns a number to the current set of RADIUS server settings. Up to 3 groups of RADIUS server settings can be entered on the switch.</p> <p><i>ipaddress <server_ip></i> – The IP address of the RADIUS server.</p> <p><i>key</i> – Specifies that a password and encryption key will be used between the switch and the RADIUS server.</p> <p> § <i><passwd 32></i> – The shared-secret key used by the RADIUS server and the switch. Up to 32 characters can be used.</p> <p><i>auth_port <udp_port_number></i> – The UDP port number for authentication requests. The default is 1812.</p> <p><i>acct_port <udp_port_number></i> – 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 the RADIUS settings:

```

local>config radius 1 10.48.74.121 key dlink default
Command: config radius 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 Acct-Port Status  Key
      Number      Number
-----
1  10.1.1.1      1812      1813      Active  kizzel
2  10.1.1.2      1812      1813      Active  mynizzel
Total Entries:2

local>

```

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

Command	Parameters
create access_profile	[ethernet {vlan source_mac <macmask> destination_mac <macmask> 802.1p ethernet_type} ip {vlan source_ip_mask <netmask> destination_ip_mask <netmask> dscp [icmp {type code } igmp {type } tcp {src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xffff> flag_mask [all {urg ack psh rst syn fin}]} 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 {vlan <vlan_name 32> source_ip <ipaddr> destination_ip <ipaddr> dscp <value 0-63> [icmp {type <value 0-255> code <value 0-255>} igmp {type <value 0-255>} tcp {src_port <value 0-65535> dst_port <value 0-65535> flag_mask [all {urg ack psh rst syn fin}]} udp {src_port <value 0-65535> dst_port <value 0-65535>} protocol_id <value 0 - 255> {user_define <hex 0x0-0xffffffff>}} 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>} permit {priority <value 0-7> {replace_priority} replace_dscp_with <value 0-63> } deny] delete access_id <value 1-255>]
show access_profile	{profile_id <value 1-255>}

Access profiles allow you to establish criteria to determine whether or not 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:

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

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

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

config access_profile profile_id 1 add access_id 1 ip source_ip 10.42.73.1 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.

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.

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



NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

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.
---------	--

create access_profile

Syntax	<pre>[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> flag_mask [all {urg ack psh rst syn fin}]} 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 <hex0x0-0xffffffff> <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>]</pre>
Description	<p>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.</p>

create access_profile

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 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 examine each frame's Internet Group Management Protocol (IGMP) field.
 - *type* – Specifies that the switch will examine each frame's IGMP Type field.
- *tcp* – Specifies that the switch will examine each frames Transport Control Protocol (TCP) field.
 - *src_port_mask <hex 0x0-0xffff>* – Specifies a TCP port mask for the source port.
 - *dst_port_mask <hex 0x0-0xffff>* – Specifies a TCP port mask for the destination port.
 - *flag_mask [all | {urg | ack | psh | rst | syn | fin}]* – Enter the appropriate flag_mask parameter. All incoming packets have TCP port numbers contained in them as the forwarding

create access_profile

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

Example usage:

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

```

local>create access_profile ip vlan source_ip_mask 20.0.0.0
destination_ip_mask 10.0.0.0 dscp icmp type code permit profile_id 101
Command: create access_profile ip vlan source_ip_mask 20.0.0.0
destination_ip_mask 10.0.0.0 dscp icmp type code permit profile_id 101

Success.

DES-3350SR

```

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.
Parameters	<i>profile_id <value 1-255></i> – Enter 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

config access_profile

Purpose	Used to configure an access profile on the switch and to define specific values that will be used to by the switch to determine if a given packet should be forwarded or filtered. Masks entered using the create access_profile command will be combined, using a logical AND operation, with the values the switch finds in the specified frame header fields. Specific values for the rules are entered using the config access_profile command, below.
Syntax	<pre> config access_profile <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 {vlan <vlan_name 32> source_ip <ipaddr> destination_ip <ipaddr> dscp <value 0-63> [icmp {type <value 0-255> } code <value 0-255>} igmp {type <value 0-255>} tcp {src_port <value 0-65535> dst_port <value 0-65535> flag_mask [all {urg ack psh rst syn fin}] } udp {src_port <value 0- 65535> dst_port <value 0-65535>} protocol_id <value 0 - 255> {user_define <hex 0x0-0xffffffff>}] 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>}] [permit {replace_priority_with <value 0-7> replace_dscp_with <value 0-63> } deny] delete access_id <value 1-255>] </pre>
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.

config access_profile

Parameters

profile_id <value 1-255> – Enter 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.

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. The lower access ID, the higher the priority the rule will be given.

ethernet – Specifies that the switch will look only into the layer 2 part of each packet.

- *vlan* <vlan_name 32> – Specifies that the access profile will apply to only to this VLAN.
- *source_mac* <macaddr> – Specifies that the access profile will apply to only packets with this source MAC address.
- *destination_mac* <macaddr> – Specifies that the access profile will apply to only packets with this destination MAC address.
- *802.1p* <value 0-7> – Specifies that the access profile will apply only to packets with this 802.1p priority value.
- *ethernet_type* <hex 0x0-0xffff> – Specifies that the access profile will apply only to packets with this 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_ip* <ipaddr> – Specifies that the access profile will apply to only packets with this destination IP address.
- *dscp* <value 0-63> – Specifies that the access profile will apply only to packets that have this value in their Type-of-Service (DiffServ code point, DSCP) field in their IP packet header.
- *icmp* – Specifies that the switch will examine the Internet Control Message Protocol (ICMP) field within each packet.
 - *type* <value 0-255> – 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.

config access_profile

Restrictions Only administrator-level users can issue this command.

Example usage:

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

```
local> config access_profile profile_id 2 add access_id 1 ip source_ip
10.42.73.1 deny
Command: config access_profile profile_id 1 add access_id 1 ip source_ip
10.42.73.1 deny

Success.

local>
```

show access_profile

Purpose	Used to display the currently configured access profiles on the switch.
Syntax	show access_profile {profile_id <value 1-255>}
Description	The show access_profile command is used to display the currently configured access profiles
Parameters	<i>profile_id <value 1-255></i> - Enter this parameter, along with the appropriate value between 1 and 255, to view a specific access profile. Entering this command without a parameter will display all access profiles currently set on the switch.
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: 2

TYPE : Ethernet Frame Filter

Ports:1

Masks : VLAN 802.1P

ID	Mode		
3	Permit	0	0-x

```
local>
```

TRAFFIC SEGMENTATION COMMANDS

Traffic segmentation allows you to further sub-divide VLANs into smaller groups of ports that will help to reduce traffic on the VLAN. The VLAN rules take precedence, and then the traffic segmentation rules are applied. The traffic segmentation commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
config traffic_segmentation	<portlist> forward_list [null <portlist>]
show traffic_segmentation	{<portlist>}

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



NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

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><i><portlist></i> – Specifies a range of ports that will be configured for traffic segmentation.</p> <p><i>forward_list</i> – Specifies a range of ports that will receive forwarded frames from the ports specified in the portlist, above.</p> <p><i>null</i> – no ports are specified</p> <p><i><portlist></i> – Specifies a range of ports for the forwarding list. This list must be on the same switch previously specified for traffic segmentation (i.e. following the <i><portlist></i> specified above for config traffic_segmentation).</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure ports 1 through 9 to be able to forward frames to port 10 through 12:

```
local> config traffic_segmentation 1-9 forward_list 10-12
Command: config traffic_segmentation 1-9 forward_list 1-12

Success.

local>
```

show traffic_segmentation

Purpose	Used to display the current traffic segmentation configuration on the switch.
Syntax	show traffic_segmentation <portlist>
Description	The show traffic_segmentation command is used to display the current traffic segmentation configuration on the switch.
Parameters	<i><portlist></i> – Specifies a port or range of ports for which the current traffic segmentation configuration on the switch will be displayed.
Restrictions	The port lists for segmentation and the forward list must be on the same switch.

Example usage:

To display the current traffic segmentation configuration on the switch.

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

Traffic Segmentation Table

Port Forward Portlist

```
-----
1  1-50
2  1-50
3  1-50
4  1-50
5  1-50
6  1-50
7  1-50
8  1-50
9  1-50
10 1-50
11 1-50
12 1-50
13 1-50
14 1-50
15 1-50
16 1-50
17 1-50
18 1-50
```

```
local>
```

TIME AND SNTP COMMANDS

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

Command	Parameters
config sntp	{primary <ipaddr> secondary <ipaddr> poll-interval <int 30-99999>}
show sntp	
enable sntp	
disable sntp	
config time	{time <time hh:mm:ss> date <date ddmmyyyy> time-zone {operator [+ -] hour <gmt_hour 0-13> min <minute 0-59>} dst [disable repeating {s-which <start_which 1-4,last> s-day <start_day sun-sat> s-mth <start_mth 1-12> s-time <start_time hh:mm> e-which<end_which 1-4,last> e-day <end_day sun-sat> e-mth<end_mth 1-12> e-time <end_time hh:mm> offset [30 60]} annual {s-date <start_date 1-31> s-mth <start_mth 1-12> s-time <start_time hh:mm> e-date <end_date 1-31> e-mth <end_mth 1-12> e-time <end_time hh:mm> offset [30 60]}}
show time	

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

config sntp	
Purpose	Used to setup SNTP service.
Syntax	config sntp {primary <ipaddr> secondary <ipaddr> poll-interval <int 30-99999>}
Description	Use this command to configure SNTP service from an SNTP server. SNTP must be enabled for this command to function (See enable sntp).
Parameters	<p><i>primary</i> – This is the primary server the SNTP information will be taken from.</p> <p>§ <ipaddr> – The IP address of the primary server.</p> <p><i>secondary</i> – This is the secondary server the SNTP information will be taken from in the event the primary server is unavailable.</p> <p>§ <ipaddr> – The IP address for the secondary server.</p> <p><i>poll-interval <int 30-99999></i> – This is the interval between requests for updated SNTP information. The polling interval ranges from 30 to 99,999 seconds.</p>
Restrictions	Only administrator-level users can issue this command. SNTP service must be enabled for this command to function (enable sntp).

Example usage:

To configure SNTP settings:

```
local>config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 30
Command: config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 30

Success.

local>
```

show sntp

Purpose	Used to display the SNTP information.
Syntax	show sntp
Description	This command will display SNTP settings information including the source IP address, time and poll interval.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To display SNTP configuration information:

```
local>show sntp
Command: show sntp

Current Time Source : System Clock
SNTP : Disabled
SNTP Primary Server   : 10.1.1.1
SNTP Secondary Server : 10.1.1.2
SNTP Poll Interval   : 720 sec

local>
```

enable sntp

Purpose	Enables SNTP server support.
Syntax	enable sntp
Description	This will enable SNTP support. SNTP service must be separately configured (see config sntp). Enabling and configuring SNTP support will override any manually configured system time settings.

enable sntp

Parameters	None.
Restrictions	Only administrator-level users can issue this command. SNTP settings must be configured for SNTP to function (config sntp).

Example usage:

To enable the SNTP function:

```
local>enable sntp
Command: enable sntp

Success.

local>
```

disable sntp

Purpose	Disables SNTP server support.
Syntax	disable sntp
Description	This will disable SNTP support. SNTP service must be separately configured (see config sntp).
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example:

To stop SNTP support:

```
local>disable sntp
Command: disable sntp

Success.

local>
```

config time

Purpose	Used to manually configure system time and date settings.
---------	---

config time

Syntax	{time <time hh:mm:ss> date <date ddmmyyyy> time-zone {operator [+ -] hour <gmt_hour 0-13> min <minute 0-59>} dst [disable repeating {s-which <start_which 1-4,last> s-day <start_day sun-sat> s-mth <start_mth 1-12> s-time <start_time hh:mm> e-which<end_which 1-4,last> e-day <end_day sun-sat> e-mth<end_mth 1-12> e-time <end_time hh:mm> offset [30 60]} annual {s-date <start_date 1-31> s-mth <start_mth 1-12> s-time <start_time hh:mm> e-date <end_date 1-31> e-mth <end_mth 1-12> e-time <end_time hh:mm> offset [30 60]}}}
Description	This will configure the system time and date settings. These will be overridden if SNTP is configured and enabled.
Parameters	<p><i>date</i> – Express the date using two numerical characters for the day of the month, three alphabetical characters for the name of the month, and four numerical characters for the year.</p> <p><i>time</i> – Express the system time using the format hh:mm:ss, that is, two numerical characters each for the hour using a 24-hour clock, the minute and second. For example: 19:42:30.</p>
Restrictions	Only administrator-level users can issue this command. Manually configured system time and date settings are overridden if SNTP support is enabled.

Example usage:

To manually set system time and date settings:

```
local>config time 17012005 17:28:30
Command: config time 17jan2005 17:28:30

Success.

local>
```

show time

Purpose	Used to display the current time settings and status.
Syntax	show time
Description	This will display system time and date configuration as well as display current system time.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To show the time currently set on the switch's System clock:

```
local>show time
Command: show time

Current Time Source : System Clock
Boot Time   : 0 Days 00:00:00
Current Time : 0 Days 01:16:47
Time zone   : GMT -06:00
Daylight Saving Time : Disabled
Offset in minutes : 60
Repeating   From : Apr 1st Sun 02:00
           To  : Oct last Sun 02:00
Annual     From : 29 Apr 02:00
           To  : 12 Oct 02:00

local>
```

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>
config arpentry	<ipaddr> <macaddr>
delete arpentry	[<ipaddr> all]
show arpentry	{ipif <ipif_name 12> ipaddress <ipaddr> static local}
config arp_aging time	<value 0-65535>
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 and the corresponding MAC 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>
```

config arpentry

Purpose Used to configure a static entry in the ARP table.

config arpentry

Syntax	config arpentry <ipaddr> <macaddr>
Description	This command is used to configure a static entry in the ARP Table. The user may specify the IP address and the corresponding MAC address of an entry in the switch's ARP table.
Parameters	<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 configure a static ARP entry for the IP address 10.48.74.12 and MAC address 00:50:BA:00:07:36:

```

local>config arpentry 10.48.74.12 00-50-BA-00-07-36
Command: config arpentry 10.48.74.12 00-50-BA-00-07-36

Success.

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 <i>all</i> clears the switch's ARP table.
Parameters	<p><ipaddr> – The IP address of the end node or station.</p> <p><i>all</i> – Deletes all ARP entries.</p>
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 minutes, that an ARP entry can remain in the switch's ARP table, without being accessed, before it is dropped from the table.
Parameters	<i>time <value 0-65535></i> – The ARP age-out time, in minutes. The value may be set in the range of 0-65535 minutes with a default setting of 20 minutes.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure ARP aging time:

```

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

Success.

local>

```

show arpentry

Purpose	Used to display the ARP table.
Syntax	show arpentry {ipif <ipif_name 12> ipaddress <ipaddr> static local}
Description	This command is used to display the current contents of the switch's ARP table.

show arpentry

Parameters	<p><i><ipif_name 12></i> – The name of the IP interface the end node or station for which the ARP table entry was made, resides on.</p> <p><i><ipaddr></i> – The network address corresponding to the IP interface name above.</p> <p><i>static</i> – Displays the static entries of the ARP table.</p> <p><i>local</i> – Displays the local entries of 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

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>
```

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	<network_address> <ipaddr> {<metric 1-65535>} {[primary backup]}
create iproute default	<ipaddr> {<metric 1-65535>}
delete iproute default	
delete iproute	<network_address> <ipaddr> {[primary backup]}
show iproute	{<network_address>} {[static rip ospf]}

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

create iproute	
Purpose	Used to create IP route entries to the switch's IP routing table.
Syntax	create iproute <network_address> <ipaddr> {<metric 1-65535>} {[primary backup]}
Description	This command is used to create a primary and backup IP route entry to the switch's 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, 10.1.2.3/8).</p> <p><ipaddr> – The gateway IP address for the next hop router.</p> <p><metric 1-65535> – Allows the entry of a routing protocol metric entry, representing the number of routers between the Switch and the IP address above. The default setting is 1.</p> <p>[primary backup] - The user may choose between <i>Primary</i> and <i>Backup</i>. If the Primary Static/Default Route fails, the Backup Route will support the entry. Please take note that the Primary and Backup entries cannot have the same Gateway.</p>
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To add a single static address 10.48.74.121, mask 255.0.0.0 and gateway 10.1.1.254 to the routing table:

```

local>create iproute 10.48.74.121/255.0.0.0 10.1.1.254 1
Command: create iproute 10.48.74.121/8 10.1.1.254 1

Success.

local>

```

create iproute default

Purpose	Used to create IP route entries to the switch's IP routing table.
Syntax	create iproute default <ipaddr> {<metric>}
Description	This command is used to create a default static IP route entry to the switch's IP routing table.
Parameters	<p><i><ipaddr></i> – The gateway IP address for the next hop router.</p> <p><i><metric></i> – Allows the entry of a routing protocol metric entry representing the number of routers between the Switch and the IP address above. The default setting is 1.</p>
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To add the default static address 10.48.74.121, with a metric setting of 1, to the routing table:

```

local>create iproute default 10.48.74.121 1
Command: create iproute default 10.48.74.121 1

Success.

local>

```

delete iproute

Purpose	Used to delete an IP route entry from the switch's IP routing table.
Syntax	delete iproute <network_address> <ipaddr> {[primary backup]}
Description	This command will delete an existing entry from the switch's IP routing table.

delete iproute

Parameters	<p><i><network_address></i> – 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, 10.1.2.3/8).</p> <p><i><ipaddr></i> – The gateway IP address for the next hop router.</p> <p><i>[primary backup]</i> – The user may choose between <i>Primary</i> and <i>Backup</i>. If the Primary Static/Default Route fails, the Backup Route will support the entry. Please take note that the Primary and Backup entries cannot have the same Gateway.</p>
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete a backup static address 10.48.75.121, mask 255.0.0.0 and gateway (ipaddr) entry of 10.1.1.254 from the routing table:

```
local>delete iproute 10.48.74.121/8 10.1.1.254
Command: delete iproute 10.48.74.121/8 10.1.1.254

Success.

local>
```

delete iproute default

Purpose	Used to delete a default IP route entry from the switch's IP routing table.
Syntax	delete iproute default
Description	This command will delete an existing default entry from the switch's IP routing table.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete the default IP route 10.53.13.254:

```

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><i><network_address></i> – 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, 10.1.2.3/8).</p> <p><i>static</i> – Use this parameter to display static iproute entries.</p> <p><i>rip</i> – Use this parameter to display RIP iproute entries.</p> <p><i>ospf</i> – Use this parameter to display OSPF iproute entries.</p>
Restrictions	None.

Example Usage:

To display the contents of the IP routing table:

```

local>show iproute
Command: show iproute

IP Address/Netmask Gateway Interface Hops Protocol
-----
0.0.0.0 10.1.1.254 System 1 Default
10.0.0.0 10.48.74.122 System 1 Local

Total Entries: 2

local>

```

ROUTE REDISTRIBUTION COMMANDS

The route redistribution 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	[local static ospf {all internal external type_1 type_2 inter+e1 inter+e2}] {metric <value>}
config route redistribute dst ospf src	[static rip local] {mettype [1 2] metric <value>}
config route redistribute dst rip src	[local static ospf {all internal external type_1 type_2 inter+e1 inter+e2}] {metric <value>}
delete route redistribute	{dst [rip ospf] src [rip local static 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 src

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><i>src</i> [static rip local] – Allows for the selection of the protocol for the source device.</p> <p><i>mettype</i> [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> <p><i>metric <value></i> – Allows the entry of an OSPF interface cost. This is analogous to a Hop Count in the RIP routing protocol.</p>
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 src

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 {all internal external type_1 type_2 inter+e1 inter+e2}] {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	<i>src</i> {all internal external type_1 type_2 inter+e1 inter+e2} – Allows the selection of the protocol of the source device. <i>metric <value></i> – 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 inter+e1 inter+e2 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>
```

config route redistribute dst ospf src

Purpose	Used configure route redistribution settings for the exchange of RIP routes to OSPF routes on the switch.
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.

config route redistribute dst ospf src

Parameters	<p><i>src</i> [<i>static</i> <i>rip</i> <i>local</i>] – Allows the selection of the protocol of the source device.</p> <p><i>mettype</i> – 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.</p> <p><i>metric</i> <value> – Allows the entry of an OSPF interface cost. This is analogous to a Hop Count in the RIP routing protocol.</p>
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 ospf src all metric 2
Command: config route redistribute dst ospf src all metric 2

Success.

local>
```

config route redistribute dst rip src

Purpose	Used configure route redistribution settings for the exchange of RIP routes to OSPF routes on the switch.
---------	---

config route redistribute dst rip src

Syntax	config route redistribute dst rip src [local static ospf [all internal external type_1 type_2 inter+e1 inter+e2]] {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	<i>src {all internal external type_1 type_2 inter+e1 inter+e2}</i> – Allows the selection of the protocol of the source device. <i>metric <value></i> – 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.

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>
```

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	<i>dst [rip ospf]</i> – Allows the selection of the protocol on the destination device. <i>src [rip static local ospf]</i> – Allows the selection of the protocol on the source device.

delete route redistribute

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>
```

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	<i>src [rip static local ospf]</i> – Allows the selection of the routing protocol on the source device. <i>dst [rip ospf]</i> – 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 Protocol  Destination Protocol  Type      Metric
-----
STATIC  RIP              All       1
LOCAL   OSPF             Type-2    20

Total Entries : 2

local>
```


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><i>hops <value 1-16></i> – Specifies the maximum number of relay agent hops that the BOOTP packets can cross.</p> <p><i>time <sec 0-65535></i> – If this time is exceeded, the switch will relay 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 in which BOOTP relay is to be enabled.</p> <p><ipaddr> – The BOOTP server IP address.</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 an 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 an 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 BOOTP server IP address.</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>}
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
-----
System    10.48.74.122  10.23.12.34  10.12.34.12  10.48.75.121

Total Entries: 1

local>

```


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> [add delete] static <domain_name 32> <ipaddr>}
enable dnsr	{cache static}
disable dnsr	{cache 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> [add delete] static <domain_name 32> <ipaddr>}
Description	This command is used to configure the DNS relay function on the switch.
Parameters	<p><i>primary</i> – Indicates that the IP address below is the address of the primary DNS server.</p> <p><i>secondary</i> – Indicates that the IP address below is the address of the secondary DNS server.</p> <p><i>nameserver <ipaddr></i> – The IP address of the DNS nameserver.</p> <p><i>[add delete]</i> – Indicates if the user wishes to add or delete the DNS relay function.</p> <p><i><domain_name 32></i> – The domain name of the entry.</p> <p><i><ipaddr></i> – The IP address of the entry.</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 10.43.21.12
Command: config dnsr primary 10.43.21.12

Success

local>

```

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 {cache static}
Description	This command is used, in combination with the disable dnsr command below, to enable and disable DNS Relay on the switch.
Parameters	<p><i>cache</i> - This parameter will allow the user to enable the cache lookup for the DNS rely on the switch.</p> <p><i>static</i> - This parameter will allow the user to enable the static table lookup for the DNS rely on the switch.</p>
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>

```

Example Usage:

To enable cache lookup for DNS relay.

```

local>enable dnsr cache
Command: enable dnsr cache

Success.

local>

```

Example Usage:

To enable static table lookup for DNS relay.

```

local>enable dnsr static
Command: enable dnsr static

Success.

local>

```

disable dnsr

Purpose	Used to disable DNS relay on the switch.
Syntax	disable dnsr {cache static}
Description	This command is used, in combination with the enable dnsr command above, to enable and disable DNS Relay on the switch.
Parameters	<p><i>cache</i> – This parameter will allow the user to disable the cache lookup for the DNS rely on the switch.</p> <p><i>static</i> - This parameter will allow the user to disable the static table lookup for the DNS rely on the switch.</p>
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>

```

Example Usage:

To disable cache lookup for DNS relay.

```

local>disable dnsr cache
Command: disable dnsr cache

Success.

local>

```

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	<i>static</i> – 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 DNS relay 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 Cache Table Status : Disabled

DNS Relay Static Table

Domain Name           IP Address
-----
www.123.com.tw       10.12.12.123
bbs.ntu.edu.tw       140.112.1.23

Total Entries: 2

local>
```

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> all] {authentication [enable <password 16> disable] tx_mode [disable v1_only v1_compatible v2_only] rx_mode [v1_only v2_only v1_or_v2 disable] state [enable disable]}
enable rip	
disable rip	
show rip	ipif <ipif_name 12>

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

config rip	
Purpose	Used to configure RIP on the switch.
Syntax	config rip [ipif <ipif_name 12> all] {authentication [enable <password 16> disable] tx_mode [disable v1_only v1_compatible v2_only] rx_mode [v1_only v2_only v1_or_v2 disable] state [enable disable]}
Description	This command is used to configure RIP on the switch.

config rip

Parameters	<p><i><ipif_name 12></i> – The name of the IP interface.</p> <p><i>all</i> – To configure all RIP receiving mode for all IP interfaces.</p> <p><i>authentication [enable disable]</i> – Enables or disables authentication for RIP on the switch.</p> <p>§ <i><password 16></i> – Allows the specification of a case-sensitive password.</p> <p><i>tx_mode</i> – Determines how received RIP packets will be interpreted – as RIP version V1 only, V2 Only, or V1 Compatible (V1 and V2). This entry specifies which version of the RIP protocol will be used to transfer RIP packets. The Disabled entry prevents the reception of RIP packets.</p> <p>§ <i>disable</i> – Prevents the transmission of RIP packets.</p> <p>§ <i>v1_only</i> – Specifies that only RIP v1 packets will be transmitted.</p> <p>§ <i>v1_compatible</i> – Specifies that only RIP v1 compatible packets will be transmitted.</p> <p>§ <i>v2_only</i> - Specifies that only RIP v2 packets will be transmitted.</p> <p><i>rx_mode</i> – Determines how received RIP packets will be interpreted – as RIP version V1 only, V2 Only, or V1 or V2. This entry specifies which version of the RIP protocol will be used to receive RIP packets. The Disabled entry prevents the reception of RIP packets.</p> <p>§ <i>v1_only</i> – Specifies that only RIP v1 packets will be transmitted.</p> <p>§ <i>v2_only</i> - Specifies that only RIP v2 packets will be transmitted.</p> <p>§ <i>v1_or_v2</i> - Specifies that only RIP v1 or v2 packets will be transmitted.</p> <p><i>state [enable disable]</i> – Allows RIP to be enabled and disabled on the switch.</p>
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>

```

enable rip

Purpose	Used to enable RIP.
Syntax	enable rip
Description	This command is used to enable 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 to 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 and statistics for a given IP interface or for all IP interfaces.
Parameters	<i>ipif <ipif_name 12></i> – 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 display RIP configuration:

```

local>show rip
Command: show rip

RIP Global State : Disabled

RIP Interface Settings

Interface   IP Address      TX Mode  RX Mode  Authen-  State
-----   -
System     10.41.44.33/8  Disabled Disabled  Disabled Disabled

Total Entries : 1

local>

```

DVMRP COMMANDS

The DVMRP 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 [enable disable]}
enable dvmrp	
disable dvmrp	
show dvmrp neighbor	{ipif <ipif_name 12> ipaddress <network_address>}
show dvmrp nexthop	{ipaddress <network_address> ipif <ipif_name 12>}
show dvmrp routing_table	{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 <sec 1-65535> neighbor_timeout <sec 1-65535> state [enable disable]}
Description	This command is used to configure DVMRP on the switch.

config dvmrp

Parameters	<p><i><ipif_name 12></i> – The name of the IP interface for which DVMRP is to be configured.</p> <p><i>all</i> – Specifies that DVMRP is to be configured for all IP interfaces on the switch.</p> <p><i>metric <value 1-31></i> – 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><i>probe <second 1-65535></i> – DVMRP defined an extension to IGMP that allows routers to query other routers to determine if a DVMRP neighbor is present on a given subnetwork or not. This is referred to as a 'probe'. This entry will set an intermittent probe (in seconds) on the device that will transmit dvmrp messages, depending on the time specified. This probe is also used to "keep alive" the connection between DVMRP enabled devices. The default value is 10 seconds.</p> <p><i>neighbor_timeout <second 1-65535></i> – The time period for which DVMRP will hold Neighbor Router reports before issuing poison route messages. The default value is 35 seconds.</p> <p><i>state [enable disable]</i> – Allows DVMRP to be enabled or disabled.</p>
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.

show dvmrp routing_table

Parameters	<i>ipaddress <network_address></i> – 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/Netmask  Upstream Neighbor  Metric  Learned  Interface  Expire
-----
10.0.0.0/8              10.90.90.90        2       Local    System     -
20.0.0.0/8              20.1.1.1           2       Local    ip2        117
30.0.0.0/8              30.1.1.1           2       Dynamic  ip3        106

Total Entries: 3

local>
```

show dvmrp neighbor

Purpose	Used to display the DVMRP neighbor table.
Syntax	show dvmrp neighbor {ipif <ipif_name 12> ipaddress <network_address>}
Description	This command will display the current DVMRP neighbor table.
Parameters	<p><i><ipif_name 12></i> – The name of the IP interface for which you want to display the DVMRP neighbor table.</p> <p><i>ipaddress <network_address></i> – 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 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

local>

```

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><i><ipif_name 12></i> – The name of the IP interface for which you want to display the current DVMRP routing next hop table.</p> <p><i>ipaddress <network_address></i> – 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 display DVMRP routing next hop table:

```

local>show dvmrp nexthop
Command: show dvmrp nexthop

Source IP Address/Netmask Interface Name Type
-----
10.0.0.0/8                ip2                Leaf
10.0.0.0/8                ip3                Leaf
20.0.0.0/8                System             Leaf
20.0.0.0/8                ip3                Leaf
30.0.0.0/8                System             Leaf
30.0.0.0/8                ip2                Leaf

Total Entries: 6

local>

```

show dvmrp

Purpose	Used to display the current DVMRP routing table.
Syntax	show dvmrp {<ipif_name 12>}
Description	The command will display the current DVMRP routing table.
Parameters	<ipif_name 12> – The name of the IP interface for which you want to display the DVMRP routing table.
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    10.90.90.90/8    35                10    1    Disabled

Total Entries: 1

local>

```

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 [enable disable]}
enable pim	
disable pim	
show pim neighbor	{ipif <ipif_name 12> ipaddress <network_address>}
show pim	{ipif <ipif_name 12>}

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

config pim	
Purpose	Used to configure PIM settings for the switch or for specified IP interfaces.
Syntax	config pim [ipif <ipif_name 12> all] { hello <sec 1-18724> jp_interval <sec 1-18724> state [enable disable]}
Description	The config pim command is used to configure PIM settings and enable or disable PIM settings for specified IP interfaces. PIM must also be globally enabled to function (see enable pim).
Parameters	<p><i>ipif <ipif_name 12></i> – Name assigned to the specific IP interface being configured for PIM settings.</p> <p><i>all</i> – Used to configure PIM settings for all IP interfaces.</p> <p><i>hello <sec 1-18724></i> - The time, in seconds, between issuing hello packets to find neighboring routers.</p> <p><i>jp_interval <sec 1-18724></i> – The join/prune interval is the time value (seconds) between transmitting (flooding to all interfaces) multicast messages to downstream routers, and automatically ‘pruning’ a branch from the multicast delivery tree. The <i>jp_interval</i> is also the interval used by the router to automatically remove prune information from a branch of a multicast delivery tree and begin to flood multicast messages to all branches of that delivery tree. These two actions are equivalent. The range is between 1 and 18724 seconds. The default is 60 seconds.</p> <p><i>state [enable disable]</i> – This can enable or disable PIM for the specified IP interface. The default is disabled. Note that PIM settings must also be enabled globally for the switch with the enable pim described below for PIM to operate on any configured IP interfaces.</p>

config pim

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

Usage Example:

To configure PIM settings for IP interface “System”:

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

Success.

local>
```

enable pim

Purpose	Used to enable PIM function on the switch.
Syntax	enable pim
Description	This command will enable PIM for the switch. PIM settings must first be configured for specific IP interfaces using the config pim command.
Parameters	None.
Restrictions	Only administrator-level users can use this command.

Usage Example:

To enable PIM as previously configured on the switch:

```
local>enable pim
Command: enable pim

Success.

local>
```

disable pim

Purpose	Used to disable PIM function on the switch.
Syntax	disable pim
Description	This command will disable PIM for the switch. Any previously configured PIM settings will remain unchanged and may be enabled at a later time with the enable pim command.

disable pim

Parameters	None.
Restrictions	Only administrator-level users can use this command.

Usage Example:

To disable PIM on the switch:

```
local>disable pim
Command: disable pim

Success.

local>
```

show pim neighbor

Purpose	Used to display PIM neighbor router table entries.
Syntax	show pim neighbor {ipif <ipif_name 12> ipaddress <network_address>}
Description	This command will list current entries in the PIM neighbor table for a specified IP interface or destination router IP address.
Parameters	<p><i>ipif <ipif_name 12></i> – The name of an IP interface for which you want to view the PIM neighbor router table.</p> <p><i>ipaddress <network_address></i> The IP address and netmask of the destination routing device for which you want to view the neighbor router table. 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> <p>If no parameters are specified, all PIM neighbor router tables are displayed.</p>
Restrictions	None.

Example usage:

To display PIM settings as configured on the switch:

```

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

local>

```

show pim

Purpose	Used to display current PIM configuration.
Syntax	show pim {ipif <ipif_name 12>}
Description	This command will list current PIM configuration settings for a specified IP interface or all IP interfaces.
Parameters	<i>ipif <ipif_name 12></i> – The name of an IP interface for which PIM settings are listed. If no parameters are specified, all PIM settings are displayed for all interfaces.
Restrictions	None.

Usage Example:

To display PIM settings as configured on the switch:

```
local>show pim
Command: show pim

PIM Global State : Disabled

PIM-DM Interface Table

      Hello   Join/Prune
Interface  IP Address  Interval  Interval  State
-----
System    10.90.90.90/8  35        60        Enabled

Total Entries : 1

local>
```

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_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>}
Description	This command will display the current IP multicast forwarding cache.
Parameters	<p><i><group></i> – The multicast group ID.</p> <p><i>ipaddress <network_address></i> – 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      Source Address/Netmask  Upstream   Expire   Routing
  Group          -----
  -----
  224.1.1.1      10.48.74.121/32        10.48.75.63  30      dvmrp
  224.1.1.1      20.48.74.25 /32        20.48.75.25  20      dvmrp
  224.1.2.3      10.48.75.3 /3         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><i><ipif_name 12></i> – The name of the IP interface for which you want to display the IP multicast interface table for.</p> <p><i>protocol [dvmrp pim]</i> – Allows the user to specify whether or not to use the DVMRP or PIM protocol to display 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 by DVMRP entry:

```

local>show ipmc ipif System protocol dvmrp
Command: show ipmc ipif System protocol dvmrp

Interface Name  IP Address  Multicast Routing
-----
System          10.90.90.90  DVMRP

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

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

create md5 key

Purpose	Used to create a new entry in the MD5 key table.
Syntax	create md5 key <key_id 1-255> <password 16>
Description	This command is used to create an entry for the MD5 key table.
Parameters	<p><key_id 1-255> – The MD5 key ID. The user may enter a key ranging from 1 to 255.</p> <p><password> – An MD5 password of up to 16 bytes.</p>
Restrictions	Only administrator-level users can issue this command.

Usage Example

To create an entry in the MD5 key table:

```

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

Success.

local>

```

config md5 key

Purpose	Used to enter configure the password for an MD5 key.
Syntax	config md5 key <key_id 1-255> <password 16>
Description	This command is used to configure an MD5 key and password.

config md5 key

Parameters	<p><i><key_id 1-255></i> – The previously defined MD5 key ID.</p> <p><i><password 16></i> – The user may change the MD5 password for the md5 key. A new password of up to 16 characters can be created.</p>
Restrictions	Only administrator-level users can issue this command.

Usage Example

To configure an MD5 Key password:

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

Success.

local>
```

delete md5 key

Purpose	Used to delete an entry in the MD5 key table.
Syntax	delete md5 key <key_id 1-255>
Description	This command is used to delete a specific entry in the MD5 key table.
Parameters	<i><key_id 1-255></i> – The MD5 key ID the user wishes to delete.
Restrictions	Only administrator-level users can issue this command.

Usage Example

The delete an entry in the 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.
---------	-----------------------------------

show md5

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.
Restrictions	None.

Usage Example

To display the current MD5 key:

```
local>show md5
Command: show md5

MD5 Key Table Configurations

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

Total Entries: 4

local>
```

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 [enable disable] metric <value 0-16777215>}]
delete ospf area	<area_id>
config ospf area	<area_id> type [normal stub {stub_summary [enable disable] metric <value 0-16777215>}]
show ospf area	{<area_id>}
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 1-65535>}
show ospf host_route	<ipaddr>
create ospf aggregation	<area_id> <network_address> lsdb_type summary {advertise [enable disable]}
delete ospf aggregation	<area_id> <network_address> lsdb_type summary
config ospf aggregation	<area_id> <network_address> lsdb_type summary {advertise [enable disable]}
show ospf aggregation	<area_id>
show ospf lsdb	{area <area_id> advertise_router <ipaddr> type [rtrlink netlink summary assummary asexmlink]}
show ospf neighbor	<ipaddr>
show ospf virtual_neighbor	{<area_id> <neighbor_id>}
config ospf ipif	<ipif_name 12> {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 1-65535> state [enable disable]}
config ospf all	{area <area_id> priority <value> hello_interval <1-65535 sec> dead_interval <1-65535 sec> authentication [none simple <password 8> md5 <key_id 1-255>] metric <value 1-65535> state [enable disable]}
show ospf ipif	<ipif_name 12>
show ospf all	

Command	Parameters
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>]}
config 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>]}
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 router_id	
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 IP address of the OSPF router.
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.

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

Success.

local>
```

show ospf

Purpose	Used to display the current OSPF state on the switch.
Syntax	show ospf

show ospf

Description	This command will display the current state of OSPF on the switch, divided into the following categories: General OSPF settings OSPF Interface settings OSPF Area settings OSPF Virtual Interface settings OSPF Area Aggregation settings OSPF Host 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
		2/4	

create ospf area

Purpose	Used to configure OSPF area settings.
Syntax	create ospf area <area_id> type [normal stub {stub_summary [enable disable] metric <value 0-16777215>}]
Description	This command is used to create an OSPF area and configure its settings.
Parameters	<p><i><area_id></i> – The OSPF area ID. The user may enter 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><i>type [normal stub]</i> – The OSPF area mode of operation – stub or normal.</p> <p><i>stub_summary [enable disable]</i> – Enables or disables the OSPF area to import summary LSA advertisements.</p> <p><i>metric <value 0-16777215></i> – The OSPF area cost between 0 and 16777215. 0 denotes that the value will be automatically assigned. The default setting is 0.</p>
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.
Parameters	<i><area_id></i> – 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 [enable disable] metric <value 0-16777215>}]
Description	This command is used to configure an OSPF area's settings.
Parameters	<p><i><area_id></i> – The OSPF area ID. The user may enter 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><i>type [normal stub]</i> – Allows the specification of the OSPF mode of operation – stub or normal.</p> <p><i>stub_summary [enable disable]</i> – Allows the OSPF area import of LSA advertisements to be enabled or disabled.</p> <p><i>metric <value 0-16777215></i> – The OSPF area stub default cost.</p>
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 enable metric 1
Command: config ospf area 10.48.74.122 type stub stub_summary enable
metric 1

Success.

local>
```

show ospf area

Purpose	Used to display an OSPF area's configuration.
---------	---

show ospf area

Syntax	show ospf area {<area_id>}
Description	This command will display the current OSPF area configuration.
Parameters	<i><area_id></i> – 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
10.48.74.122 Stub       Enabled
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>}
Description	This command is used to configure the OSPF host route settings.
Parameters	<i><ipaddr></i> – The host's IP address. <i><area_id></i> – 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. <i>metric <value 1-65535></i> – A metric between 1 and 65535, which will be advertised.
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.
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>}
Description	This command is used to configure an OSPF host route settings.
Parameters	<p><ipaddr> – The IP address of the host.</p> <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><value> – A metric value between 1 and 65535 that will be advertised for the route.</p>
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.
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
10.48.74.122 1           10.1.1.1

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 [enable disable]}
Description	This command is used to create an OSPF area aggregation.

create ospf 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 [enable disable] – 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 enable
Command: create ospf aggregation 10.1.1.1 10.48.76.122/16
lsdb_type summary advertise enable

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 [enable disable]}
Description	This command is used to configure the OSPF area aggregation settings.
Parameters	<p><i><area_id></i> – 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><i><network_address></i> – The 32-bit number in the form of an IP address that uniquely identifies the network that corresponds to the OSPF Area.</p> <p><i>lsdb_type summary</i> – Specifies the type of address aggregation.</p> <p><i>advertise [enable disable]</i> – 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 enable
Command: config ospf aggregation 10.1.1.1 10.48.76.122/16 lsdb_type
summary advertise enable

Success.

local>

```

show ospf aggregation

Purpose	Used to display the current OSPF area aggregation settings.
---------	---

show ospf aggregation

Syntax	show ospf aggregation {<area_id>}
Description	This command will display the current OSPF area aggregation settings.
Parameters	<i><area_id></i> – Enter this parameter if you wish to view this table by a specific 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<br>Network Address | LSDB<br>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	<p><i>area_id <area_id></i> – 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><i>advertise_router <ipaddr></i> – The router ID of the advertising router.</p> <p><i>type [rtrlink netlink summary assummary asextlink]</i> – The type of link.</p>

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.
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>}
Description	This command will display the current OSPF virtual neighbor router table.
Parameters	<p><i><area_id></i> – 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><i><neighbor_id></i> – The OSPF router ID for the neighbor. 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

Total Entries : 1

local>

```

config ospf ipif

config ospf ipif

Purpose	Used to configure the OSPF interface settings.
Syntax	config ospf ipif <ipif_name 12> {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 1-65535> state [enable disable]}
Description	This command is used to configure the OSPF interface settings.
Parameters	<p><i><ipif_name 12></i> – The name of the IP interface.</p> <p><i>area <area_id></i> - 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><i>priority <value></i> – The priority used in the election of the Designated Router (DR). A number between 0 and 255.</p> <p><i>hello_interval <sec 1-65535></i> – 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><i>dead_interval <sec 1-65535></i> – 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 65535 seconds can be specified. The <i>dead interval</i> must be evenly divisible by the Hello Interval.</p> <p><i>metric <value 1-65535 ></i> – The interface metric (1 to 65535). Entering a 0 will allow automatic calculation of the metric.</p> <p><i>authentication</i> – Enter the type of authentication preferred. The user may choose between:</p> <ul style="list-style-type: none"> § <i>none</i> – Choosing this parameter will require no authentication. § <i>simple <password 8></i> – Choosing this parameter will set a simple authentication which includes a case-sensitive password of no more than 8 characters. § <i>md5 <key_id 1-255></i> – Choosing this parameter will set authentication based on md5 encryption. A previously configured MD5 key ID (1 to 255) is required. <p><i>metric <value 1-65535></i> – 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 1.</p> <p><i>state [enable disable]</i> – Used to enable or disable this function.</p>
Restrictions	Only administrator-level users can issue this command.

Usage Example

To configure OSPF interface settings:

```

local>config ospf ipif System priority 2 hello_interval 15 metric 2
state enable

Command: config ospf ipif System priority 2 hello_interval 15
metric 2 state enable

Success.

local>

```

config ospf all

Purpose	Used to configure all of the OSPF interfaces on the switch at one time.
Syntax	config ospf 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 1-65535> state [enable disable]}
Description	This command is used to configure all of the OSPF interfaces on the switch, using a single group of parameters, at one time.

config ospf all

Parameters	<p><i>area</i> <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><i>priority</i> <value> – The priority used in the election of the Designated Router (DR). A number between 0 and 255.</p> <p><i>hello_interval</i> <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><i>dead_interval</i> <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 65535 seconds can be specified. The Dead Interval must be evenly divisible by the Hello Interval.</p> <p><i>metric</i> <value 1-65535 > – The interface metric (1 to 65535). Entering a 0 will allow automatic calculation of the metric.</p> <p><i>authentication</i> – Enter the type of authentication preferred. The user may choose between:</p> <ul style="list-style-type: none"> § <i>none</i> – Choosing this parameter will require no authentication. § <i>simple</i> <password 8> – Choosing this parameter will set a simple authentication which includes a case-sensitive password of no more than 8 characters. § <i>md5</i> <key_id 1-255> – Choosing this parameter will set authentication based on md5 encryption. A previously configured MD5 key ID (1 to 255) is required. <p><i>metric</i> <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 1.</p> <p><i>state</i> [<i>enable</i> <i>disable</i>] – Used to enable or disable this function.</p>
Restrictions	Only administrator-level users can issue this command.

Usage Example

To configure all of the OSPF interfaces on the switch with a single group of parameters:

```

local>config ospf all state enable
Command: config ospf all state enable

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> all}
Description	This command will display the current OSPF interface settings for the specified interface name.
Parameters	<i><ipif_name 12></i> – The IP interface name for which you want to display the current OSPF interface settings. <i>all</i> – Entering this parameter will display all ospf Interface settings.
Restrictions	None.

Usage Example

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

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

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>
```

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.
Parameters	<p><i><area_id></i> – 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><i><neighbor_id></i> – 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><i>hello_interval <sec 1-65535></i> – 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><i>dead_interval <sec 1-65535></i> – 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 65535 seconds can be specified. The Dead Interval must be evenly divisible by the Hello Interval.</p> <p><i>authentication</i> – Enter the type of authentication preferred. The user may choose between:</p> <ul style="list-style-type: none"> § <i>none</i> – Choosing this parameter will require no authentication. § <i>simple <password 8></i> – Choosing this parameter will set a simple authentication which includes a case-sensitive password of no more than 8 characters. § <i>md5 <key_id 1-255></i> – Choosing this parameter will set authentication based on md5 encryption. A previously configured MD5 key ID (1 to 255) is required.
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>

```

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 [none simple <password 8> md5 <key_id 1-255>]}
Description	This command is used to configure the OSPF virtual interface settings.
Parameters	<p><i><area_id></i> – 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><i><neighbor_id></i> – 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><i>hello_interval <sec 1-65535></i> – 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><i>dead_interval <sec 1-65535></i> – 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 65535 seconds can be specified. The Dead Interval must be evenly divisible by the Hello Interval.</p> <p><i>authentication</i> – Enter the type of authentication preferred. The user may choose between:</p> <ul style="list-style-type: none"> § <i>none</i> – Choosing this parameter will require no authentication. § <i>simple <password 8></i> – Choosing this parameter will set a simple authentication which includes a case-sensitive password of no more than 8 characters. § <i>md5 <key_id 1-255></i> – Choosing this parameter will set authentication based on md5 encryption. A previously configured MD5 key ID (1 to 255) is required.

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>
```

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	<p><i><area_id></i> – 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><i><neighbor_id></i> – 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>
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.
---------	---

show ospf virtual_link

Syntax	show ospf virtual_link {<area_id> <neighbor_id>}
Description	This command will display the current OSPF virtual interface configuration.
Parameters	<p><i><area_id></i> – 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><i><neighbor_id></i> – 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.</p>
Restrictions	None.

Usage Example:

To display the current OSPF virtual interface configuration:

```

local>show ospf virtual_link

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

Total Entries: 1

local>

```

COMMAND HISTORY LIST

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

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

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

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

Example usage

To display all of the commands in the CLI:

```

local>?
..
?
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 auth_protocol
config 802.1x capability ports
config 802.1x init
config 802.1x reauth
config access profile profile_id
config account
config admin local_enable
config all_boxes_id
config arp_aging time
config authen_application
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All

```

show command_history

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

Example usage

To display the command history:

```

local>show command_history
Command: show command_history

?
? show
show vlan
config router_ports vlan2 add 1:1-1:10
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>

```

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> – The number of previously executed commands maintained in the buffer. Up to 40 of the latest executed commands may be viewed.
Restrictions	None.

Example usage

To configure the command history:

```

local>config command_history 20
Command: config command_history 20

Success.

local>

```

TECHNICAL SPECIFICATIONS

Physical and Environmental	
AC Input & External Redundant power Supply:	100 – 120; 200 - 240 VAC, 50/60 Hz (internal universal power supply)
Power Consumption:	90 watts maximum
DC Fans:	2 built-in 40 x 40 x10 mm fans
Operating Temperature:	0 to 40 degrees Celsius
Storage Temperature:	-25 to 55 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
Weight:	3.15 kg
EMC:	FCC Class A , CE Mark, C-Tick
Safety:	CSA International

General	
Standards:	IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.1 P/Q VLAN IEEE 802.3x Full-duplex Flow Control IEEE 802.3 Nway auto-negotiation IEEE 802.3z SFP ports IEEE 802.1D/w/s Spanning trees. IEEE 802.1p QoS (Priority Bits) IEEE 802.1X Access Control
Protocols:	CSMA/CD

General	
Data Transfer Rates:	Half-duplex Full-duplex
Ethernet	10 Mbps 20Mbps
Fast Ethernet	100Mbps 200Mbps
Gigabit Ethernet	n/a 2000Mbps
Fiber Optic	SFP (Mini GBIC) Support IEEE 802.3z 1000BASE-LX (DEM-310GT transceiver) IEEE 802.3z 1000BASE-SX (DEM-311GT transceiver) IEEE 802.3z 1000BASE-LH (DEM-314GT transceiver) IEEE 802.3z 1000BASE-ZX (DEM-315GT transceiver)
Network Cables:	
10BASE-T:	UTP Cat.5, Cat.5 Enhanced for 1000Mbps UTP Cat.5 for 100Mbps UTP Cat.3, 4, 5 for 10Mbps
100BASE-TX:	EIA/TIA-568 100-ohm screened twisted-pair (STP)(100m)
Number of Ports:	48 10/100 + 2 Gigabit Ethernet ports

Performance	
Transmission Method:	Store-and-forward
RAM Buffer:	1 MB per device
Filtering Address Table:	16K MAC address per device
Packet Filtering/Forwarding Rate:	Full-wire speed for all connections. 148,810 pps per port (for 100Mbps) 1,488,100 pps per port (for 1000Mbps)
MAC Address Learning:	Automatic update.
Forwarding Table Age Time:	Max age: 10 - 1000000 seconds. Default = 300.