



DES-3326S

Stackable Layer 3 Switch

Command Line Interface Reference Manual

May 2005

651E3326055

Trademarks

Copyright ©2005 D-Link Corporation.

Contents subject to change without prior notice.

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

Copyright Statement

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

FCC Warning

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

CE Mark Warning

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

VCCI Warning

注意

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

Table of Contents

Introduction.....	1
Using the Console CLI.....	4
Command Syntax.....	8
Basic Switch Commands	12
Switch Port Commands.....	32
Port Security Commands	35
Network Management Commands.....	40
MAC Notification Commands	66
Download/Upload Commands.....	71
Network Monitoring Commands	74
Spanning Tree Commands.....	93
Forwarding Database Commands	101
Broadcast Storm Control Commands.....	110
QOS Commands	113
Port Mirroring Commands	125
VLAN Commands	131
Link Aggregation Commands.....	140
Basic IP Commands	148
IGMP Snooping Commands	151
802.1X Commands	160
Access Control List and CPU Interface Filtering Commands	176
Traffic Segmentation Commands	198
Stacking Commands	201
Time and SNTP Commands	205
ARP Commands.....	214
Routing Table Commands	220
Route Redistribution Commands	224
IGMP Commands	231
Bootp Relay Commands	235
DNS Relay Commands	242
RIP Commands	250
DVMRP Commands	255
PIM Commands	262
IP Multicasting Commands.....	268
MD5 Configuration Commands.....	271
OSPF Configuration Commands	276
Command History List.....	305
Technical Specifications	310

Glossary	312
----------------	-----

INTRODUCTION

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

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

Accessing the Switch via the Serial Port

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

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

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

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

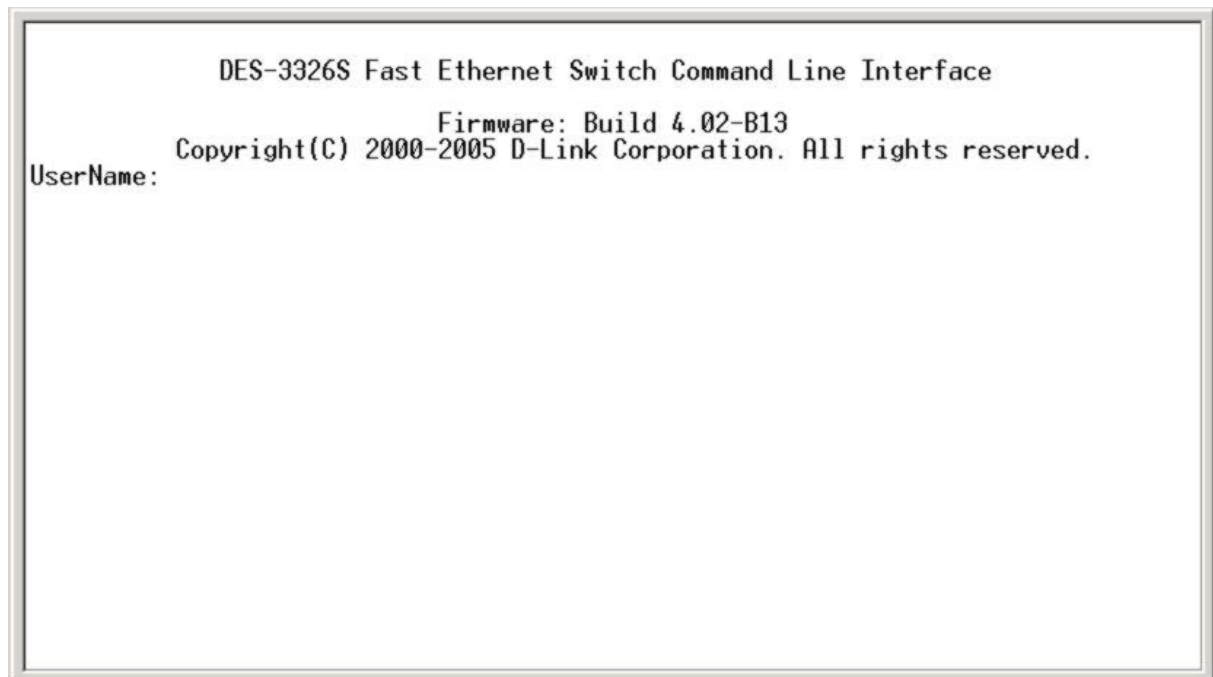


Figure 1-1. Initial Console screen

There is no initial username or password. Just press the **Enter** key twice to display the CLI input cursor – **DES-3326S:4#**. This is the command line where all commands are input.

Setting the Switch's IP Address

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

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

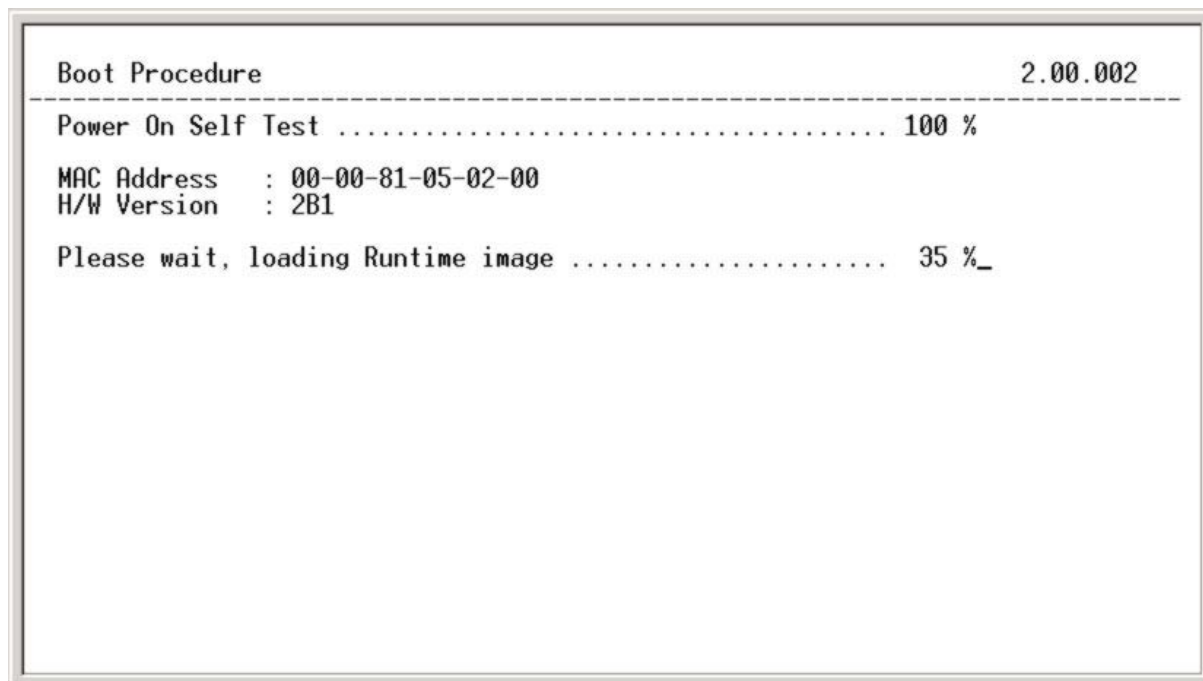


Figure 1-2. Boot Screen

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

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

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

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.

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.


```
DES-3326S Fast Ethernet Switch Command Line Interface
                               Firmware: Build 4.02-B13
        Copyright(C) 2000-2005 D-Link Corporation. All rights reserved.
UserName:
PassWord:

DES-3326S:4#config ipif System ipaddress 10.41.44.33/8
Command: config ipif System ipaddress 10.41.44.33/8

Success.
DES-3326S:4#
```

Figure 1-3. Assigning the Switch an IP Address

In the above example, the Switch was assigned an IP address of 10.41.44.33 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.



Note: Some nonalphanumeric characters may cause the Switch to reboot if entered using the CLI interface. Be careful to use only alphanumeric characters when entering commands.

USING THE CONSOLE CLI

The DES-3326S 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
- 9,600 baud
- 8 data bits
- No parity
- One stop bit
- No flow control

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

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

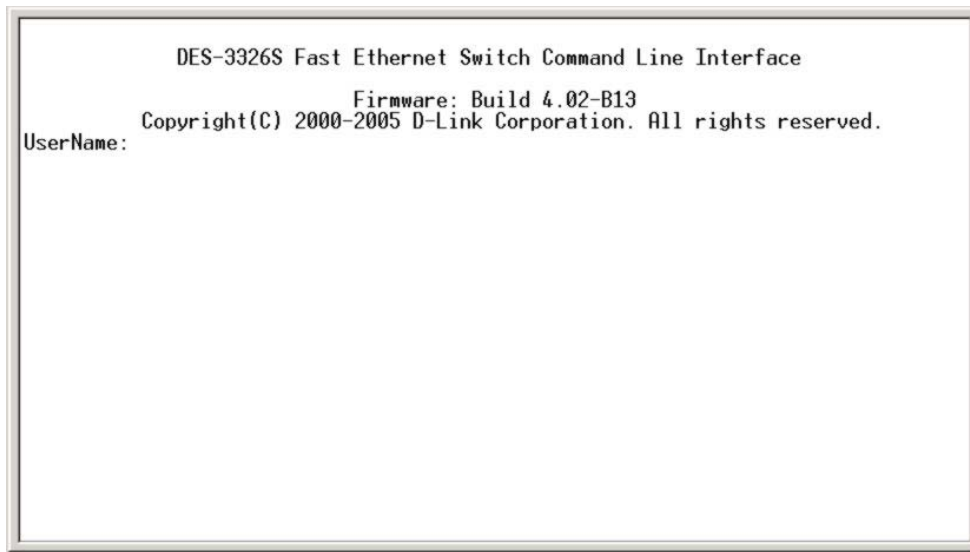


Figure 2-1. Initial Console Screen

Commands are entered at the command prompt, **DES-3326S:4#**.

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



Figure 2-2. The ? Command

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

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

```
DES-3326S Fast Ethernet Switch Command Line Interface
                          Firmware: Build 4.02-B13
Copyright(C) 2000-2005 D-Link Corporation. All rights reserved.
UserName:
PassWord:

DES-3326S:4#config account
Command: config account

Next possible completions:
<username>

DES-3326S:4#_
```

Figure 2-3. Example Command Parameter Help

In this case, the command **config account** was entered with the parameter **<username>**. The CLI will then prompt 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.

```
DES-3326S Fast Ethernet Switch Command Line Interface
                          Firmware: Build 4.02-B13
Copyright(C) 2000-2005 D-Link Corporation. All rights reserved.
UserName:
PassWord:

DES-3326S:4#config account
Command: config account

Next possible completions:
<username>

DES-3326S:4#config account
```

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

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

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

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

```

PassWord:
DES-3326S:4#config account
Command: config account

Next possible completions:
<username>

DES-3326S:4#config account
Command: config account

Next possible completions:
<username>

DES-3326S:4#lookup

Available commands:
..                ?                clear                config
create            delete            dir                  disable
download          enable            login                logout
ping              reboot            reset                save
show              traceroute        upload
DES-3326S:4#

```

Figure 2-5. The Next Available Commands Prompt

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

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

```

create            delete            dir                disable
download          enable            login              logout
ping              reboot            reset              save
show              traceroute        upload

DES-3326S:4#show
Command: show

Next possible completions:
802.1p            802.1x            account            arprentry
bandwidth_control bootp_relay        command_history    dnsr
dvmrp             error             fdb                gvrp
igmp              igmp_snooping     ipfdb              ipif
ipmc              iproute           lacp_port          link_aggregation
log               mac_notification  md5                mirror
multicast_fdb     ospf              packet             pim
port_security     ports             radius             rip
route             router_ports      scheduling          serial_port
session           snmp              sntp               stacking
stp               switch            syslog              time
traffic           traffic_segmentation
utilization       vlan              cpu                trusted_host
access_profile

DES-3326S:4#_

```

Figure 2-6. Next possible completions: Show Command

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

COMMAND SYNTAX

The following symbols are used to describe how command entries are made and values and arguments are specified in this manual. 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}	
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 detail . 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>
config account	<username>
show account	
show session	
show switch	
show serial_port	
config serial_port	baud_rate [9600 19200 38400 115200] auto_logout [never 2_minutes 5_minutes 10_minutes 15_minutes]
enable clipaging	
disable clipaging	
enable telnet	<tcp_port_number>
disable telnet	
enable web	<tcp_port_number>
disable web	
save	
reboot	
reset	{config system}
login	
logout	

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

create account

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

Example Usage:

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

```
DES-3326S:4#create account admin dlink
```

```
Command: create account admin dlink
```

```
Enter a case-sensitive new password:****
```

```
Enter the new password again for confirmation:****
```

```
Success.
```

```
DES-3326S:4#
```

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:

DES-3326S:4#config account dlink

Command: config account dlink

Enter a old password:****

Enter a case-sensitive new password:****

Enter the new password again for confirmation:****

Success.

DES-3326S:4#

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:

```
DES-3326S:4#show account
```

```
Command: show account
```

```
Current Accounts:
```

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

```
DES-3326S:4#
```

delete account

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

Example Usage:

To delete the user account "System":

```
DES-3326S:4#delete account System
```

```
Command: delete account System
```

```
Success.
```

```
DES-3326S:4#
```

show session

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

Example Usage:

To display the way that the users logged in:

DES-3326S:4#show session

Command: show session

ID	Login Time	Live Time	From	Level	Name

*8	00000 days 03:27:34	0:0:32.670	Serial Port	4	Anonymous

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:

```
DES-3326S:4#show serial_port
```

```
Command: show serial_port
```

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

```
DES-3326S:4#
```


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:

```
DES-3326S:4#show switch
Command: show switch

Device Type      : DES-3326S Fast-Ethernet Switch
Module Type      : DES-332GS 1-port GBIC Gigabit Ethernet and 1 Stacking Port
Unit ID          : 1
MAC Address      : 00-05-5D-17-FF-60
IP Address       : 10.90.90.90 (Manual)
VLAN Name        : default
Subnet Mask      : 255.0.0.0
Default Gateway  : 10.1.1.254
Boot PROM Version : Build 0.00.001
Firmware Version : Build 4.01-B12
Hardware Version  : 2B1
Device S/N       :
System Name      :
System Location   :
System Contact    :
Spanning Tree    : Disabled
GVRP             : Disabled
IGMP Snooping    : Disabled
TELNET           : Enabled (TCP 23)
WEB              : Enabled (TCP 80)
RMON             : Disabled
RIP              : Disabled
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

show serial_port

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

Example Usage:

To display the serial port setting:

```
DES-3326S:4#show serial_port
```

```
Command: show serial_port
```

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

```
DES-3326S:4#
```

config serial_port

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

Example Usage:

To configure baud rate:

DES-3326S:4#config serial_port baud_rate 9600

Command: config serial_port baud_rate 9600

Success.

DES-3326S:4#

enable clipaging

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

Example Usage:

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

DES-3326S:4#enable clipaging**Command: enable clipaging****Success.**

DES-3326S:4#

disable clipaging

Purpose	Used to disable the pausing of the console screen scrolling at the end of each page when the show command would display more than one screen of information.
Syntax	disable clipaging
Description	This command is used to disable the pausing of the console screen at the end of each page when the show command would display more than one screen of information.
Parameters	none.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

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

```
DES-3326S:4#disable clipaging
```

```
Command: disable clipaging
```

```
Success.
```

```
DES-3326S:4#
```

enable telnet

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

Example Usage:

To enable Telnet and configure port number:

```
DES-3326S:4#enable telnet 23
```

```
Command: enable telnet 23
```

```
Success.
```

```
DES-3326S:4#
```

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:

```
DES-3326S:4#disable telnet
```

```
Command: disable telnet
```

```
Success.
```

```
DES-3326S:4#
```

enable web

Purpose	Used to enable the HTTP-based management software on the Switch.
Syntax	enable web <tcp_port_number>
Description	This command is used to enable the Web-based management software on the Switch. The user can specify the TCP port number the Switch will use to listen for Telnet requests.
Parameters	<tcp_port_number> – The TCP port number. TCP ports are numbered between 1 and 65535. The “well-known” port for the Web-based management software is 80.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable HTTP and configure port number:

```
DES-3326S:4#enable web 80
```

```
Command: enable web 80
```

```
Success.
```

```
DES-3326S:4#
```


disable web

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

Example Usage:

To disable HTTP:

```
DES-3326S:4#disable web
```

```
Command: disable web
```

```
Success.
```

```
DES-3326S:4#
```

save

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

Example Usage:

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

```
DES-3326S:4#save
```

```
Command: save
```

```
Saving all settings to NV-RAM... 100%
```

```
done.
```

```
DES-3326S:4#
```

reboot

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

Example Usage:

To restart the Switch:

DES-3326S:4#reboot

Command: reboot

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

Please wait, the Switch is rebooting...

reset	
Purpose	Used to reset the Switch to the factory default settings.
Syntax	reset {config system}
Description	This command is used to restore the Switch's configuration to the default settings assigned from the factory.
Parameters	<p>config – If config is specified, all of the factory default settings are restored on the Switch including the IP address, user accounts, and the Switch history log. The Switch will not reboot. New user accounts information and IP settings will need to be assigned.</p> <p>system – If system is specified all of the factory default settings are restored on the Switch. The Switch will reboot. New user accounts information and IP settings will need to be assigned.</p> <p>If no parameter is specified, the Switch's current IP address, user accounts, and the Switch history log are retained. All other parameters are restored to their factory default settings. The Switch will not reboot.</p>
Restrictions	Only administrator-level users can issue this command.

Example Usage:

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

DES-3326S:4#reset config

Command: reset config

Success.

DES-3326S:4#

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:

DES-3326S:4#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:

DES-3326S:4#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_half 1000_full]] learning [enable disable] state [enable disable]}
show ports	<portlist all>

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

config ports

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

Example Usage:

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

```
DES-3326S:4#config ports 1-3 speed 10_full learning on state enable
Command: config ports 1-3 speed 10_full learning on state enable
Success.
DES-3326S:4#
```

show ports

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

Example Usage:

To display ports status:

DES-3326S:4#show ports

Command: show ports

Port	Port State	Settings Speed/Duplex/FlowCtrl	Connection Speed/Duplex/FlowCtrl	Address Learning
1	Enabled	Auto/Disabled	Link Down	Enabled
2	Enabled	Auto/Disabled	Link Down	Enabled
3	Enabled	Auto/Disabled	Link Down	Enabled
4	Enabled	Auto/Disabled	Link Down	Enabled
5	Enabled	Auto/Disabled	Link Down	Enabled
6	Enabled	Auto/Disabled	Link Down	Enabled
7	Enabled	Auto/Disabled	Link Down	Enabled
8	Enabled	Auto/Disabled	Link Down	Enabled
9	Enabled	Auto/Disabled	Link Down	Enabled
10	Enabled	Auto/Disabled	100M/Full/None	Enabled
11	Enabled	Auto/Disabled	Link Down	Enabled
12	Enabled	Auto/Disabled	Link Down	Enabled
13	Enabled	Auto/Disabled	Link Down	Enabled
14	Enabled	Auto/Disabled	Link Down	Enabled
15	Enabled	Auto/Disabled	Link Down	Enabled
16	Enabled	Auto/Disabled	Link Down	Enabled
17	Enabled	Auto/Disabled	100M/Full/None	Enabled
18	Enabled	Auto/Disabled	Link Down	Enabled
19	Enabled	Auto/Disabled	Link Down	Enabled
20	Enabled	Auto/Disabled	Link Down	Enabled

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	<portlist> all admin_state [enable disable] max_learning_addr <0-10> lock_address_mode [Permanent DeleteOnTimeout DeleteOnReset]
delete port_security_entry	vlan_name <vlan_name 32> mac_address <macaddr> port <port>
clear port_security_entry	port <portlist>
show port_security	

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

config port_security

Purpose	Used to configure port lock settings.
Syntax	<pre>config port_security <portlist> all admin_state [enable disable] max_learning_addr <max_lock_no 0-10> lock_address_mode [Permanent DeleteOnTimeout DeleteOnReset]</pre>
Description	This command allows for the configuration of the port lock security feature. Only the ports listed in the <portlist> are effected.
Parameters	<p>all – configure port lock for all ports on the Switch.</p> <p>portlist – specifies a range of ports to be configured. The port list is specified by listing the lowest Switch number and the beginning port number on that Switch, separated by a colon. Then highest Switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are seperated by a dash. For example, 1:3 would specify 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>admin_state [enable disaled] – enable or disable port lock for the listed ports.</p> <p>max_learning_addr <1-10> - use this to limit the number of MAC addresses dynamically listed in the FDB for the ports.</p> <p>lock_address_mode[Permanent DeleteOnTimeout DeleteOnReset] – The options for clearing the aging out locked addresses for the port are as follows:</p> <p>Permanent – Locked MAC addresses do not age out. MAC addresses retain locked status even if the Switch is restarted.</p> <p>DeleteOnTimeout – Removes locked MAC addresses upon aging out of the FDB. MAC address aging is set using FDB commands. (See config fdb aging_time in Forwarding Database Commands).</p> <p>DeleteOnReset – Locked MAC addresses do not age out. If the Switch is restarted reset, the MAC addresses will no longer have locked status. Any previously learned addresses will need to be relearned.</p>
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure the port lock for ports 1:12 – 1:14 to delete the dynamic address table entries on timeout:

```
DES-3326S:4#config port_security ports 12-14
lock_address_mode DeleteOnTimeout
Command: config port_security ports 12-14 lock_address_mode
DeleteOnTimeout

Success.

DES-3326S:4#
```

delete port_security_entry

Purpose	Used to remove port security from specific devices according to VLAN and port.
Syntax	delete port_security_entry vlan_name <vlan_name 32> mac_address <macaddr> port <port>
Description	This allows specific MAC addresses to be excluded from port locked status for individual ports.
Parameters	<p><vlan_name 32> – The name of the VLAN on which the port resides.</p> <p><macaddr> – The MAC address that will be removed from eligibility for locked status.</p> <p><port> – The port number corresponding to the MAC address of the device being removed.</p>
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To remove a port eligibility for a specific device:

```
DES-3326S:4#delete port_security_entry vlan_name default
mac_address a1-01-01-01-01-01 port 4
Command: delete port_security_entry vlan_name default
mac_address A1-01-01-01-01-01 port 1:4

Success

DES-3326S:4#
```

config port_security_entry

Purpose	Used to clear the MAC entries learned from the specified port(s) for the port security function
Syntax	clear port_security_entry port <portlist>
Description	This will delete all entries from the forwarding data base for a specific port or range of ports.
Parameters	portlist – specifies a range of ports to be configured. The port list is specified by listing the lowest Switch number and the beginning port number on that Switch, separated by a colon. Then highest Switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 would specify 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 clear the port security entries for a specific port (port 10):

DES-3326S:4#clear port_security_entry port 10

Command: clear port_security_entry port 10

Success.

DES-3326S:4#

show port_security

Purpose	Used to display the current port lock configuration.
Syntax	show port_security {<portlist>}
Description	This command is used to display the current port lock configuration of a range of ports.
Parameters	<portlist> – specifies a range of ports to 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 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 would specify 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 the port security configuration on the entire Switch:

DES-3326S:4#show port_security				
Command: show port_security				
Port#	Admin	State	Max. Learning	Addr. Lock Address Mode
----	-----	-----	-----	-----
1	Disabled	1	1	DeleteOnReset
2	Disabled	1	1	DeleteOnReset
3	Disabled	1	1	DeleteOnReset
4	Disabled	1	1	DeleteOnReset
5	Disabled	1	1	DeleteOnReset
6	Disabled	1	1	DeleteOnReset
7	Enabled	10	10	DeleteOnReset
8	Disabled	1	1	DeleteOnReset
9	Disabled	1	1	DeleteOnReset
10	Disabled	1	1	DeleteOnReset
11	Disabled	1	1	DeleteOnReset
12	Disabled	1	1	DeleteOnReset
13	Disabled	1	1	DeleteOnReset
14	Disabled	1	1	DeleteOnReset
15	Disabled	1	1	DeleteOnReset
16	Disabled	1	1	DeleteOnReset
17	Disabled	1	1	DeleteOnReset
18	Disabled	1	1	DeleteOnReset
19	Disabled	1	1	DeleteOnReset
20	Disabled	1	1	DeleteOnReset
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh				



NETWORK MANAGEMENT COMMANDS

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

The DES-3326S 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:

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

Command	Parameters
create snmp user	<username 32> <groupname 32> v1 v2c v3 encrypted auth [md5 sha] <auth_password 8-16> priv [none des <priv_password 8-16>]
delete snmp user	<username 32>
show snmp user	
show snmp groups	
create snmp view	<view_name 32> <oid> view_type [included excluded]
delete snmp view	<view_name 32> [all oid]
show snmp view	<view_name 32>
create snmp community	<community_string 32> view <view_name 32> [read_only read_write]
delete snmp community	<community_string 32>
show snmp community	
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>
create snmp host	<ipaddr> v1 v2c v3 noauth_nopriv <auth_string 32> auth_nopriv <auth_string 32> auth_priv <auth_string 32>
delete snmp host	<ipaddr>
show snmp host	<ipaddr>
enable rmon	
disable rmon	
ping	<ipaddr> times <value 1-255> timeout <sec 1-99>
traceroute	<ipaddr> port <value 30000-64900> timeout <sec 1-65525> probe <value 1-9> ttl <value 1-60>

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> [v1 v2c v3 {encrypted auth [md5 sha] <auth_password> priv [none des <priv_password>}}]
Description	The create snmp user command creates a new SNMP user and adds the user to an SNMP group that is also created by this command.
Parameters	<p><username 32> – An alphanumeric name of up to 32 characters that will identify the new SNMP user.</p> <p><groupname 32> – An alphanumeric name of up to 32 characters that will identify the SNMP group the new SNMP user will be associated with.</p> <p>v1 – Specifies that SNMP version 1 will be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices.</p> <p>v2c – Specifies that SNMP version 2c will be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features.</p> <p>v3 – Specifies that the SNMP version 3 will be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds:</p> <p>Message integrity – ensures that packets have not been tampered with in transit.</p> <p>Authentication – determines that an SNMP message is from a valid source.</p> <p>Encryption – scrambles the contents of messages to prevent it being seen by an unauthorized source.</p> <p>encrypted – Specifies that the password will be in an encrypted format.</p> <p>auth [md5 sha] – Initiate an authentication-level setting session.</p> <p>md5 – Specifies that the HMAC-MD5-96 authentication level will be used.</p> <p>sha – Specifies that the HMAC-SHA-96 authentication level will be used.</p> <p><auth_password 8-16> – An alphanumeric sting of between 8 and 16 characters that will be used to authorize the agent to receive packets for the host.</p> <p>des <priv_password 8-16> – An alphanumeric string of between 8 and 16 characters that will be used to encrypt the contents of messages the host sends to the agent.</p>
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To create an SNMP user on the Switch:

```
DES-3326S:4#create snmp user dlink default v3 encrypted auth
md5 auth_password priv none
Command: create snmp user dlink default v3 encrypted auth md5
auth_password priv none

Success.

DES-3326S:4#
```

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	<username 32> – An alphanumeric string of up to 32 characters that identifies the SNMP user that will be deleted.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete a previously entered SNMP user on the Switch:

```
DES-3326S:4#delete snmp user dlink
```

```
Command: delete snmp user dlink
```

```
Success.
```

```
DES-3326S:4#
```

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:

```
DES-3326S:4#show snmp user
```

```
Command: show snmp user
```

Username	Group Name	SNMP	Version	Auth-Protocol	PrivProtocol
----------	------------	------	---------	---------------	--------------

initial	initial	V3	None	None	
---------	---------	----	------	------	--

```
Total Entries: 1
```

```
DES-3326S:4#
```

show snmp groups

Purpose	Used to display the group-names of SNMP groups currently configured on the Switch. The security model, level, and status of each group is also displayed.
Syntax	show snmp groups
Description	The show snmp groups command displays the group-names of SNMP groups currently configured on the Switch. The security model, level, and status of each group is also displayed.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To display the currently configured SNMP groups on the Switch:

DES-3326S:4#show snmp groups

Command: show snmp groups

Vacm Access Table Settings

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

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

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

Group Name	: Group6
ReadView Name	: ReadView
WriteView Name	: WriteView
Notify View Name	: NotifyView
Securiy Model	: SNMPv3
Securiy Level	: authPriv
Group Name	: Group7
ReadView Name	: ReadView
WriteView Name	: WriteView
Notify View Name	: NotifyView
Securiy Model	: SNMPv3
Securiy Level	: authPriv
Group Name	: initial
ReadView Name	: restricted
WriteView Name	:
Notify View Name	: restricted
Securiy Model	: SNMPv3
Securiy Level	: NoAuthNoPriv
Group Name	: ReadGroup
ReadView Name	: CommunityView
WriteView Name	:
Notify View Name	: CommunityView
Securiy Model	: SNMPv1
Securiy Level	: NoAuthNoPriv

Group Name : ReadGroup
ReadView Name : CommunityView
WriteView Name :
Notify View Name : CommunityView
Securiy Model : SNMPv2
Securiy Level : NoAuthNoPriv

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

Group Name : WriteGroup
ReadView Name : CommunityView
WriteView Name : CommunityView
Notify View Name : CommunityView
Securiy Model : SNMPv2
Securiy Level : NoAuthNoPriv

Total Entries: 10

DES-3326S:4#

create snmp view

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

DES-3326S:4#create snmp view dlinkview 1.3.6 view_type included

Command: create snmp view dlinkview 1.3.6 view_type included

Success.

DES-3326S:4#

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><view_name 32> – An alphanumeric string of up to 32 characters that identifies the SNMP view to be deleted.</p> <p>all – Specifies that all of the SNMP views on the Switch will be deleted.</p> <p><oid> – The object ID that identifies an object tree (MIB tree) that will be deleted from the Switch.</p>
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete a previously configured SNMP view from the Switch:

DES-3326S:4#delete snmp view dlinkview

Command: delete snmp view dlinkview

Success.

DES-3326S:4#

show snmp view

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

Example Usage:

To display the previously created SNMP view:

```
DES-3326S:4#show snmp view
Command: show snmp view
Vacm View Table Settings
View Name      Subtree      View Type
-----
ReadView       1            Included
WriteView      1            Included
NotifyView     1.3.6        Included
restricted     1.3.6.1.2.1.1 Included
restricted     1.3.6.1.2.1.11 Included
restricted     1.3.6.1.6.3.10.2.1 Included
restricted     1.3.6.1.6.3.11.2.1 Included
restricted     1.3.6.1.6.3.15.1.1 Included
CommunityView  1.3.6.1.6.3  Excluded
CommunityView  .3.6.1.6.3.1 Included
Total Entries: 10
DES-3326S:4#
```

create snmp community

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

Example Usage:

To create the SNMP community string "dlink:"

DES-3326S:4#create snmp community dlink view ReadView read_write

Command: create snmp community dlink view ReadView read_write

Success.

delete snmp community

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

Example Usage:

To delete the SNMP community string "dlink:"

DES-3326S:4#delete snmp community dlink

Command: delete snmp community dlink

Success.

DES-3326S:4#

show snmp community

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

Example Usage:

To display the currently entered SNMP community strings:

DES-3326S:4#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		

config snmp engineID

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

Example Usage:

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

```
DES-3326S:4#config snmp 0035636666
```

```
Command: config snmp engineID 0035636666
```

```
Success.
```

```
DES-3326S:4#
```

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> notify_view <view_name 32> notify_view <view_name 32>}
Description	The create snmp group command creates a new SNMP group, or a table that maps SNMP users to SNMP views.
Parameters	<p><groupname 32> – An alphanumeric name of up to 32 characters that will identify the SNMP group the new SNMP user will be associated with.</p> <p>v1 – Specifies that SNMP version 1 will be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices.</p> <p>v2c – Specifies that SNMP version 2c will be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features.</p> <p>v3 – Specifies that the SNMP version 3 will be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds:</p> <p>Message integrity – ensures that packets have not been tampered with in transit.</p> <p>Authentication – determines that an SNMP message is from a valid source.</p> <p>Encryption – scrambles the contents of messages to prevent it being seen by an unauthorized source.</p> <p>noauth_nopriv – Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager.</p> <p>auth_nopriv – Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager.</p> <p>auth_priv – Specifies that authorization will be required, and that packets sent between the switch and a remote SNMP manger will be encrypted.</p> <p>read_view – Specifies that the SNMP group being created can request SNMP messages.</p> <p><view_name 32> – An alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the Switch.</p> <p>notify_view – 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:”

```
DES-3326S:4#create snmp group sg1 v3 noauth_nopriv
read_view v1 write_view v1 notify_view v1
```

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

Success.

```
DES-3326S:4#
```

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:

```
DES-3326S:4#show snmp engineID
```

Command: show snmp engineID

SNMP Engine ID : 0035636666

```
DES-3326S:4#
```

delete snmp group

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

Example Usage:

To delete the SNMP group named “sg1”.

DES-3326S:4#delete snmp group sg1

Command: delete snmp group sg1

Success.

DES-3326S:4#

show snmp host

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

Example Usage:

To display the currently configured SNMP hosts on the Switch:

DES-3326S:4#show snmp host

Command: show snmp host

SNMP Host Table

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

Total Entries: 2

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><ipaddr> – The IP address of the remote management station that will serve as the SNMP host for the Switch.</p> <p>v1 – Specifies that SNMP version 1 will be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices.</p> <p>v2c – Specifies that SNMP version 2c will be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features.</p> <p>v3 – Specifies that the SNMP version 3 will be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds:</p> <p>Message integrity – ensures that packets have not been tampered with in transit.</p> <p>Authentication – determines that an SNMP message is from a valid source.</p> <p>Encryption – scrambles the contents of messages to prevent it being seen by an unauthorized source.</p> <p>noauth_nopriv – Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager.</p> <p>auth_nopriv – Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager.</p> <p>auth_priv – Specifies that authorization will be required, and that packets sent between the switch and a remote SNMP manger will be encrypted.</p> <p><auth_sting 32> – An alphanumeric string used to authorize a remote SNMP manager to access the Switch's SNMP agent.</p>
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To create an SNMP host to receive SNMP messages:

DES-3326S:4#create snmp host 10.48.74.100 v3 auth_priv public

Command: create snmp host 10.48.74.100 v3 auth_priv public

Success.

DES-3326S:4#

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:

```
DES-3326S:4#delete snmp host 10.48.74.100
```

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

```
Success.
```

```
DES-3326S:4#
```

show snmp host

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

Example Usage:

To display the currently configured SNMP hosts on the Switch:

DES-3326S:4#show snmp host

Command: show snmp host

SNMP Host Table

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

Total Entries: 2

DES-3326S:4#

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:

```
DES-3326S:4#enable rmon
```

```
Command: enable rmon
```

```
Success.
```

```
DES-3326S:4#
```

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:

```
DES-3326S:4#disable rmon
```

```
Command: disable rmon
```

```
Success.
```

```
DES-3326S:4#
```

ping

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

Example Usage:

To send ICMP echo message to “10.48.74.121” for 4 times:

```
DES-3326S:4#ping 10.48.74.121 times 4
Command: ping 10.48.74.121
Reply from 10.48.74.121, time<10ms
Reply from 10.48.74.121, time<10ms
Reply from 10.48.74.121, time<10ms
Reply from 10.48.74.121, time<10ms
Ping Statistics for 10.48.74.121
Packets: Sent =4, Received =4, Lost =0
DES-3326S:4#
```

traceroute

Purpose	Used to determine the network path between two devices.
Syntax	traceroute <ipaddr> {ttl <value 1-60>} {port <value 30000-64900>} {timeout <sec 1-65525>} {probe <value 1-9>}
Description	This command allows you to trace a route between the Switch and a give host on the network.
Parameters	<p><ipaddr> – the IP address of the remote device.</p> <p>ttl <value 1-60> – the time to live value of the trace route request. This is the maximum number of routers the traceroute command will cross while seeking the network path between two devices. The maximum value is</p> <p>port <value 30000-64900> – the port number. Must be above 1024.</p> <p>timeout <sec 1–65525> defines the time-out period while waiting for a response from the remote device.</p> <p>probe <value 1-9> – the number of probing.</p>
Restrictions	Only administrator-level users can issue this command.

Example Usage:

Trace the routed path between the Switch and 10.48.74.121.

```
DES-3326S:4#traceroute 10.48.74.121 probe 3
```

```
Command: traceroute 10.48.74.121 probe 3
```

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

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

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

```
DES-3326S:4#
```

MAC NOTIFICATION COMMANDS

Command	Parameters
config mac_notification	ports <portlist> all interval <int 1-2147483647> historysize <int 1 - 500>
enable mac_notification	
disable mac_notification	
show mac_notification	{ports}

config mac_notification

Purpose	Used to configure MAC address notification.
Syntax	config mac_notification ports <portlist> all interval <sec> historysize <1 - 500>
Description	MAC address notification is used to monitor MAC addresses learned and entered into the FDB.
Parameters	<p>ports <portlist> - specifies a range of ports to be configured. The port list is specified by listing the lowest Switch number and the beginning port number on that Switch, separated by a colon. Then highest Switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 would specify 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>all – to configure all ports for MAC notification.</p> <p>interval <sec 1-2147483647> - time in seconds between notifications.</p> <p>historysize <1 - 500> - maximum number of entries listed in the history log used for notification.</p>
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure a 60 second interval for MAC address notification on unit 1 ports 6-9:

```
DES-3326S:4#config mac_notification ports 1:6-1:9 60
Command: config mac_notification ports 1:6-1:9 interval 60

Success.

DES-3326S:4#
```

enable mac_notification

Purpose	Used to globally enable MAC address notification without changing the mac_notification configuration.
Syntax	enable mac_notification
Description	Enables MAC notification on the Switch.
Parameters	none.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To globally enable MAC notification:

```
DES-3326S:4#enable mac_notification
Command: enable mac_notification
Success.
DES-3326S:4#
```

disable mac_notification

Purpose	Used to disable MAC address notification globally without changing mac_notification configuration..
Syntax	disable mac_notification
Description	Disables MAC notification on the Switch.
Parameters	none.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To globally disable MAC notification:

```
DES-3326S:4#disable mac_notification
Command: disable mac_notification
Success.
DES-3326S:4#
```

show mac_notification

Purpose	Used to display MAC address notification.
Syntax	show mac_notification {ports}
Description	Displays MAC notification settings either per port or globally as desired.
Parameters	none – this will display global MAC notification settings currently configured including Interval, History Size and State. ports – this displays per ports MAC notification settings.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To display global MAC notification settings:

```
DES-3326S:4#show mac_notification
```

```
Command: show mac_notification
```

Global Mac Notification Settings

```
State      : Disabled
```

```
Interval   : 1
```

```
History Size : 1
```

```
DES-3326S:4#
```

Example Usage:

To display per port MAC notification settings:

```
DES-3326S:4#show mac_notification ports
Command: show mac_notification ports

Port #  MAC Address Table Notification State
-----  -
1                Enabled
2                Enabled
3                Enabled
4                Enabled
5                Enabled
6                Enabled
7                Enabled
8                Enabled
9                Enabled
10               Enabled
11               Enabled
12               Enabled
13               Enabled
14               Enabled
15               Enabled
16               Enabled
17               Enabled
18               Enabled
19               Enabled
20               Enabled
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

DOWNLOAD/UPLOAD COMMANDS

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

Command	Parameters
download	firmware <ipaddr> <path_filename> unit [all <unitid>] configuration <ipaddr> <path_filename> {increment}
upload	configuration log <ipaddr> <path_filename>

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

download

Purpose	Used to download and install new firmware or a Switch configuration file from a TFTP server.
Syntax	download [firmware <ipaddr> <path_filename> {unit [all]<unitid>}] configuration <ipaddr> <path_filename> {increment}]
Description	This command is used to download a new firmware or a Switch configuration file from a TFTP server.
Parameters	<p>firmware – Download and install new firmware on the Switch from a TFTP server.</p> <p>configuration – Download a Switch configuration file from a TFTP server.</p> <p><ipaddr> – The IP address of the TFTP server.</p> <p><path_filename> – The DOS path and filename of the firmware or Switch configuration file on the TFTP server. For example, C:\3226S.had.</p> <p>unit [all]<unitid>] – all specifies all units (Switches), <unitid> is the unit id of the Switch that will receive the download.</p> <p>increment – Allows the download of a partial Switch configuration file. This allows a file to be downloaded that will change only the Switch parameters explicitly stated in the configuration file. All other Switch parameters will remain unchanged.</p>
Restrictions	The TFTP server must be on the same IP subnet as the Switch. Only administrator-level users can issue this command.

Example usage:

To download a configuration file:

```
DES-3326S:4#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.

DES-3326S:4#
```

upload

Purpose	Used to upload the current Switch settings or the Switch history log to a TFTP server.
Syntax	upload [configuration log] <ipaddr> <path_filename>
Description	This command is used to upload either the Switch's current settings or the Switch's history log to a TFTP server.
Parameters	<p>configuration – Specifies that the Switch's current settings will be uploaded to the TFTP server.</p> <p>log – Specifies that the Switch history log will be uploaded to the TFTP server.</p> <p><ipaddr> – The IP address of the TFTP server. The TFTP server must be on the same IP subnet as the Switch.</p> <p><path_filename> – 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:

```
DES-3326S:4#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.
```

```
DES-3326S:4#
```

NETWORK MONITORING COMMANDS

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

Command	Parameters
show packet ports	<portlist>
show error ports	<portlist>
show utilization	
clear counters	ports <portlist>
clear log	
show log	index <value>
enable syslog	
disable syslog	
show syslog	
create syslog host	all <index 1-4> severity informational warning all facility local0 local1 local2 local3 local4 local5 local6 local7 udp_port <int> ipaddress <ipaddr> state [enable disable]
config syslog host	all <index 1-4> severity informational warning all facility local0 local1 local2 local3 local4

Command	Parameters
	local5 local6 local7 udp_port <int> ipaddress <ipaddr> state [enable disable]
delete syslog host	<index 1-4> all
show syslog host	<index 1-4>

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

show packet ports

Purpose	Used to display statistics about the packets sent and received by the Switch.
Syntax	show packet ports <portlist>
Description	This command is used to display statistics about packets sent and received by ports specified in the port list.
Parameters	<portlist> – specifies a range of ports to be configured. The port list is specified by listing the lowest Switch number and the beginning port number on that Switch, separated by a colon. Then highest Switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 would specify 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 the packets analysis for port 14:

DES-3326S:4#show packet port 14

Command: show packet ports 14

Port number : 14

Frame Size	Frame Counts	Frames/sec	Frame Type	Total	Total/sec
-----	-----	-----	-----	-----	-----
64	254290	52	RX Bytes	41286744	17290
65-127	38129	12	RX Frames	359507	86
128-255	51878	13			
256-511	8058	3	TX Bytes	72755	0
512-1023	2046	0	TX Frames	335	0
1024-1518	5441	6			
Unicast RX	2245	0			
Multicast RX	57480	20			
Broadcast RX	299782	66			

show error ports

Purpose	Used to display the error statistics for a range of ports.
Syntax	show error ports <portlist>
Description	This command will display all of the packet error statistics collected and logged by the switch for a given port list.
Parameters	<portlist> – Specifies a range of ports to be configured. The port list is specified by listing the lowest Switch number and the beginning port number on that Switch, separated by a colon. Then highest Switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 would specify 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 the error statistics of the port 3 of module 1:

DES-3326S:4#show errors port 1:3			
RX Frames		TX Frames	
-----		-----	
CRC Error	0	Excessive Deferral	0
Undersize	0	CRC Error	0
Oversize	0	Late Collision	0
Fragment	0	Excessive Collision	0
Jabber	0	Single Collision	0
Drop Pkts	0	Collision	0

show utilization

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

Example Usage:

To display the port utilization statistics:

DES-3326S:4#show utilization							
Port	TX/sec	RX/sec	Util	Port	TX/sec	RX/sec	Util
---	-----	-----	---	---	-----	-----	---
1:1	0	0	0	1:22	0	0	0
1:2	0	0	0	1:23	0	0	0
1:3	0	0	0	1:24	0	0	0
1:4	0	0	0	1:25	0	0	0
1:5	0	0	0	1:26	19	49	1
1:6	0	0	0	2:1	0	0	0
1:7	0	0	0	2:2	0	0	0
1:8	0	0	0	2:3	0	0	0
1:9	0	0	0	2:4	0	0	0
1:10	0	0	0	2:5	0	0	0
1:11	0	0	0	2:6	0	0	0
1:12	0	0	0	2:7	0	30	1
1:13	0	0	0	2:8	0	0	0
1:14	0	0	0	2:9	30	0	1
1:15	0	0	0	2:10	0	0	0
1:16	0	0	0	2:11	0	0	0
1:17	0	0	0	2:12	0	0	0
1:18	0	0	0	2:13	0	0	0
1:19	0	0	0	2:14	0	0	0
1:20	0	0	0	2:15	0	0	0
1:21	0	0	0	2:16	0	0	0

clear counters

Purpose	Used to clear the Switch's statistics counters.
Syntax	clear counters {ports <portlist>}
Description	This command will clear the counters used by the Switch to compile statistics.
Parameters	<portlist> – Specifies a range of ports to be configured. The port list is specified by listing the lowest Switch number and the beginning port number on that Switch, separated by a colon. Then highest Switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 would specify 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 clear the counters:

DES-3326S:4#clear counters ports 2:7-2:9

Command: clear counters ports 2:7-2:9

Success.

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:

```
DES-3326S:4#clear log
```

```
Command: clear log
```

```
Success.
```

```
DES-3326S:4#
```

show log

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

Example Usage:

To display the Switch history log:

DES-3326S:4#show log

Command: show log

Index	Time	Log Text
75	00000 days 01:17:05	Successful login through Telnet (Username: Anonymous)
74	00000 days 01:02:56	Successful login through Console (Username: Anonymous)
73	00000 days 01:01:49	Successful login through Web (Username: Anonymous)
72	00000 days 01:01:22	Port 4 link up, 100Mbps FULL duplex
71	00000 days 00:45:55	Internal Power is recovered
70	00000 days 00:43:58	Internal Power failed
69	00000 days 00:19:37	Console session timed out (Username: Anonymous)
68	00000 days 00:07:43	Redundant Power is working
67	00000 days 00:05:37	Successful login through Console (Username: Anonymous)
66	00000 days 00:04:20	Logout through Console (Username: Anonymous)
65	00000 days 00:04:11	Successful login through Console (Username: Anonymous)
64	00000 days 00:00:01	System started up
63	00000 days 00:00:01	Spanning Tree Protocol is disabled
62	00000 days 00:06:19	Spanning Tree Protocol is disabled
61	00000 days 00:06:16	Configuration saved to flash (Username: Anonymous)

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

enable syslog

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

Example Usage:

To enable the syslog function on the Switch:

```
DES-3326S:4#enable syslog
```

```
Command: enable syslog
```

```
Success.
```

```
DES-3326S:4#
```


disable syslog

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

Example Usage:

To disable the syslog function on the switch:

```
DES-3326S:4#disable syslog
```

```
Command: disable syslog
```

```
Success.
```

```
DES-3326S:4#
```

show syslog

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

Example Usage:

To display the current status of the syslog function:

```
DES-3326S:4#show syslog
```

```
Command: show syslog
```

```
Syslog Global State: Enabled
```

```
DES-3326S:4#
```

create syslog host

Purpose	Used to create a new syslog host.																		
Syntax	config syslog host [all <index 1-4>] { severity [informational warning all] facility [local0 local1 local2 local3 local4 local5 local6 local7] udp_port <int> ipaddress <ipaddr> state [enable disable] }																		
Description	The create syslog host command is used to create a new syslog host.																		
Parameters	<p>all – Specifies that the command will be applied to all hosts.</p> <p><index 1-4> – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4.</p> <p>severity – Severity level indicator. These are described in the following:</p> <p>Bold font indicates that the corresponding severity level is currently supported on the Switch.</p> <table> <thead> <tr> <th>Numerical Code</th><th>Severity</th></tr> </thead> <tbody> <tr> <td>0</td><td>Emergency: system is unusable</td></tr> <tr> <td>1</td><td>Alert: action must be taken immediately</td></tr> <tr> <td>2</td><td>Critical: critical conditions</td></tr> <tr> <td>3</td><td>Error: error conditions</td></tr> <tr> <td>4</td><td>Warning: warning conditions</td></tr> <tr> <td>5</td><td>Notice: normal but significant condition</td></tr> <tr> <td>6</td><td>Informational: informational messages</td></tr> <tr> <td>7</td><td>Debug: debug-level messages</td></tr> </tbody> </table> <p>informational – Specifies that informational messages will be sent to the remote host. This corresponds to number 6 from the list above.</p> <p>warning – Specifies that warning messages will be sent to the remote host. This corresponds to number 4 from the list above.</p> <p>all – Specifies that all of the currently supported syslog messages that are generated by the Switch will be sent to the remote host.</p> <p>facility – Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the "local use" facilities or they may use the "user-level" Facility. Those Facilities that have been designated are shown in the following: Bold font indicates the facility values that the Switch currently supports.</p>	Numerical Code	Severity	0	Emergency: system is unusable	1	Alert: action must be taken immediately	2	Critical: critical conditions	3	Error: error conditions	4	Warning: warning conditions	5	Notice: normal but significant condition	6	Informational: informational messages	7	Debug: debug-level messages
Numerical Code	Severity																		
0	Emergency: system is unusable																		
1	Alert: action must be taken immediately																		
2	Critical: critical conditions																		
3	Error: error conditions																		
4	Warning: warning conditions																		
5	Notice: normal but significant condition																		
6	Informational: informational messages																		
7	Debug: debug-level messages																		

create syslog host

Parameters	Numerical Code	Facility
	0	kernel messages
	1	user-level messages
	2	mail system
	3	system daemons
	4	security authorization messages
	5	messages generated internally by syslog
	6	line printer subsystem
	7	network news subsystem
	8	UUCP subsystem
	9	clock daemon
	10	security authorization messages
	11	FTP daemon
	12	NTP subsystem
	13	log audit
	14	log alert
	15	clock daemon
	16	local use 0 (local0)
	17	local use 1 (local1)
	18	local use 2 (local2)
	19	local use 3 (local3)
	20	local use 4 (local4)
	21	local use 5 (local5)
	22	local use 6 (local6)
	23	local use 7 (local7)

create syslog host

Parameters	<p>local0 – Specifies that local use 0 messages will be sent to the remote host. This corresponds to number 16 from the list above.</p> <p>local1 – Specifies that local use 1 messages will be sent to the remote host. This corresponds to number 17 from the list above.</p> <p>local2 – Specifies that local use 2 messages will be sent to the remote host. This corresponds to number 18 from the list above.</p> <p>local3 – Specifies that local use 3 messages will be sent to the remote host. This corresponds to number 19 from the list above.</p> <p>local4 – Specifies that local use 4 messages will be sent to the remote host. This corresponds to number 20 from the list above.</p> <p>local5 – Specifies that local use 5 messages will be sent to the remote host. This corresponds to number 21 from the list above.</p> <p>local6 – Specifies that local use 6 messages will be sent to the remote host. This corresponds to number 22 from the list above.</p> <p>local7 – Specifies that local use 7 messages will be sent to the remote host. This corresponds to number 23 from the list above.</p> <p>udp_port <int> – Specifies the UDP port number that the syslog protocol will use to send messages to the remote host.</p> <p>ipaddress <ipaddr> – Specifies the IP address of the remote host where syslog messages will be sent.</p> <p>state [enable disable] – Allows the sending of syslog messages to the remote host, specified above, to be enabled and disabled.</p>
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To create syslog host:

DES-3326S:4#create syslog host 1 severity all facility local0

Command: create syslog host 1 severity all facility local0

Success.

DES-3326S:4#

config syslog host

Purpose	Used to configure the syslog protocol to send system log data to a remote host.																		
Syntax	config syslog host [all <index 1-4>] { severity [informational warning all] facility [local0 local1 local2 local3 local4 local5 local6 local7] udp_port <int> ipaddress <ipaddr> state [enable disable] }																		
Description	The config syslog host command is used to configure the syslog protocol to send system log information to a remote host.																		
Parameters	<p>all – Specifies that the command will be applied to all hosts.</p> <p><index 1-4> – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4.</p> <p>severity – Severity level indicator. These are described in the following:</p> <p>Bold font indicates that the corresponding severity level is currently supported on the Switch.</p> <table> <thead> <tr> <th>Numerical Code</th><th>Severity</th></tr> </thead> <tbody> <tr> <td>0</td><td>Emergency: system is unusable</td></tr> <tr> <td>1</td><td>Alert: action must be taken immediately</td></tr> <tr> <td>2</td><td>Critical: critical conditions</td></tr> <tr> <td>3</td><td>Error: error conditions</td></tr> <tr> <td>4</td><td>Warning: warning conditions</td></tr> <tr> <td>5</td><td>Notice: normal but significant condition</td></tr> <tr> <td>6</td><td>Informational: informational messages</td></tr> <tr> <td>7</td><td>Debug: debug-level messages</td></tr> </tbody> </table>	Numerical Code	Severity	0	Emergency: system is unusable	1	Alert: action must be taken immediately	2	Critical: critical conditions	3	Error: error conditions	4	Warning: warning conditions	5	Notice: normal but significant condition	6	Informational: informational messages	7	Debug: debug-level messages
Numerical Code	Severity																		
0	Emergency: system is unusable																		
1	Alert: action must be taken immediately																		
2	Critical: critical conditions																		
3	Error: error conditions																		
4	Warning: warning conditions																		
5	Notice: normal but significant condition																		
6	Informational: informational messages																		
7	Debug: debug-level messages																		

config syslog host**Parameters**

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

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

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

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

Numerical Facility

Code

0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security authorization messages
5	messages generated internally by syslog
6	line printer subsystem
7	network news subsystem
8	UUCP subsystem
9	clock daemon
10	security authorization messages
11	FTP daemon
12	NTP subsystem
13	log audit
14	log alert
15	clock daemon

config syslog host

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

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

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

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

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

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

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

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

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

udp_port <int> – Specifies the UDP port number that the syslog protocol will use to send messages to the remote host.

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

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

Parameters

Restrictions Only administrator-level users can issue this command.

Example Usage:

To create syslog host:

DES-3326S:4#config syslog host all severity all facility local0

Command: config syslog host all severity all facility local0

Success.

DES-3326S:4#

delete syslog host

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

Example Usage:

To delete a previously configured syslog host:

```
DES-3326S:4#delete syslog host 4
```

```
Command: delete syslog host 4
```

```
Success.
```

```
DES-3326S:4#
```

show syslog host

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

Example Usage:

To show Syslog host information:

DES-3326S:4#show syslog host

Command: show syslog host

Syslog Global State: Disabled

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

Total Entries : 3

DES-3326S:4#

SPANNING TREE COMMANDS

The Switch supports 802.1w Rapid STP and 802.1d 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> hellotime <value> forwarddelay <value> priority <value> fdpdu [enable disable] txholdcount <1-10> version [rstp stp]
config stp ports	<portlist> cost <value> priority <value> 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.

config stp

Purpose	Used to setup STP and RSTP on the Switch.
Syntax	config stp {maxage <value> hellotime <value> forwarddelay <value> priority <value> fbpdu [enable disable] txholdcount <1-10> version[rstp stp]}
Description	This command is used to setup the Spanning Tree Protocol for the entire Switch. By default, the Switch uses Rapid Spanning Tree Protocol (RSTP) when it is enabled. The default settings for the Switch have Spanning Tree Protocol disabled (see enable/disable stp commands).
Parameters	<p>maxage <value> – The maximum amount of time (in seconds) that the Switch will wait to receive a BPDU packet before reconfiguring STP. The default is 20 seconds.</p> <p>hellotime <value> – The time interval between transmission of configuration messages by the root device. The default is 2 seconds.</p> <p>forwarddelay <value> – The maximum amount of time (in seconds) that the root device will wait before changing states. The default is 15 seconds.</p> <p>priority <value> – 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>fbpdu [enable disable] – Allows the forwarding of STP BPDU packets from other network devices when STP is disabled on the Switch. The default is enabled.</p> <p>txholdcount <1-10> – the maximum number of Hello packets transmitted per interval. Default value = 3.</p> <p>version [rstp stp] – select the Spanning Tree Protocol version used for the Switch. For IEEE 802.1d STP select stp. Select rstp for IEEE 802.1w Rapid STP.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure STP with maxage 18 and hellotime 4:

```
DES-3326S:4#config stp maxage 18 hellotime 4
```

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

```
Success.
```

```
DES-3326S:4#
```

config stp ports

Purpose	Used to setup STP on the port level.
Syntax	config stp ports <portlist> {cost <value> priority <value> migrate [yes no] edge [true false] p2p [true false] state [enable disable]}
Description	This command is used to create and configure STP for a group of ports.
Parameters	<p>cost <value> – This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set from 1 to 200000000. The lower the number, the greater the probability the port will be chosen to forward packets.</p> <p>Default port cost: 100Mbps port = 200000 Gigabit port = 20000</p> <p>priority <value> – 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><portlist> – Specifies a range of ports to be configured. The port list is specified by listing the lowest Switch number and the beginning port number on that Switch, separated by a colon. Then 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>migrate [yes no] – yes will enable the port to migrate from 802.1d STP status to 802.1w RSTP status. RSTP can coexist with standard STP, however the benefits of RSTP are not realized on a port where an 802.1d network connects to an 802.1w enabled network. Migration should be enabled (yes) on ports connected to network stations or segments that will be upgraded to 802.1w RSTP on all or some portion of the segment.</p> <p>edge [true false] – true designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received it automatically loses edge port status. False indicates that the port does not have edge port status.</p> <p>p2p [true false auto] – true indicates a point-to-point (P2P) shared link. P2P ports are similar to edge ports however they are restricted in that a P2P port must operate in full-duplex. Like edge ports, P2P ports transition to a forwarding state rapidly thus benefiting from RSTP. A p2p value of false indicates that the port cannot have p2p status. <i>Auto</i> allows the port to have p2p status whenever possible and operate as if the p2p status were <i>true</i>. If the port cannot maintain this status (for example if the port is forced to half-duplex operation) the p2p status changes to operate as if the p2p value were <i>false</i>.</p> <p>state [enable disable] – 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 19, priority 15, and state enabled for ports 1-5 of module 1.

```
DES-3326S:4#config stp ports 1:1-1:5 cost 19 priority 15 state enable
```

```
Command: config stp ports 1-5 cost 19 priority 15 state enable
```

Success.

```
DES-3326S:4#
```

enable stp

Purpose	Used to globally enable STP on the Switch.
Syntax	enable stp
Description	This command allows the Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP) to be globally enabled on the Switch. By default, Spanning Tree is not enabled and the default Spanning Tree version is RSTP (see config stp command).
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable STP, globally, on the Switch:

```
DES-3326S:4#enable stp
```

```
Command: enable stp
```

Success.

```
DES-3326S:4#
```

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:

```
DES-3326S:4#disable stp
```

```
Command: disable stp
```

```
Success.
```

```
DES-3326S:4#
```

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

```
DES-3326S:4#show stp
Command: show stp

Bridge Parameters Settings
STP Status      : Enabled
Max Age        : 20
Hello Time     : 2
Forward Delay  : 15
Priority       : 32768
STP Version    : STP compatible
TX Hold Count  : 3
Forwarding BPDU : Enabled

Bridge Current Status
Designated Root Bridge : 00-00-51-43-70-00
Root Priority          : 32768
Cost to Root          : 200000
Root Port             : 10
Last Topology Change  : 53sec
Topology Changes Count : 1
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

DES-3326S:4#
```


Status 2 : STP disabled

DES-3326S:4#show stp

Command: show stp

Bridge Parameters Settings

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

DES-3326S:4#

show stp ports

Purpose	Used to display the Switch's current per-port group STP configuration.
Syntax	show stp ports <portlist>
Description	This command displays the Switch's current per-port group STP configuration.
Parameters	<portlist> – Specifies a range of ports to be configured. The port list is specified by listing the lowest Switch number and the beginning port number on that Switch, separated by a colon. Then 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 STP state of port 1-9 of module 1:

```
DES-3326S:4#show stp ports
Command: show ports
Port  Designated Bridge  State  Cost   Pri  Edge P2P Status   Role
-----
1    N/A                Yes *200000 128 No  Yes Disabled Disabled
2    N/A                Yes *200000 128 No  Yes Disabled Disabled
3    N/A                Yes *200000 128 No  Yes Disabled Disabled
4    N/A                Yes *200000 128 No  Yes Disabled Disabled
5    N/A                Yes *200000 128 No  Yes Disabled Disabled
6    N/A                Yes *200000 128 No  Yes Disabled Disabled
7    N/A                Yes *200000 128 No  Yes Disabled Disabled
8    N/A                Yes *200000 128 No  Yes Disabled Disabled
9    N/A                Yes *200000 128 No  Yes Disabled Disabled
10   N/A                Yes *200000 128 No  Yes Forwarding NonStp
11   N/A                Yes *200000 128 No  Yes Disabled Disabled
12   N/A                Yes *200000 128 No  Yes Disabled Disabled
13   N/A                Yes *200000 128 No  Yes Disabled Disabled
14   N/A                Yes *200000 128 No  Yes Disabled Disabled
15   N/A                Yes *200000 128 No  Yes Disabled Disabled
16   N/A                Yes *200000 128 No  Yes Disabled Disabled
17   N/A                Yes *200000 128 No  Yes Disabled Disabled
18   N/A                Yes *200000 128 No  Yes Disabled Disabled
19   N/A                Yes *200000 128 No  Yes Disabled Disabled
20   N/A                Yes *200000 128 No  Yes Disabled Disabled
21   N/A                Yes *200000 128 No  Yes Disabled Disabled
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
DES-3326S:4#
```

FORWARDING DATABASE COMMANDS

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

Command	Parameters
create fdb	<vlan_name 32> <macaddr> port <port>
create multicast_fdb	<vlan_name 32> <macaddr>
config multicast_fdb	<vlan_name 32> <macaddr> [add delete] <portlist>
config fdb aging_time	<sec 10-1000000>
delete fdb	<vlan_name 32> <macaddr>
clear fdb	vlan <vlan_name 32> port <port> all
show multicast_fdb	vlan <vlan_name 32> mac_address <macaddr>
show fdb	port <port> vlan <vlan_name 32> mac_address <macaddr> static aging_time

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

create fdb

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

Example usage:

To create a unicast MAC FDB entry:

```
DES-3326S:4#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.
```

```
DES-3326S:4#
```

create multicast_fdb

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

Example usage:

To create multicast MAC forwarding:

```
DES-3326S:4#create multicast_fdb default 01-00-5E-00-00-00
```

```
Command: create multicast_fdb default 01-00-5E-00-00-00
```

```
Success.
```

```
DES-3326S:4#
```

config multicast_fdb

Purpose	Used to configure the Switch's multicast MAC address forwarding database.
Syntax	config multicast_fdb <vlan_name 32> <macaddr> [add delete] <portlist>
Description	This command configures the multicast MAC address forwarding table.
Parameters	<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>[add delete] – Add will add the MAC address to the forwarding table. Delete will remove the MAC address from the forwarding table.</p> <p><portlist> – Specifies a range of ports to be configured. The port list is specified by listing the lowest Switch number and the beginning port number on that Switch, separated by a colon. Then 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>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To add multicast MAC forwarding:

```
DES-3326S:4#config multicast_fdb default 01-00-5E-00-00-00 add 1:1-1:5
```

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

Success.

```
DES-3326S:4#
```

config fdb aging_time

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

Example usage:

To set the fdb aging time:

```
DES-3326S:4#config fdb aging_time 300
```

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

```
Success.
```

```
DES-3326S:4#
```

delete fdb

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

Example usage:

To delete a permanent FDB entry:

DES-3326S:4#delete fdb default 00-00-00-00-01-02

Command: delete fdb default 00-00-00-00-01-02

Success.

DES-3326S:4#

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><vlan_name 32> – The name of the VLAN on which the MAC address resides.</p> <p><port> – The port number corresponding to the MAC destination address. The Switch will always forward traffic to the specified device through this port.</p> <p>all – Clears all dynamic entries to the Switch's forwarding database.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To clear all FDB dynamic entries:

DES-3326S:4#clear fdb all

Command: clear fdb all

Success.

DES-3326S:4#

show multicast_fdb

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

Example usage:

To display multicast MAC address table:

DES-3326S:4#show multicast_fdb

Command: show multicast_fdb

VLAN Name : default
MAC Address : 01-00-5E-00-00-00
Egress Ports : 1:1-1:5,1:26,2:26
Mode : Static

Total Entries : 1

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><port> – The port number corresponding to the MAC destination address. The Switch will always forward traffic to the specified device through this port.</p> <p><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>static – Displays the static MAC address entries.</p> <p>aging_time – Displays the aging time for the MAC address forwarding database.</p>
Restrictions	None.

Example usage:

To display unicast MAC address table:

DES-3326S:4#show fdb

Command: show fdb

Unicast MAC Address Ageing 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

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> all broadcast [enable disable] multicast [enable disable] dlf [enable disable] threshold <value>
show traffic control	group_list <storm_grouplist>

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

config traffic control

Purpose	Used to configure broadcast multicast traffic control.
Syntax	config traffic control [<storm_grouplist> all] broadcast [enable disable] multicast [enable disable] dlf [enable disable] threshold <value>
Description	This command is used to configure broadcast storm control.
Parameters	<p><storm_grouplist> – Used to specify a broadcast storm control group with the syntax: module_id:group_id.</p> <p>all – Specifies all broadcast storm control groups on the Switch.</p> <p>broadcast [enable disable] – Enables or disables broadcast storm control.</p> <p>multicast [enable disable] – Enables or disables multicast storm control.</p> <p>dlf [enable disable] – Enables or disables dlf traffic control.</p> <p>threshold <value> – 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>
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

DES-3326S:4#config traffic control all broadcast enable

Command: config traffic control all broadcast enable

Success.

DES-3326S:4#

show traffic control

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

Example usage:

To display traffic control setting:

DES-3326S:4#show traffic control

Command: show traffic control

Traffic Control**Broadcast Multicast Destination**

Module	Group [ports]	Threshold	Storm	Storm	Lookup Fail
--------	---------------	-----------	-------	-------	-------------

1	1 [1 - 8]	128	Disabled	Disabled	Disabled
1	2 [9 - 16]	128	Disabled	Disabled	Disabled
1	3 [17 - 24]	128	Disabled	Disabled	Disabled
1	4 [25]	128	Disabled	Disabled	Disabled
1	5 [26]	128	Disabled	Disabled	Disabled

Total Entries: 5

DES-3326S:4#

QOS COMMANDS

The DES-3326S Switch supports 802.1p priority queuing. The Switch has 4 priority queues. These priority queues are numbered from 0 (Class 0) — the lowest priority queue — to 3 (Class 3) — the highest priority queue. The eight priority queues specified in IEEE 802.1p (p0 to p7) are mapped to the Switch's priority queues as follows:

- p1 and p2 are assigned to the Switch's Class 0 queue.
- p0 and p3 are assigned to the Switch's Class 1 queue.
- p4 and p5 are assigned to the Switch's Class 2 queue.
- p6 and p7 are assigned to the Switch's Class 3 queue.

Priority scheduling is implemented using two types of methods, strict priority and round-robin priority. If no changes are made to the QoS priority scheduling settings the method used is strict priority.

For strict priority-based scheduling, packets residing in the higher priority queues are transmitted first. Only when these queues are empty, are packets of lower priority allowed to be transmitted. Higher priority packets always receive preference regardless of the amount of lower priority packets in the buffer and regardless of the time elapsed since any lower priority packets have been transmitted. By default the Switch is configured to empty the buffer using strict priority.



NOTICE: The default QoS scheduling arrangement is a strict priority schedule. To customize scheduling to set up round-robin queue clearing, the MAX. Latency and MAX. Packets values need to be changed using the config scheduling command. See **config scheduling** below.

To implement round-robin (weighted) priority, the Switch's four priority queues can be configured to reduce the buffer in a round-robin fashion - beginning with the highest priority queue, and proceeding to the lowest priority queue before returning to the highest priority queue.

The weighted-priority based scheduling alleviates the main disadvantage of strict priority-based scheduling – in that lower priority queues get starved of bandwidth – by providing a minimum bandwidth to all queues for transmission. This is accomplished by configuring the maximum number of packets allowed to be transmitted from a given priority queue and the maximum amount of time a given priority queue will have to wait before being allowed to transmit its accumulated packets. This establishes a Class of Service (CoS) for each of the Switch's four hardware priority queues.

The possible range for maximum packets is: 0 to 255 packets.

The possible range for maximum latency is: 0 to 255 (in increments of 16 microseconds each).

Command	Parameters
config bandwidth_control	<portlist> rx_rate no_limit <value 1-1000> tx_rate no_limit <value 1-1000>
show bandwidth_control	<portlist>
config scheduling	<class_id 0-3> max_packet <value 0-255> max_latency <value 0-255>
show scheduling	
config 802.1p user_priority	<priority 0-7> <class_id 0-3>
show 802.1p user_priority	
config 802.1p default_priority	<portlist> all <priority 0-7>
show 802.1p default_priority	<portlist>

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	config bandwidth_control <portlist> {re_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><portlist> – Specifies a range of ports to be configured. The port list is specified by listing the lowest Switch number and the beginning port number on that Switch, separated by a colon. Then 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>rx_rate – Specifies that one of the parameters below (no_limit or <value 1-1000>) will be applied to the rate at which the above specified ports will be allowed to receive packets</p> <p>no_limit – Specifies that there will be no limit on the rate of packets received by the above specified ports.</p> <p><value 1-1000> – Specifies the packet limit, in Mbps, that the above ports will be allowed to receive.</p> <p>tx_rate – Specifies that one of the parameters below (no_limit or <value 1-1000>) will be applied to the rate at which the above specified ports will be allowed to transmit packets.</p> <p>no_limit – Specifies that there will be no limit on the rate of packets received by the above specified ports.</p> <p><value 1-1000> – Specifies the packet limit, in Mbps, that the above ports will be allowed to receive. Gigabit ports must be configured to using a limit value that is a multiple of 8 i.e. for Gigabit ports <value 8-1000 in increments of 8>.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure bandwidth control:

DES-3326S:4#config bandwidth_control 1-10 tx_rate 10

Command: config bandwidth_control 1-10 tx_rate 10

Success.

DES-3326S:4#

show bandwidth_control

Purpose	Used to display the bandwidth control configuration on the Switch.
Syntax	show bandwidth_control {<portlist>}
Description	The show bandwidth_control command displays the current bandwidth control configuration on the Switch, on a port-by-port basis.
Parameters	<portlist> – Specifies a range of ports to be configured. The port list is specified by listing the 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 bandwidth control settings:

DES-3326S:4#show bandwidth_control 1-10

Command: show bandwidth_control 1-10

Bandwidth Control Table

Port RX Rate (Mbit|sec) TX_RATE (Mbit|sec)

1	no_limit	10
2	no_limit	10
3	no_limit	10
4	no_limit	10
5	no_limit	10
6	no_limit	10
7	no_limit	10
8	no_limit	10
9	no_limit	10
10	no_limit	10

DES-3326S:4#

config scheduling

Purpose	Used to configure traffic scheduling for each of the Switch's QoS queues.
Syntax	config scheduling <class_id 0-3> {max_packet <value 0-255> max_latency <value 0-255>}
Description	<p>The Switch contains four hardware priority queues per device. The Switch's default settings draw down the four hardware queues in order, from the highest priority (Class 3) to the lowest priority (Class 0). Starting with the highest priority queue (Class 3), the highest priority queue will transmit all of the packets and empty its buffer before allowing the next lower priority queue to transmit its packets. The next highest priority queue will empty before proceeding to the next queue and so on. Lower priority queues are allowed to transmit <u>only if</u> the higher priority queue(s) in the buffer are completely emptied. Packets in the higher priority queues are always emptied before any in the lower priority queues regardless of latency or volume of the lower priority queues.</p> <p>The default settings for QoS scheduling employ this strict priority scheme to empty priority queues.</p> <p>The config scheduling command can be used to specify the round robin rotation by which these four hardware priority queues are reduced. To use a round-robin scheme, the max_packets parameters and/or the max_latency parameters must be changed from the default value of 0.</p> <p>The max_packets parameter allows you to specify the maximum number of packets a given priority queue can transmit before allowing the next lowest priority queue to begin transmitting its packets. A value between 0 and 255 packets can be specified. For example, if a value of 5 is specified, then the highest priority queue (queue 3) will be allowed to transmit 5 packets. Then the next lower priority queue (queue 2) will be allowed to transmit 5 packets, and so on, until all of the queues have transmitted 5 packets. The process will then repeat.</p> <p>The max_latency parameter allows you to specify the maximum amount of time that packets will be delayed before being transmitted. For a given priority queue, a value between 0 and 255 can be specified. This number is then multiplied by 16 milliseconds to determine the maximum allowed latency. For example, if 3 is specified for queue 3, the maximum latency allowed will be 3 X 16 ms = 48 ms. When queue 3 has been waiting to transmit packets for longer than 48 ms, the currently transmitting priority queue is allowed to finish transmitting its current packet, and then queue 2 is allowed to begin transmitting its packets.</p>
Parameters	<p><class_id> – Specifies which of the four priority queues the config scheduling command will be applied to. The four priority queues are identified by number – from 0 to 3 – with queue 3 being the highest priority.</p> <p>max_packet <value 0-255> – Specifies the maximum number of packets the above specified priority queue will be allowed to transmit before allowing the next lowest priority queue to transmit its packets. A value between 0 and 255 packets can be</p>

config scheduling

specified. The default value is 0.

max_latency <value 0-255> – Specifies the maximum amount of time the above specified priority queue will have to wait before being allowed to transmit any packets that have accumulated in its transmit buffer. A value between 0 and 255 can be specified. This value multiplied by 16 ms is the total time the priority queue will have to wait. The default value is 0.

Restrictions

Only administrator-level users can issue this command.



NOTICE: The default QoS scheduling arrangement is a strict priority schedule. To customize scheduling to set up weighted or round-robin queue clearing the **max_latency** and **max_packets** values need to be changed.

Example usage:

To configure traffic scheduling:

```
DES-3326S:4# config scheduling 0 max_packet 100 max_latency 150
```

```
Command: config scheduling 0 max_packet 100 max_latency 150
```

Success.

```
DES-3326S:4#
```

show scheduling

Purpose	Used to display the currently configured traffic scheduling on the Switch.
Syntax	show scheduling
Description	The show scheduling command displays the current configuration for the maximum number of packets (max_packets) and the maximum latency (max_latency) values assigned to the four priority queues on the Switch. The Switch's default max_latency = 0. At this value, it will empty the four hardware queues in order, from the highest priority (queue 3) to the lowest priority (queue 0).
Parameters	None.
Restrictions	None.

Example usage:

To display the current scheduling configuration:

DES-3326S:4# show scheduling

Command: show scheduling

QOS Output Scheduling

	MAX. Packets	MAX. Latency
	-----	-----
Class-0	50	1
Class-1	100	1
Class-2	150	1
Class-3	200	1

DES-3326S:4#

config 802.1p user_priority

Purpose	Used to map the 802.1p user priority of an incoming packet to one of the four hardware queues available on the Switch.																											
Syntax	config 802.1p user_priority <priority 0-7> <class_id 0-3>																											
Description	<p>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 four hardware priority queues available on the Switch. The Switch's default is to map the incoming 802.1p priority values to the four hardware queues according to the following chart:</p> <table><tr><th>802.1p Value</th><th>Switch Priority Queue</th><th>Remark</th></tr><tr><td>0</td><td>1</td><td></td></tr><tr><td>1</td><td>0</td><td></td></tr><tr><td>2</td><td>0</td><td></td></tr><tr><td>3</td><td>1</td><td></td></tr><tr><td>4</td><td>2</td><td></td></tr><tr><td>5</td><td>2</td><td></td></tr><tr><td>6</td><td>3</td><td></td></tr><tr><td>7</td><td>3</td><td></td></tr></table>	802.1p Value	Switch Priority Queue	Remark	0	1		1	0		2	0		3	1		4	2		5	2		6	3		7	3	
802.1p Value	Switch Priority Queue	Remark																										
0	1																											
1	0																											
2	0																											
3	1																											
4	2																											
5	2																											
6	3																											
7	3																											
Parameters	<p><priority 0-7> – Specifies which of the 8 802.1p priority values (0 through 7) you want to map to one of the Switch's hardware priority queues (<class_id>, 0 through 3).</p> <p><class_id 0-3> – Specifies which of the Switch's hardware priority queues the 802.1p priority value (specified above) will be mapped to.</p>																											
Restrictions	Only administrator-level users can issue this command.																											

Example usage:

To configure 802.1p user priority on the Switch:

```
DES-3326S:4# config 802.1p user_priority 1 3
```

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

```
Success.
```

```
DES-3326S:4#
```

show 802.1p user_priority

Purpose	Used to display the current mapping between an incoming packet's 802.1p priority value and one of the Switch's four hardware priority queues.
Syntax	show 802.1p user_priority
Description	The show 802.1p user_priority command displays the current mapping of an incoming packet's 802.1p priority value to one of the Switch's four hardware priority queues.
Parameters	None.
Restrictions	None.

Example usage:

To show 802.1p user priority:

```
DES-3326S:4# show 802.1p user_priority
```

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

COS Class of Traffic

```
Priority-0 -> <Class-1>
```

```
Priority-1 -> <Class-0>
```

```
Priority-2 -> <Class-0>
```

```
Priority-3 -> <Class-1>
```

```
Priority-4 -> <Class-2>
```

```
Priority-5 -> <Class-2>
```

```
Priority-6 -> <Class-3>
```

```
Priority-7 -> <Class-3>
```

```
DES-3326S:4#
```

config 802.1p default_priority

Purpose	Used to specify how to map an incoming packet that has no 802.1p priority tag to one of the Switch's four hardware priority queues.
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.
Parameters	<p><portlist> – Specifies a range of ports to be configured. The port list is specified by listing the lowest Switch number and the beginning port number on that Switch, separated by a colon. Then 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>all – Specifies that the config 802.1p default_priority command will be applied to all ports on the Switch.</p> <p><priority 0-7> – Specifies the 802.1p priority value 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:

```
DES-3326S:4#config 802.1p default_priority all 5
Command: config 802.1p default_priority all 5
```

Success.

```
DES-3326S:4#
```


show 802.1 default_priority

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

Example usage:

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

```
DES-3326S:4# show 802.1p default_priority
Command: show 802.1p default_priority
```

Port	Priority
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0
13	0
14	0
15	0
16	0
17	0
18	0
19	0
20	0
21	0
22	0
23	0
24	0
25	0
26	0

```
DES-3326S:4#
```

PORT MIRRORING COMMANDS

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

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

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

config mirror port

Purpose	Used to configure a mirror port – source port pair on the Switch.
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><port> – This specifies the Target port (the port where mirrored packets will be sent).</p> <p>source ports – The port or ports being mirrored. This cannot include the Target port.</p> <p><portlist> – 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. 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>rx – Allows the mirroring of only packets received by (flowing into) the port or ports in the port list.</p> <p>tx – Allows the mirroring of only packets sent to (flowing out of) the port or ports in the port list.</p> <p>both – Mirrors all the packets received or sent by the port or ports in the port list.</p>
Restrictions	The Target port cannot be listed as a source port. Only administrator-level users can issue this command.

Example usage:

To add the mirroring ports:

DES-3326S:4# 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.

DES-3326S:4#

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><port> – This specifies the Target port (the port where mirrored packets will be sent).</p> <p><portlist> – 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>rx – Allows the mirroring of only packets received by (flowing into) the port or ports in the port list.</p> <p>tx – Allows the mirroring of only packets sent to (flowing out of) the port or ports in the port list.</p> <p>both – 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:

DES-3326S:4#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.

DES-3326S:4#

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:

```
DES-3326S:4#enable mirror
```

```
Command: enable mirror
```

```
Success.
```

```
DES-3326S:4#
```

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:

DES-3326S:4#disable mirror

Command: disable mirror

Success.

DES-3326S:4#

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:

```
DES-3326S:4#show mirror
```

```
Command: show mirror
```

Current Settings

```
Target Port: 9
```

```
Mirrored Port:
```

```
    RX:
```

```
    TX: 1:1-1:5
```

```
DES-3326S:4#
```


VLAN COMMANDS

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

Command	Parameters
create vlan	<vlan_name 32> tag <vlanid> advertisement
delete vlan	<vlan_name 32>
config vlan	<vlan_name 32> add [tagged untagged forbidden] delete <portlist> advertisement [enable disable]
config vlan	<vlan_name 32> delete <portlist>
config vlan	<vlan_name 32>
config gvrp	<portlist> all state [enable disable] ingress_checking [enable disable] acceptable_frame [tagged_only accept_all]
enable gvrp	
disable gvrp	
show vlan	<vlan_name 32>
show gvrp	<portlist>

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

create vlan

Purpose	Used to create a VLAN on the Switch.
Syntax	create vlan <vlan_name 32> {tag <vlanid 1-4094> advertisement}
Description	This command allows you to create a VLAN on the Switch.
Parameters	<p><vlan_name 32> – The name of the VLAN to be created.</p> <p><vlanid> – The VLAN ID of the VLAN to be created. Allowed values = 1-4094</p> <p>advertisement – Specifies that the VLAN is able to join GVRP. If this parameter is not set, the VLAN cannot be configured to have forbidden ports.</p>
Restrictions	Each VLAN name can be up to 32 characters. 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:

DES-3326S:4#create vlan v1 tag 2

Command: create vlan v1 tag 2

Success.

DES-3326S:4#

delete vlan

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

Example usage:

To remove a vlan v1:

```
DES-3326S:4#delete vlan v1
```

```
Command: delete vlan v1
```

```
Success.
```

```
DES-3326S:4#
```

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.
Parameters	<p><vlan_name 32> – The name of the VLAN you want to add ports to.</p> <p>add – Specifies all of the ports on the Switch.</p> <p>tagged – Specifies the additional ports as tagged.</p> <p>untagged – Specifies the additional ports as untagged.</p> <p>forbidden – Specifies the additional ports as forbidden.</p> <p>delete – Deletes the above specified VLAN from the Switch.</p> <p><portlist> – A range of ports to add to the VLAN. 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>advertisement [enable disable] – 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:

DES-3326S:4#config vlan v1 add tagged 2:4-2:8

Command: config vlan v1 add tagged 2:4-2:8

Success.

DES-3326S:4#

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).
Parameters	<p><portlist> – A range of ports for which you want ingress checking. 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>all – Specifies all of the ports on the Switch.</p> <p>state [enable disable] – Enables or disables GVRP for the ports specified in the port list.</p> <p>ingress_checking [enable disable] – Enables or disables ingress checking for the specified port list.</p> <p>acceptable_frame – This allows a definition of the type of frame accepted. Acceptable frames can be limited to tagged frames only (tagged_only) or can accept tagged and untagged (accept_all).</p> <p>pvid – Specifies the default VLAN associated with the port.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DES-3326S:4#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.

```
DES-3326S:4#
```

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):

```
DES-3326S:4#enable gvrp
```

```
Command: enable gvrp
```

```
Success.
```

```
DES-3326S:4#
```

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):

```
DES-3326S:4#disable gvrp
```

```
Command: disable gvrp
```

```
Success.
```

```
DES-3326S:4#
```

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:

DES-3326S:4#show vlan

Command: show vlan

```

VID          : 1          VLAN Name    : default
VLAN TYPE    : static    Advertisement : Enabled
Member ports : 1:1-1:26,2:1-2:26
Static ports : 1:1-1:26,2:1-2:26
Untagged ports : 1:1-1:25,2:1-2:25
Forbidden ports :
VID          : 2          VLAN Name    : v1
VLAN TYPE    : static    Advertisement : Disabled
Member ports : 1:26,2:26
Static ports : 1:26,2:26
Untagged ports :
Forbidden ports :

```

Total Entries : 2

DES-3326S:4#

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. 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	None.

Example usage:

To display GVRP port status:

```
DES-3326S:4#show gvrp
Command: show gvrp

Global GVRP : Disabled
```

Port	PVID	GVRP	Ingress Checking	Acceptable Frame Type
1	1	Disabled	Enabled	All Frames
2	1	Disabled	Enabled	All Frames
3	1	Disabled	Enabled	All Frames
4	1	Disabled	Enabled	All Frames
5	1	Disabled	Enabled	All Frames
6	1	Disabled	Enabled	All Frames
7	1	Disabled	Enabled	All Frames
8	1	Disabled	Enabled	All Frames
9	1	Disabled	Enabled	All Frames
10	1	Disabled	Enabled	All Frames
11	1	Disabled	Enabled	All Frames
12	1	Disabled	Enabled	All Frames
13	1	Disabled	Enabled	All Frames
14	1	Disabled	Enabled	All Frames
15	1	Disabled	Enabled	All Frames
16	1	Disabled	Enabled	All Frames
17	1	Disabled	Enabled	All Frames
18	1	Disabled	Enabled	All Frames
19	1	Disabled	Enabled	All Frames
20	1	Disabled	Enabled	All Frames
21	1	Disabled	Enabled	All Frames
22	1	Disabled	Enabled	All Frames
23	1	Disabled	Enabled	All Frames
24	1	Disabled	Enabled	All Frames
25	1	Disabled	Enabled	All Frames
26	1	Disabled	Enabled	All Frames

```
Total Entries : 26
DES-3326S:4#
```

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> {type[lacp static]}
delete link_aggregation	group_id <value>
config link_aggregation	group_id <value> 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> algorithm
config lacp_ports	<portlist> mode [active passive]
show lacp_ports	{<portlist>}

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

create link_aggregation

Purpose	Used to create a link aggregation group on the Switch.
Syntax	create link_aggregation group_id <value> {type[lacp static]}
Description	This command will create a link aggregation group with a unique identifier.
Parameters	<p><value> – Specifies the group id. The Switch allows up to 6 link aggregation groups to be configured. The group number identifies each of the groups.</p> <p>type – Specify the type of link aggregation used for the group. If the type is not specified the default type is static.</p> <p>lacp – 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>static – 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:

DES-3226S:4#create link_aggregation group_id 1

Command: create link_aggregation group_id 1

Success.

DES-3226S:4#

delete link_aggregation group_id

Purpose	Used to delete a previously configured link aggregation group.
Syntax	delete link_aggregation group_id <value>
Description	This command is used to delete a previously configured link aggregation group.
Parameters	<value> – Specifies the group id. The Switch allows up to 6 link aggregation groups to be configured. The group number identifies each of the groups.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete link aggregation group:

```
DES-3226S:4#delete link_aggregation group_id 6
```

```
Command: delete link_aggregation group_id 6
```

```
Success.
```

```
DES-3226S:4#
```

config link_aggregation

Purpose	Used to configure a previously created link aggregation group.
Syntax	config link_aggregation group_id <value> {master_port <port> ports <portlist>} state [enable disable]
Description	This command allows you to configure a link aggregation group that was created with the create link_aggregation command above.
Parameters	<p><value> – Specifies the group id. The Switch allows up to 6 link aggregation groups to be configured. The group number identifies each of the groups.</p> <p><port> – Master port ID. Specifies which port (by port number) of the link aggregation group will be the master port. All of the ports in a link aggregation group will share the port configuration with the master port.</p> <p><portlist> – Specifies a range of ports that will belong to the link aggregation group. Ports are specified by entering the lowest port number in a group, and then the highest port number in a group, separated by a dash such as 1-3. Additional ports can be individually entered by their port number, separated by commas. So, a port group including the Switch ports 1, 2, and 3 would be entered as 1-3. Ports that are not contained within a group are specified by entering their port number, separated by a comma. So, the port group 1-3 and port 26 would be entered as 1-3,26. All ports in the portlist must be on a single Switch unit. Ports may be listed in only one port aggregation group, that is, link aggregation groups may not overlap.</p> <p>state [enable disable] – 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 and must be contained on a single Switch.

Example usage:

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

DES-3226S:4#config link_aggregation group_id 1 master_port 5 ports 5-7,9

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

Success.

DES-3226S:4#

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>mac_source – Indicates that the Switch should examine the MAC source address.</p> <p>mac_destination – Indicates that the Switch should examine the MAC destination address.</p> <p>mac_source_dest – Indicates that the Switch should examine the MAC source and destination addresses</p> <p>ip_source – Indicates that the Switch should examine the IP source address.</p> <p>ip_destination – Indicates that the Switch should examine the IP destination address.</p> <p>ip_source_dest – Indicates that the Switch should examine the IP source address and the destination address.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DES-3226S:4#config link_aggregation algorithm
mac_source_dest
Command: config link_aggregation algorithm mac_source_dest

Success.

DES-3226S:4#
```

show link_aggregation

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

Example usage:

To display Link Aggregation configuration

DES-3226S:4#show link_aggregation

Command: show link_aggregation

Link Aggregation Algorithm = MAC-source-dest

Group ID : 1

Master Port : 2:17

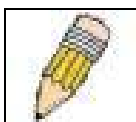
Member Port : 1:5-1:10,2:17

Status : Disabled

Flooding Port : 1:5

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).
Parameters	<p><portlist> – Specifies a range of ports to be configured. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 specifies port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order. Up to 6 ports can be linked.</p> <p>mode – Select the mode to determine if LACP ports will process LACP control frames.</p> <p>active – 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. Only one side is designated active while the other side is designated passive.</p> <p>passive – 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.



Note: For LACP implementations, both devices utilizing the aggregated link must support IEEE 802.1ad Link Aggregation Control Protocol and one device must designate the participating ports as “active” while this other device must designate the participating ports as “passive”.

Example usage:

To configure LACP port mode settings:

DES-3226S:4#config lacp_port 1-12 mode active

Command: config lacp_port 1-12 mode active

Success.

DES-3226S:4#

show lacp_ports

Purpose	Used to display current LACP port mode settings.
Syntax	show lacp_ports {<portlist>}
Description	This command will display the LACP mode settings as they are currently configured.
Parameters	<portlist> -
Restrictions	Only administrator-level users can issue this command.

Example usage:

To display LACP port mode settings:

```
DES-3226S:4#show lacp_ports
Command: show lacp_ports
```

```
Port  Activity
```

```
-----
1     Active
2     Active
3     Active
4     Active
5     Active
6     Active
7     Active
8     Active
9     Active
10    Active
11    Active
Active
```

```
DES-3226S:4#
```

BASIC IP COMMANDS

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

Command	Parameters
config ipif System	ipaddress <network_address> vlan <vlan_name 32> state [enable disable] bootp dhcp
show ipif	

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

config ipif System

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

DES-3326S:4#config ipif System ipaddress 10.1.1.33|8

Command: config ipif System ipaddress 10.1.1.33|8

Success.

DES-3326S:4#

show ipif

Purpose	Used to display the configuration of an IP interface on the Switch.
Syntax	show ipif
Description	This command will display the configuration of an IP interface on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display IP interface settings.

```
DES-3326S:4#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 : 1-26

```
DES-3326S:4#
```

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 0-16711450> robustness_variable <value 1-255> last_member_query_interval <sec 1-25> 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]
config router_ports	<vlan_name 32> [add delete] <portlist>
enable igmp snooping	forward_mcrouter_only
show igmp snooping	vlan <vlan_name 32>
show igmp snooping group	vlan <vlan_name 32>
show router ports	vlan <vlan_name 32> static dynamic

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

config igmp_snooping

Purpose	Used to configure IGMP snooping on the Switch.
Syntax	config igmp_snooping [<vlan_name 32> all] {host_timeout <sec> router_timeout <sec> leave_timer <sec> state [enable disable]}
Description	This command allows you to configure IGMP snooping on the Switch.
Parameters	<p><vlan_name 32> – The name of the VLAN for which IGMP snooping is to be configured.</p> <p>host_timeout <sec> – 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>route_timeout <sec> – 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>leave_timer <sec 0-16711450> – Leave timer. The default is 2 seconds.</p> <p>state [enable disable] – 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:

```
DES-3326S:4#config igmp_snooping default host_timeout 250
state enable
Command: config igmp_snooping default host_timeout 250 state
enable

Success.

DES-3326S:4#
```

config igmp_snooping querier

Purpose	Used to configure the time in seconds between general query transmissions, the maximum time in seconds to wait for reports from members and the permitted packet loss that guarantees IGMP snooping.
Syntax	config igmp_snooping querier [<vlan_name 32> all] {query_interval <sec> max_response_time <sec> robustness_variable <value> last_member_query_interval <sec> state [enable disable]}
Description	This command configures IGMP snooping querier.
Parameters	<p><vlan_name 32> – The name of the VLAN for which IGMP snooping querier is to be configured.</p> <p>query_interval <sec> – Specifies the amount of time in seconds between general query transmissions. The default setting is 125 seconds.</p> <p>max_response_time <sec> – Specifies the maximum time in seconds to wait for reports from members. The default setting is 10 seconds.</p> <p>robustness_variable <value> – Provides fine-tuning to allow for expected packet loss on a subnet. The value of the robustness variable is used in calculating the following IGMP message intervals:</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>last_member_query_interval <sec> – The maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. You might lower this interval to reduce the amount of time it takes a router to detect the loss of the last member of a group.</p> <p>state [enable disable] – 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:

```
DES-3326S:4#config igmp_snooping querier default query_interval 125 state enable
```

```
Command: config igmp_snooping querier default query_interval 125 state enable
```

```
Success.
```

```
DES-3326S:4#
```

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><vlan_name 32> – The name of the VLAN on which the router port resides.</p> <p><portlist> – Specifies a range of ports that will be configured as router ports. The port list is specified by listing the lowest Switch number and the beginning port number on that Switch, separated by a colon. Then 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>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To set up static router ports:

```
DES-3326S:4#config router_ports default add 2:1-2:10
```

```
Command: config router_ports default add 2:1-2:10
```

Success.

```
DES-3326S:4#
```


enable igmp_snooping

Purpose	Used to enable IGMP snooping on the Switch.
Syntax	enable igmp_snooping {forward_mcrouter_only}
Description	This command allows you to enable IGMP snooping on the Switch. If forward_mcrouter_only is specified, the Switch will only forward all multicast traffic to the multicast router, only. Otherwise, the Switch forwards all multicast traffic to any IP router.
Parameters	forward_mcrouter_only – Specifies that the Switch should only forward all multicast traffic to a multicast-enabled router. Otherwise, the Switch will forward all multicast traffic to any IP router.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable IGMP snooping on the Switch:

DES-3326S:4#enable igmp_snooping

Command: enable igmp_snooping

Success.

disable igmp_snooping

Purpose	Used to enable IGMP snooping on the Switch.
Syntax	disable igmp_snooping
Description	This command disables IGMP snooping on the Switch. IGMP snooping can be disabled only if IP multicast routing is not being used. Disabling IGMP snooping allows all IGMP and IP multicast traffic to flood within a given IP interface.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To disable IGMP snooping on the Switch:

DES-3326S:4#disable igmp_snooping

Command: disable igmp_snooping

Success.

DES-3326S:4#

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:

```
DES-3326S:4#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

DES-3326S:4#
```

show igmp_snooping group

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

Example usage:

To show igmp snooping group:

```
DES-3326S:4#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     : 1:26,2:7
```

```
VLAN Name      : default
Multicast group: 224.0.0.9
MAC address     : 01-00-5E-00-00-09
Reports        : 1
Port Member     : 1:26,2:7
```

```
VLAN Name      : default
Multicast group: 234.5.6.7
MAC address     : 01-00-5E-05-06-07
Reports        : 1
Port Member     : 1:26,2:9
```

```
VLAN Name      : default
Multicast group: 236.54.63.75
MAC address     : 01-00-5E-36-3F-4B
Reports        : 1
Port Member     : 1:26,2:7
```

```
VLAN Name      : default
Multicast group: 239.255.255.250
MAC address     : 01-00-5E-7F-FF-FA
Reports        : 2
Port Member     : 1:26,2:7
```

```
Total Entries  : 5
```

```
DES-3326S:4#
```

show router_ports

Purpose	Used to display the currently configured router ports on the Switch.
Syntax	show router_ports {vlan <vlan_name 32>}{static dynamic}
Description	This command will display the router ports currently configured on the Switch.
Parameters	<vlan_name 32> – The name of the VLAN on which the router port resides. static – Displays router ports that have been statically configured. dynamic – Displays router ports that have been dynamically configured.
Restrictions	None.

Example usage:

To display the router ports.

```
DES-3326S:4#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
```

```
DES-3326S:4#
```

802.1X COMMANDS

The DES-3326S implements the server-side of the IEEE 802.1x Port-based and MAC-based Network Access Control. This mechanism is intended to allow only authorized users, or other network devices, access to network resources by establishing criteria for each port on the Switch that a user or network device must meet before allowing that port to forward or receive frames.

Command	Parameters
enable 802.1x	
disable 802.1x	
show 802.1x	[auth_state auth_configuration] {ports <portlist>}
config 802.1x capability	ports <portlist> all authenticator none
config 802.1x auth_parameter	ports <portlist> all default direction [both in] port_control [force_unauth auto force_auth] quiet_period <sec 0-65535> tx_period <sec 1-65535> supp_timeout <sec 1-65535> server_timeout <sec 1-65535> max_req <value 1-10> reauth_period <sec 1-65535> enable_reauth [enable disable]
config 802.1x auth_mode	[port_based mac_based]
config 802.1x auth_protocol	[radius_eap radius_pap]
config 802.1x init	config 802.1x init [port_based ports [<portlist> all] mac_based ports [<portlist> all] {mac_address <macaddr>}]
config 802.1x reauth	[port_based ports [<portlist> all] mac_based ports [<portlist> all] {mac_address <macaddr>}]
config radius add	<server_index 1-3> <server_ip> key <passwd 32> default auth_port <udp_port_number> acct_port <udp_port_number>
config radius delete	<server_index 1-3>

Command	Parameters
config radius	<server_index 1-3> ipaddress <server_ip> key <passwd 32> auth_port <udp_port_number> acct_port <udp_port_number>
show radius	

enable 802.1x

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

Example usage:

To enable 802.1x Switch wide:

```
DES-3326S:4#enable 802.1x
```

```
Command: enable 802.1x
```

```
Success.
```

```
DES-3326S:4#
```

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:

```
DES-3326S:4#disable 802.1x
```

```
Command: disable 802.1x
```

```
Success.
```

```
DES-3326S:4#
```


show 802.1x

Purpose	Used to display the current configuration of the 802.1x server on the Switch.
Syntax	show 802.1x [auth_state 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.
Parameters	<p>auth_state – Displays the current 802.1x authentication state of the specified ports.</p> <p>auth_configuration - Displays the current 802.1x authentication configuration of the specified ports.</p> <p>ports <portlist> – Specifies a range of ports. The port list is specified by listing the lowest Switch number and the beginning port number on that Switch, separated by a colon. Then 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>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: – Shows the authentication protocol suite in use between the Switch and a Radius server. The Switch supports EAP and PAP.</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 four 802.1x capabilities that can be set on the Switch: Authenticator, Supplicant, Authenticator and Supplicant, and None.</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 can not access the network.</p>

show 802.1x

Parameters	<p>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 Initalize – Shows the current state of the Backend Authenticator.</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 Identiy 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 (stacking disabled):

DES-3326S:4#show 802.1x auth_state ports 1-5

Command: show 802.1x auth_state ports 1-5

Port	Auth PAE State	Backend State	Port Status
-----	-----	-----	-----
15:1	ForceAuth	Success	Authorized
15:2	ForceAuth	Success	Authorized
15:3	ForceAuth	Success	Authorized
15:4	ForceAuth	Success	Authorized
15:5	ForceAuth	Success	Authorized

DES-3326S:4#

To display the 802.1x configuration settings:

```
DES-3326S:4#show 802.1x auth_configuration ports 1
```

```
Command: show 802.1x auth_configuration ports 1
```

```
802.1X           : Enabled
```

```
Authentication Mode   : Port_based
```

```
Authentication Protocol : Radius_Eap
```

```
Port number   : 15:1
```

```
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
```

```
DES-3326S:4#
```

config 802.1x capability

Purpose	Used to configure the 802.1x capability of a range of ports on the Switch.
Syntax	config 802.1x capability ports [<portlist> all] [authenticator none]
Description	The config 802.1x command has four capabilities that can be set for each port. Authenticator, Supplicant, Authenticator and Supplicant, and None.
Parameters	<p><portlist> – Specifies a range of ports. The port list is specified by listing the lowest Switch number and the beginning port number on that Switch, separated by a colon. Then 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>all – Specifies all of the ports on the Switch.</p> <p>authenticator – A user must pass the authentication process to gain access to the network.</p> <p>none – 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:

```
DES-3326S:4#config 802.1x capability ports 1:1 – 1:10
authenticator
```

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

```
Success.
```

```
DES-3326S:4#
```

config 802.1x auth_parameter

Purpose	Used to configure the 802.1x Authentication parameters on a range of ports. The default parameter will return all ports in the specified range to their default 802.1x settings.
Syntax	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.
Parameters	<p><portlist> – Specifies a range of ports. The port list is specified by listing the lowest Switch number and the beginning port number on that Switch, separated by a colon. Then 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>all – Specifies all of the ports on the Switch.</p> <p>default – Returns all of the ports in the specified range to their 802.1x default settings.</p> <p>direction [both in] – Determines whether a controlled port blocks communication in both the receiving and transmitting directions, or just the receiving direction.</p> <p>port_control – Configures the administrative control over the authentication process for the range of ports.</p> <p>force_auth – Forces the Authenticator for the port to become authorized. Network access is allowed.</p> <p>auto – Allows the port's status to reflect the outcome of the authentication process.</p> <p>force_unauth – Forces the Authenticator for the port to become unauthorized. Network access will be blocked.</p> <p>quiet_period <sec 0-65535> – Configures the time interval between authentication failure and the start of a new authentication attempt.</p> <p>tx_period <sec 1-65535> - Configures the time to wait for a response from a supplicant (user) to send EAP Request/Identity packets.</p> <p>supp_timeout <sec 1-65535> - Configures the time to wait for a response from a supplicant (user) for all EAP packets, except for the Request/Identity packets.</p> <p>server_timeout <sec 1-65535> - Configure the length of time to wait for a response from a Radius server.</p> <p>max_req <value 1-10> – Configures the number of times to retry sending packets to a supplicant (user).</p> <p>reauth_period <sec 1-65535> – Configures the time interval between successive re-authentications.</p> <p>enable_reauth [enable disable] – 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:

```
DES-3326S:4#config 802.1x auth_parameter ports 1:1 – 1:20 direction both
Command: config 802.1x auth_parameter ports 1:1-1:20 direction both

Success.

DES-3326S:4#
```

config 802.1x auth_mode

Purpose	Used to configure 802.1x authentication mode.
Syntax	config 802.1x auth_mode [port_based mac_based]
Description	The config 802.1x auth_mode command configures the authentication mode. 802.1x authorization can be based on the port from which the request is made or a list of authorized MAC addresses can be consulted.
Parameters	<p>port_based – Authorization can be port based. Ports listed in the 802.1x authorized port list are authorized and subject to any authorization parameters as configured. This requires additional configuration to select the ports that are authorized. See config 802.1 init below.</p> <p>mac_based - Authorization can be based on MAC address. Authorized MAC addresses are listed in the 802.1x authorized MAC address. Additional configuration is required to list the MAC address in the authorization list and to specify the port from which request is made. See config 802.1 init below.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the authentication mode.:

```
DES-3326S:4#config 802.1x auth_mode port_based
Command: config 802.1x auth_mode port_based

Success.

DES-3326S:4#
```

config 802.1x auth_protocol

Purpose	Used to configure 802.1x the authentication protocol used for RADIUS authentication.
Syntax	config 802.1x auth_protocol [radius_eap radius_pap]
Description	The config 802.1x auth_protocol command allows for a choice of protocol used by the RADIUS server and client for authentication.
Parameters	radius_eap - Instructs the Switch to use Extensible Authentication Protocol (EAP) used for RADIUS authentication. radius_pap - Instructs the Switch to use Password Authentication Protocol (PAP) used for RADIUS authentication.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the RADIUS authentication protocol used:

```
DES-3326S:4# config 802.1x auth_protocol radius_pap
```

```
Command: config 802.1x auth_protocol radius_pap
```

```
Success.
```

```
DES-3326S:4#
```

config 802.1x init

Purpose	Used to initialize the 802.1x function on a range of ports or a list of MAC addresses.
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>port_based – 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 range of ports. The port list is specified by listing the lowest Switch number and the beginning port number on that Switch, separated by a colon. Then 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>all – Specifies all of the ports on the Switch.</p> <p>mac_based - This instructs the Switch to initialize 802.1x functions based on the MAC address requesting 802.1x initialization. MAC addresses approved for initialization can then be added to a list of approved MAC addresses. Request for 802.1x initialization is approved only for devices with a MAC address that matches one from the list. Additional restrictions can be added by requiring a match for both MAC address and port.</p> <p><macaddr> - Specify the MAC address to add to the list for MAC based 802.1x initialization.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To initialize the authentication state machine of some or all.:

DES-3326S:4# config 802.1x init port_based ports all

Command: config 802.1x init port_based ports all

Success.

DES-3326S:4#

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 either MAC address or port number.
Parameters	<p>port_based – 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>ports <portlist> – Specifies a range of ports. The port list is specified by listing the lowest Switch number and the beginning port number on that Switch, separated by a colon. Then 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>all – Specifies all of the ports on the Switch.</p> <p>mac_based - This instructs the Switch to re-authenticate 802.1x function for a device based on MAC address. MAC addresses approved for re-authentication can then be added to a list of approved MAC addresses. Re-authentication is approved only for devices with a MAC address that matches one from the list. Additional restrictions can be added by requiring a match for both MAC address and port.</p> <p><macaddr> - Specify the MAC address to add to the list for MAC based 802.1x initialization.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure 802.1x reauthentication for ports 1-18:

DES-3326S:4#config 802.1x reauth mac_based ports 1-18

Command: config 802.1x reauth mac_based ports 1-18

Success.

DES-3326S:4#

config radius add

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

Example usage:

To configure Radius server communication settings:

DES-3326S:4#config radius add 1 10.48.74.121 key dlink default

Command: config radius add 1 10.48.74.121 key dlink default

Success.

DES-3326S:4#

config radius delete

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

Example usage:

To delete previously configured Radius server communication settings:

```
DES-3326S:4#config radius delete 1
```

```
Command: config radius delete 1
```

```
Success.
```

```
DES-3326S:4#
```

config radius

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

Example usage:

To configure Radius settings:

DES-3326S:4#config radius 1 10.48.74.121 key dlink default

Command: config radius 1 10.48.74.121 key dlink default

Success.

DES-3326S:4#

show radius

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

Example usage:

To display Radius settings on th Switch:

DES-3326S:4#show radius					
Command: show radius					
Index	IP Address	Auth-Port Number	Acct-Port Number	Status	Key
1	10.1.1.1	1812	1813	Active	Switch
2	20.1.1.1	1800	1813	Active	des3326
3	30.1.1.1	1812	1813	Active	dlink
Total Entries : 3					
DES-3326S:4#					

ACCESS CONTROL LIST AND CPU INTERFACE FILTERING COMMANDS

Command	Parameters
create access_profile	<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> flag_mask [all { urg ack psh rst syn fin }] } dst_port_mask <hex 0x0-0xffff> } udp { src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xffff> } protocol_id { user_mask <hex 0x0-0xffffffff> }] }] { profile_id <value 1-255> }</pre>
config access_profile	<pre>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 [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> }] }] [permit { priority <value 0-7> { replace_priority } replace_dscp <value 0-63> } deny] delete access_id <value 1-255>]</pre>
show access_profile	{ profile_id <value 1-255> { access_id <value 1-65535> } }
delete access_profile	profile_id <value 1-255>
create cpu access_profile	<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> }] }] { profile_id <value 1-255> }</pre>
config cpu access_profile	<pre>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> </pre>

Command	Parameters
	<pre> 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 [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> }] }] [permit deny] delete access_id <value 1-255>] </pre>
enable cpu_interface_filtering	
disable cpu_interface_filtering	
show cpu access_profile	profile_id <value 1-255>
delete cpu access_profile	profile_id <value 1-255>

The Switch allows you to establish criteria to determine whether or not it will forward packets based on the information contained in each packet's header. This system of packet filtering known as an Access Control Lists or ACL are intended to limit network traffic or restrict access to specific devices, users or protocols. The ACL is composed of rule-based profiles configured to permit or deny ingress packets based on a sequential set of conditions. The conditions are used to test each packet in the established order of priority. A positive match (condition match) immediately stops the testing sequence and applies the specified action (permit, deny or replace content). An ACL may be implemented system-wide, or port-based access control can restrict ingress based on source or destination MAC or IP, or TCP/UDP port.

The ACL includes two basic parts, a mask and a rule or set of rules. Therefore setting up an access profile is divided into two parts, create the profile (mask); then configure the conditions for the profile (rule). The parameters that define an access profile include the Profile ID, Access ID, the content of the filter rule (i.e. the match conditions) and the action taken (permit, deny or replace priority tag/DSCP).

The Profile ID is especially important as it establishes the order of the match conditions used for packet examination. Conditions are tested in sequence according to the Profile ID of the rule, the first match stops the testing and applies the action specified. If no conditions match there is no action taken.

Creating the mask (create access_profile) impose a broad and limited criteria used for filtering, where the rules (config access_profile) may be numerous and very specific. Hardware limitations restrict the number of profiles that may be created (see below).

We can illustrate ACL with a simple example:

First an access profile is 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.

First create an access profile that uses IP addresses as the criteria for examination:

create access_profile ip source_ip_mask 255.255.255.0 profile_id 1

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

and it is used to assign a priority in case a conflict occurs. The `profile_id` establishes a priority within the list of profiles. A lower `profile_id` gives the rule a higher priority. In case of a conflict in the rules entered for different profiles, the rule with the highest priority (lowest `profile_id`) will take precedence. *See below for information regarding limitations on access profiles and access rules.*

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

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

Now that an access profile has been created, we add the criteria the Switch will use to decide if a given frame should be forwarded or filtered. We will use the **config access_profile** command to create a new rule that defines the criteria we want. Let's specify in the new rule to deny access to a range of IP addresses. 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
```

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 identifies the rule within the list of rules. The `access_id` is an index number only and does not effect priority within the `profile_id`. This `access_id` may be used later if you want to remove the individual rule from the profile.

The **ip** parameter instructs the Switch that this new rule will be applied to the IP addresses contained within each frame's header. **source_ip** tells the Switch that this rule will apply to the source IP addresses in each frame's header. The IP address **10.42.73.1** will be combined with the **source_ip_mask 255.255.255.0** (specified in the `create access_profile` command) to give the IP address 10.42.73.0 for any source IP address between 10.42.73.0 to 10.42.73.255.

Due to a chipset limitation, the Switch supports a maximum of 10 access profiles. The rules used to define the access profiles are limited to a total of 50 rules for the Switch.

In the example used above - `config access_profile profile_id 1 add access_id 1 ip source_ip 10.42.73.1 deny` – a single access rule was created. This rule will subtract one rule from the total available rules.

It must be noted that there are specific circumstances under which the ACL cannot filter a packet even when there is a condition match that should deny forwarding. This is a limitation that may arise if:

- the destination MAC is the same as the Switch (system) MAC
- a packet is directed to the system IP interface such as multicast IP packets or if the hardware IP routing table is full and Switch software routes the packet according to routing protocol.

In order to address this functional limitation of the chip set, an additional function, **CPU Interface Filtering**, has been added. CPU Filtering may be universally enabled or disabled. Setting up CPU Interface Filtering follows the same syntax as ACL configuration and requires some of the same input parameters. To configure CPU Interface Filtering, see the descriptions below for **create cpu_access_profile** and **config cpu_access_profile**. To enable CPU Interface Filtering, see **enable cpu_interface_filtering**.

The Switch supports up to 5 CPU access profiles, with up to 5 rules for each profile.

create access_profile

Purpose	Used to create an access profile on the Switch and to define which parts of each incoming frame's header the Switch will examine. Masks can be entered that will be combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the config access_profile command, below.
Syntax	create access_profile [ethernet {vlan source_mac <macmask> destination_mac <macmask> 802.1p ethernet_type} ip {vlan source_ip_mask<netmask> destination_ip_mask <netmask> dscp [icmp {type code} igmp {type} tcp {src_port_mask <hex 0x0-0xffff> flag_mask [all { urg ack psh rst syn fin }] } dst_port_mask <hex 0x0-0xffff>} udp {src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xffff>} protocol_id { user_mask <hex 0x0-0xffffffff> }] }
Description	The create access_profile command is used to create an access profile on the Switch and to define which parts of each incoming frame's header the Switch will examine. Masks can be entered that will be combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the config access_profile command, below.
Parameters	<p>ethernet – Specifies that the Switch will examine the layer 2 part of each packet header.</p> <p>vlan – Specifies that the Switch will examine the VLAN part of each packet header.</p> <p>source_mac <macmask> – Specifies a MAC address mask for the source MAC address. This mask is entered in the following hexadecimal format:</p> <p>destination_mac <macmask> – Specifies a MAC address mask for the destination MAC address.</p> <p>802.1p – Specifies that the Switch will examine the 802.1p priority value in the frame's header.</p> <p>ethernet_type – Specifies that the Switch will examine the Ethernet type value in each frame's header.</p> <p>ip – Specifies that the Switch will examine the IP address in each frame's header.</p> <p>vlan – Specifies a VLAN mask.</p> <p>source_ip_mask <netmask> – Specifies an IP address mask for the source IP address.</p> <p>destination_ip_mask <netmask> – Specifies an IP address mask for the destination IP address.</p> <p>dscp – Specifies that the Switch will examine the DiffServ Code Point (DSCP) field in each frame's header.</p> <p>icmp – Specifies that the Switch will examine the Internet Control Message Protocol (ICMP) field in each frame's header.</p> <p>type – Specifies that the Switch will examine each frame's ICMP Type field.</p> <p>code – Specifies that the Switch will examine each frame's ICMP Code field.</p> <p>igmp – Specifies that the Switch will examine each frame's Internet Group Management Protocol (IGMP) field.</p> <p>type – Specifies that the Switch will examine each frame's IGMP Type field.</p> <p>tcp – Specifies that the Switch will examine each frames Transport Control Protocol (TCP) field.</p> <p>src_port_mask <hex 0x0-0xffff> – Specifies a TCP port mask for the source port.</p> <p>dst_port_mask <hex 0x0-0xffff> – Specifies a TCP port mask for the destination port.</p>

create access_profile

create access_profile

Parameters

- flag_mask** – Specifies examination of TCP flag field according to the type of flag. Specify all to examine all type of TCP flag fields.
- urg** – Specifies urgent TCP flag field.
- ack** – Specifies acknowledge TCP flag field.
- psh** – Specifies push TCP flag field.
- rst** – Specifies reset TCP flag field.
- syn** – Specifies synchronize TCP flag field. Specifying the SYN flag will prevent any client from making TCP connections to the system.
- fin** – Specifies finish TCP flag field.
- udp** – Specifies that the Switch will examine each frame's Universal Datagram Protocol (UDP) field.
- src_port_mask** <hex 0x0-0xffff> – Specifies a UDP port mask for the source port.
- dst_port_mask** <hex 0x0-0xffff> – Specifies a UDP port mask for the destination port.
- protocol_id** – Specifies that the Switch will examine each frame's Protocol ID field.
- user_mask** <hex 0x0-0xffffffff> – Specifies that the rule applies to the IP protocol ID and the mask options behind the IP header.
- profile_id** <value 1-255> – Specifies an index number that will identify the access profile being created with this command.

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:

DES-3326S:4# create access_profile ip source_ip_mask 255.255.255.0 profile_id 1 deny

Command: create access_profile ip source_ip_mask 255.255.255.0 profile_id 1 deny

Success.

DES-3326S:4#

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

Example usage:

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

```
DES-3326S:4# delete access_profile profile_id 1
```

```
Command: delete access_profile profile_id 1
```

```
Success.
```

```
DES-3326S:4#
```

config access_profile

Purpose	Used to configure an access profile on the Switch and to define specific values that will be used to by the Switch to determine if a given packet should be forwarded or filtered. Masks entered using the create access_profile command will be combined, using a logical AND operation, with the values the Switch finds in the specified frame header fields.
Syntax	<pre> 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 [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> }]] [permit { priority <value 0-7> { replace_priority} replace_dscp <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> – Specifies the index of the access list profile.
- add access_id* <value 1-255> – Adds an additional rule to the above specified access profile. The value specifies the relative priority of the additional rule. 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_id* <value 0-255> – Specifies that the access profile will apply to only packets with this destination IP address.
- dscp* <value 0-63> – Specifies that the access profile will apply only to packets that have this value in their Type-of-Service (DiffServ code point, DSCP) field in their IP packet header.
- icmp* – Specifies that the Switch will examine the Internet Control Message Protocol (ICMP) field within each packet.
- type* <value 0-65535> – Specifies that the access profile will apply to this ICMP type value.
- code* <value 0-255> – Specifies that the access profile will apply to this ICMP code.
- igmp* – Specifies that the Switch will examine the Internet Group Management Protocol (IGMP) field within each packet.
- type* <value 0-255> – Specifies that the access profile will apply to packets that have this IGMP type value.
- tcp* – Specifies that the Switch will examine the Transmission Control Protocol (TCP) field within each packet.
- src_port* <value 0-65535> – Specifies that the access profile will apply only to packets that have this TCP source port in their TCP header.
- dst_port* <value 0-65535> – Specifies that the access profile will apply only to packets that have this TCP destination port in their TCP header.

config access_profile

Parameters	<p><i>flag</i> – Specifies examination of TCP flag field according to the type of flag. Specify all to examine all type of TCP flag fields.</p> <p><i>urg</i> – Specifies urgent TCP flag field.</p> <p><i>ack</i> – Specifies acknowledge TCP flag field.</p> <p><i>psh</i> – Specifies push TCP flag field.</p> <p><i>rst</i> – Specifies reset TCP flag field.</p> <p><i>syn</i> – Specifies synchronize TCP flag field.</p> <p><i>fin</i> – Specifies finish TCP flag field.</p> <p><i>udp</i> – Specifies that the Switch will examine the Universal Datagram Protocol (UDP) field in each packet.</p> <p><i>src_port</i> <value 0-65535> – Specifies that the access profile will apply only to packets that have this UDP source port in their header.</p> <p><i>dst_port</i> <value 0-65535> – Specifies that the access profile will apply only to packets that have this UDP destination port in their header.</p> <p><i>protocol_id</i> <value 0-255> – Specifies that the Switch will examine the Protocol field in each packet and if this field contains the value entered here, apply the following rules.</p> <p><i>user_define</i> <hex 0x0-0xffffffff> – Specifies a mask to be combined with the value found in the frame header using a logical AND operation.</p> <p><i>priority</i> <value 0-7> – Specifies that the access profile will apply to packets that contain this value in their 802.1p priority field of their header.</p> <p><i>permit</i> – Specifies that packets that match the access profile are permitted to be forwarded by the Switch.</p> <p><i>replace_priority</i> – This parameter is specified if you want to change the 802.1p user priority of a packet that meets the specified criteria. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being transmitted from the Switch.</p> <p><i>replace_dscp</i> <value 0-63> – Allows you to specify a value to be written to the DSCP field of an incoming packet that meets the criteria specified in the first part of the command. This value will over-write the value in the DSCP field of the packet.</p> <p><i>deny</i> – Specifies that packets that do not match the access profile are not permitted to be forwarded by the Switch and will be filtered.</p> <p><i>delete</i> <value 1-255> – Specifies the access ID of a rule you want to delete.</p>
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:

DES-3326S:4# config access_profile profile_id 1 add access_id 1 ip source_ip 10.42.73.1

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

Success.

DES-3326S:4#

show access_profile

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

Example usage:

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

DES-3326S:4#show access_profile

Command: show access_profile

Access Profile Table

Access Profile ID : 10

TYPE : IP Frame Filter

=====

=

MASK Option :

Source IP MASK

255.255.255.0

Access ID : 1 (250) Mode : Deny

10.123.1.0

Total Entries : 1

DES-3326S:4#

create cpu access_profile

Purpose	Used to create an access profile specifically for CPU Interface Filtering on the Switch. A CPU access profile defines the 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 cpu access_profile command, below. CPU interface filtering must be enabled to use CPU access profiles (enable cpu_interface_filtering).
Syntax	<pre> config cpu 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> }] }] { profile_id <value 1-255> } </pre>
Description	The create cpu access_profile command is used to create an access profile used only for CPU Interface Filtering. Masks can be entered that will be combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the config cpu access_profile command.
Parameters	<p><i>ethernet</i> – Specifies that the Switch will examine the layer 2 part of each packet header.</p> <p><i>vlan</i> – Specifies that the Switch will examine the VLAN part of each packet header.</p> <p><i>source_mac <macmask></i> – Specifies a MAC address mask for the source MAC address. This mask is entered in a hexadecimal format.</p> <p><i>destination_mac <macmask></i> – Specifies a MAC address mask for the destination MAC address.</p> <p><i>802.1p</i> – Specifies that the Switch will examine the 802.1p priority value in the frame's header.</p> <p><i>ethernet_type</i> – Specifies that the Switch will examine the Ethernet type value in each frame's header.</p>

create cpu access_profile

Parameters	<p><i>ip</i> – Specifies that the Switch will examine the IP address in each frame's header.</p> <p><i>vlan</i> – Specifies a VLAN mask.</p> <p><i>source_ip_mask</i> <netmask> – Specifies an IP address mask for the source IP address.</p> <p><i>destination_ip_mask</i> <netmask> – Specifies an IP address mask for the destination IP address. </p> <p><i>dscp</i> – Specifies that the Switch will examine the DiffServ Code Point (DSCP) field in each frame's header.</p> <p><i>icmp</i> – Specifies that the Switch will examine the Internet Control Message Protocol (ICMP) field in each frame's header.</p> <p><i>type</i> – Specifies that the Switch will examine each frame's ICMP Type field.</p> <p><i>code</i> – Specifies that the Switch will examine each frame's ICMP Code field.</p> <p><i>igmp</i> – Specifies that the Switch will examine each frame's Internet Group Management Protocol (IGMP) field.</p> <p><i>type</i> – Specifies that the Switch will examine each frame's IGMP Type field.</p> <p><i>tcp</i> – Specifies that the Switch will examine each frames Transport Control Protocol (TCP) field.</p> <p><i>src_port_mask</i> <hex 0x0-0xffff> – Specifies a TCP port mask for the source port.</p> <p><i>dst_port_mask</i> <hex 0x0-0xffff> – Specifies a TCP port mask for the destination port.</p> <p><i>flag_mask</i> – Enter the appropriate flag_mask parameter. All incoming packets have TCP port numbers contained in them as the forwarding criterion. These numbers have flag bits associated with them which are parts of a packet that determine what to do with the packet. The user may deny packets by denying certain flag bits within the packets. The user may choose between <i>all</i>, <i>urg</i> (urgent), <i>ack</i> (acknowledgement), <i>psh</i> (push), <i>rst</i> (reset), <i>syn</i> (synchronize) and <i>fin</i> (finish).</p> <p><i>udp</i> – Specifies that the Switch will examine each frame's Universal Datagram Protocol (UDP) field.</p> <p><i>src_port_mask</i> <hex 0x0-0xffff> – Specifies a UDP port mask for the source port.</p> <p><i>dst_port_mask</i> <hex 0x0-0xffff> – Specifies a UDP port mask for the destination port.</p> <p><i>protocol_id</i> <value 0-255> – Specifies that the Switch will examine the protocol field in each packet and if this field contains the value entered here, apply the following rules</p> <p><i>user_define_mask</i> <hex 0x0-0xffffffff> – Specifies that the rule applies to the IP protocol ID and the mask options behind the IP header.</p> <p><i>profile_id</i> <value 1-255> – Sets the relative priority for the profile. Priority is set relative to other profiles where the lowest profile ID has the highest priority.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create a cpu access profile:

```
DES-3326S:4# create cpu access_profile ethernet vlan source_mac 00-00- 00-00-00-01
```

```
Command: create cpu access_profile ethernet vlan source_mac 00-00-00- 00-00-01
```

```
Success.
```

```
DES-3326S:4#
```

config cpu access_profile

Purpose	Used to configure a cpu access profile used for CPU Interface Filtering and to define specific values that will be used to by the Switch to determine if a given packet should be forwarded or filtered. Masks entered using the create cpu access_profile profile_id command will be combined, using a logical AND operation, with the values the Switch finds in the specified frame header fields. CPU interface filtering must be enabled to use CPU access profiles (enable cpu_interface_filtering).
Syntax	<pre> config cpu 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 [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> }] } [permit deny] delete access_id <value 1-255>] </pre>
Description	The config cpu access_profile command is used to configure a cpu access profile for CPU Interface Filtering and to enter specific values that will be combined, using a logical AND operation, with masks entered with the create cpu access_profile command, above.
Parameters	<p><i>profile_id <value 1-255></i> – Enter an integer used to identify the cpu access profile that will be configured with this command. This value is assigned to the cpu access profile when it is created with the create access_profile command. The profile ID sets the relative priority for the profile and specifies an index number that will identify the access profile being created with this command. Priority is set relative to other profiles where the lowest profile ID has the highest priority.</p> <p><i>add access_id <value 1-255></i> – Adds an additional rule to the above specified access profile. The value is used to index the rule created.</p> <p><i>ethernet</i> – Specifies that the Switch will look only into the layer 2 part of each packet.</p> <p><i>vlan <vlan_name 32></i> – Specifies that the access profile will apply to only to this VLAN.</p> <p><i>source_mac <macaddr></i> – Specifies that the access profile will apply to only packets with this source MAC address.</p> <p><i>destination_mac <macaddr></i> – Specifies that the access profile will apply to only packets with this destination MAC address.</p> <p><i>802.1p <value 0-7></i> – Specifies that the access profile will apply only to packets with this 802.1p priority value.</p> <p><i>ethernet_type <hex 0x0-0xffff></i> – Specifies that the access profile will apply only to packets with this hexadecimal 802.1Q Ethernet type value in the packet header.</p>

Parameters	<p><i>ip</i> – Specifies that the Switch will look into the IP fields in each packet.</p> <p><i>vlan</i> <vlan_name 32> – Specifies that the access profile will apply to only this VLAN.</p> <p><i>source_ip</i> <ipaddr> – Specifies that the access profile will apply to only packets with this source IP address.</p> <p><i>destination_id</i> <value 0-255> – Specifies that the access profile will apply to only packets with this destination IP address.</p> <p><i>dscp</i> <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</p> <p><i>icmp</i> – Specifies that the Switch will examine the Internet Control Message Protocol (ICMP) field within each packet.</p> <p><i>type</i> <value 0-65535> – Specifies that the access profile will apply to this ICMP type value.</p> <p><i>code</i> <value 0-255> – Specifies that the access profile will apply to this ICMP code.</p> <p><i>igmp</i> – Specifies that the Switch will examine the Internet Group Management Protocol (IGMP) field within each packet.</p> <p><i>type</i> <value 0-255> – Specifies that the access profile will apply to packets that have this IGMP type value.</p> <p><i>tcp</i> – Specifies that the Switch will examine the Transmission Control Protocol (TCP) field within each packet.</p> <p><i>src_port</i> <value 0-65535> – Specifies that the access profile will apply only to packets that have this TCP source port in their TCP header.</p> <p><i>dst_port</i> <value 0-65535> – Specifies that the access profile will apply only to packets that have this TCP destination port in their TCP header.</p> <p><i>udp</i> – Specifies that the Switch will examine each frame's Universal Datagram Protocol (UDP) field.</p> <p><i>src_port</i> <value 0-65535> – Specifies that the access profile will apply only to packets that have this UDP source port in their header.</p> <p><i>dst_port</i> <value 0-65535> – Specifies that the access profile will apply only to packets that have this UDP destination port in their header.</p> <p><i>protocol_id</i> <value 0-255> – Specifies that the Switch will examine the protocol field in each packet and if this field contains the value entered here, apply the following rules.</p> <p><i>permit</i> – Specifies the rule permit access for incoming packets on the previously specified port.</p> <p><i>deny</i> – Specifies the rule will deny access for incoming packets on the previously specified port</p> <p><i>delete access_id</i> <value 1-65535> - Use this to remove a previously created access rule in a profile id.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure a cpu access profile:

```
DES-3326S:4# config cpu access_profile profile_id 101 add access_id 1 ip vlan default
source_ip 20.2.2.3 destination_ip 10.1.1.252 dscp 3 icmp type 11 code 32 deny
Command: config cpu access_profile profile_id 101 add access_id 1 ip vlan default source_ip
20.2.2.3 destination_ip 10.1.1.252 dscp 3 icmp type 11 code 32 deny

Success.

DES-3326S:4#
```

enable cpu_interface_filtering

Purpose	Used to enable CPU interface filtering on the Switch.
Syntax	enable cpu_interface_filtering
Description	This command is used, in conjunction with the create and config cpu access_profile commands, to enable CPU interface filtering on the Switch. When CPU interface filtering is enabled, the cpu access profile rules that have been created will be active.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable cpu interface filtering:

```
DES-3326S:4#enable cpu_interface_filtering
Command: enable cpu_interface_filtering

Success.

DES-3326S:4#
```

disable cpu_interface_filtering

Purpose	Used to disable CPU interface filtering on the Switch.
Syntax	disable cpu_interface_filtering
Description	This command is used to disable CPU interface filtering on the Switch. When CPU interface filtering is disabled, the cpu access profile rules that have been created will not be active.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To disable cpu interface filtering:

```
DES-3326S:4#disable cpu_interface_filtering
Command: disable cpu_interface_filtering

Success.

DES-3326S:4#
```


show cpu 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 cpu access_profile command is used to display the currently configured access profiles.
Parameters	<i>profile_id</i> – Specify the profile id to display only the access rules configuration for a single profile id.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DES-3326S:4#show cpu access_profile
Command: show cpu access_profile

CPU Interface Filtering state: [Enabled]
CPU Interface Filtering Access Profile Table

Access Profile ID : 1
TYPE : Ethernet Frame Filter
=====
MASK Option :
VLAN      Source MAC      Destination MAC  802.1p Ethernet
          FF-FF-FF-FF-FF-FF  FF-FF-FF-FF-FF-FF
-----
Access ID : 1 (250)   Mode : Permit
-----
default    00-00-00-00-00-01 00-00-00-00-00-02 0    0x800
-----

Access Profile ID : 255
TYPE : IP Frame Filter
=====
MASK Option :
VLAN      Source IP MASK  Dst. IP MASK   DSCP ICMP TYPE CODE
          255.255.255.255 255.255.255.0
-----
Access ID : 255 (251)   Mode : Deny
-----
default    10.1.1.14    10.23.23.0    63 200 200
-----

Total Entries : 2

DES-3326S:4#
```

delete cpu access_profile access_profile

Purpose	Used to delete a previously created access profile or cpu access profile.
Syntax	delete cpu access_profile profile_id <value 1-255>
Description	The delete cpu access_profile command is used to delete a previously created cpu access profile.
Parameters	<i>profile_id <value 1-255></i> – Enter an integer between 1 and 255 that is used to identify the access profile or cpu access profile to be deleted with this command. This value is assigned to the access profile when it is created with the create cpu access_profile command.

delete cpu access_profile access_profile

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

Example usage:

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

```
DES-3326S:4# delete cpu access_profile profile_id 1
```

```
Command: delete cpu access_profile profile_id 1
```

```
Success.
```

```
DES-3326S:4#
```

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.

Command	Parameters
config traffic_segmentation	<portlist> forward_list null <portlist>
show traffic_segmentation	<portlist>

config traffic_segmentation

Purpose	Used to configure traffic segmentation on the Switch.
Syntax	config traffic_segmentation <portlist> forward_list [null <portlist>]
Description	The config traffic_segmentation command is used to configure traffic segmentation on the Switch.
Parameters	<p><portlist> – Specifies a range of ports that will be configured for traffic segmentation. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 specifies port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.</p> <p>forward_list – Specifies a range of ports that will receive forwarded frames from the ports specified in the portlist, above.</p> <p>null – no ports are specified</p> <p><portlist> – 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 <portlist> specified above for config traffic_segmentation).</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure ports 1 through 10 to be able to forward frames to port 11 through 15:

```
DES-3326S:4# config traffic_segmentation 1-10 forward_list 11-15
```

```
Command: config traffic_segmentation 1-10 forward_list 11-15
```

```
Success.
```

```
DES-3326S:4#
```

show traffic_segmentation

Purpose	Used to display the current traffic segmentation configuration on the Switch.
Syntax	config traffic_segmentation <portlist> forward_list [null <portlist>]
Description	The show traffic_segmentation command is used to display the current traffic segmentation configuration on the Switch.
Parameters	<portlist> – Specifies a range of ports for which the current traffic segmentation configuration on the Switch will be displayed. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 specifies port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.
Restrictions	The port lists for segmentation and the forward list must be on the same Switch.

Example usage:

To display the current traffic segmentation configuration on the Switch.

```
DES-3326S:4#show traffic_segmentation
```

```
Command: show traffic_segmentation
```

Traffic Segmentation Table

Port	Forward Portlist
1	9-15
2	9-15
3	9-15
4	9-15
5	9-15
6	9-15
7	9-15
8	9-15
9	9-15
10	9-15
11	1-26
12	1-26
13	1-26
14	1-26
15	1-26
16	1-26
17	1-26
18	1-26
19	1-26
20	1-26
21	1-26
22	1-26
23	1-26
24	1-26
25	1-26
26	1-26

```
DES-3326S:4#
```

STACKING COMMANDS

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

Command	Parameters
config stacking mode	disable enable master auto slave
show stacking	{mode}

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



NOTE: Switch stacking requires that a stacking module be installed on every Switch used for the stacked group. If a stacking module is detected, the default settings for the Switch allow it to function as either a member of a stacked group or as a standalone device.

config stacking mode

Purpose	Used to enable or disable Switch stacking and to configure the stacking mode.
Syntax	config stacking mode [disable enable [master auto slave]]
Description	Use this command to setup Switch stacking or disable the stacking function. Each Switch should be configured separately prior to establishing the physical link through the stacking ports.
Parameters	<p>enable – Stacking mode is enabled by default. When enabled the Switch can operate as a standalone device or it can be allowed to operate with other DES-3326S Switches in a stacked group.</p> <p>auto – This is the default stacking mode setting for the Switch. In auto stacking mode the Switch is eligible for stacking or it can operate as a standalone device. If a Switch stack is connected and all Switches are configured to operate in auto stacking mode, the master-slave relationships and stacking order will be determined automatically according to MAC address. The lowest MAC address becomes the master (stack number 1). The order in which slave devices appear logically in the stack (stack number 2+) is determined by how they are connected relative to the master Switch. The auto mode serves to first determine if the device is stacked or standalone, then if stacked, it determines which Switch is the master and the remaining stack numbers for the slave Switches.</p> <p>master – This overrides the auto stacking mode. The auto mode described above may be overridden so that a properly connected Switch in a stack may be forced into master mode. Only one Switch in a stack may act as the master and all configuration settings for the stacked group - including stacking configuration - are saved in configuration files in the master Switch. The stack is managed as a single entity through the master.</p> <p>slave – This overrides the auto stacking mode. When the Switch is in slave mode it cannot function as a master and a master Switch must be properly connected to the stack for a Switch to operate in slave mode.</p> <p>disable – This forces the Switch to operate as a standalone device. In standalone mode the Switch functions as a standalone device even if a stacking module is installed. When stacking mode is disabled, configuration settings including IP settings are saved in an alternate configuration file. A Switch that has stacking mode disabled should not use stacking ports if they are present.</p>
Restrictions	The Switch's stacking mode can only be changed using the CLI interface. Only administrator-level users can issue this command.

Example usage:

To configure the stacking mode:

```
DES-3326S:4#config stack mode disable
```

```
Command: config stacking mode disable
```

```
Do you want to save the system's configuration to NV-RAM?(y/n)
```

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

```
Success.
```

```
DES-3326S:4#
```


show stacking

Purpose	Used to display the current stacking information.
Syntax	show stacking {mode}
Description	This command will display the current stacking information.
Parameters	<p>mode – When specified this will display the current stacking mode.</p> <p>none – No specification will display information for all Switches in the stack. Information displayed includes MAC address, firmware version, stacking mode, RPS status and available port range.</p>
Restrictions	None.

Example usage:

To display the current stacking (standalone mode) information:

```
DES-3326S:4#show sta
Command: show stacking

ID  MAC Address    Port Range Mode   Version  RPS Status  Model Name
-----
*1  00-05-5D-1F-5B-A0  1 - 26  STANDALONE  4.01-B27  Present    DES-3326S

Total Entries :1

DES-3326S:4#
```

To display the current stacking (auto mode) information:

```
DES-3326S:4#show sta
Command: show stacking

ID  MAC Address      Port Range Mode   Version RPS Status  Model Name
-----
*1  00-05-5D-1F-5B-A0  1 - 26    AUTO    4.01-B27  In Use    DES-3326S
2   00-05-5D-1E-5B-E0  27 - 52   AUTO    4.01-B27  In Use    DES-3326S

Total Entries :2

DES-3326S:4#
```

Example usage:

To display stacking mode:

```
DES-3326S:4#show stacking mode
Command: show stacking mode

Stacking Topology : Disable
Setting           : STANDALONE
Current           : STANDALONE

DES-3326S:4#
```

TIME AND SNTP COMMANDS

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

Command	Parameters
config sntp	{primary <ipaddr> secondary <ipaddr> poll-interval <int 30-99999>}(1)
show sntp	
enable sntp	
disable sntp	
config time	<date ddmmmyyyy > <time hh:mm:ss >
config time-zone	{operator(1) [+ -] hour(2) <gmt_hour 0-13> min(3) <minute 0-59>}
config dst	[disable repeating {s-week<start_week 1-4,last> s-wday <start_weekday sun-sat> s-mth <start_mth 1-12> s-time <start_time hh:mm> e-week <end_week 1-4,last> e-wday <end_weekday sun-sat> e-mth <end_mth 1-12> e-time <end_time hh:mm> offset [30 60 90 120]} annual {s-date <start_date 1-31> s-mth <start_mth 1-12> s-time <start_time hh:mm> e-date <end_date 1-31> e-mth <end_mth 1-12> e-time <end_time hh:mm> offset [30 60 90 120]}]}
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>primary – This is the primary server the SNTP information will be taken from.</p> <p><ipaddr> – The IP address of the primary server.</p> <p>secondary – This is the secondary server the SNTP information will be taken from in the event the primary server is unavailable.</p> <p><ipaddr> – The IP address for the secondary server.</p> <p>poll-interval – This is the interval between requests for updated SNTP information.</p> <p><int 30-99999> – The polling interval ranges from 30 to 99,999 seconds.</p>
Restrictions	Only administrator-level users can issue this command. SNTP service must be enabled for this command to function (enable sntp).

Example usage:

To configure SNTP settings:

DES-3326S:4#config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 30

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

Success.

DES-3326S:4#

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:

```
GS-3212SR:4#show sntp
```

```
Command: show sntp
```

```
Current Time Source : System Clock
```

```
SNTP : Disabled
```

```
SNTP Primary Server : 10.1.1.1
```

```
SNTP Secondary Server : 10.1.1.2
```

```
SNTP Poll Interval : 30 sec
```

```
DES-3326S:4#
```

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.
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:

DES-3326S:4#enable sntp

Command: enable sntp

Success.

DES-3326S:4#

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:

DES-3326S:4#disable sntp

Command: disable sntp

Success.

DES-3326S:4#

config time

Purpose	Used to manually configure system time and date settings.
Syntax	config time date <date ddmthyyyy> <time hh:mm:ss>
Description	This will configure the system time and date settings. These will be overridden if SNTP is configured and enabled.
Parameters	<p>date – Express the date using two numerical characters for the day of the month, three alphabetical characters for the name of the month, and four numerical characters for the year. For example: 03aug2003.</p> <p>time – 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:

DES-3326S:4#config time 30jun2003 16:30:30

Command: config time 30jun2003 16:30:30

Success.

DES-3326S:4#

config time zone

Purpose	Used to determine the time zone used in order to adjust the system clock.
Syntax	config time-zone {operator [+ -] hour <gmt_hour 0-13> min <minute 0-59>}
Description	This will adjust system clock settings according to the time zone. Time zone settings will adjust SNTP information accordingly.
Parameters	<p>operator – Choose to add (+) or subtract (-) time to adjust for time zone relative to GMT.</p> <p>hour – Select the number hours different from GMT.</p> <p>min – Select the number of minutes difference added or subtracted to adjust the time zone.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure time zone settings:

DES-3326S:4#config time_zone operator + hour 2 min 30

Command: config time_zone operator + hour 2 min 30

Success.

DES-3326S:4#

config dst

Purpose	Used to enable and configure time adjustments to allow for the use of Daylight Savings Time (DST).
Syntax	<pre> config dst [disable repeating {s-week<start_week 1-4,last> s-wday <start_weekday sun-sat> s-mth <start_mth 1-12> s-time <start_time hh:mm> e-week <end_week 1-4,last> e-wday <end_weekday sun-sat> e-mth <end_mth 1-12> e-time <end_time hh:mm> offset [30 60 90 120]} annual {s-date <start_date 1-31> s-mth <start_mth 1-12> s-time <start_time hh:mm> e-date <end_date 1-31> e-mth <end_mth 1-12> e-time <end_time hh:mm> offset [30 60 90 120]}]} </pre>
Description	DST can be enabled and configured using this command. When enabled this will adjust the system clock to comply with any DST requirement. DST adjustment effects system time for both manually configured time and time set using SNTP service.
Parameters	<p>disable - Disable the DST seasonal time adjustment for the Switch.</p> <p>repeating - Using repeating mode will enable DST seasonal time adjustment. Repeating mode requires that the DST beginning and ending date be specified using a formula. For example, specify to begin DST on Saturday during the second week of April and end DST on Sunday during the last week of October.</p> <p>annual - Using annual mode will enable DST seasonal time adjustment. Annual mode requires that the DST beginning and ending date be specified concisely. For example, specify to begin DST on April 3 and end DST on October 14.</p> <p>s-week - Configure the week of the month in which DST begins.</p> <p><start_week 1-4,last> - The number of the week during the month in which DST begins where 1 is the first month, 2 is the second month and so on, last is the last week of the month.</p> <p>e-week - Configure the week of the month in which DST ends.</p> <p><end_week 1-4,last> - The number of the week during the month in which DST ends where 1 is the first month, 2 is the second month and so on, last is the last week of the month.</p> <p>s-wday – Configure the day of the week in which DST begins.</p> <p><start_weekday sun-sat> - The day of the week in which DST begins expressed using a three character abbreviation (sun, mon, tue, wed, thu, fri, sat)</p> <p>e-wday - Configure the day of the week in which DST ends.</p> <p><end_weekday sun-sat> - The day of the week in which DST ends expressed</p>

config dst

using a three character abbreviation (sun, mon, tue, wed, thu, fri, sat)

s-mth - Configure the month in which DST begins.

<start_mth 1-12> - The month to begin DST expressed as a number.

e-mth - Configure the month in which DST ends.

<end_mth 1-12> - The month to end DST expressed as a number.

s-time - Configure the time of day to begin DST. Time is expressed using a 24-hour clock.

e-time - Configure the time of day to end DST. Time is expressed using a 24-hour clock.

s-date - Configure the specific date (day of the month) to begin DST. The date is expressed numerically.

e-date - Configure the specific date (day of the month) to begin DST. The date is expressed numerically.

offset - Indicates number of minutes to add or to subtract during the summertime. The range of offset are 30,60,90,120; default value is 60

Restrictions

Only administrator-level users can issue this command.

```
DES-3326S:4#config dst repeating s_week 2 s_day tue s_mth 4
s_time 15:00 e_week
2 e_day wed e_mth 10 e_time 15:30 offset 30
Command: config dst repeating s_week 2 s_day tue s_mth 4 s_time
15:00 e_week 2 e
_day wed e_mth 10 e_time 15:30 offset 30

Success.

DES-3326S:4#
```

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 time:

```
DES-3326S:4#show time
Command: show time

Current Time Source : System Clock
Current Time       : 01 Jul 2003 01:43:41
Time Zone         : GMT +02:30
Daylight Saving Time : Repeating
Offset in Minutes  : 30
  Repeating From   : Apr 2nd Tue 15:00
    To            : Oct 2nd Wed 15:30
  Annual From     : 29 Apr 00:00
    To           : 012 Oct 00:00

DES-3326S:4#
```

ARP COMMANDS

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

Command	Parameters
create arpentry	<ipaddr> <macaddr>
delete arpentry	<ipaddr> <macaddr>
show arpentry	ipif <ipif_name> ipaddress <ipaddr> static}
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	<ipaddr> – The IP address of the end node or station. <macaddr> – The MAC address corresponding to the IP address above.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

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

```
DES-3326S:4#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.
```

```
DES-3326S:4#
```

delete arpentry

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

Example Usage:

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

```
DES-3326S:4#delete arpentry 10.48.74.121
```

```
Command: delete arpentry 10.48.74.121
```

```
Success.
```

```
DES-3326S:4#
```

config arp_aging

Purpose	Used to configure the age-out timer for ARP table entries on the Switch.
Syntax	config arp_aging time <value>
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	time <value 0-65535> – The ARP age-out time, in minutes. The default is 20.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure ARP aging time:

```
DES-3326S:4#config arp_aging time 30
```

```
Command: config arp_aging time 30
```

```
Success.
```

```
DES-3326S:4#
```

show arpentry

Purpose	Used to display the ARP table.
Syntax	show arpentry {ipif <ipif_name> ipaddress <network_address> static}
Description	This command is used to display the current contents of the Switch's ARP table.
Parameters	<p><ipif_name> – The name of the IP interface the end node or station for which the ARP table entry was made, resides on.</p> <p><ipaddr> – The network address corresponding to the IP interface name above.</p> <p>static – Displays the static entries to the ARP table.</p>
Restrictions	None.

Example Usage:

To display the ARP table:

DES-3326S:4#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

DES-3326S:4#

clear arptable

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

Example Usage:

To remove dynamic entries in the ARP table:

```
DES-3326S:4#clear arptable
```

```
Command: clear arptable
```

```
Success.
```

```
DES-3326S:4#
```

ROUTING TABLE COMMANDS

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

Command	Parameters
create iproute	default <network_address> <ipaddr> <metric 1-65535> primary backup
delete iproute	default <network_address> <ipaddr>
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 [default]<network_address> <ipaddr> {<metric>} {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>default – creates a default IP route entry.</p> <p><network_address> – IP address and netmask of the IP interface that is the destination of the route. You can specify the address and mask information using the traditional format (for example, 10.1.2.3 255.0.0.0 or in CIDR format, 10.1.2.3 16).</p> <p><ipaddr> – The IP address for the next hop router.</p> <p><metric> – The default setting is 1.</p> <p>primary – Designates the IP route as the primary route. If a single IP route is being used it is not necessary to specify primary or backup.</p> <p>backup – Designates a secondary IP route that is enabled if the primary IP route is unavailable. Also known as "floating static route."</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:

DES-3326S:4#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.

DES-3326S:4#

delete iproute

Purpose	Used to delete an IP route entry from the Switch's IP routing table.
Syntax	delete iproute [default <network_address>] <ipaddr>
Description	This command will delete an existing entry from the Switch's IP routing table.
Parameters	<p>default – deletes a default IP route entry.</p> <p><network_address> – IP address and netmask of the IP interface that is the destination of the route. You can specify the address and mask information using the traditional format (for example, 10.1.2.3 255.0.0.0 or in CIDR format, 10.1.2.3 16).</p> <p><ipaddr> - IP address of the next hop router for removal from the routing table.</p>
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete a static address 10.48.75.121, mask 255.0.0.0 from the routing table:

DES-3326S:4#delete iproute 10.48.74.121|255.0.0.0

Command: delete iproute 10.48.74.121|8

Success.

DES-3326S:4#

show iproute

Purpose	Used to display the Switch's current IP routing table.
Syntax	show iproute {<network_address>} {static rip ospf}
Description	This command will display the Switch's current IP routing table.
Parameters	<p><network_address> – IP address and netmask of the IP interface that is the destination of the route. You can specify the address and mask information using the traditional format (for example, 10.1.2.3 255.0.0.0 or in CIDR format, 10.1.2.3 16).</p> <p>static – use this to display static iproute entries.</p> <p>rip – use this to display RIP iproute entries.</p> <p>ospf – use this to display OSPF iproute entries.</p>
Restrictions	None.

Example Usage:

To display the contents of the IP routing table:

DES-3326S:4#show iproute

Command: show iproute

IP Address	Netmask	Gateway	Interface Name	Hops	Protocol
0.0.0.0	0.0.0.0	0.1.1.254	System	1	Default
10.0.0.0	255.0.0.0	10.48.74.122	System	1	Local

Total Entries: 2

DES-3326S:4#

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

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-3326S Switch is also redistributed.
Parameters	<p>src [static rip local] – Allows for the selection of the protocol for the source device.</p> <p>mettype [1 2] – Allows for the selection of one of two methods of calculating the metric value. Type-1 calculates (for RIP to OSPF) by adding the destination's interface cost to the metric entered in the Metric field. Type-2 uses the metric entered in the Metric field without change. this field applies only when the destination field is OSPF.</p> <p>metric <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.

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:

```
DES-3326S:4#create route redistribute dst ospf src rip
```

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

```
Success.
```

```
DES-3326S:4#
```

create route redistribute dst rip

Purpose	Used to add route redistribution settings for the exchange of OSPF routes to RIP routes on the Switch.
Syntax	create route redistribute dst rip src [static ospf {all internal external type_1 type_2}] {metric <value>}
Description	This command will redistribute routing information between the OSPF and Rip routing protocols to all routers on the network that are running OSPF or RIP. Routing information entered into the Static Routing Table on the local DES-3326S Switch is also redistributed
Parameters	src [static ospf {all internal external type_1 type_2}] – Allows the selection of the protocol of the source device. metric <value> – Allows the entry of an OSPF interface cost. this is analogous to a HOP Count in the RIP routing protocol.
Restrictions	Only administrator-level users can issue this command.

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

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

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

Entering the metric **0** specifies transparency.

Example Usage:

To add route redistribution settings:

DES-3326S:4#create route redistribute dst rip src ospf all metric 2

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

Success.

DES-3326S:4#

delete route redistribute

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

Example Usage:

To delete route redistribution settings:

```
DES-3326S:4#delete route redistribute dst rip src ospf
```

```
Command: delete route redistribute dst rip src ospf
```

```
Success.
```

```
DES-3326S:4#
```

config route redistribute dst ospf

Purpose	Used to configure route redistribution from RIP to OSPF.
Syntax	config route redistribute dst ospf src [static rip local] {mettype [1 2]} metric <value>}
Description	Route redistribution allows routers on the network – that are running different routing protocols to exchange routing information. this is accomplished by comparing the routes stored in the various router's routing tables and assigning appropriate metrics. This information is then exchanged among the various routers according to the individual routers current routing protocol. The Switch can redistribute routing information between the OSPF and RIP routing protocols to all routers on the network that are running OSPF or RIP. Routing information entered into the Static Routing Table on the local Switch is also redistributed.
Parameters	src – Allows the selection of the protocol of the source device. dst – Allows the selection of the protocol of the destination device. mettype – allows the selection of one of the methods for calculating the metric value. Type-a calculates the metric (for RIP to OSPF) by adding the destination's interface cost to the metric entered in the Metric field. Type-2 uses the metric entered in the Metric field without change. This field applies only when the destination field is OSPF. metric <value> – Allows the entry of an OSPF interface cost. This is analogous to a Hop Count in the RIP routing protocol.
Restrictions	Only administrator-level users can issue this command.

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

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

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

Example Usage:

To configure route redistributions:

DES-3326S:4#config route redistribute dst rip src ospf all metric 2

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

Success.

DES-3326S:4#

config route redistribute dst rip

Purpose	Used to configure route redistribution from OSPF to RIP.
Syntax	config route redistribute dist rip src [local static ospf {all internal external type_1 type_2}] {metric <value>}
Description	Route redistribution allows routers on the network – that are running different routing protocols to exchange routing information. this is accomplished by comparing the routes stored in the various router's routing tables and assigning appropriate metrics. this information is then exchanged among the various routers according to the individual routers current routing protocol. The Switch can redistribute routing information between the OSPF and RIP routing protocols to all routers on the network that are running OSPF or RIP. Routing information entered into the Static Routing Table on the local Switch is also redistributed.
Parameters	src – Allows the selection of the routing protocol on the source device. dst – Allows the selection of the routing protocol on the destination device. metric <value> – Allows the entry of an OSPF interface cost. this is analogous to a HOP Count in the RIP routing protocol.
Restrictions	Only administrator-level users can issue this command.

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

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

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

Entering the metric **0** specifies transparency.

Example Usage:

To configure route redistributions:

```
DES-3326S:4#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.

```
DES-3326S:4#
```

show route redistribute

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

Example Usage:

To display route redistributions:

DES-3326S:4#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

DES-3326S:4#

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 <1-65535 sec> max_response_time <1-25 sec> robustness_variable <value 1-255> last_member_query_interval <value 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_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 <value 1-25> state [enable disable]}
Description	This command is used to configure IGMP on the Switch.
Parameters	<p><ipif_name 12> – The name of the IP interface for which you want to configure IGMP.</p> <p>all – Specifies all the IP interfaces on the Switch.</p> <p>version <value 1-2> – The IGMP version number.</p> <p>query_interval <1-65535 sec> – The time in seconds between general query transmissions, in seconds.</p> <p>max_response_time <1-25 sec> – the maximum time in seconds that the Switch will wait for reports from members.</p> <p>robustness_variable <value1-255> – the permitted packet loss that guarantees IGMP.</p> <p>last_member_query_interval <value1-25> – the Max Response Time inserted into Group-Specific Queries sent in response to Leave Group messages, and is also the amount of time between Group-Specific Query messages. The default is 1 second</p> <p>state [enable disable] – 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.

DES-3326S:4#config igmp all version 1 state enable

Command: config igmp all version 1 state enable

Success.

DES-3326S:4#

show igmp

Purpose	Used to display the IGMP configuration for the Switch of for a specified IP interface.
Syntax	show igmp {ipif <ipif_name>}
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> – The name of the IP interface for which the IGMP configuration will be displayed.
Restrictions	None.

Example Usage:

To display IGMP configurations:

DES-3326S:4#show igmp							
Command: show igmp							
Interface	I P Address	Ver-	Query	Maximum	Robust-	Last Member	State
		sion		Response	ness	Query	
				Time	Value	Interval	
-----	-----	---	----	-----	-----	----	-----
System	10.90.90.90	1	125	10	2	1	Enabled
Develop	20.1.1.1	1	125	10	2	1	Enabled
Total Entries: 2							
DES-3326S:4#							

show igmp group

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

Example Usage:

To display IGMP group table:

```
DES-3326S:4#show igmp group
Command: show igmp group
```

Interface	Multicast Group	Last Reporter	Querier IP Address	IP	Expire Time
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
DES-3326S:4#
```

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> time <sec>
config bootp_relay add	ipif <ipif_name> <ipaddr>
config bootp_relay delete	ipif <ipif_name> <ipaddr>
enable bootp_relay	
disable bootp_relay	
show bootp_relay	ipif <ipif_name>

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>} {time <sec>}
Description	This command is used to configure the BOOTP relay feature.
Parameters	<p>hops <value> – Specifies the maximum number of relay agent hops that the BOOTP packets can cross.</p> <p>time <sec> – 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.

DES-3326S:4#config bootp_relay hops 4 time 2

Command: config bootp_relay hops 4 time 2

Success.

DES-3326S:4#

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> <ipaddr>
Description	This command adds an IP address as a destination to forward (relay) BOOTP packets to.
Parameters	<ipif_name> – The name of the IP interface in which BOOTP relay is to be enabled. <ipaddr> – The BOOTP server IP address.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To add a BOOTP relay.

DES-3326S:4#config bootp_relay add ipif System 10.43.21.12

Command: config bootp_relay add ipif System 10.43.21.12

Success.

DES-3326S:4#

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> <ipaddr>
Description	This command is used to delete an IP destination addresses in the Switch's BOOTP relay table.
Parameters	<ipif_name> – The name of the IP interface that contains the IP address below. <ipaddr> – The BOOTP server IP address.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete a BOOTP relay.

DES-3326S:4#config bootp_relay delete ipif System 10.43.21.12

Command: config bootp_relay delete ipif System 10.43.21.12

Success.

DES-3326S:4#

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.

```
DES-3326S:4#enable bootp_relay
```

```
Command: enable bootp_relay
```

```
Success.
```

```
DES-3326S:4#
```

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:

```
DES-3326S:4#disable bootp_relay
```

```
Command: disable bootp_relay
```

```
Success.
```

```
DES-3326S:4#
```

show bootp_relay

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

DES-3326S:4#show bootp_relay ipif System				
Command: show bootp_relay ipif System				
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				
DES-3326S:4#				

DNS RELAY COMMANDS

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

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

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

config dnsr

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

Example Usage:

To set IP address 10.43.21.12 of primary.

DES-3326S:4#config dnsr primary 10.43.21.12**Command: config dnsr primary 10.43.21.12****Success****DES-3326S:4#**

config dnsr [add|delete] static

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

Example Usage:

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

DES-3326S:4#config dnsr add static dns1 10.43.21.12

Command: config dnsr add static dns1 10.43.21.12

Success.

DES-3326S:4#

Example Usage:

To delete an entry domain name dns1, IPaddress 10.43.21.12 from DNS static table.

DES-3326S:4#config dnsr delete static dns1 10.43.21.12

Command: config dnsr delete static dns1 10.43.21.12

Success.

DES-3326S:4#

enable dnsr

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

Example Usage:

To enable status of DNS relay:

```
DES-3326S:4#enable dnsr
```

Command: enable dnsr

Success.

```
DES-3326S:4#
```

disable dnsr

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

Example Usage:

To disable status of DNS relay.

```
DES-3326S:4#disable dnsr
```

Command: disable dnsr

Success.

```
DES-3326S:4#
```

enable dnsr cache

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

Example Usage:

To enable cache lookup for DNS relay.

```
DES-3326S:4#enable dnsr cache
```

Command: enable dnsr cache

Success.

```
DES-3326S:4#
```

disable dnsr cache

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

Example Usage:

To disable cache lookup for DNS relay.

```
DES-3326S:4#disable dnsr cache
```

Command: disable dnsr cache

Success.

```
DES-3326S:4#
```

enable dnsr static

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

Example Usage:

To enable static table lookup for DNS relay:

```
DES-3326S:4#enable dnsr static
```

```
Command: enable dnsr static
```

```
Success.
```

```
DES-3326S:4#
```

disable dnsr static

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

Example Usage:

To disable static table lookup for DNS relay.

```
DES-3326S:4#disable dnsr static
```

```
Command: disable dnsr static
```

```
Success.
```

```
DES-3326S:4#
```

show dnsr

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

Example Usage:

To display DNS relay status:

DES-3326S:4#show dnsr static

Command: show dnsr static

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

DES-3326S:4#

To display DNS relay table:

```
DES-3326S:4#show dnsr
```

```
Command: show dnsr
```

```
DNSR Status           : Disabled
Primary Name Server    : 10.48.74.122
Secondary Name Server  : 20.48.74.123
DNSR Cache Status      : Enabled
DNSR Static Table Status : Enabled
```

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
```

```
DES-3326S:4#
```

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> disable] tx_mode <value 1-16> [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 rx_mode

Purpose	Used to configure RIP on the Switch.
Syntax	config rip [ipif <ipif_name 12> all] rx_mode [[disable v1_only] v2_only v1_or_v2] authentication [enable disable] <password>]
Description	This command is used to configure RIP on the Switch.
Parameters	<p><ipif_name 12> – The name of the IP interface.</p> <p>all – To configure all RIP receiving mode for all IP interfaces.</p> <p>rx_mode – Determines how received RIP packets will be interpreted – as RIP version V1 only, V2 Only, or V1 Compatible (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>disable – Prevents the reception of RIP packets.</p> <p>v1_only – Specifies that only RIP v1 packets will be accepted.</p> <p>v2_only – Specifies that only RIP v2 packets will be accepted.</p> <p>v1_or_v2 – Specifies that both RIP v1 and v2 packets will be accepted.</p> <p>authentication [enable disable] – Enables or disables authentication for RIP on the Switch.</p> <p><password> – Allows the specification of a case-sensitive password.</p> <p>state [enable disable] – 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.

DES-3326S:4#config rip ipif System rx_mode v1_only

Command: config rip ipif System rx_mode v1_only

Success.

DES-3326S:4#

config rip tx_mode

Purpose	Used to configure RIP's transmission mode.
Syntax	config rip [ipif <ipif_name> all] tx_mode [disable] authentication [enable disable] <password>
Description	This command is used to configure RIP's transmission mode.
Parameters	<p><ipif_name> – The name of the IP interface.</p> <p>all – To configure all RIP transmitting mode for all IP interfaces.</p> <p>disable – Prevents the transmission of RIP packets.</p> <p>v1_only – Specifies that only RIP v1 packets will be transmitted.</p> <p>v2_only – Specifies that only RIP v2 packets will be transmitted.</p> <p>v1_compatible – Specifies that both RIP v1 and v2 packets will be transmitted.</p> <p>authentication [enable disable] – Enables or disables</p> <p>authentication [enable disable] – Enables or disables authentication for RIP on the Switch.</p> <p><password> – Allows the specification of a case-sensitive password.</p>
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To change the RIP transmission mode for the IP interface System.

DES-3326S:4#config rip ipif System tx_mode v1_only

Command: config rip ipif System tx_mode v1_only

Success.

DES-3326S:4#

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.

```
DES-3326S:4#enable rip
```

```
Command: enable rip
```

```
Success.
```

```
DES-3326S:4#
```

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.

```
DES-3326S:4#disable rip
```

```
Command: disable rip
```

```
Success.
```

```
DES-3326S:4#
```

show rip

Purpose	Used to display the RIP configuration and statistics for the Switch.
Syntax	show rip {ipif <ipif_name>}
Description	This command will display the RIP configuration and statistics for a given IP interface or for all IP interfaces.
Parameters	<ipif_name> – 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.

DES-3326S:4#show rip

Command: show rip

RIP Interface Settings

RIP Global State : Disabled

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

Total Entries : 1

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	ipif <ipif_name 12> ipaddress <network_address>
show dvmrp routing_table	ipaddress <network_address>
show dvmrp	ipif <ipif_name>

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> all] {metric <value> probe <second> neighbor_timeout <second> state [enable disable]}
Description	This command is used to configure DVMRP on the Switch.
Parameters	<p><ipif_name> – The name of the IP interface for which DVMRP is to be configured.</p> <p>all – Specifies that DVMRP is to be configured for all IP interfaces on the Switch.</p> <p>metric <value> – Allows the assignment of a DVMRP route cost to the above IP interface. A DVMRP route cost is a relative number that represents the real cost of using this route in the construction of a multicast delivery tree. It is similar to, but not defined as, the hop count in RIP. The default is 1.</p> <p>probe <second> – DVMRP defined an extension to IGMP that allows routers to query other routers to determine if a multicast group is present on a given router subnetwork or not. This is referred to as a 'probe'. The default value is 10 seconds.</p> <p>neighbor_timeout <second> – The time period for which DVMRP will hold Neighbor Router reports before issuing poison route messages. The default value is 35 seconds.</p> <p>state [enable disable] – 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:

DES-3326S:4#config dvmrp ipif System neighbor_timeout 30 metric 1 probe 5

Command: config dvmrp ipif System neighbor_timeout 30 metric 1 probe 5

Success

DES-3326S:4#

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

Example Usage:

To enable DVMRP:

```
DES-3326S:4#enable dvmrp
```

Command: enable dvmrp

Success.

```
DES-3326S:4#
```

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:

```
DES-3326S:4#disable dvmrp
```

Command: disable dvmrp

Success.

```
DES-3326S:4#
```

show dvmrp routing_table

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

Example Usage:

To display DVMRP routing table:

DES-3326S:4#show dvmrp routing_table

Command: show dvmrp routing_table

DVMRP Routing Table

Source Address	Source Mask	Next Hop Router	Hop	Learned	Interface	Expire
10.0.0.0	255.0.0.0	10.90.90.90	2	Local	System	-
20.0.0.0	255.0.0.0	20.1.1.1	2	Local	ip2	-
30.0.0.0	255.0.0.0	30.1.1.1	2	Local	ip3	-

Total Entries: 3

DES-3326S:4#

show dvmrp neighbor

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

Example Usage:

To display DVMRP neighbor table:

DES-3326S:4#show dvmrp neighbor

Command: show dvmrp neighbor

Interface	Neighbor Address	Generation ID	Expire Time
-----	-----	-----	-----
System	10.2.1.123	2	250

Total Entries: 1

show dvmrp nexthop

Purpose	Used to display the current DVMRP routing next hop table.
Syntax	show dvmrp nexthop {ipaddress <network_address> ipif <ipif_name>}
Description	This command will display the DVMRP routing next hop table.
Parameters	<p><ipif_name> – The name of the IP interface for which you want to display the current DVMRP routing next hop table.</p> <p>ipaddress <network_address> – The IP address and netmask of the destination. You can specify the IP address and netmask information using the traditional format or the CIDR format. For example, 10.1.2.3 255.255.0.0 or 10.2.3.4 16.</p>
Restrictions	None.

Example Usage:

To display DVMRP routing next hop table:

DES-3326S:4#show dvmrp nexthop

Command: show dvmrp nexthop

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

Total Entries: 6

DES-3326S:4#

show dvmrp

Purpose	Used to display the current DVMRP routing table.
Syntax	show dvmrp {<ipif_name>}
Description	The command will display the current DVMRP routing table.
Parameters	<ipif_name> – The name of the IP interface for which you want to display the DVMRP routing table.
Restrictions	None.

Example Usage:

To show DVMRP configurations:

```
DES-3326S:4#show dvmrp
```

```
Command: show dvmrp
```

```
DVMRP Global State : Disabled
```

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

```
Total Entries: 1
```

```
DES-3326S:4#
```

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>ipif – Name assigned to the specific IP interface being configured for PIM settings.</p> <p>all – Used to configure PIM settings for all IP interfaces.</p> <p>hello - The time, in seconds, between issuing hello packets to find neighboring routers.</p> <p>jp_interval – 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 jp_interval 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 65535 seconds. The default is 60 seconds.</p> <p>state – 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>
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To configure PIM settings for IP interface “System”:

```
DES-3326S:4#config pim ipif System hello 35 jp_interval 70 state enable
```

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

Success.

```
DES-3326S:4#
```

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 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:

```
DES-3326S:4#enable pim
```

```
Command: enable pim
```

```
Success.
```

```
DES-3326S:4#
```

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

Usage Example:

To disable PIM on the Switch:

```
DES-3326S:4#disable pim
```

```
Command: disable pim
```

```
Success.
```

```
DES-3326S:4#
```

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>ipif – The name of an IP interface for which you want to view the PIM neighbor router table.</p> <p>ipaddress - The IP address and netmask of the destination routing device for which you want to view the neighbor raouter table. You can specify the IP address and netmask information usnig 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.

Usage Example:

To display PIM settings as configured on the Switch:

DES-3326S:4#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

DES-3326S:4#

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	ipif – 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:

```
DES-3326S:4#show pim
Command: show pim

PIM Global State : Disabled
PIM-DM Interface Table

Interface  IP Address      Hello   Join|Prune
-----  -
System    10.90.90.90     35      0         Enabled

Total Entries : 1

DES-3326S:4#
```

IP MULTICASTING COMMANDS

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

Command	Parameters
show ipmc cache	group <group> ipaddress <network_address>
show ipmc	ipif {ipif <ipif_name> 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><group> – The multicast group ID.</p> <p><network_address> – The IP address and netmask of the destination. You can specify the IP address and netmask information using the traditional format or the CIDR format. For example, 10.1.2.3 255.255.0.0 or 10.2.3.4 16.</p>
Restrictions	None.

Usage Example:

To display the current IP multicast forwarding cache:

DES-3326S:4#show ipmc cache

Command: show ipmc cache

Multicast Group	Source IP Address	Source IP Mask	Upstream Neighbor	Expire Time	Routing Protocol
224.1.1.1	10.48.74.121	255.0.0.0	10.48.75.63	30	dvmrp
224.1.1.1	20.48.74.25	255.0.0.0	20.48.75.25	20	pim-dm
224.1.2.3	10.48.75.3	255.0.0.0	10.48.76.6	30	dvmrp

Total Entries: 3

DES-3326S:4#

show ipmc

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

Usage Example

To display the current IP multicast interface table:

DES-3326S:4#show ipmc

Command: show ipmc

Interface	IP Address	Multicast Routing
System	10.90.90.90	INACT

Total Entries: 1

DES-3326S:4#

MD5 CONFIGURATION COMMANDS

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

Command	Parameters
config md5	key <key_id> <password>
create md5	key <key_id> <password>
delete md5	key <key_id>
show md5	key <key_id>

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

config md5

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

Usage Example

To configure an MD5 Key password:

```
DES-3326S:4#config md5 key 1 dlink
```

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

```
Success.
```

```
DES-3326S:4#
```

create md5

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

Usage Example

To create an entry in the MD5 key table:

```
DES-3326S:4# create md5 key 1 dlink
```

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

```
Success.
```

```
DES-3326S:4#
```

delete md5

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

Usage Example

The delete an entry in the MD5 key table:

```
DES-3326S:4# delete md5 key 1
```

```
Command: delete md5 key 1
```

```
Success.
```

```
DES-3326S:4#
```


show md5

Purpose	Used to display an MD5 key table.
Syntax	show md5 {key <key_id>}
Description	This command will display the current MD5 key table.
Parameters	<key_id> – The MD5 key ID.
Restrictions	None.

Usage Example

To display the current MD5 key:

```
DES-3326S:4#show md5
```

```
Command: show md5
```

MD5 Key Table

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

```
Total Entries: 4
```

```
DES-3326S:4#
```

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 0-65535>
delete ospf area	<area_id>
config ospf area	<area_id> type [normal stub] stub_summary [enable disable] metric <value 1-65535>
show ospf area	<area_id>
create ospf host_route	<ipaddr> area <area_id> metric <value>
delete ospf host_route	<ipaddr>
config ospf host_route	<ipaddr> area <area_id> metric <value>
show ospf host_route	<ipaddr>
create ospf aggregation	<area_id> <network_address> lsdb_type [summary] advertise [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 asextl

Command	Parameters
	ink]
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 <1-65535 sec> dead_interval <1-65535 sec> authentication [none simple <password> 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> md5 <key_id>] metric <value> state [enable disable]
show ospf ipif	<ipif_name 12>
show ospf all	
config ospf virtual_link	<area_id> <neighbor_id> hello_interval <1-65535 sec> dead_interval <1-65535 sec> authentication [simple <password> md5 <key_id> none]
delete ospf virtual_link	<area_id> <neighbor_id>
show ospf virtual_link	<area_id> <neighbor_id>

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

config ospf

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

Usage Example

To configure the OSPF router ID:

```
DES-3326S:4#config ospf router_id 10.48.74.122
Command: config ospf router_id 10.48.74.122
Success.
DES-3326S:4#
```

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:

```
DES-3326S:4#enable ospf
Command: enable ospf
Success.
DES-3326S:4#
```

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:

DES-3326S:4#disable ospf

Command: disable ospf

DES-3326S:4#

show ospf

Purpose	Used to display the current OSPF state on the Switch.
Syntax	show ospf
Description	This command will display the current state of OSPF on the Switch, divided into the following categories: <ul style="list-style-type: none">General OSPF settingsOSPF Interface settingsOSPF Area settingsOSPF Virtual Interface settingsOSPF Area Aggregation settingsOSPF Host Route settings
Parameters	None.
Restrictions	None.

Usage Example:

To show OSPF state:

DES-3326S:4#show ospf

Command: show ospf

OSPF Router ID : 10.1.1.2

State : Enabled

OSPF Interface Settings

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

Total Entries : 3

OSPF Area Settings

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

Total Entries : 4

Virtual Interface Configuration

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

Total Entries : 2

OSPF Area Aggregation Settings

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

Total Entries : 0

OSPF Host Route Settings

Host Address	Metric	Area ID	TOS
10.3.3.3	1	10.1.1.1	0

Total Entries : 1

DES-3326S: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>}}
Description	This command is used to create an OSPF area and configure its settings.
Parameters	<p><area_id> – The OSPF area ID.</p> <p>type – The OSPF area mode of operation – stub or normal.</p> <p>stub_summary – enables or disables the OSPF area to import summary LSA advertisements.</p> <p><value> – The OSPF area cost between 0 and 65535. The default is 0.</p>
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To create an OSPF area:

DES-3326S:4#create ospf area 10.48.74.122 type normal

Command: create ospf area 10.48.74.122 type normal

Success.

DES-3326S:4#

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

Usage Example:

To delete an OSPF area:

```
DES-3326S:4#delete ospf area 10.48.74.122
```

```
Command: delete ospf area 10.48.74.122
```

```
Success.
```

```
DES-3326S:4#
```

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>}]
Description	This command is used to configure an OSPF area's settings.
Parameters	<p><area_id> – The OSPF area ID.</p> <p>type – Allows the specification of the OSPF mode of operation – stub or normal.</p> <p>stub_summary [enable disable] – Allows the OSPF area import of LSA advertisements to be enabled or disabled.</p> <p><value> – 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:

```
DES-3326S:4#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.

```
DES-3326S:4#
```

show ospf area

Purpose	Used to display an OSPF area's configuration.
Syntax	show ospf area {<area_id>}
Description	This command will display the current OSPF area configuration.
Parameters	<area_id> – <area_id> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.
Restrictions	None.

Usage Example

To display an OSPF area's settings:

DES-3326S:4#show ospf area

Command: show ospf area

Area_id	Type	Stub Import Summary LSA	Stub Default Cost
0.0.0.0	Normal	None	None
10.48.74.122	Stub	Enabled	1

Total Entries: 2

DES-3326S:4#

create ospf host_route

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

Usage Example

To configure the OSPF host route settings:

```
DES-3326S:4#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.
```

```
DES-3326S:4#
```

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:

```
DES-3326S:4#delete ospf host_route 10.48.74.122
```

```
Command: delete ospf host_route 10.48.74.122
```

```
Success.
```

```
DES-3326S:4#
```

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> – <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 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:

```
DES-3326S:4#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.
```

```
DES-3326S:4#
```

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:

DES-3326S:4#show ospf host_route

Command: show ospf host_route

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

Total Entries: 2

DES-3326S:4#

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.
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:

**DES-3326S:4#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.

DES-3326S:4#

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:

```
DES-3326S:4#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.

DES-3326S:4#
```

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><area_id> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.</p> <p><network_address> – The 32-bit number in the form of an IP address that uniquely identifies the network that corresponds to the OSPF Area.</p> <p>lsdb_type [summary] – Specifies the type of address aggregation.</p> <p>advertise [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 configure the OSPF area aggregation settings:

```
DES-3326S:4#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.

```
DES-3326S:4#
```

show ospf aggregation

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

Usage Example

To display OSPF area aggregation settings:

DES-3326S:4#show ospf aggregation

Command: show ospf aggregation

OSPF Area Aggregation Settings

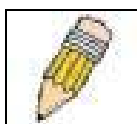
Area ID	Aggregated Network Address	LSDB Type	Advertise
10.1.1.1	10.0.0.0 8	Summary	Enabled
10.1.1.1	20.2.0.0 16	Summary	Enabled

Total Entries: 2

DES-3326S:4#

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>area_id <area_id> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.</p> <p>advertise_router <ipaddr> – The router ID of the advertising router.</p> <p>type [rtrlink netlink summary assummary asextlink] – The type of link.</p>
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:

DES-3326S:4#show ospf lsdb

Command: show ospf lsdb

Area Sequence	LSDB Type	Advertising Router ID	Link State ID	Cost	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

DES-3326S:4#

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:

DES-3326S:4#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

DES-3326S:4#

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><area_id> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.</p> <p><neighbor_id> – The OSPF router ID for the 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:

DES-3326S:4#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

DES-3326S:4#

config ospf ipif

Purpose	Used to configure the OSPF interface settings.
Syntax	config ospf ipif <ipif_name> {area <area_id> priority <value> hello_interval <sec> dead_interval <sec> authentication [none simple <password> md5 <key_id>] metric <value> state [enable disable]}
Description	This command is used to configure the OSPF interface settings.
Parameters	<p><ipif_name> – The name of the IP interface.</p> <p>priority <value> – The priority used in the election of the Designated Router (DR). A number between 0 and 255.</p> <p>metric <value> – The interface metric (1 to 65535). Entering a 0 will allow automatic calculation of the metric.</p> <p>hello_interval <sec> – Allows the specification of the interval between the transmission of OSPF Hello packets, in seconds. Between 1 and 65535 seconds can be specified. The Hello Interval, Dead Interval, Authorization Type, and Authorization Key should be the same for all routers on the same network.</p> <p>dead_interval <sec> – 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><password> – A case-sensitive password.</p> <p><key_id> – A previously configured MD5 key ID (1 to 255).</p> <p>metric <value> – 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>
Restrictions	Only administrator-level users can issue this command.

Usage Example

To configure OSPF interface settings:

```
DES-3326S:4#config ospf ipif System priority 2 hello_interval 15 metric 2 state enable
```

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

Success.

```
DES-3326S:4#
```

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> dead_interval <sec> authentication [none simple <password> md5 <key_id>] metric <value> 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.
Parameters	<p>priority <value> – The priority used in the election of the Designated Router (DR). A number between 0 and 255.</p> <p>metric <value> – The interface metric (1 to 65535). Entering a 0 will allow automatic calculation of the metric.</p> <p>hello_interval <sec> – Allows the specification of the interval between the transmission of OSPF Hello packets, in seconds. Between 1 and 65535 seconds can be specified. The Hello Interval, Dead Interval, Authorization Type, and Authorization Key should be the same for all routers on the same network.</p> <p>dead_interval <sec> – 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>
Parameters	<p><password> – A case-sensitive password.</p> <p><key_id> – A previously configured MD5 key ID (1 to 255).</p> <p>metric <value> – 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>
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:

```
DES-3326S:4#config ospf all state enable
```

```
Command: config ospf all state enable
```

```
Success.
```

```
DES-3326S:4#
```


show ospf ipif

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

Usage Example

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

```
DES-3326S:4#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:
5Authentication: None
Total Entries: 1

DES-3326S:4#
```

show ospf all

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

Usage Example:

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

```
DES-3326S:4#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

DES-3326S:4#
```

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> dead_interval <sec> authentication [simple <password> md5 <key_id> none]}
Description	This command is used to configure the OSPF virtual interface settings.
Parameters	<p><area_id> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.</p> <p><neighbor_id> – The OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router.</p> <p>hello_interval <sec> – Allows the specification of the interval between the transmission of OSPF Hello packets, in seconds. Between 1 and 65535 seconds can be specified. The Hello Interval, Dead Interval, Authorization Type, and Authorization Key should be the same for all routers on the same network.</p> <p>dead_interval <sec> – 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><password> – A case-sensitive password.</p> <p><key_id> – A previously configured MD5 key. A value between 1 and 255 seconds can be entered.</p>
Restrictions	Only administrator-level users can issue this command.

Usage Example

To configure the OSPF virtual interface settings:

```
DES-3326S:4#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.

```
DES-3326S:4#
```

create ospf virtual_link

Purpose	Used to create an OSPF virtual interface.
Syntax	create ospf virtual_link <area_id> <neighbor_id> {hello_interval <sec> authentication [none simple <password> md5 <key_id>]}
Description	This command is used to create an OSPF virtual interface.
Parameters	<p><area_id> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.</p> <p><neighbor_id> – The OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router. The router ID of the neighbor router.</p> <p>hello_interval <sec> – 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>
Parameters	<p>dead_interval <sec> – dead_interval <sec> – 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><password> – A case-sensitive password.</p> <p><key_id> – A previously configured MD5 key ID (1 to 255).</p>
Restrictions	Only administrator-level users can issue this command.

Usage Example

To create an OSPF virtual interface:

```
DES-3326S:4#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.

```
DES-3326S:4#
```

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><area_id> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.</p> <p><neighbor_id> – The OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router. The router ID of the neighbor router.</p>
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To delete an OSPF virtual interface from the Switch:

DES-3326S:4#delete ospf virtual_link 10.1.12 20.1.1.1

Command: delete ospf virtual_link 10.1.12 20.1.1.1

Success.

DES-3326S:4#

show ospf virtual_link

Purpose	Used to display the current OSPF virtual interface configuration.
Syntax	show ospf virtual_link {<area_id> <neighbor_id>}
Description	This command will display the current OSPF virtual interface configuration.
Parameters	<p><area_id> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.</p> <p><neighbor_id> – The OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router. This is the router ID of the neighbor router.</p>
Restrictions	None.

Usage Example:

To display the current OSPF virtual interface configuration:

DES-3326S:4#show ospf virtual_link

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

Total Entries: 1

DES-3326S:4#

COMMAND HISTORY LIST

The 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	
dir	
config command_history	<value>

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:

```
DES-3326S:4#?  
Command: ?  
..  
?  
clear  
clear arptable  
clear counters  
clear fdb  
clear log  
clear port_security_entry port  
config 802.1p default_priority  
config 802.1p user_priority  
config 802.1x auth_mode  
config 802.1x auth_parameter ports  
config 802.1x auth_protocol  
config 802.1x capability ports  
config 802.1x init  
config 802.1x reauth  
config access_profile profile_id  
config account  
config arp_aging time  
config arpentry  
config bandwidth_control  
config bootp_relay
```


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:

```
DES-3326S:4#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

DES-3326S:4#
```

dir

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

Example usage

To display all of the commands:

```
DES-3326S:4#dir
Command: dir
..
?
clear
clear arptable
clear counters
clear fdb
clear log
clear port_security_entry port
config 802.1p default_priority
config 802.1p user_priority
config 802.1x auth_mode
config 802.1x auth_parameter ports
config 802.1x auth_protocol
config 802.1x capability ports
config 802.1x init
config 802.1x reauth
config access_profile profile_id
config account
config arp_aging time
config arpentry
config bandwidth_control
config bootp_relay
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

config command_history

Purpose	Used to configure the command history.
Syntax	config command_history <value>
Description	This command is used to configure the command history.
Parameters	<1-40> – the number of previously executed commands maintained in the buffer. Up to 40 of the latest executed commands may be viewed.
Restrictions	None.

Example usage

To configure the command history:

```
DES-3326S:4#config command_history 20
```

```
Command: config command_history 20
```

```
Success.
```

```
DES-3326S:4#
```

TECHNICAL SPECIFICATIONS

General									
Standard	IEEE 802.3 10BASE-T Ethernet 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 802.3z 1000BASE-X Ethernet								
Protocols	CSMA/CD								
Data Transfer Rates: Ethernet Fast Ethernet Gigabit Ethernet Fiber Optic	<table> <tr> <td>Half-duplex</td><td>Full-duplex</td></tr> <tr> <td>10 Mbps</td><td>20Mbps</td></tr> <tr> <td>100Mbps</td><td>200Mbps</td></tr> <tr> <td></td><td>2000Mbps</td></tr> </table> IEC 793-2:1992 Type A1a - 50/125um multimode Type A1b - 62.5/125um multimode Both types use SC optical connector	Half-duplex	Full-duplex	10 Mbps	20Mbps	100Mbps	200Mbps		2000Mbps
Half-duplex	Full-duplex								
10 Mbps	20Mbps								
100Mbps	200Mbps								
	2000Mbps								
Topology	Star								
Network Cables	UTP Cat.5 for 100Mbps UTP Cat.3, 4, 5 for 10Mbps EIA/TIA-568 100-ohm screened twisted-pair (STP)(100m)								

Performance	
Transmission Method:	Store-and-forward
Packet Buffer Memory:	16 MB per device
Filtering Address Table:	8 K MAC address per device
Packet Filtering/ Forwarding Rate:	Full-wire speed for all connections. 148,800 pps per port (for 100Mbps) 1,488,000 pps per port (for 1000Mbps)
MAC Address Learning:	Automatic update.
Forwarding Table Age Time:	Max age: 10 - 1000000 seconds. Default = 300.

Physical & Environmental	
AC inputs:	100 - 240 VAC, 50/60 Hz (internal universal power supply)
Power Consumption:	29 watts maximum
DC fans:	1 built-in 40 x 40 x10 mm fan
Operating Temperature:	0 to 50 degrees Celsius (32 to 122 degrees Fahrenheit)
Storage Temperature:	-25 to 55 degrees Celsius (-13 to 131 degrees Fahrenheit)
Humidity:	Operating: 5% to 95% RH, non-condensing Storage: 0% to 95% RH, non-condensing
Dimensions:	441 mm x 210 mm x 43 mm (17.36 x 8.26 x 1.69 inches) 1UHeight, 19 inch rack-mount width
Weight:	2.5 kg (5.5 lbs.)
EMI:	FCC Class A, CE Mark, C-Tick
Safety:	CSA International



GLOSSARY

100BASE-FX: 100Mbps Ethernet implementation over fiber.

100BASE-TX: 100Mbps Ethernet implementation over Category 5 and Type 1 Twisted Pair cabling.

10BASE-T: The IEEE 802.3 specification for Ethernet over Unshielded Twisted Pair (UTP) cabling.

ageing: The automatic removal of dynamic entries from the Switch Database which have timed-out and are no longer valid.

ATM: Asynchronous Transfer Mode. A connection oriented transmission protocol based on fixed length cells (packets). ATM is designed to carry a complete range of user traffic, including voice, data, and video signals.

auto-negotiation: A feature on a port that allows it to advertise its capabilities for speed, duplex, and flow control. When connected to an end station that also supports auto-negotiation, the link can self-detect its optimum operating setup.

backbone port: A port that does not learn device addresses, and which receives all frames with an unknown address. Backbone ports are normally used to connect the Switch to the backbone of your network. Note that backbone ports were formerly known as designated downlink ports.

Backbone: The part of a network used as the primary path for transporting traffic between network segments.

bandwidth: Information capacity, measured in bits per second, that a channel can transmit. The bandwidth of Ethernet is 10Mbps, the bandwidth of Fast Ethernet is 100Mbps.

baud rate: The Switching speed of a line. Also known as line speed.

BOOTP: The BOOTP protocol allows you to automatically map an IP address to a given MAC address each time a device is started. In addition, the protocol can assign the subnet mask and default gateway to a device.

bridge: A device that interconnects local or remote networks no matter what higher level protocols are involved. Bridges form a single logical network, centralizing network administration.

broadcast: A message sent to all destination devices on the network.

broadcast storm: Multiple simultaneous broadcasts that typically absorb available network bandwidth and can cause network failure.

console port: The port on the Switch accepting a terminal or modem connector. It changes the parallel arrangement of data within computers to the serial form used on data transmission links. This port is most often used for dedicated local management.

CSMA/CD: Channel access method used by Ethernet and IEEE 802.3 standards in which devices transmit only after finding the data channel clear for some period of time. When two devices transmit simultaneously, a collision occurs and the colliding devices delay their retransmissions for a random amount of time.

data center Switching: The point of aggregation within a corporate network where a Switch provides high-performance access to server farms, a high-speed backbone connection, and a control point for network management and security.

edge port: A configurable designation for RSTP operations. It defines a port that is directly connected to a segment where a loop cannot exist. For example, a port connected to a server with a single Ethernet connection. Edge ports transition to a forwarding state more quickly where RSTP is used.

Ethernet: A LAN specification developed jointly by Xerox, Intel, and Digital Equipment Corporation. Ethernet networks operate at 10Mbps using CSMA/CD to run over cabling.

Fast Ethernet: 100Mbps technology based on the Ethernet/CD network access method.

Flow Control: (IEEE 802.3z) A means of holding packets back at the transmit port of the connected end station. Prevents packet loss at a congested Switch port.

forwarding: The process of sending a packet toward its destination by an internetworking device.

full-duplex: A system that allows packets to be transmitted and received at the same time and, in effect, doubles the potential throughput of a link.

half-duplex: A system that allows packets to be transmitted and received, but not at the same time. Contrast with full duplex.

IP address: Internet Protocol address. A unique identifier for a device attached to a network using TCP/IP. The address is written as four octets separated with full-stops (periods), and is made up of a network section, an optional subnet section, and a host section.

IPX: Internetwork Packet Exchange. A protocol allowing communication in a NetWare network.

LAN: Local Area Network. A network of connected computing resources (such as PCs, printers, servers) covering a relatively small geographic area (usually not larger than a floor or building). Characterized by high data rates and low error rates.

latency: The delay between the time a device receives a packet and the time the packet is forwarded out of the destination port.

line speed: See baud rate.

main port: The port in a resilient link that carries data traffic in normal operating conditions.

MDI: Medium Dependent Interface. An Ethernet port connection where the transmitter of one device is connected to the receiver of another device.

MDI-X: Medium Dependent Interface Cross-over. An Ethernet port connection where the internal transmit and receive lines are crossed.

MIB: Management Information Base. Stores a device's management characteristics and parameters. MIBs are used by the Simple Network Management Protocol (SNMP) to contain attributes of their managed systems. The Switch contains its own internal MIB.

multicast: Single packets copied to a specific subset of network addresses. These addresses are specified in the destination-address field of the packet.

protocol: A set of rules for communication between devices on a network. The rules dictate format, timing, sequencing, and error control.

RJ-45: Standard 8-wire connectors for IEEE 802.3 10BASE-T networks.

RMON: Remote Monitoring. Subset of SNMP MIB II that allows monitoring and management capabilities by addressing up to ten different groups of information.

RPS: Redundant Power System. A device that provides a backup source of power when connected to the Switch.

RSTP: Rapid Spanning Tree Protocol as defined by IEEE 802.1w.

server farm: A cluster of servers in a centralized location serving a large user population.

SLIP: Serial Line Internet Protocol. A protocol that allows IP to run over a serial line connection.

SNMP: Simple Network Management Protocol. A protocol originally designed to be used in managing TCP/IP internets. SNMP is presently implemented on a wide range of computers and networking equipment and may be used to manage many aspects of network and end station operation.

Spanning Tree Protocol: (STP) A bridge-based system for providing fault tolerance on networks. STP works by allowing you to implement parallel paths for network traffic, and ensure that redundant paths are disabled when the main paths are operational and enabled if the main paths fail. The IEEE standard 802.1d describes how the protocol.

stack: A group of network devices that are integrated to form a single logical device.

Switch: A device which filters, forwards, and floods packets based on the packet's destination address. The Switch learns the addresses associated with each Switch port and builds tables based on this information to be used for the Switching decision.

TCP/IP: A layered set of communications protocols providing Telnet terminal emulation, FTP file transfer, and other services for communication among a wide range of computer equipment.

Telnet: A TCP/IP application protocol that provides virtual terminal service, letting a user log in to another computer system and access a host as if the user were connected directly to the host.

TFTP: Trivial File Transfer Protocol. Allows you to transfer files (such as software upgrades) from a remote device using your Switch's local management capabilities.

UDP: User Datagram Protocol. An Internet standard protocol that allows an application program on one device to send a datagram to an application program on another device.

VLAN: Virtual LAN. A group of location- and topology-independent devices that communicate as if they are on a common physical LAN.

VLT: Virtual LAN Trunk. A Switch-to-Switch link which carries traffic for all the VLANs on each Switch.

VT100: A type of terminal that uses ASCII characters. VT100 screens have a text-based appearance.