D-Link®

# DES-3526

## Layer 2 Switch

Command Line Interface Reference Manual

First Edition (March 2004)

**651ES3526015**

Printed In Taiwan

RECYCLABLE

## Wichtige Sicherheitshinweise

1. Bitte lesen Sie sich diese Hinweise sorgfältig durch.
2. Heben Sie diese Anleitung für den spätern Gebrauch auf.
3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Vervenden Sie keine Flüssig- oder Aerosolreiniger. Am besten dient ein angefeuchtetes Tuch zur Reinigung.
4. Um eine Beschädigung des Gerätes zu vermeiden sollten Sie nur Zubehörteile verwenden, die vom Hersteller zugelassen sind.
5. Das Gerät is vor Feuchtigkeit zu schützen.
6. Bei der Aufstellung des Gerätes ist auf sichern Stand zu achten. Ein Kippen oder Fallen könnte Verletzungen hervorrufen. Verwenden Sie nur sichere Standorte und beachten Sie die Aufstellhinweise des Herstellers.
7. Die Belüftungsöffnungen dienen zur Luftzirkulation die das Gerät vor Überhitzung schützt. Sorgen Sie dafür, daß diese Öffnungen nicht abgedeckt werden.
8. Beachten Sie beim Anschluß an das Stromnetz die Anschlußwerte.
9. Die Netzanschlußsteckdose muß aus Gründen der elektrischen Sicherheit einen Schutzleiterkontakt haben.
10. Verlegen Sie die Netzanschlußleitung so, daß niemand darüber fallen kann. Es sollete auch nichts auf der Leitung abgestellt werden.
11. Alle Hinweise und Warnungen die sich am Geräten befinden sind zu beachten.
12. Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.
13. Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. Elektrischen Schlag auslösen.
14. Öffnen Sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von authorisiertem Servicepersonal geöffnet werden.
15. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:
    a – Netzkabel oder Netzstecker sint beschädigt.
    b – Flüssigkeit ist in das Gerät eingedrungen.
    c – Das Gerät war Feuchtigkeit ausgesetzt.
    d – Wenn das Gerät nicht der Bedienungsanleitung ensprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
    e – Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.
    f – Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.
16. Bei Reparaturen dürfen nur Orginalersatzteile bzw. den Orginalteilen entsprechende Teile verwendet werden. Der Einsatz von ungeeigneten Ersatzteilen kann eine weitere Beschädigung hervorrufen.
17. Wenden Sie sich mit allen Fragen die Service und Repartur betreffen an Ihren Servicepartner. Somit stellen Sie die Betriebssicherheit des Gerätes sicher.
18. Zum Netzanschluß dieses Gerätes ist eine geprüfte Leitung zu verwenden, Für einen Nennstrom bis 6A und einem Gerätegewicht größer 3kg ist eine Leitung nicht leichter als H05VV-F, 3G, 0.75mm2 einzusetzen.

### WARRANTIES EXCLUSIVE

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

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

LIMITATION OF LIABILITY

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

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

## Limited Warranty

### Hardware:

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

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

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

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

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

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

### Software:

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

D-Link warrants that its software products will perform in substantial conformance with the applicable product documentation provided by D-Link with such software product, for a period of ninety (90) days from the date of purchase from D-Link or its Authorized Reseller. D-Link warrants the magnetic media, on which D-Link provides its software product, against failure during the same warranty period. This warranty applies to purchased software, and to replacement software provided by D-Link pursuant to this warranty, but shall not apply to any update or replacement which may be provided for download via the Internet, or to any update which may otherwise be provided free of charge.

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

D-Link®
Building Networks for People

# Limited Warranty
## (USA Only)

Subject to the terms and conditions set forth herein, D-Link Systems, Inc. ("D-Link") provides this Limited warranty for its product only to the person or entity that originally purchased the product from:

- D-Link or its authorized reseller or distributor and
- Products purchased and delivered within the fifty states of the United States, the District of Columbia, U.S. Possessions or Protectorates, and U.S. Military Installations, addresses with an APO or FPO.

***Limited Warranty:*** D-Link warrants that the hardware portion of the D-Link products described below will be free from material defects in workmanship and materials from the date of original retail purchase of the product, for the period set forth below applicable to the product type ("Warranty Period"), except as otherwise stated herein.

5-Year Limited Warranty for the Product(s) is defined as follows:

- Hardware (excluding power supplies and fans) Five (5) Years
- Power Supplies and Fans Three (3) Year
- Spare parts and spare kits Ninety (90) days

D-Link's sole obligation shall be to repair or replace the defective Hardware during the Warranty Period at no charge to the original owner or to refund at D-Link's sole discretion. Such repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement Hardware need not be new or have an identical make, model or part. D-Link may in its sole discretion replace the defective Hardware (or any part thereof) with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. Repaired or replacement Hardware will be warranted for the remainder of the original Warranty Period from the date of original retail purchase. If a material defect is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to repair or replace the defective Hardware, the price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware (or part thereof) that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

***Limited Software Warranty:*** D-Link warrants that the software portion of the product ("Software") will substantially conform to D-Link's then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original retail purchase of the Software for a period of ninety (90) days ("Warranty Period"), provided that the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. D-Link's sole obligation shall be to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link's functional specifications for the Software or to refund at D-Link's sole discretion. Except as otherwise agreed by D-Link in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. Software will be warranted for the remainder of the original Warranty Period from the date or original retail purchase. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

***Non-Applicability of Warranty:*** The Limited Warranty provided hereunder for hardware and software of D-Link's products, will not be applied to and does not cover any product purchased through the inventory clearance or liquidation sale or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product and in that case, the product is being sold "As-Is" without any warranty whatsoever including, without limitation, the Limited Warranty as described herein, notwithstanding anything stated herein to the contrary.

***Submitting A Claim***: Any claim under this limited warranty must be submitted in writing before the end of the Warranty Period to an Authorized D-Link Service Office.

- The customer must submit as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same.
- The original product owner must obtain a Return Material Authorization ("RMA") number from the Authorized D-Link Service Office and, if requested, provide written proof of purchase of the product (such as a copy of the dated purchase invoice for the product) before the warranty service is provided.
- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the Product and will not ship back any accessories.
- The customer is responsible for all shipping charges to D-Link. No Charge on Delivery ("COD") is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products should be fully insured by the customer and shipped to D-Link Systems, Inc., 53 Discovery Drive, Irvine, CA 92618. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped via UPS Ground or any common carrier selected by D-Link, with shipping charges prepaid. Expedited shipping is available if shipping charges are prepaid by the customer.

D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

***What Is Not Covered:*** This limited warranty provided by D-Link does not cover: Products, if in D-Link's judgment, have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed; Initial

installation, installation and removal of the product for repair, and shipping costs; Operational adjustments covered in the operating manual for the product, and normal maintenance; Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; Any hardware, software, firmware or other products or services provided by anyone other than D-Link; Products that have been purchased from inventory clearance or liquidation sales or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product. Repair by anyone other than D-Link or an Authorized D-Link Service Office will void this Warranty.

***Disclaimer of Other Warranties:*** EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO NINETY (90) DAYS. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

***Limitation of Liability:*** TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF REVENUE OR PROFIT, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, FAILURE OF OTHER EQUIPMENT OR COMPUTER PROGRAMS TO WHICH D-LINK'S PRODUCT IS CONNECTED WITH, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NON-CONFORMING PRODUCT. THE MAXIMUM LIABILITY OF D-LINK UNDER THIS WARRANTY IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT COVERED BY THE WARRANTY. THE FOREGOING EXPRESS WRITTEN WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ANY OTHER WARRANTIES OR REMEDIES, EXPRESS, IMPLIED OR STATUTORY.

***Governing Law***: This Limited Warranty shall be governed by the laws of the state of California. Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may not apply. This limited warranty provides specific legal rights and the product owner may also have other rights which vary from state to state

**For detailed warranty outside the United States, please contact corresponding local D-Link office.**

**Register online your D-Link product at http://support.dlink.com/register/**

D-Link Offices for Registration and Warranty Service

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

## Trademarks



## Copyright Statement



## FCC Warning

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

## CE Mark Warning

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

## VCCI Warning

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

# Table of Contents

# 1

# INTRODUCTION

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

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

## Accessing the Switch via the Serial Port

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

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

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

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

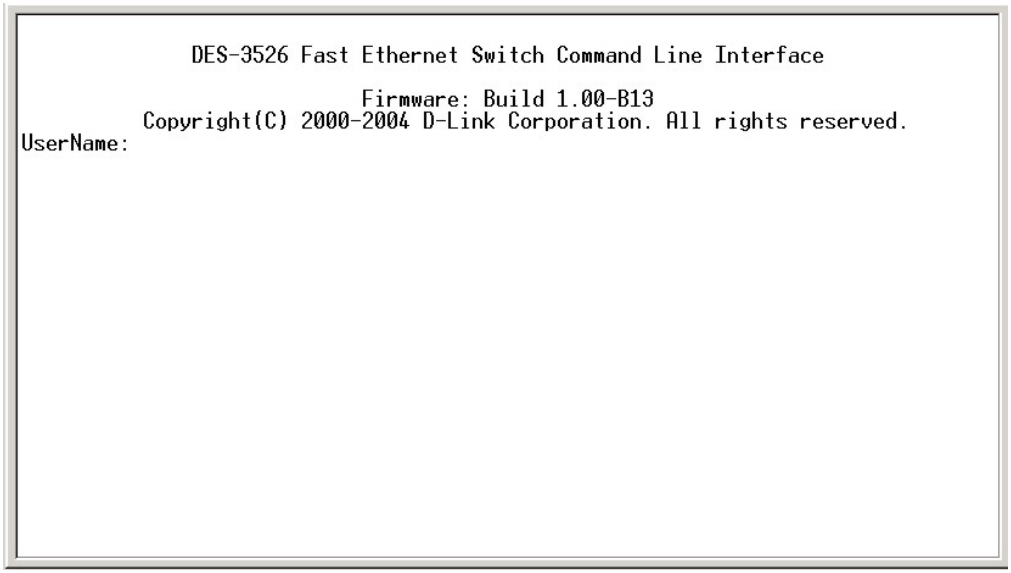


**Figure 1-1. Initial CLI screen**

There is no initial username or password. Just press the **Enter** key twice to display the CLI input cursor – **DES-3526:4#**. 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 on the initial boot console screen – shown below.

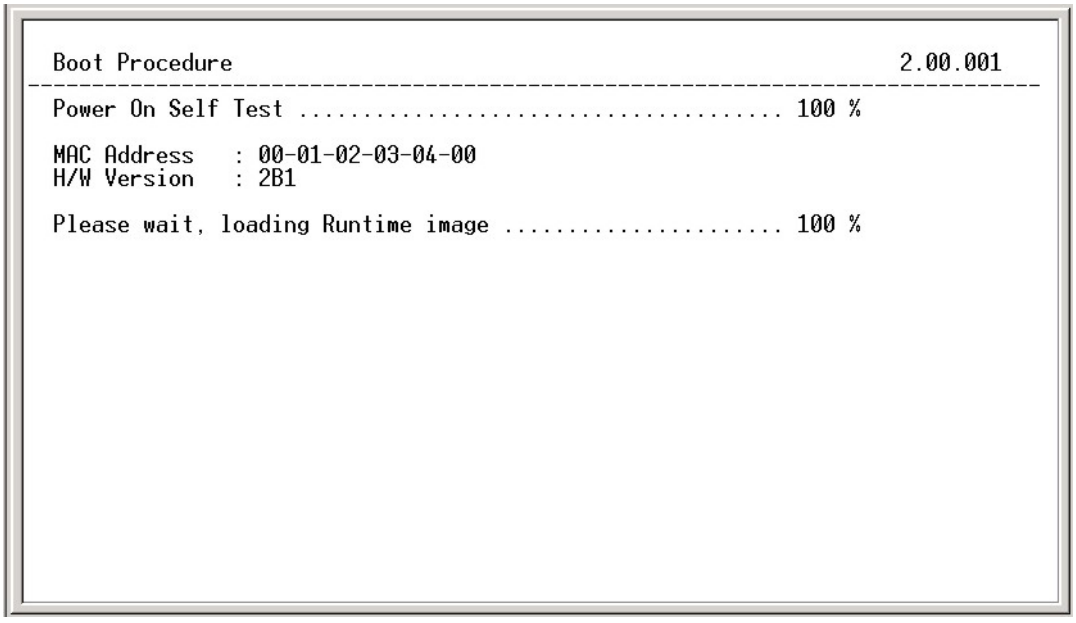


**Figure 1-2. Boot Screen**

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

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

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

1. Starting at the command line prompt, enter the commands **config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy**. Where the **x**'s represent the IP address to be assigned to the IP interface named **System** and the **y**'s represent the corresponding subnet mask.
2. Alternatively, you can enter **config ipif System ipaddress xxx.xxx.xxx.xxx/z**. Where the **x**'s represent the IP address to be assigned to the IP interface named **System** and the **z** represents the corresponding number of subnets in CIDR notation.

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

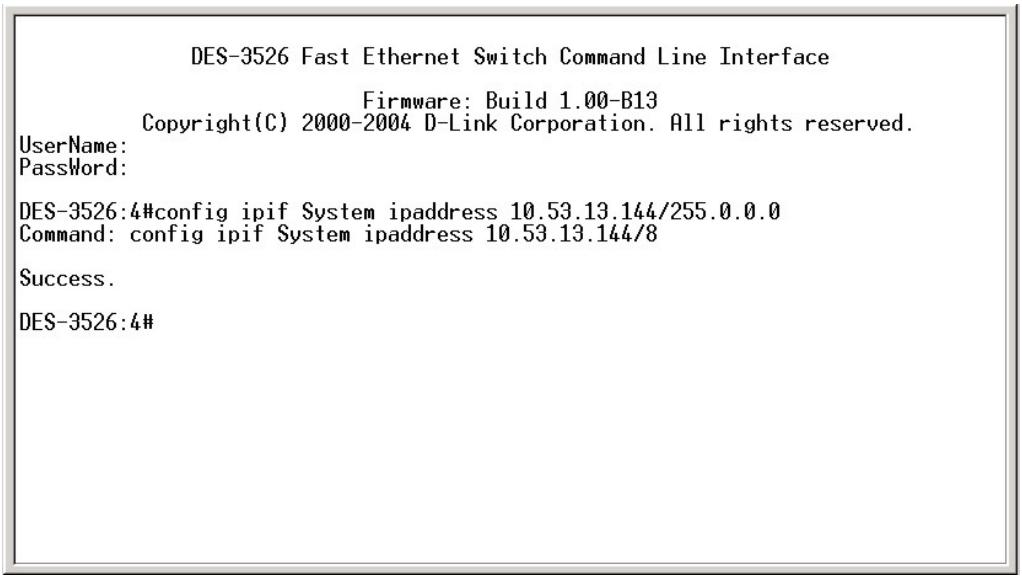


**Figure 1-3. Assigning an IP Address**

In the above example, the Switch was assigned an IP address of 10.53.13.144 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, SNMP MIB browser and the CLI or via the Web-based management agent using the above IP address to connect to the Switch.

# 2

# USING THE CONSOLE CLI

The DES-3526 supports a console management interface that allows the user to connect to the switch's management agent via a serial port and a terminal or a computer running a terminal emulation program. The console can also be used over the network using the TCP/IP Telnet protocol. The console program can be used to configure the Switch to use an SNMP-based network management software over the network.

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

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

## Connecting to the Switch

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

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

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

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

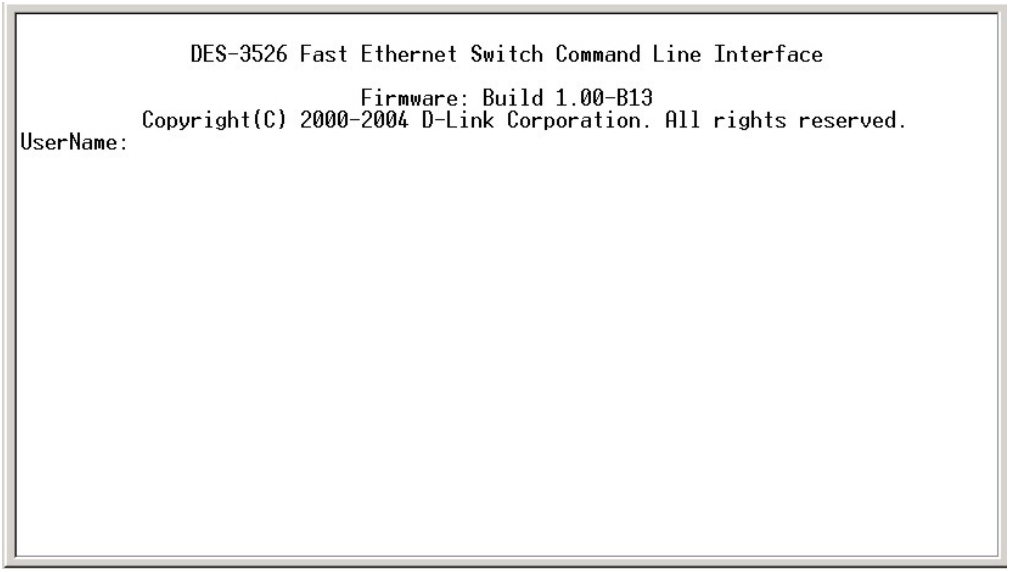


**Figure 2-1. Initial Console Screen**

Commands are entered at the command prompt, **DES-3526:4#**.

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**

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


**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-3526:4#config account
Command: config account

Next possible completions:
<username>

DES-3526:4#config account
Command: config account

Next possible completions:
<username>

DES-3526:4#
```

**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 username 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.

```
DES-3526:4#the

Available commands:
..                  ?                   clear               config
create              delete              dir                 disable
download            enable              login               logout
ping                reboot              reconfig            reset
save                show                upload

DES-3526:4#
```

**Figure 2-5. The Next Available Commands Prompt**

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

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

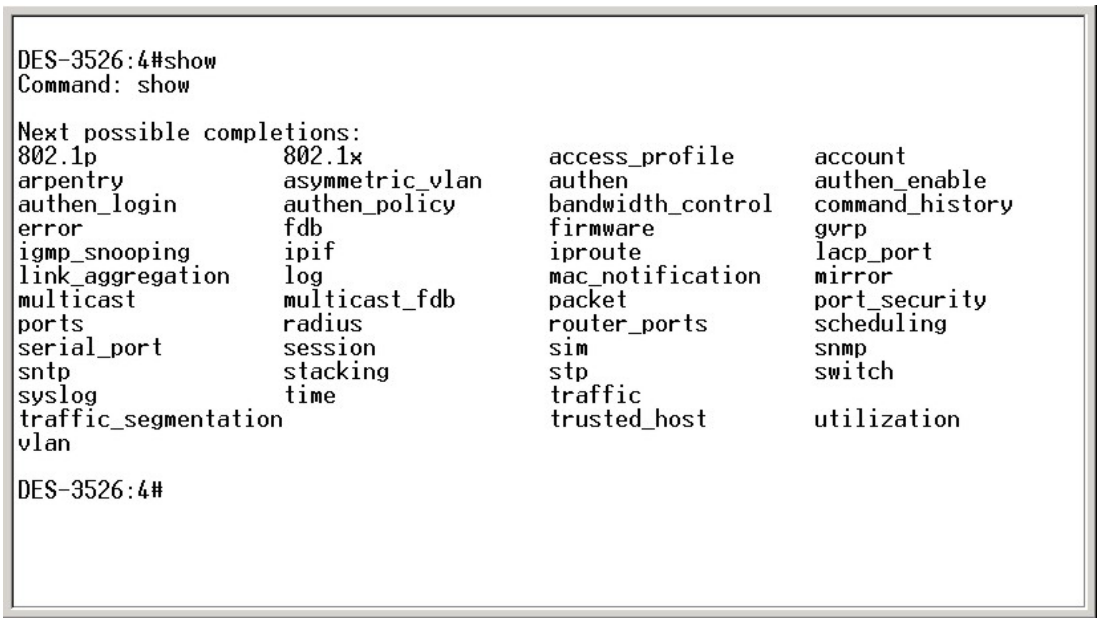


**Figure 2-6. Next possible completions: Show Command**

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

# 3

# COMMAND SYNTAX

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

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 |

| {braces} | |
|---|---|
| | 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. |
| Insert or Ctrl+R | Toggle on and off. When toggled on, inserts text and shifts previous text to right. |
| 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. |

# 4

# BASIC SWITCH COMMANDS

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

| Command | Parameters |
|---|---|
| create account | [admin\|user]<br><username 15> |
| config account | <username 15> |
| show account | |
| delete account | <username 15> |
| show session | |
| show switch | |
| show serial_port | |
| config serial_port | {baud_rate [9600\|19200\|38400\|115200]<br>auto_logout [never\|2_minutes\|5_minutes<br>\|10_minutes\|15_minutes]} |
| enable clipaging | |
| disable clipaging | |
| enable telnet | <tcp_port_number 1-65535> |
| disable telnet | |
| enable web | <tcp_port_number 1-65535> |
| disable web | |
| save | |
| reboot | |
| reset | {[config\|system]} |
| login | |
| logout | |

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

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

Example usage:

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

```
DES-3526:4#create account admin dlink
Command: create account admin dlink

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

 Success.

DES-3526:4#
```

## 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.<br><br>Usernames can be between 1 and 15 characters.<br><br>Passwords can be between 0 and 15 characters. |

Example usage:

To configure the user password of “dlink” account:

```
DES-3526:4#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-3526:4#
```

## 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. |

| show account | |
|---|---|
| | accounts can exist on the switch at one time. |
| **Parameters** | None. |
| **Restrictions** | Only Administrator-level users can issue this command. |

Example usage:

To display the accounts that have been created:

```
DES-3526:4#show account
Command: show account

Current Accounts:
Username         Access Level
---------------  ------------
  dlink            Admin

Total Entries: 1

DES-3526:4#
```

| 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-3526:4#delete account System
Command: delete account System

Success.

DES-3526:4#
```

| show session | |
|---|---|
| **Purpose** | Used to display a list of currently logged-in users. |

| show session | |
|---|---|
| **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-3526:4#show session
Command: show session

ID   Login Time                  Live Time  From          Level  Name
--   ----------------------------  ---------  ------------  -----  -----------
*8   00000 days 00:00:37    03:36:27   Serial  Port   4    Anonymous
```

| show switch | |
|---|---|
| **Purpose** | Used to display information about the switch. |
| **Syntax** | **show switch** |
| **Description** | This command displays information about the switch. |
| **Parameters** | None. |
| **Restrictions** | Only Administrator-level users can issue this command. |

Example usage:

To display the switch information:

```
DES-3526:4#show switch
Command: show switch

Device Type         : DES-3526 Fast Ethernet Switch
Combo Port          : 1000Base-T + 1000Base-T
MAC Address         : 00-01-02-03-04-00
IP Address          : 10.41.44.22 (Manual)
VLAN Name           : default
Subnet Mask         : 255.0.0.0
Default Gateway     : 0.0.0.0
Boot PROM Version : Build 3.00.000
Firmware Version    : Build 1.00-B13
Hardware Version    : 0A1
Device S/N          :
Power Status        : Main – Normal, Redundant – Not Present
System Name         : DES-3526
```

```
System Location      : 7th_flr_east_cabinet
System Contact       : Julius_Erving_212-555-6666
Spanning Tree        : Disabled
GVRP                 : Disabled
IGMP Snooping        : Disabled
TELNET               : Enabled (TCP 23)
WEB                  : Enabled (TCP 80)
RMON                 : Enabled
Asymmetric VLAN  : Disabled
DES-3526:4#
```

## 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-3526:4#show serial_port
Command: show serial_port

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

DES-3526:4#
```

## 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** | baud_rate[9600\|19200\|38400\|115200]– The serial bit rate that will be used to communicate with the management host. There are four options: 9600, 19200, 38400, 115200.<br><br>never – No time limit on the length of time the console can be open with |

## config serial_port

| | |
|---|---|
| | no user input.<br><br>2_minutes – The console will log out the current user if there is no user input for 2 minutes.<br><br>5_minutes – The console will log out the current user if there is no user input for 5 minutes.<br><br>10_minutes – The console will log out the current user if there is no user input for 10 minutes.<br><br>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-3526:4#config serial_port baud_rate 115200
Command: config serial_port baud_rate 115200

 Success.

DES-3526:4#
```

## 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 which causes the console screen to rapidly scroll through several pages. This command will cause the console to pause at the end of each page. The default setting is enabled. |
| **Parameters** | None. |
| **Restrictions** | Only administrator-level users can issue this command. |

Example usage:

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

```
DES-3526:4#enable clipaging
Command: enable clipaging

 Success.

DES-3526:4#
```

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

Example usage:

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

```
DES-3526:4#disable clipaging
Command: disable clipaging

 Success.

DES-3526:4#
```

| 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-3526:4#enable telnet 23
Command: enable telnet 23

 Success.

DES-3526:4#
```

| 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-3526:4#disable telnet
Command: disable telnet

 Success.

DES-3526:4#
```

| enable web | |
|---|---|
| **Purpose** | Used to enable the HTTP-based management software on the switch. |
| **Syntax** | **enable web <tcp_port_number 1-65535>** |
| **Description** | This command is used to enable the Web-based management software on the switch. The user can specify the TCP port number the switch will use to listen for Telnet requests. |
| **Parameters** | <tcp_port_number> – 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-3526:4#enable web 80
Command: enable web 80

 Success.

DES-3526:4#
```

| 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-3526:4#disable web
Command: disable web

 Success.

DES-3526:4#
```

| 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-3526:4#save
Command: save

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

DES-3526:4#
```

| 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-3526:4#reboot
Command: reboot
Are you sure want to proceed with the system reboot? (y|n)
Please wait, the switch is rebooting...
```

| reset | |
|---|---|
| **Purpose** | Used to reset the switch to the factory default settings. |
| **Syntax** | **reset {[config\|system]}** |
| **Description** | This command is used to restore the switch's configuration to the default settings assigned from the factory. |
| **Parameters** | config – If the keyword 'config' is specified, all of the factory default settings are restored on the switch including the IP address, user accounts, and the switch history log. The switch will not save or reboot.<br><br>system – If the keyword 'system' is specified all of the factory default settings are restored on the switch. The switch will save and reboot after the settings are changed to default. Rebooting will clear all entries in the Forwarding Data Base.<br><br>If no parameter is specified, the switch's current IP address, user accounts, and the switch history log are not changed. All other parameters are restored to the factory default settings. The switch will not save or reboot. |
| **Restrictions** | Only administrator-level users can issue this command. |

Example usage:

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

```
DES-3526:4#reset config
Command: reset config
Are you sure to proceed with system reset?(y/n)

 Success.

DES-3526:4#
```

| 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-3526:4#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-3526:4#logout
```

# 5

# SWITCH PORT COMMANDS

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

| Command | Parameters |
|---|---|
| config ports | [<portlist \| all> {speed [auto \| 10_half \| 10_full \|100_half \| 100_full \| 1000_full} \| flow_control [enable \| disable] \| learning [enable \| disable] state [enable \| disable]} description <desc 32> |
| show ports | <portlist> {description} |

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

## config ports

**Purpose** Used to configure the Switch's Ethernet port settings.

**Syntax** config ports[<portlist | all> {speed [auto | 10_half | 10_full |100_half | 100_full | 1000_full} | flow_control [enable | disable] | learning [enable | disable] state [enable | disable] description <desc 32>

**Description** This command allows for the configuration of the switch's Ethernet ports. Only the ports listed in the <portlist> will be affected.

**Parameters** all – Configure all ports on the switch.

<portlist> – Specifies a port or range of ports to be configured. Tauto – Enables auto-negotiation for the specified range of ports.

[10|100|1000] – Configures the speed in Mbps for the specified range of ports. Gigabit ports are statically set to 1000 and cannot be set to slower speeds.

[half|full] – Configures the specified range of ports as either full- or half-duplex.

[master | slave] This parameter denotes whether the ports selected will be of the master switch or the slave switch and is only used when the port speed is selected to be 1000_full.

flow_control [enabled | disabled] – Enable or disable flow control for the specified ports.

learning [enabled | disabled] – Enables or disables the MAC address learning on the specified range of ports.

state [enabled | disabled] – Enables or disables the specified range of ports.

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

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

Example usage:

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

```
DES-3526:4#config ports 1-3 speed 10_full learning enabled state enabled

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

Success.

DES-3526:4#
```

## show ports

| | |
|---|---|
| **Purpose** | Used to display the current configuration of a range of ports. |
| **Syntax** | **show ports <portlist> {description}** |
| **Description** | This command is used to display the current configuration of a range of ports. |
| **Parameters** | <portlist> – Specifies a port or range of ports to be displayed.<br><br>{description} – Adding this parameter to the **show ports** command indicates that the port description will be included in the display. |
| **Restrictions** | None. |

Example usage:

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

```
DES-3526:4#show ports
Command show ports:

Port   Port     Settings                 Connection               Address
       State    Speed/Duplex/FlowCtrl    Speed/Duplex/FlowCtrl    Learning
------ -------- ------------------------ ------------------------ --------
1      Enabled  Auto/Enabled             Link Down                Enabled
2      Enabled  Auto/Enabled             Link Down                Enabled
3      Enabled  Auto/Enabled             Link Down                Enabled
4      Enabled  Auto/Enabled             Link Down                Enabled
5      Enabled  Auto/Enabled             Link Down                Enabled
6      Enabled  Auto/Enabled             Link Down                Enabled
7      Enabled  Auto/Enabled             Link Down                Enabled
8      Enabled  Auto/Enabled             Link Down                Enabled
9      Enabled  Auto/Enabled             Link Down                Enabled
10     Enabled  Auto/Enabled             100M/Full/None           Enabled
11     Enabled  Auto/Enabled             Link Down                Enabled
12     Enabled  Auto/Enabled             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            Link Down                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
```

Example usage:

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

```
DES-3526:4#show ports description
Command: show ports description

Port   Port      Settings                 Connection               Address
       State     Speed/Duplex/FlowCtrl    Speed/Duplex/FlowCtrl    Learning
------ --------  ---------------------    ---------------------    --------
1      Enabled   Auto/Disabled            Link Down                Enabled
 Description: dads1
2      Enabled   Auto/Disabled            Link Down                Enabled
 Description:
3      Enabled   Auto/Disabled            Link Down                Enabled
 Description:
4      Enabled   Auto/Disabled            Link Down                Enabled
 Description:
5      Enabled   Auto/Disabled            Link Down                Enabled
 Description:
6      Enabled   Auto/Disabled            Link Down                Enabled
 Description:
7      Enabled   Auto/Disabled            Link Down                Enabled
 Description:
8      Enabled   Auto/Disabled            Link Down                Enabled
 Description:
9      Enabled   Auto/Disabled            Link Down                Enabled
 Description:
10     Enabled   Auto/Disabled            Link Down                Enabled
 Description:
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

# 6

# PORT SECURITY COMMANDS

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

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

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

## config port_security ports

**Purpose** Used to configure port security settings.

**Syntax** **config port_security ports[<portlist>| all ] {admin_state [enable| disable] | max_learning_addr <max_lock_no 0-10> | lock_address_mode [Permanent | DeleteOnTimeout | DeleteOnReset]}**

**Description** This command allows for the configuration of the port security feature. Only the ports listed in the <portlist> are effected.

**Parameters** portlist – specifies a port or range of ports to be configured.

all – configure port security for all ports on the switch.

admin_state [enable|disable] – enable or disable port security for the listed ports.

max_learning_addr <max_lock_no 0-10> - use this to limit the number of MAC addresses dynamically listed in the FDB for the ports.

lock_address_mode[Permanent | DeleteOnTimout | DeleteOnReset] – Indicates the method of locking addresses. The user has three choices:

- Permanent – The locked addresses will not age out after the aging timer expires.
- DeleteOnTimeout – The locked addresses will age out after the aging timer expires.
- DeleteOnReset – The locked addresses will not age out until the switch has been reset.

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

Example usage:

To configure the port security:

```
DES-3526:4#config port_security ports 1-5 admin_state enable
max_learning_addr 5 lock_address_mode DeleteOnReset

Command: config port_security ports 1-5 admin_state enable
max_learning_addr 5 lock_address_mode DeleteOnReset

Success.

DES-3526:4#
```

## delete port_security_entry

| | |
|---|---|
| **Purpose** | Used to delete a port security entry by MAC address, port number and VLAN ID. |
| **Syntax** | **delete port_security_entry vlan name <vlan_name 32> mac_address <macaddr> port <port>** |
| **Description** | This command is used to delete a single, previously learned port security entry by port, VLAN name, and MAC Address. |
| **Parameters** | vlan name <vlan_name 32> Enter the corresponding vlan name of the port which the user wishes to delete.<br><br>mac_address <macaddr> - Enter the corresponding MAC address, previously learned by the port, which the user wishes to delete.<br><br>port <port> - Enter the port number which has learned the previously enterd MAC address. |
| **Restrictions** | Only administrator-level users can issue this command. |

Example usage:

To delete a port security entry:

```
DES-3526:4#delete port_security_entry vlan_name default
mac_address 00-01-30-10-2C-C7 port 6

Command: delete port_security_entry vlan_name default
mac_address 00-01-30-10-2C-C7 port 6

Success.

DES-3526:4#
```

## clear port_security_entry

| | |
|---|---|
| **Purpose** | Used to clear MAC address entries learned from a specified port for the port security function. |
| **Syntax** | **clear port_security_entry ports <portlist>** |
| **Description** | This command is used to clear MAC address entries which were learned by the switch by a specified port. This command only relates to the port security function. |

| clear port_security_entry | |
|---|---|
| **Parameters** | <portlist> – specifies a port or port range the user wishes to clear. |
| **Restrictions** | Only administrator-level users can issue this command. |

Example usage:

To clear a port security entry by port:

```
DES-3526:4# clear port_security_entry port 6
Command: clear port_security_entry port 6

Success.

DES-3526:4#
```

| show port_security | |
|---|---|
| **Purpose** | Used to display the current port security configuration. |
| **Syntax** | **show port_security {ports <portlist>}** |
| **Description** | This command is used to display port security information of the switch ports. The information displayed includes port security admin state, maximum number of learning address and lock mode. |
| **Parameters** | <portlist> – specifies a port or range of ports to be viewed. |
| **Restrictions** | None. |

Example usage:

To display the port security configuration:

```
DES-3526:4#show port_security ports 1-5
Command: show port_security ports 1-5

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

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

# 7

# NETWORK MANAGEMENT (SNMP) COMMANDS

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

The DES-3526 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.<br>DES 56-bit encryption is added based on the CBC-DES (DES-56) standard |

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

| Command | Parameters |
|---|---|
| show snmp community | <community_string 32> |
| config snmp engineID | <snmp_engineID> |
| show snmp engineID | |
| create snmp group | <groupname 32> {v1 \| v2c \|v3 [noauth_nopriv \| auth_nopriv \| auth_priv ]} {read_view <view_name 32> \| write_view <view_name 32> \| notify_view <view_name 32>} |
| delete snmp group | <groupname 32> |
| show snmp groups | |
| create snmp host | <ipaddr> {v1 \|v2c \| v3 [noauth_nopriv \| auth_nopriv \| auth_priv]} <auth_string 32> |
| delete snmp host | <ipaddr> |
| show snmp host | <ipaddr> |
| create trusted_host | <ipaddr> |
| delete trusted_host | <ipaddr> |
| show trusted_host | <ipaddr> |
| enable snmp traps | |
| enable snmp authenticate_traps | |
| show snmp traps | |
| disable snmp traps | |
| disable snmp authenticate_traps | |
| config snmp system contact | <sw_contact> |
| config snmp system location | <sw_location> |
| config snmp system name | <sw_name> |
| enable rmon | |
| disable rmon | |

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

## create snmp user

| | |
|---|---|
| Purpose | Used to create a new SNMP user and adds the user to an SNMP group that is also created by this command. |
| Syntax | **create snmp user <username 32> <groupname 32> {encrypted [by_password auth [md5 <auth_password 8-16 > \| sha <auth_password 8-20 >] priv [none \| des <priv_password 8-16> ]\|by_key auth [md5 <auth_key 32-32>\| sha <auth_key 40-40>] priv [none \| des <priv_key 32-32> ]]}** |
| Description | The **create snmp user** command creates a new SNMP user and adds the user to an SNMP group that is also created by this command. |
| Parameters | <username 32> – An alphanumeric name of up to 32 characters that will identify the new SNMP user.<br><br><groupname 32> – An alphanumeric name of up to 32 characters that will identify the SNMP group the new SNMP user will be associated with.<br><br>by_password – Requires the SNMP user to enter a password for authentication and privacy. The password is defined by specifying the auth_password below. This method is recommended.<br><br>by_key - Requires the SNMP user to enter a encryption key for authentication and privacy. The key is defined by specifying the priv_password below. This method is not recommended.<br><br>Message integrity – ensures that packets have not been tampered with during transit.<br><br>Authentication – determines if an SNMP message is from a valid source.<br><br>Encryption – scrambles the contents of messages to prevent it being viewed by an unauthorized source.<br><br>encrypted – Specifies that the password will be in an encrypted format.<br><br>auth [md5\|sha] – Initiate an authentication-level setting session.<br><br>**md5** – Specifies that the HMAC-MD5-96 authentication level will be used.<br><br>**sha** – Specifies that the HMAC-SHA-96 authentication level will be used.<br><br><auth_password 8-20> – An alphanumeric sting of between 8 and 20 characters that will be used to authorize the agent to receive packets for the host.<br><br>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. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To create an SNMP user on the switch:

```
DES-3526:4#create snmp user dlink default encrypted
by_password auth md5 auth_password priv none
Command: create snmp user dlink default encrypted
by_password auth md5 auth_password priv none

Success.

DES-3526:4#
```

## 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-3526:4#delete snmp user dlink
Command: delete snmp user dlink

 Success.

DES-3526:4#
```

## 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-3526:4#show snmp user
Command: show snmp user

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

Total Entries: 1

DES-3526:4#
```

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

Example usage:

To create an SNMP view:

```
DES-3526:4#create snmp view dlinkview 1.3.6 view_type
included
Command: create snmp view dlinkview 1.3.6 view_type included

 Success.

DES-3526:4#
```

## delete snmp view

| | |
|---|---|
| Purpose | Used to remove an SNMP view entry previously created on the switch. |

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

Example usage:

To delete a previously configured SNMP view from the switch:

```
DES-3526:4#delete snmp view dlinkview all
Command: delete snmp view dlinkview all

Success.

DES-3526:4#
```

| 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 | None. |

Example usage:

To display SNMP view configuration:

```
DES-3526:4#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                       Included
CommunityView       1.3.6.1.6.3             Excluded
CommunityView       1.3.6.1.6.3.1           Included

Total Entries: 11

DES-3526:4#
```

## create snmp community

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

Example usage:

To create the SNMP community string "dlink:"

```
DES-3526:4#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-3526:4#delete snmp community dlink
Command: delete snmp community dlink

Success.

DES-3526:4#
```

| 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 | None. |

Example usage:

To display the currently entered SNMP community strings:

```
DES-3526:4#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

DES-3526:4#
```

## 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-3526:4#config snmp 0035636666
Command: config snmp engineID 0035636666

 Success.

DES-3526:4#
```

## 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. |

| show snmp engineID | |
|---|---|
| Restrictions | None. |

Example usage:

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

```
DES-3526:4#show snmp engineID
Command: show snmp engineID

SNMP Engine ID : 0035636666

DES-3526:4#
```

| 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> \| write_view <view_name 32> \| notify_view <view_name 32>}** |
| Description | The **create snmp group** command creates a new SNMP group, or a table that maps SNMP users to SNMP views. |
| Parameters | <groupname 32> – An alphanumeric name of up to 32 characters that will identify the SNMP group the new SNMP user will be associated with.<br><br>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.<br><br>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.<br><br>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:<br><br>Message integrity – ensures that packets have not been tampered with during transit.<br><br>Authentication – determines if an SNMP message is from a valid source.<br><br>Encryption – scrambles the contents of messages to prevent it being viewed by an unauthorized source.<br><br>noauth_nopriv – Specifies that there will be no authorization and no encryption of packets sent between the switch and a remote SNMP |

| create snmp group | |
|---|---|
| | manager.<br><br>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.<br><br>auth_priv – Specifies that authorization will be required, and that packets sent between the switch and a remote SNMP manger will be encrypted.<br><br>read_view – Specifies that the SNMP group being created can request SNMP messages.<br><br>write_view – Specifies that the SNMP group being created has write privileges.<br><br><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.<br><br>notify_view – Specifies that the SNMP group being created can receive SNMP trap messages generated by the switch's SNMP agent. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To create an SNMP group named "sg1:"

```
DES-3526:4#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-3526:4#
```

| 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-3526:4#delete snmp group sg1
Command: delete snmp group sg1

Success.

DES-3526:4#
```

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

Example usage:

To display the currently configured SNMP groups on the switch:

```
DES-3526:4#show snmp groups
Command: show snmp groups
Vacm Access      Table Settings

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


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

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

Group    Name      : Group6
ReadView Name    : ReadView
WriteView Name   : WriteView
```

```
Notify View Name  : NotifyView
Security Model      : SNMPv3
Security Level       : authPriv

Group    Name       : Group7
ReadView Name    : ReadView
WriteView Name    : WriteView
Notify View Name  : NotifyView
Security Model      : SNMPv3
Security Level       : authPriv

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

Group    Name      : ReadGroup
ReadView Name    : CommunityView
WriteView Name    :
Notify View Name  : CommunityView
Security Model      : SNMPv1
Security Level       : NoAuthNoPriv

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


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

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

Total Entries: 10

DES-3526:4#
```

## 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>]** |

| create snmp host | |
|---|---|
| Description | The **create snmp host** command creates a recipient of SNMP traps generated by the switch's SNMP agent. |
| Parameters | <ipaddr> – The IP address of the remote management station that will serve as the SNMP host for the switch.<br><br>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.<br><br>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.<br><br>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:<br><br>Message integrity – ensures that packets have not been tampered with during transit.<br><br>Authentication – determines if an SNMP message is from a valid source.<br><br>Encryption – scrambles the contents of messages to prevent it being viewed by an unauthorized source.<br><br>noauth_nopriv – Specifies that there will be no authorization and no encryption of packets sent between the switch and a remote SNMP manager.<br><br>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.<br><br>auth_priv – Specifies that authorization will be required, and that packets sent between the switch and a remote SNMP manger will be encrypted.<br><br><auth_sting 32> – An alphanumeric string used to authorize a remote SNMP manager to access the switch's SNMP agent. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To create an SNMP host to receive SNMP messages:

```
DES-3526:4#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-3526:4#
```

| 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-3526:4#delete snmp host 10.48.74.100
Command: delete snmp host 10.48.74.100

 Success.

DES-3526:4#
```

| 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 | None. |

Example usage:

To display the currently configured SNMP hosts on the switch:

```
DES-3526:4#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-3526:4#
```

## create trusted_host

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

Example usage:

To create the trusted host:

```
DES-3526:4#create trusted_host 10.48.74.121
Command: create trusted_host 10.48.74.121

Success.

DES-3526:4#
```

## show trusted_host

| | |
|---|---|
| Purpose | Used to display a list of trusted hosts entered on the switch using the **create trusted_host** command above. |
| Syntax | **show trusted_host <ipaddr>** |
| Description | This command is used to display a list of trusted hosts entered on the switch using the **create trusted_host** command above. |

| show trusted_host | |
|---|---|
| | the switch using the **create trusted_host** command above. |
| Parameters | <ipaddr> – The IP address of the trusted host. |
| Restrictions | none. |

Example Usage:

To display the list of trust hosts:

```
DES-3526:4#show trusted_host
Command: show trusted_host

 Management Stations

 IP Address
----------------------
10.53.13.94

Total Entries: 1

DES-3526:4#
```

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

Example Usage:

To delete a trusted host with an IP address 10.48.74.121:

```
DES-3526:4#delete trusted_host 10.48.74.121
Command: delete trusted_host 10.48.74.121

Success.
DES-3526:4#
```

| enable snmp traps | |
|---|---|
| Purpose | Used to enable SNMP trap support. |
| Syntax | **enable snmp traps** |

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

Example usage:

To enable SNMP trap support on the switch:

```
DES-3526:4#enable snmp traps
Command: enable snmp traps

Success.

DES-3526:4#
```

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

Example Usage:

To turn on SNMP authentication trap support:

```
DES-3526:4#enable snmp authenticate_traps
Command: enable snmp authenticate_traps

 Success.

DES-3526:4#
```

| show snmp traps | |
|---|---|
| Purpose | Used to show SNMP trap support on the switch . |
| Syntax | **show snmp traps** |
| Description | This command is used to view the SNMP trap support status currently configured on the Switch. |
| Parameters | none. |

| show snmp traps | |
|---|---|
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To view the current SNMP trap support:

```
DES-3526:4#show snmp traps
Command: show snmp traps

SNMP Traps          : Enabled
Authenticate Traps  : Enabled

DES-3526:4#
```

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

Example Usage:

To prevent SNMP traps from being sent from the Switch:

```
DES-3526:4#disable snmp traps
Command: disable snmp traps

Success.

DES-3526:4#
```

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

Example Usage:

To disable the SNMP authentication trap support:

```
DES-3526:4#disable snmp authenticate_traps
Command: disable snmp authenticate_traps

 Success.

DES-3526:4#
```

## config snmp system_contact

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

Example usage:

To configure the switch contact to "`MIS Department II`":

```
DES-3526:4#config snmp system_contact MIS Department II
Command: config snmp system_contact MIS Department II

Success.

DES-3526:4#
```

## config snmp system_location

| | |
|---|---|
| Purpose | Used to enter a description of the location of the switch. |
| Syntax | **config snmp system_location {<sw_location>}** |
| Description | The config snmp system_location command is used to enter a description of the location of the switch. A maximum of 255 characters can be used. |
| Parameters | <sw_location> - A maximum of 255 characters is allowed. A NULL string is accepted if there is no location desired. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To configure the switch location for "**HQ 5F**":

```
DES-3526:4#config snmp system_location HQ 5F
Command: config snmp system_location HQ 5F

Success.

DES-3526:4#
```

## config snmp system_name

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

Example usage:

To configure the switch name for "**DES-3526 Switch**":

```
DES-3526:4#config snmp system_name DES-3526 Switch
Command: config snmp system_name DES-3526 Switch

Success.

DES-3526:4#
```

## 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-3526:4#enable rmon
Command: enable rmon

 Success.

DES-3526:4#
```

| 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-3526:4#disable rmon
Command: disable rmon

 Success.

DES-3526:4#
```

# 8

# SWITCH UTILITY COMMANDS

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

| Command | Parameters |
|---|---|
| download | [ firmware <ipaddr> <path_filename 64> {section_id <int 1-2>} configuration <ipaddr> <path_filename 64> {increment} ] |
| config firmware | section_id <value 1-2> [delete \| boot_up] |
| show firmware_information | |
| upload | [ configuration \| log ] <ipaddr> <path_filename 64> |
| ping | <ipaddr> {times <value 1-255>} {timeout <sec 1-99>} |
| traceroute | <ipaddr> {ttl <value 1-60> \| port <value 30000-64900> \| timeout <sec 1-65535> \| probe <value <1-9> |

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

| download | |
|---|---|
| Purpose | Used to download and install new firmware or a switch configuration file from a TFTP server. |
| Syntax | download[ firmware <ipaddr> <path_filename 64> {section_id <int 1-2>} configuration <ipaddr> <path_filename 64> {increment} ] |
| Description | This command is used to download a new firmware or a switch configuration file from a TFTP server. |
| Parameters | firmware – Download and install new firmware on the switch from a TFTP server.<br><br>configuration – Download a switch configuration file from a TFTP server.<br><br><ipaddr> – The IP address of the TFTP server.<br><br><path_filename> – The DOS path and filename of the firmware or switch configuration file on the TFTP server. For example, C:\3226S.had.<br><br>section_id <int 1-2> - Specify the working section id. The Switch can hold two firmware versions for the user to select from, which are specified by section id.<br><br>increment – Allows the download of a partial switch configuration file. This allows a file to be downloaded that will change only the switch parameters explicitly stated in the configuration file. All other switch parameters will remain unchanged. |
| Restrictions | The TFTP server must be on the same IP subnet as the switch. Only administrator-level users can issue this command. |

Example usage:

To download a configuration file:

```
DES-3526:4#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-3526:4#
```

## config firmware

| | |
|---|---|
| Purpose | Used to configure the firmware section as a boot up section, or to delete the firmware section |
| Syntax | **config firmware section_id <int 1-2> [delete \| boot_up]** |
| Description | This command is used to configure the firmware section. The user may choose to remove the firmware section or use it as a boot up section. |
| Parameters | section_id – Specifies the working section. The Switch can hold two firmware versions for the user to select from, which are specified by section id.<br><br>delete – Entering this parameter will delete the specified firmware section.<br><br>boot_up – Entering this parameter will specify the firmware section id as a boot up section. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To configure firmware section 1 as a boot up section:

```
DES-3526:4# config firmware section_id 1 boot_up
Command: config firmware section_id 1 boot_up

Success.

DES-3526:4#
```

## show firmware information

| | |
|---|---|
| Purpose | Used to display the firmware section information. |
| Syntax | **show firmware information** |
| Description | This command is used to display the firmware section information |
| Parameters | none |

| show firmware information | |
|---|---|
| Restrictions | none |

Example usage:

To display the current firmware information on the switch:

```
DES-3526:4#show firmware information
Command: show firmware information

ID   Version    Size(B)    Update Time            From              User
--   --------   -------    -------------------    ----------------  ---------------
 1   1.00-B00   1360471    00000 days 00:00:00    Serial Port (PROM)  Unknown
*2   1.00-B02   2052372    00000 days 00:00:56    10.53.13.94         Anonymous

'*' means boot up section
(T) means firmware update thru TELNET
(S) means firmware update thru SNMP
(W) means firmware update thru WEB

Free space: 3145728 bytes

DES-3526:4#
```

| upload | |
|---|---|
| Purpose | Used to upload the current switch settings or the switch history log to a TFTP. |
| Syntax | **upload [ configuration \| log ] <ipaddr> <path_filename 64>** |
| Description | This command is used to upload either the switch's current settings or the switch's history log to a TFTP server. |
| Parameters | configuration – Specifies that the switch's current settings will be uploaded to the TFTP server.<br><br>log – Specifies that the switch history log will be uploaded to the TFTP server.<br><br><ipaddr> – The IP address of the TFTP server. The TFTP server must be on the same IP subnet as the switch.<br><br><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. |
| 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-3526:4#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-3526:4#
```

| ping | |
|---|---|
| Purpose | Used to test the connectivity between network devices. |
| Syntax | **ping <ipaddr> {times <value 1-255>} {timeout <sec 1-99>}** |
| Description | The ping command sends Internet Control Message Protocol (ICMP) echo messages to a remote IP address. The remote IP address will then “echo” or return the message. This is used to confirm connectivity between the switch and the remote device. |
| Parameters | <ipaddr> - Specifies the IP address of the host.<br>times - The number of individual ICMP echo messages to be sent.<br>A value of 0 will send an infinite ICMP echo messages. The maximum value is 255. The default is 0.<br>timeout - Defines the time-out period while waiting for a response from the remote device.<br>A value of 1 to 99 seconds can be specified. The default is 1 second |
| Restrictions | None. |

Example usage:

To ping the IP address 10.48.74.121 four times:

```
DES-3526:4#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-3526:4#
```

# 9

# NETWORK MONITORING COMMANDS

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

| Command | Parameters |
|---|---|
| show packet ports | <portlist> |
| show error ports | <portlist> |
| show utilitzation | [cpu \| ports {<portlist>}] |
| clear counters | ports <portlist> |
| clear log | |
| show log | index <value_list> |
| enable syslog | |
| disable syslog | |
| show syslog | |
| create syslog host | <index 1-4> ipaddress <ipaddr> {severity [informational\|warning\|all]\| facility[local0\|local1\|local2\|local3\| local4\|local5\|local6\|local7] \|udp_port<udp_port_number>\| state[enable\|disable] |
| config syslog host | [all \| <index 1-4>] {severity [informational \| warning \|all] \|facility [local0\|local1\|local2\|local3\|local4\|local5\|local6\|local7] \|udp_port <udp_port_number> \| ipaddress <ipaddr> \| state [enable \| disable]} |
| delete syslog host | <index 1-4><br>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 port or range of ports to be displayed. |
| Restrictions | None. |

Example usage:

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

```
DES-3526:4#show packet port 2
Port number : 2
Frame Size   Frame Counts   Frame/sec     Frame Type     Total    Total/sec
-----------  ------------   ----------    ----------     -------  ---------
64           3275           10            RX Bytes       408973   1657
65-127       755            10            RX Frames      395      19
128-255      316            1
256-511      145            0             TX Bytes       7918     178
512-1023     15             0             TX Frames      111      2
1024-1518    0              0

Unicast RX       152    1
Multicast RX     557    2
Broadcast RX     3686   16

DES-3526:4#
```

## show error ports

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

Example usage:

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

```
DES-3526:4#show errors port 3
                RX Frames                       TX Frames
                ---------                       ---------
CRC Error       19          Excessive Deferral  0
Undersize       0           CRC Error           0
Oversize        0           Late Collision      0
Fragment        0           Excessive Collision 0
Jabber          11          Single Collision    0
Drop Pkts       20837       Collision           0

DES-3526:4#
```

| show utilization | |
|---|---|
| Purpose | Used to display real-time port and cpu utilization statistics. |
| Syntax | **show utilization [cpu \| ports {<portlist>}]** |
| Description | This command will display the real-time port and cpu utilization statistics for the switch. |
| Parameters | cpu – Entering this parameter will display the current cpu utilization of the switch.<br><br>ports - Entering this parameter will display the current port utilization of the switch.<br><br>▪ <portlist> Specifies a port or range of ports to be displayed. |
| Restrictions | None. |

Example usage:

To display the port utilization statistics:

**DES-3526:4#show utilization ports**

**Command: show utilization ports**

| Port | TX/sec | RX/sec | Util | Port | TX/sec | RX/sec | Util |
|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 22 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 23 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 24 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 25 | 0 | 26 | 1 |
| 5 | 0 | 0 | 0 | 26 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | | | | |
| 7 | 0 | 0 | 0 | | | | |
| 8 | 0 | 0 | 0 | | | | |
| 9 | 0 | 0 | 0 | | | | |
| 10 | 0 | 0 | 0 | | | | |
| 11 | 0 | 0 | 0 | | | | |
| 12 | 0 | 0 | 0 | | | | |
| 13 | 0 | 0 | 0 | | | | |
| 14 | 0 | 0 | 0 | | | | |
| 15 | 0 | 0 | 0 | | | | |
| 16 | 0 | 0 | 0 | | | | |
| 17 | 0 | 0 | 0 | | | | |
| 18 | 0 | 0 | 0 | | | | |
| 19 | 0 | 0 | 0 | | | | |
| 20 | 0 | 0 | 0 | | | | |
| 21 | 0 | 0 | 0 | | | | |

To display the current cpu utilization:

```
DES-3526:4#show utilization cpu
Command: show utilization cpu

CPU utilization :
--------------------------------------------------------------------------------
Five seconds - 15%        One minute - 25%        Five minutes - 14%

DES-3526:4#
```

| clear counters | |
|---|---|
| Purpose | Used to clear the switch's statistics counters. |
| Syntax | **clear counters {ports <portlist>}** |
| Description | This command will clear the counters used by the switch to compile statistics. |
| Parameters | <portlist> – specifies a port or range of ports to be displayed. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To clear the counters:

```
DES-3526:4#clear counters ports 2-9
Command: clear counters ports 2-9

 Success.
DES-3526:4#
```

| 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-3526:4#clear log
Command: clear log

 Success.

DES-3526:4#
```

## 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> – This command will display the history log, beginning at 1 and ending at the value specified by the user in the <value> field.<br><br>If no parameter is specified, all history log entries will be displayed. |
| Restrictions | None. |

Example usage:

To display the switch history log**:**

```
DES-3526:4#show log index 5
Command: show log index 5

Index  Time                  Log Text
-----  --------------------  ------------------------------------------------------
5      00000 days 00:01:09   Successful login through Console (Username: Anonymous)
4      00000 days 00:00:14   System started up
3      00000 days 00:00:06   Port 1 link up, 100Mbps FULL duplex
2      00000 days 00:00:01   Spanning Tree Protocol is disabled
1      00000 days 00:06:31   Configuration saved to flash (Username: Anonymous)

DES-3526:4#
```

## 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. |

| enable syslog | |
|---|---|
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To the syslog function on the switch:

```
DES-3526:4#enable syslog
Command: enable syslog

Success.

DES-3526:4#
```

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

Example usage:

To disable the syslog function on the switch:

```
DES-3526:4#disable syslog
Command: disable syslog

Success.

DES-3526:4#
```

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

Example usage:

To display the current status of the syslog function:

```
DES-3526:4#show syslog
Command: show syslog

Syslog Global State: Enabled

DES-3526:4#
```

## create syslog host

| | |
|---|---|
| Purpose | Used to create a new syslog host. |
| Syntax | **create syslog host <index 1-4> ipaddress <ipaddr> {severity [informational\|warning\|all] \| facility[local0\|local1\|local2\|local3\| local4\|local5\|local6\|local7] \| udp_port <udp_port_number> \| state [enable \| disable]** |
| Description | The **create syslog host** command is used to create a new syslog host. |
| 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.<br><br>ipaddress <ipaddr> – Specifies the IP address of the remote host where syslog messages will be sent.<br><br>severity – Severity level indicator. These are described in the following:<br><br>Bold font indicates that the corresponding severity level is currently supported on the switch.<br><br>Numerical Code – Severity<br><br>0 Emergency: system is unusable<br><br>1 Alert: action must be taken immediately<br><br>2 Critical: critical conditions<br><br>3 Error: error conditions<br><br>**4 Warning: warning conditions**<br><br>5 Notice: normal but significant condition<br><br>**6 Informational: informational messages**<br><br>7 Debug: debug-level messages<br><br>informational – Specifies that informational messages will be sent to the remote host. This corresponds to number 6 from the list above.<br><br>warning – Specifies that warning messages will be sent to the remote host. This corresponds to number 4 from the list above.<br><br>all – Specifies that all of the currently supported syslog messages that |

## create syslog host

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 the facility values that the switch currently supports.

| 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

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

Example usage:

To create syslog host:

```
DES-3526:4#create syslog host 1 severity all facility local0
Command: create syslog host 1 severity all facility local0

 Success.

DES-3526:4#
```

## 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 <udp_port_number> \| 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. |

## config syslog host

Parameters

all – Specifies that the command will be applied to all hosts.

<index 1-4> – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4.

severity – Severity level indicator. These are described in the following:

Bold font indicates that the corresponding severity level is currently supported on the switch.

| Numerical Code | Severity |
|---|---|
| 0 | Emergency: system is unusable |
| 1 | Alert: action must be taken immediately |
| 2 | Critical: critical conditions |
| 3 | Error: error conditions |
| **4** | **Warning: warning conditions** |
| 5 | Notice: normal but significant condition |
| **6** | **Informational: informational messages** |
| 7 | Debug: debug-level messages |

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

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

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

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

| 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 |

| config syslog host | |
|---|---|
| | 14 log alert<br>15 clock daemon<br>**16 local use 0 (local0)**<br>**17 local use 1 (local1)**<br>**18 local use 2 (local2)**<br>**19 local use 3 (local3)**<br>**20 local use 4 (local4)**<br>**21 local use 5 (local5)**<br>**22 local use 6 (local6)**<br>**23 local use 7 (local7)**<br>local0 – Specifies that local use 0 messages will be sent to the remote host. This corresponds to number 16 from the list above.<br>local1 – Specifies that local use 1 messages will be sent to the remote host. This corresponds to number 17 from the list above.<br>local2 – Specifies that local use 2 messages will be sent to the remote host. This corresponds to number 18 from the list above.<br>local3 – Specifies that local use 3 messages will be sent to the remote host. This corresponds to number 19 from the list above.<br>local4 – Specifies that local use 4 messages will be sent to the remote host. This corresponds to number 20 from the list above.<br>local5 – Specifies that local use 5 messages will be sent to the remote host. This corresponds to number 21 from the list above.<br>local6 – Specifies that local use 6 messages will be sent to the remote host. This corresponds to number 22 from the list above.<br>local7 – Specifies that local use 7 messages will be sent to the remote host. This corresponds to number 23 from the list above.<br>udp_port <udp_port_number> – Specifies the UDP port number that the syslog protocol will use to send messages to the remote host.<br>ipaddress <ipaddr> – Specifies the IP address of the remote host where syslog messages will be sent.<br>state [enable \| disable] – Allows the sending of syslog messages to the remote host, specified above, to be enabled and disabled. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To configure a syslog host:

```
DES-3526:4#config syslog host 1 severity all facility local0
Command: config syslog host all severity all facility local0
 Success.
DES-3526:4#
```

Example usage:

To configure a syslog host for all hosts:

```
DES-3526:4#config syslog host all severity all facility local0
Command: config syslog host all severity all facility local0

 Success.

DES-3526:4#
```

| 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.<br><br>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-3526:4#delete syslog host 4
Command: delete syslog host 4

 Success.

DES-3526:4#
```

| 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-3526:4#show syslog host
Command: show syslog host

 Syslog Global State: Disabled

 Host Id  Host IP Address   Severity    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-3526:4#
```

# 10

# SPANNING TREE COMMANDS

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

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

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

## config stp

| | |
|---|---|
| Purpose | Used to setup STP and RSTP on the switch. |
| Syntax | **config stp {maxage <value 6-40> \| hellotime <value 1-10> \| forwarddelay <value 4-30> \| priority <value 0-61440> \| version[rstp \| stp] \| txholdcount <value 1-10>\| fbpdu [enable \| disable]}** |
| Description | This command is used to setup the Spanning Tree Protocol (STP) for the entire switch. |
| Parameters | maxage <value> – The maximum amount of time (in seconds) that the switch will wait to receive a BPDU packet before reconfiguring STP. The user may choose a time between 6 and 40 seconds. The default is 20 seconds.<br><br>hellotime <value> – The time interval between transmission of configuration messages by the root device. The user may choose a time between 1 and 10 seconds. The default is 2 seconds.<br><br>forwarddelay <value> – The maximum amount of time (in seconds) that the root device will wait before changing states. The user may choose a time between 4 and 30 seconds. The default is 15 seconds.<br><br>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.<br><br>version [rstp \| stp] - select the Spanning Tree Protocol version used for the switch. |

| config stp | |
|---|---|
| | • stp – Selct this parameter for IEEE 802.1d STP and for IEEE 802.1w STP compatibility mode.<br>• rstp - Select this paramter for IEEE 802.1w Rapid STP mode.<br><br>txholdcount <1-10> - the maximum number of Hello packets transmitted per interval. Default value = 3.<br><br>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. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To configure STP with maxage 18 and hellotime 4:

```
DES-3526:4#config stp maxage 18 hellotime 4
Command: config stp maxage 18 hellotime 4

Success.

DES-3526:4#
```

| config stp ports | |
|---|---|
| Purpose | Used to setup STP on the port level. |
| Syntax | **config stp ports <portlist> {cost [auto \| <value>] \| priority <value> \| migrate [yes \| no] \| edge [true \| false] \| p2p [true \| false \| auto] \| state [enable \| disable]** |
| Description | This command is used to create and configure STP for a group of ports. |
| Parameters | 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.<br><br>Default port cost: 100Mbps port = 200000 Gigabit port = 20000<br><br>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.<br><br><portlist> – Specifies a port or range of ports to be configured.<br><br>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 |

| config stp ports | |
|---|---|
| | stations or segments that will be upgraded to 802.1w RSTP onall or some portion of the segment.<br><br>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.<br><br>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. *Auto* allows the port to have p2p status whenever possible and operate as if the p2p status were *true*. 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 *false*.<br><br>state [enable \| disable] – Allows STP to be enabled or disabled for the ports specified in the port list. The default is disabled. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To configure STP with path cost 19, priority 16, and state enabled for ports 1-5 of the switch.

```
DES-3526:4#config stp ports 1-5 cost 19 priority 16 state enabled
Command: config stp ports 1-5 cost 19 priority 16 state enabled

Success.

DES-3526:4#
```

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

Example usage:

To enable STP, globally, on the switch:

```
DES-3526:4#enable stp
Command: enable stp

 Success.

DES-3526:4#
```

| 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-3526:4#disable stp
Command: disable stp

 Success.

DES-3526:4#
```

| 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-3526:4#show stp
Command: show stp

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

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
```

**Status 2 : STP disabled**

```
DES-3526:4#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-3526:4#
```

## 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. |

| show stp ports | |
|---|---|
| | configuration. |
| Parameters | <portlist> – Specifies a port or range of ports to be displayed. |
| Restrictions | None |

Example usage:

To display STP state of all ports:

```
DES-3526:4#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    8000/000102030400     Yes  *200000    128  No    Yes  Forwarding  Designated
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
```

# 11

# 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} |
| config multicast port_filtering_mode | [<portlist> \| all] [forward_all_groups \| forward_unregistered_groups \| filter_unregistered_groups] |
| show multicast port_filtering_mode | {<portlist>} |

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.<br><br><macaddr> – The MAC address that will be added to the forwarding table.<br><br><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-3526:4#create fdb default 00-00-00-00-01-02 port 5
Command: create fdb default 00-00-00-00-01-02 port 5

 Success.
DES-3526:4#
```

## 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.<br><br><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-3526:4#create multicast_fdb default 01-00-00-00-00-01
Command: create multicast_fdb default 01-00-00-00-00-01

Success.

DES-3526:4#
```

## 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 | <vlan_name 32> – The name of the VLAN on which the MAC address resides.<br><br><macaddr> – The MAC address that will be added to the multicast forwarding table.<br><br>[add \| delete] – Add will add ports to the forwarding table. Delete will remove ports from the multicast forwarding table. |

| config multicast_fdb | |
|---|---|
| | <portlist> – Specifies a range of ports to be configured. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To add multicast MAC forwarding:

```
DES-3526:4#config multicast_fdb default 01-00-00-00-00-01 add
1-5
Command: config multicast_fdb default 01-00-00-00-00-01 add 1-
1-5

Success.

DES-3526:4#
```

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

Example usage:

To set the fdb aging time:

```
DES-3526:4#config fdb aging_time 300
Command: config fdb aging_time 300

Success.

DES-3526:4#
```

## 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.<br><br><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-3526:4#delete fdb default 00-00-00-00-01-02
Command: delete fdb default 00-00-00-00-01-02

 Success.

DES-3526:4#
```

Example usage:

To delete a multicast fdb entry:

```
DES-3526:4#delete fdb default 01-00-00-00-01-02
Command: delete fdb default 01-00-00-00-01-02

 Success.

DES-3526:4#
```

## 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]** |

| clear fdb | |
|---|---|
| Description | This command is used to clear dynamically learned entries to the switch's forwarding database. |
| Parameters | <vlan_name 32> – The name of the VLAN on which the MAC address resides.<br><br><port> – The port number corresponding to the MAC destination address. The switch will always forward traffic to the specified device through this port.<br><br>all – Clears all dynamic entries to the switch's forwarding database. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To clear all FDB dynamic entries**:**

```
DES-3526:4#clear fdb all
Command: clear fdb all

 Success.

DES-3526:4#
```

| 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.<br><br><macaddr> – The MAC address that is present in the forwarding database table. |
| Restrictions | None. |

Example usage:

To display multicast MAC address table:

```
DES-3526:4#show multicast_fdb vlan default
Command: show multicast_fdb vlan default
```

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

Total Entries  : 1

DES-3526:4#
```

## show fdb

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

Example usage:

To display unicast MAC address table:

```
DES-3526:4#show fdb
Command: show fdb

Unicast MAC Address Aging Time = 300

VID   VLAN Name       MAC Address         Port       Type
----  ---------------  -----------------  ------  ---------------
1      default         00-00-39-34-66-9A   10      Dynamic
1      default         00-00-51-43-70-00   10      Dynamic
1      default         00-00-5E-00-01-01   10      Dynamic
1     default          00-00-74-60-72-2D   10      Dynamic
1     default          00-00-81-05-00-80    10     Dynamic
1     default          00-00-81-05-02-00    10     Dynamic
```

| | | | | |
|---|---|---|---|---|
| 1 | default | 00-00-81-48-70-01 | 10 | Dynamic |
| 1 | default | 00-00-E2-4F-57-03 | 10 | Dynamic |
| 1 | default | 00-00-E2-61-53-18 | 10 | Dynamic |
| 1 | default | 00-00-E2-6B-BC-F6 | 10 | Dynamic |
| 1 | default | 00-00-E2-7F-6B-53 | 10 | Dynamic |
| 1 | default | 00-00-E2-82-7D-90 | 10 | Dynamic |
| 1 | default | 00-00-F8-7C-1C-29 | 10 | Dynamic |
| 1 | default | 00-01-02-03-04-00 | CPU | Self |
| 1 | default | 00-01-02-03-04-05 | 10 | Dynamic |
| 1 | default | 00-01-30-10-2C-C7 | 10 | Dynamic |
| 1 | default | 00-01-30-FA-5F-00 | 10 | Dynamic |
| 1 | default | 00-02-3F-63-DD-68 | 10 | Dynamic |

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

## config multicast port_filtering_mode

| | |
|---|---|
| Purpose | Used to configure the multicast packet filtering mode on a port per port basis. |
| Syntax | **config multicast port_filtering_mode [<portlist> \| all] [forward_all_groups \| forward_unregistered_groups \| filter_unregistered_groups]** |
| Description | This command will configure the multicast packet filtering mode for specified ports on the switch. |
| Parameters | <portlist> Specifies a port or range of ports to view.<br><br>[forward_all_groups \| forward_unregistered_groups \| filter_unregistered_groups] – The user may set the filtering mode to any of these three options |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To configure the multicast filtering mode to forward all groups on ports 1 through 4.

**DES-3526:4#config multicast port_filtering_mode 1-4 forward_all_groups**

**Command: config multicast port_filtering_mode 1-4 forward_all_groups**

**Success.**

**DES-3526:4#**

## show multicast port_filtering_mode

| | |
|---|---|
| Purpose | Used to show the multicast packet filtering mode on a port per port basis. |
| Syntax | **show multicast port_filtering_mode {<portlist>}** |

| show multicast port_filtering_mode | |
|---|---|
| Description | This command will display the current multicast packet filtering mode for specified ports on the switch. |
| Parameters | <portlist> Specifies a port or range of ports to view. |
| Restrictions | None. |

Example usage:

To view the multicast port filtering mode for all ports:

```
DES-3526:4#show multicast port_filtering_mode
Command: show multicast port_filtering_mode

Port      Multicast Filter Mode
------    ---------------------------
1         forward_unregistered_groups
2         forward_unregistered_groups
3         forward_unregistered_groups
4         forward_unregistered_groups
5         forward_unregistered_groups
6         forward_unregistered_groups
7         forward_unregistered_groups
8         forward_unregistered_groups
9         forward_unregistered_groups
10        forward_unregistered_groups
11        forward_unregistered_groups
12        forward_unregistered_groups
13        forward_unregistered_groups
14        forward_unregistered_groups
15        forward_unregistered_groups
16        forward_unregistered_groups
17        forward_unregistered_groups
18        forward_unregistered_groups
19        forward_unregistered_groups
20        forward_unregistered_groups
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

# 12

# 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 [enabled \| disabled] \| multicast [enabled \| disabled] \| dlf [enabled \| disabled] \| threshold <value 0-255> } |
| 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 0-255>** |
| Description | This command is used to configure broadcast storm control. |
| Parameters | <storm_grouplist> – Used to specify a broadcast storm control group. This is specified by entering the syntax unit_id.<br><br>all – Specifies all broadcast storm control groups on the switch.<br><br>broadcast [enable \| disable] – Enables or disables broadcast storm control.<br><br>multicast [enable \| disable] – Enables or disables multicast storm control.<br><br>dlf [enable \| disable] – Enables or disables dlf traffic control.<br><br>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. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

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

```
DES-3526:4#config traffic control all broadcast enabled
Command: config traffic control all broadcast enabled

Success.

DES-3526:4#
```

| show traffic control | |
|---|---|
| Purpose | Used to display current traffic control settings. |
| Syntax | **show traffic control {group_list <storm_grouplist>}** |
| Description | This command displays the current storm traffic control configuration on the switch. |
| Parameters | group_list <storm_grouplist> – Used to specify a broadcast storm control group. This is specified by entering the syntax unit_id. |
| Restrictions | None. |

Example usage:

To display traffic control setting:

```
DES-3526:4#show traffic control
Command: show traffic control
Traffic Control

Module  Group [ports]   Threshold   Broadcast Storm   Multicast Storm   Destination 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-3526:4#
```

# 13

# QOS COMMANDS

The DES-3526 switch supports 802.1p priority queuing. The switch has 4 priority queues. These priority queues are numbered from 3 (Class 3) — the highest priority queue — to 0 (Class 0) — the lowest priority queue. The eight priority tags specified in IEEE 802.1p (p0 to p7) are mapped to the switch's priority queues as follows:

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

Priority scheduling is implemented by the priority queues stated above. The switch will empty the four hardware priority queues in order, beginning with the highest priority queue, 4, to the lowest priority queue, 0. Each hardware queue will transmit all of the packets in its buffer before permitting the next lower priority to transmit its packets. When the lowest hardware priority queue has finished transmitting all of its packets, the highest hardware priority queue will begin transmitting any packets it may have received.

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

| 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>] {rx_rate [no_limit \| <value 1-1000>] \| tx_rate [no_limit<value 1-1000>]}** |
| Description | The **config bandwidth_control** command is used to configure bandwidth on a by-port basis. |

| config bandwidth_control | |
|---|---|
| | bandwidth on a by-port basis. |
| Parameters | <portlist> – Specifies a port or range of ports to be configured.<br><br>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<br><br>▪ no_limit – Specifies that there will be no limit on the rate of packets received by the above specified ports.<br><br>▪ <value 1-1000> – Specifies the packet limit, in Mbps, that the above ports will be allowed to receive.<br><br>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.<br><br>▪ no_limit – Specifies that there will be no limit on the rate of packets received by the above specified ports.<br><br>▪ <value 1-1000> – Specifies the packet limit, in Mbps, that the above ports will be allowed to receive.<br><br>The transfer(tx) and receive(rx) rate of packets for Gigabit ports must be configured in a multiple of 8 Mbits. (8, 16, 24…) |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To configure bandwidth control:

```
DES-3526:4#config bandwidth_control 1-10 tx_rate 10
Command: config bandwidth_control 1-10 tx_rate 10

 Success.

DES-3526:4#
```

| show bandwidth_control | |
|---|---|
| Purpose | Used to display the bandwidth control table. |
| 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 port or range of ports to be viewed. |
| Restrictions | None. |

Example usage:

To display bandwidth control settings:

```
DES-3526:4#show bandwidth_control  1-10
Command: show bandwidth_control 1-10

Bandwidth Control Table

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

DES-3526:4#
```

## config scheduling

| | |
|---|---|
| Purpose | Used to configure the traffic scheduling mechanism for each COS queue. |
| Syntax | **config scheduling <class_id 0-3> [max_packet <value 0-255>\|max_latency <value 0-255>]** |
| Description | The switch contains 4 hardware priority queues. Incoming packets must be mapped to one of these four queues. This command is used to specify the rotation by which these four hardware priority queues are emptied.<br>The switch's default (if the config scheduling command is not used, or if the config scheduling command is entered with both max_packet and max_latency parameters are set to 0) is to empty the 4 hardware priority queues in order – from the highest priority queue (hardware queue 3) to the lowest priority queue (hardware queue 0). Each hardware queue will transmit all of the packets in its buffer before allowing the next lower priority queue to transmit its packets. When the lowest hardware priority queue has finished transmitting all of its packets, the highest hardware priority queue can again transmit any packets it may have received.<br>The max_packets parameter allows you to specify the maximum number of packets a given hardware priority queue can transmit before allowing the next lowest hardware priority queue to begin transmitting its packets. A value between 0 and 255 can be specified. For example, if a value of 3 is specified, then the highest hardware priority queue (number 3) will be allowed to transmit 3 packets – then the next lowest hardware priority queue (number 2) will be allowed to transmit 3 packets, and so on, until all of the queues have transmitted 3 packets. The process will then repeat. |

| config scheduling | |
|---|---|
| | The max_latency parameter allows you to specify the maximum amount of time that packets are delayed before being transmitted to a given hardware priority queue. A value between 0 and 255 can be specified. This number is then multiplied by 16 ms to determine the maximum latency. For example, if 3 is specified, the maximum latency allowed will be 3 X 16 = 48 ms.<br><br>When the specified hardware priority queue has been waiting to transmit packets for this amount of time, the current queue will finish transmitting its current packet, and then allow the hardware priority queue whose max_latency timer has expired to begin transmitting packets. |
| Parameters | <class_id 0-3> – This specifies which of the four hardware priority queues the config scheduling command will apply to. The four hardware priority queues are identified by number – from 0 to 3 – with the 0 queue being the lowest priority.<br><br>max_packet <value 0-255> – Specifies the maximum number of packets the above specified hardware priority queue will be allowed to transmit before allowing the next lowest priority queue to transmit its packets. A value between 0 and 255 can be specified.<br><br>max_latency <value 0-255> – Specifies the maximum amount of time the above specified hardware priority queue will be allowed to transmit packets before allowing the next lowest hardware priority queue to begin transmitting its packets. A value between 0 and 255 can be specified – with this value multiplied by 16 ms to arrive at the total allowed time for the queue to transmit packets. For example, a value of 3 specifies 3 X 16 = 48 ms. The queue will continue transmitting the last packet until it is finished when the max_latency timer expires. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To configure the traffic scheduling mechanism for each queue:

```
DES-3526:4# config scheduling 0 max_packet 100
max_latency 150

Command: config scheduling 0 max_packet 100
max_latency 150


 Success.


DES-3526:4#
```

| show scheduling | |
|---|---|
| Purpose | Used to display the currently configured traffic scheduling on the switch. |
| Syntax | **show scheduling** |
| Description | The **show scheduling** command will display the current traffic scheduling mechanisms in use on the switch. |
| Parameters | None. |

## show scheduling

| | |
|---|---|
| Restrictions | None. |

Example usage:

To display the current scheduling configuration:

```
DES-3526:4# show scheduling
Command: show scheduling


QOS Output Scheduling

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

DES-3526:4#
```

## 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 | This command allows you to configure the way the switch will map an incoming packet, based on its 802.1p user priority, to one of the four available hardware priority queues on the switch.<br><br>The switch's default is to map the following incoming 802.1p user priority values to the four hardware priority queues:<br><br>802.1p Hardware Queue Remark<br><br>0 1 Mid-low<br><br>1 0 Lowest<br><br>2 0 Lowest<br><br>3 1 Mid-low<br><br>4 2 Mid-high<br><br>5 2 Mid-high<br><br>6 3 Highest<br><br>7 3 Highest. |

## config 802.1p user_priority

| | |
|---|---|
| | This mapping scheme is based upon recommendations contained in IEEE 802.1D.<br><br>You can change this mapping by specifying the 802.1p user priority you want to go to the <class_id 0-3> (the number of the hardware queue).<br><br><priority 0-7> – The 802.1p user priority you want to associate with the <class_id 0-3> (the number of the hardware queue) with.<br><br><class_id 0-3> – The number of the switch's hardware priority queue. The switch has four hardware priority queues available. They are numbered between 0 (the lowest priority) and 3 (the highest priority). |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To configure 802.1 user priority on the switch:

```
DES-3526:4# config 802.1p user_priority 1 3
Command: config 802.1p user_priority 1 3

 Success.

DES-3526:4#
```

## 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-3526:4# show 802.1p user_priority
Command: show 802.1p user_priority

QOS Class of Traffic

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

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

DES-3526:4#
```

## config 802.1p default_priority

| | |
|---|---|
| Purpose | Used to configure the 802.1p default priority settings on the switch. If an untagged packet is received by the switch, the priority configured with this command will be written to the packet's priority field. |
| Syntax | **config 802.1p default_priority [<portlist>\|all] <priority 0-7>** |
| Description | This command allows you to specify default priority handling of untagged packets received by the switch. The priority value entered with this command will be used to determine which of the four hardware priority queues the packet is forwarded to. |
| Parameters | <portlist> – Specifies a port or range of ports to be configured.<br><br>all – Specifies that the command applies to all ports on the switch.<br><br><priority 0-7> – The priority value you want to assign to untagged packets received by the switch or a range of ports on the switch. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To configure 802.1p default priority on the switch:

```
DES-3526:4#config 802.1p default_priority all 5
Command: config 802.1p default_priority all 5

Success.

DES-3526:4#
```

## 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 port or range of ports to be configured. |

| show 802.1 default_priority | |
|---|---|
| Restrictions | None. |

Example usage:

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

```
DES-3526:4# 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

DES-3526:4#
```

# 14

# 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. Traffic from any source port to a target port can be mirrored for real-time analysis. A logic analyzer or an RMON proble can then be attached to study the traffic crossing the source port in a completely obtrusive manner. |
| 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 | <port> – This specifies the Target port (the port where mirrored packets will be received). The target port must be configured in the same VLAN and must be operationg at the same speed a s the source port. If the target port is operating at a lower speed, the source port will be forced to drop its operating speed to match that of the target port.<br><br>source ports – The port or ports being mirrored. This cannot include the Target port.<br><br><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.<br><br>rx – Allows the mirroring of only packets received by (flowing into) the port or ports in the port list.<br><br>tx – Allows the mirroring of only packets sent to (flowing out of) the port or ports in the port list.<br><br>both – Mirrors all the packets received or sent by the port or ports in the port list. |
| 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-3526:4# config mirror port 1 add source ports 2-7 both
Command: config mirror port 1 add source ports 2-7 both

Success.

DES-3526:4#
```

## 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 | <port> – This specifies the Target port (the port where mirrored packets will be received).<br><br><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.<br><br>rx – Allows the mirroring of only packets received by (flowing into) the port or ports in the port list.<br><br>tx – Allows the mirroring of only packets sent to (flowing out of) the port or ports in the port list.<br><br>both – Mirrors all the packets received or sent by the port or ports in the port list. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To delete the mirroring ports:

```
DES-3526:4#config mirror port 1 delete source port 2-4
Command: config mirror 1 delete source 2-4

Success.

DES-3526:4#
```

## enable mirror

| | |
|---|---|
| Purpose | Used to enable a previously entered port mirroring configuration. |
| Syntax | **enable mirror** |

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

Example usage:

To enable mirroring configurations:

```
DES-3526:4#enable mirror
Command: enable mirror

 Success.

DES-3526:4#
```

| 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-3526:4#disable mirror
Command: disable mirror

 Success.

DES-3526:4#
```

| show mirror | |
|---|---|
| Purpose | Used to show the current port mirroring configuration on the switch. |
| Syntax | **show mirror** |

| 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-3526:4#show mirror
Command: show mirror

 Current Settings
Mirror Status: Enabled
 Target Port: 1
 Mirrored Port:
        RX:
        TX: 5-7

DES-3526:4#
```

# 15

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

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

| 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 | <vlan_name 32> – The name of the VLAN to be created.<br><br><vlanid> – The VLAN ID of the VLAN to be created. Allowed values = 1-4094<br><br>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. |
| 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-3526:4#create vlan v1 tag 2
Command: create vlan v1 tag 2

 Success.

DES-3526:4#
```

| 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 the vlan "v1":

```
DES-3526:4#delete vlan v1
Command: delete vlan v1

 Success.

DES-3526:4#
```

| 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 | <vlan_name 32> – The name of the VLAN you want to add ports to.<br>add – Specifies all of the ports on the switch.<br>tagged – Specifies the additional ports as tagged.<br>untagged – Specifies the additional ports as untagged.<br>forbidden – Specifies the additional ports as forbidden. |

| config vlan | |
|---|---|
| | delete – Deletes the above specified VLAN from the switch.<br><br><portlist> – A port or range of ports to add to the VLAN.<br><br>advertisement [enable\|disable] – Enables or disables GVRP on the specified VLAN. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

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

```
DES-3526:4#config vlan v1 add tagged 4-8
Command: config vlan v1 add tagged 4-8

Success.

DES-3526:4#
```

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

Example usage:

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

```
DES-3526:4#config gvrp 1-4 state enable ingress_checking enable
acceptable_frame tagged_only pvid 2

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


Success.


DES-3526:4#
```

## 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-3526:4#enable gvrp

Command: enable gvrp


 Success.


DES-3526:4#
```

## 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-3526:4#disable gvrp
Command: disable gvrp

 Success.

DES-3526:4#
```

## 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-3526:4#show vlan
Command: show vlan

VID              : 1          VLAN Name     : default
VLAN TYPE        : static     Advertisement : Enabled
Member ports     : 1-26
Static ports     : 1-26
Untagged ports   : 1-26
Forbidden ports  : 1-26

 Total Entries :

DES-3526:4#
```

## 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 port or range of ports for which the GVRP status is to be displayed. |

| show gvrp | |
|---|---|
| Restrictions | None. |

Example usage:

To display GVRP port status:

```
DES-3526:4#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

Total Entries : 24

DES-3526:4#
```

# 16

# ASYMMETRIC VLAN COMMANDS

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

| Command | Parameters |
|---|---|
| enable asymmetric_vlan | |
| disable asymmetric_vlan | |
| show asymmetric_vlan | |

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

| enable asymmetric_vlan | |
|---|---|
| Purpose | Used to enable the asymmetric VLAN function on the switch. |
| Syntax | enable asymmetric_vlan |
| Description | This command enables the asymmetric VLAN function on the switch |
| Parameters | None. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To enable asymmetric VLANs:

```
DES-3526:4#enable asymmetric_vlan
Command: enable asymmetric_vlan

Success.

DES-3526:4#
```

| disable asymmetric_vlan | |
|---|---|
| Purpose | Used to disable the asymmetric VLAN function on the switch. |
| Syntax | **disable asymmetric_vlan** |
| Description | This command disables the asymmetric VLAN function on the switch |
| Parameters | None. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To disable asymmetric VLANs:

```
DES-3526:4#disable asymmetric_vlan
Command: disable asymmetric_vlan

Success.

DES-3526:4#
```

| show asymmetric_vlan | |
|---|---|
| Purpose | Used to view the asymmetric VLAN state on the switch. |
| Syntax | **show asymmetric_vlan** |
| Description | This command displays the asymmetric VLAN state on the switch |
| Parameters | None. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To display the asymmetric VLAN state cuurently set on the switch:

```
DES-3526:4#show asymmetric_vlan
Command: show asymmetric_vlan

Asymmetric Vlan: Enabled

DES-3526:4#
```

# 17

# LINK AGGREGATION COMMANDS

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

| Command | Parameters |
|---|---|
| create link_aggregation | group_id <value 1-6> {type[lacp\|static]} |
| delete link_aggregation | group_id <value 1-6> |
| config link_aggregation | group_id <value1-6> {master_port <port> \| ports <portlist> state [enable \| disable]} |
| config link_aggregation algorithm | [mac_source \| mac_destination \|mac_source_dest \| ip_source \| ip_destination \| ip_source_dest] |
| show link_aggregation | {group_id <value 1-6> \| algorithm} |
| config lacp_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 1-6> {type[lacp \| static]}** |
| Description | This command will create a link aggregation group with a unique identifier. |
| 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.<br><br>type – Specify the type of link aggregation used for the group. If the type is not specified the default type is static.<br><br>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.<br><br>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. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To create a link aggregation group:

```
DES-3526:4#create link_aggregation group_id 1
Command: create link_aggregation group_id 1

Success.

DES-3526:4#
```

## delete link_aggregation group_id

| | |
|---|---|
| Purpose | Used to delete a previously configured link aggregation group. |
| Syntax | **delete link_aggregation group_id <value 1-6>** |
| Description | This command is used to delete a previously configured link aggregation group. |
| Parameters | <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-3526:4#delete link_aggregation group_id 6
Command: delete link_aggregation group_id 6

Success.

DES-3526:4#
```

## config link_aggregation

| | |
|---|---|
| Purpose | Used to configure a previously created link aggregation group. |
| Syntax | **config link_aggregation group_id <value 1-6> {master_port <port> \| ports <portlist> \| state [enable \| disable]** |
| Description | This command allows you to configure a link aggregation group that was created with the **create link_aggregation** command above. The DES-3526 supports link_aggregation cross box which specifies that link aggregation groups may be spread over multiple switches in the switching stack. |
| Parameters | group _id<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.<br><br>master_port<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 |

| config link_aggregation | |
|---|---|
| | with the master port.<br><br>ports<portlist> – Specifies a range of ports that will belong to the link aggregation group.<br><br>state [enable \| disable] – Allows you to enable or disable the specified link aggregation group. |
| Restrictions | Only administrator-level users can issue this command. Link aggregation groups may not overlap. |

Example usage:

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

```
DES-3526:4#config link_aggregation group_id 1 master_port 1 ports 5-7, 9
Command: config link_aggregation group_id 1 master_port 1 ports 5-7, 9

Success.

DES-3526:4#
```

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

Example usage:

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

```
DES-3526:4#config link_aggregation algorithm mac_source_dest
Command: config link_aggregation algorithm mac_source_dest

Success.

DES-3526:4#
```

## show link_aggregation

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

Example usage:

To display Link Aggregation configuration:

```
DES-3526:4#show link_aggregation
Command: show link_aggregation

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

| config lacp_ports | |
|---|---|
| Parameters | <portlist> – Specifies a port or range of ports to be configured.<br><br>mode – Select the mode to determine if LACP ports will process LACP control frames.<br><br>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.<br><br>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). |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To configure LACP port mode settings:

```
DES-3526:4#config lacp_port 1-12 mode active
Command: config lacp_port 1-12 mode active

Success.

DES-3526:4#
```

| show lacp_port | |
|---|---|
| Purpose | Used to display current LACP port mode settings. |
| Syntax | **show lacp_port {<portlist>}** |
| Description | This command will display the LACP mode settings as they are currently configured. |
| Parameters | <portlist> - Specifies a port or range of ports to be configured.<br><br>If no parameter is specified, the system will display the current LACP status for all ports. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To display LACP port mode settings:

```
DES-3526:4#show lacp_port 1-10
Command: show lacp_port 1-10

Port    Activity
```

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

DES-3526:4#
```

# 18

# 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 | <ipif_name 12> [{ipaddress <network_address> \| vlan <vlan_name 32> \|state [enable \| disable]} bootp \|dhcp] |
| show ipif | <ipif_name 12> |

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

## config ipif

| | |
|---|---|
| Purpose | Used to configure the System IP interface. |
| Syntax | **config ipif <ipif_name 12> [{ ipaddress <network_address> [ vlan <vlan_name 32> \| state [enabled \| disabled]} \| bootp \| dhcp]** |
| Description | This command is used to configure the System IP interface on the switch. |
| Parameters | <ipif_name 12> Enter an alphanumeric string of up to 12 characters to identify this ip interface.<br><br><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\|8).<br><br><vlan_name 32> – The name of the VLAN corresponding to the System IP interface.<br><br>state [enable \| disable] – Allows you to enable or disable the IP interface.<br><br>bootp – Allows the selection of the BOOTP protocol for the assignment of an IP address to the switch's System IP interface.<br><br>dhcp – Allows the selection of the DHCP protocol for the assignment of an IP address to the switch's System IP interface. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To configure the IP interface System:

```
DES-3526:4#config ipif System ipaddress 10.48.74.122/8
Command: config ipif System ipaddress 10.48.74.122/8

 Success.

DES-3526:4#
```

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

Example usage:

To display IP interface settings.

```
DES-3526:4#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

Total Entries : 1

DES-3526:4#
```

# 19

# 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> \| 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> |
| disable igmp snooping | |
| show igmp snooping group | vlan <vlan_name 32> |
| show router ports | {vlan <vlan_name 32>} {static \| dynamic \| forbidden} |
| show igmp_snooping forwarding | {vlan<vlan_name 32>} |
| show igmp_snooping group | {vlan<vlan_name 32>} |

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

## config igmp_snooping

| | |
|---|---|
| Purpose | Used to configure IGMP snooping on the switch. |
| Syntax | **config igmp_snooping [<vlan_name 32> \| all] {host_timeout <sec 1-16711450> \| router_timeout < sec 1-16711450> \| leave_timer < sec 0-16711450> \| state [enable \| disable]}** |
| Description | This command allows you to configure IGMP snooping on the switch. |
| Parameters | <vlan_name 32> – The name of the VLAN for which IGMP snooping is to be configured.<br><br>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.<br><br>router_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.<br><br>leave_timer <sec> – Specifies the amount of time a Multicast address will stay in the database before it is deleted, after it has sent out a leave group message. An entry of zero (0) specifies an immediate deletion of the Multicast address. The default is 2 |

| config igmp_snooping | |
|---|---|
| | seconds.<br><br>state [enable \| disable] – Allows you to enable or disable IGMP snooping for the specified VLAN. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To configure the igmp snooping:

```
DES-3526:4#config igmp_snooping default host_timeout 250 state
enable
Command: config igmp_snooping default host_timeout 250 state
enable

Success.

DES-3526:4#
```

| config igmp_snooping querier | |
|---|---|
| Purpose | This command configures IGMP snooping querier. |
| Syntax | **config igmp_snooping querier [<vlan_name 32> \| all] {query_interval <sec 1-65535> \| max_response_time <sec 1-25> \| robustness_variable <value 1-255> \| last_member_query_interval <sec 1-25> \| state [enable \| disable]** |
| Description | Used to configure the time in seconds between general query transmissions, the maximum time in seconds to wait for reports from members and the permitted packet loss that guarantees IGMP snooping. |
| Parameters | <vlan_name 32> – The name of the VLAN for which IGMP snooping querier is to be configured.<br><br>query_interval <sec> – Specifies the amount of time in seconds between general query transmissions. The default setting is 125 seconds.<br><br>max_response_time <sec> – Specifies the maximum time in seconds to wait for reports from members. The default setting is 10 seconds.<br><br>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:<br><br>• 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).<br><br>• Other querier present interval—Amount of time that must pass before a multicast router decides that there is no longer |

| config igmp_snooping querier | |
|---|---|
| | another multicast router that is the querier. This interval is calculated as follows: (robustness variable x query interval) + (0.5 x query response interval).<br><br>• 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.<br><br>• By default, the robustness variable is set to 2. You might want to increase this value if you expect a subnet to be lossy. Although 1 is specified as a valid entry, the roubustness variable should not be one or problems may arise.<br><br>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.<br><br>state [enable \| disable] – Allows the switch to be specified as an IGMP Querier or Non-querier. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To configure the igmp snooping:

```
DES-3526:4#config igmp_snooping querier default query_interval
125 state enable

Command: config igmp_snooping querier default query_interval
125 state enable

Success.

DES-3526:4#
```

| 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 | <vlan_name 32> – The name of the VLAN on which the router port resides.<br><br><portlist> – Specifies a port or range of ports that will be configured as router ports. |

| config router_ports | |
|---|---|
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To set up static router ports:

```
DES-3526:4#config router_ports default add 1-10
Command: config router_ports default add 1-10

 Success.

DES-3526:4#
```

| 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-3526:4#enable igmp_snooping
Command: enable igmp_snooping

 Success.
DES-3526:4#
```

| disable igmp_snooping | |
|---|---|
| Purpose | Used to enable IGMP snooping on the switch. |
| Syntax | **disable igmp_snooping {forward_mcrouter_only}** |
| 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 | forward_mcrouter_only – Adding this parameter to this command will disable forwarding all multicast traffic to a multicast-enabled |

| disable igmp_snooping | |
|---|---|
| | routers .The switch will then forward all multicast traffic to any IP router.<br><br>Entering this command without the parameter will disable igmp snooping on the switch. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To disable IGMP snooping on the switch:

```
DES-3526:4#disable igmp_snooping
Command: disable igmp_snooping

 Success.

DES-3526:4#
```

Example usage:

To disable forwarding all multicast traffic to a multicast-enabled router:

```
DES-3526:4#disable igmp_snooping forward_mcrouter_only
Command: disable igmp_snooping forward_mcrouter_only

 Success.

DES-3526:4#
```

| 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-3526:4#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-3526:4#
```

## 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-3526:4#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    : 2,5

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

```
Reports          : 1
Port Member      : 6,8

VLAN Name        : default
Multicast group: 234.5.6.7
MAC address      : 01-00-5E-05-06-07
Reports          : 1
Port Member      : 4,10

VLAN Name        : default
Multicast group: 236.54.63.75
MAC address      : 01-00-5E-36-3F-4B
Reports          : 1
Port Member      : 18,22

VLAN Name        : default
Multicast group: 239.255.255.250
MAC address      : 01-00-5E-7F-FF-FA
Reports          : 2
Port Member      : 9,19

VLAN Name        : default
Multicast group: 239.255.255.254
MAC address      : 01-00-5E-7F-FF-FE
Reports          : 1
Port Member      : 13,17

Total Entries    : 6

DES-3526:4#
```

## 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.<br><br>static – Displays router ports that have been statically configured.<br><br>dynamic – Displays router ports that have been dynamically configured. |
| Restrictions | None. |

Example usage:

To display the router ports.

```
DES-3526:4#show router_ports
Command: show router_ports

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

Total Entries: 1

DES-3526:4#
```

## show igmp_snooping forwarding

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

Example usage:

To view the IGMP snooping forwarding table for VLAN "Trinity":

```
DES-3526:4#show igmp_snooping forwarding vlan Trinity
Command: show igmp_snooping forwarding vlan Trinity

 VLAN Name       : Trinity
 Multicast group : 224.0.0.2
 MAC address     : 01-00-5E-00-00-02
 Port Member     : 17

Total Entries: 1

DES-3526:4#
```

## show igmp_snooping group

| | |
|---|---|
| Purpose | Used to display the current IGMP snooping configuration on the switch. |
| Syntax | **show igmp_snooping group {vlan <vlan_name 32>}** |
| Description | This command will display the current IGMP setup currently configured on the switch. |
| Parameters | <vlan_name 32> – The name of the VLAN for which you want to view IGMP snooping forwarding table information. |

| show igmp_snooping group | |
|---|---|
| Restrictions | None. |

Example usage:

To view the current IGMP snooping group:

```
DES-XXXXS: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   : 2,4

VLAN Name     : default
Multicast group: 224.0.0.9
MAC address   : 01-00-5E-00-00-09
Reports       : 1
Port Member   : 6,8

VLAN Name     : default
Multicast group: 234.5.6.7
MAC address   : 01-00-5E-05-06-07
Reports       : 1
Port Member   : 10,12

VLAN Name     : default
Multicast group: 236.54.63.75
MAC address   : 01-00-5E-36-3F-4B
Reports       : 1
Port Member   : 14,16

VLAN Name     : default
Multicast group: 239.255.255.250
MAC address   : 01-00-5E-7F-FF-FA
Reports       : 2
Port Member   : 18,20

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

```
Port Member    : 22,24

Total Entries : 6

DES-XXXXS:4#
```

# 20

# 802.1X COMMANDS

The DES-3526 implements the server-side of the IEEE 802.1x Port-based Network Access Control. This mechanism is intended to allow only authorized users, or other network devices, access to network resources by establishing criteria for each port on the switch that a user or network device must meet before allowing that port to forward or receive frames.

| Command | Parameters |
|---|---|
| enable 802.1x | |
| disable 802.1x | |
| show 802.1x auth_state | {ports <portlist>} |
| show 802.1x 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_protocol | [radius eap \| radius pap] |
| config 802.1x init | {port_based ports [<portlist> \| all] \| mac_based [ports] [<portlist> \|all] {mac_address <macaddr>}] |
| config 802.1x auth_mode | [port_based \| mac_based] |
| 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 1-65535> \| acct_port <udp_port_number 1-65535>}] |
| config radius delete | <server_index 1-3> |
| config radius | <server_index 1-3> {ipaddress <server_ip> \| key <passwd 32> [auth_port <udp_port_number 1-65535> acct_port <udp_port_number 1-65535>]} |
| show radius | |

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

## 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. |

## enable 802.1x

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

Example usage:

To enable 802.1x switch wide:

```
DES-3526:4#enable 802.1x
Command: enable 802.1x

Success.

DES-3526:4#
```

## 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-3526:4#disable 802.1x
Command: disable 802.1x

Success.

DES-3526:4#
```

## show 802.1x auth_configuration

| | |
|---|---|
| Purpose | Used to display the current configuration of the 802.1x server on the switch. |
| Syntax | **show 802.1x auth_configuration {ports <portlist>}** |
| Description | The show 802.1x command is used to display the current configuration of the 802.1x Port-based Network Access Control server application on the switch. |
| Parameters | ports <portlist> – Specifies a port or range of ports to view.<br><br>The following details what is displayed: |

| show 802.1x auth_configuration | |
|---|---|
| | 802.1x Enabled \| Disabled – Shows the current status of 802.1x functions on the switch.<br><br>Authentication Mode – Shows the authentication mode, whether it be by mac address or by port.<br><br>Authentication Protocol: Radius_Eap – Shows the authentication protocol suite in use between the switch and a Radius server. May read Radius_Eap or Radius_Pap.<br><br>Port number – Shows the physical port number on the switch.<br><br>Capability: Authenticator\|None – Shows the capability of 802.1x functions on the port number displayed above. There are two 802.1x capabilities that can be set on the switch: Authenticator and None.<br><br>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.<br><br>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.<br><br>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.<br><br>QuietPeriod – Shows the time interval between authentication failure and the start of a new authentication attempt.<br><br>TxPeriod – Shows the time to wait for a response from a supplicant (user) to send EAP Request\|Identiy packets.<br><br>SuppTimeout – Shows the time to wait for a response from a supplicant (user) for all EAP packets, except for the Request\|Identity packets.<br><br>ServerTimeout – Shows the length of time to wait for a response from a Radius server.<br><br>MaxReq – Shows the maximum number of times to retry sending packets to the supplicant.<br><br>ReAuthPeriod – shows the time interval between successive re-authentications.<br><br>ReAuthenticate: Enabled\|Disabled – Shows whether or not to re-authenticate. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To display the 802.1x authtication states (stacking disabled):

```
DES-3526:4#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
AdminCrlDir   : Both
OpenCrlDir    : Both
Port Control  : Auto
QuietPeriod   : 60   sec
TxPeriod      : 30   sec
SuppTimeout   : 30   sec
ServerTimeout : 30   sec
MaxReq        : 2    times
ReAuthPeriod  : 3600 sec
ReAuthenticate : Disabled

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

## show 802.1x auth_state

| | |
|---|---|
| Purpose | Used to display the current authentication state of the 802.1x server on the switch. |
| Syntax | **show 802.1x auth_state {ports <portlist>}** |
| Description | The show 802.1x auth_state command is used to display the current authentication state of the 802.1x Port-based Network Access Control server application on the switch. |
| Parameters | ports<portlist> – Specifies a port or range of ports to be viewed.<br><br>The following details what is displayed:<br><br>Port number – Shows the physical port number on the switch.<br><br>Auth PAE State: Initalize\|Disconnected\|Connecting\| Authenticating\|Authenticated\|Held \|ForceAuth\|ForceUnauth – Shows the current state of the Authenticator PAE.<br><br>Backend State: Request\|Response\|Fail\| Idle\|Initalize\|Success \|Timeout – Shows the current state of the Backend Authenticator.<br><br>Port Status: Authorized\|Unauthorized – Shows the result of the authentication process. Authorized means that the user was authenticated, and can access the network. Unauthorized means that the user was not authenticated, and cannot access the network. |

## show 802.1x auth_state

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

Example usage:

To display the 802.1x auth state:

```
DES-3526:4#show 802.1x auth_state
Command: show 802.1x auth_state

Port      Auth   PAE State      Backend State      Port Status
------    ------------------    ----------------   ----------------
1         ForceAuth            Success            Authorized
2         ForceAuth            Success            Authorized
3         ForceAuth            Success            Authorized
4         ForceAuth            Success            Authorized
5         ForceAuth            Success            Authorized
6         ForceAuth            Success            Authorized
7         ForceAuth            Success            Authorized
8         ForceAuth            Success            Authorized
9         ForceAuth            Success            Authorized
10        ForceAuth            Success            Authorized
11        ForceAuth            Success            Authorized
12        ForceAuth            Success            Authorized
13        ForceAuth            Success            Authorized
14        ForceAuth            Success            Authorized
15        ForceAuth            Success            Authorized
16        ForceAuth            Success            Authorized
17        ForceAuth            Success            Authorized
18        ForceAuth            Success            Authorized
19        ForceAuth            Success            Authorized
20        ForceAuth            Success            Authorized
CTRL+C ESC q Quit SPACE n Next Page Enter Next Entry a All
```

## config 802.1x capability ports

| | |
|---|---|
| Purpose | Used to configure the 802.1x capability of a range of ports on the switch. |
| Syntax | **config 802.1x capability ports [<portlist> \| all] [authenticator \| none]** |
| Description | The **config 802.1x** command has four capabilities that can be set for each port. Authenticator, Supplicant, Authenticator and Supplicant, and None. |
| Parameters | <portlist> – Specifies a port or range of ports to be configured. |

| config 802.1x capability ports | |
|---|---|
| | all – Specifies all of the ports on the switch.<br><br>authenticator – A user must pass the authentication process to gain access to the network.<br><br>none – The port is not controlled by the 802.1x functions. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

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

```
DES-3526:4#config 802.1x capability ports 1 –10 authenticator
Command: config 802.1x capability ports 1-10 authenticator

Success.

DES-3526:4#
```

| 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 | <portlist> – Specifies a port or range of ports to be configured.<br><br>all – Specifies all of the ports on the switch.<br><br>default – Returns all of the ports in the specified range to their 802.1x default settings.<br><br>direction [both \| in] – Determines whether a controlled port blocks communication in both the receiving and transmitting directions, or just the receiving direction.<br><br>port_control – Configures the administrative control over the authentication process for the range of ports.The user has the following authentication options:<br><br>• force_auth – Forces the Authenticator for the port to become authorized. Network access is allowed. |

## config 802.1x auth_parameter

| | |
|---|---|
| | • auto – Allows the port's status to reflect the outcome of the authentication process.<br>• force_unauth – Forces the Authenticator for the port to become unauthorized. Network access will be blocked.<br><br>quiet_period <sec 0-65535> – Configures the time interval between authentication failure and the start of a new authentication attempt.<br><br>tx_period <sec 1-65535> - Configures the time to wait for a response from a supplicant (user) to send EAP Request/Identity packets.<br><br>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.<br><br>server_timeout <sec 1-65535> - Configure the length of time to wait for a response from a Radius server.<br><br>max_req <value 1-10> – Configures the number of times to retry sending packets to a supplicant (user).<br><br>reauth_period <sec 1-65535> – Configures the time interval between successive re-authentications.<br><br>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. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

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

```
DES-3526:4#config 802.1x auth_parameter ports 1–20 direction
both

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


Success.


DES-3526:4#
```

## config 802.1x auth_protocol

| | |
|---|---|
| Purpose | Used to configure the 802.1x authentication protocol on the switch. |
| Syntax | **config 802.1x auth_protocol [radius_eap \| radius_pap]** |
| Description | The config 802.1x auth_protocol command enables you to configure the authentication protocol. |

| config 802.1x auth_protocol | |
|---|---|
| Parameters | radius_eap \| radius_pap – Specify the type of authentication protocol desired. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To configure the authentication protocol on the switch:

```
DES-3526:4# config 802.1x auth_protocol radius_pap
Command: config 802.1x auth_protocol local radius_pap

 Success.

DES-3526:4#
```

| config 802.1x init | |
|---|---|
| Purpose | Used to initialize the 802.1x function on a range of ports. |
| Syntax | **config 802.1x init {port_based ports [<portlist> \| all] \| mac_based [ports] [ <portlist> \| all] {mac_address <macaddr>}]** |
| Description | The **config 802.1x init** command is used to immediately initialize the 802.1x functions on a specified range of ports or for specified MAC addresses operating from a specified range of ports. |
| Parameters | 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.<br><br>mac_based ports – This instructs the switch to initialize 802.1x functions based only on the MAC address. MAC addresses approved for initialization can then be specified.<br><br><portlist> – Specifies a port or range of ports to be configured.<br><br>mac_address <macaddr> - Enter the MAC address to be initialized.<br><br>all – Specifies all of the ports on the switch. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To initialize the authentication state machine of some or all:

```
DES-3526:4# config 802.1x init port_based ports all
Command: config 802.1x init port_based ports all

Success.

DES-3526:4#
```

| config 802.1x auth_mode | |
|---|---|
| Purpose | Used to configure the 802.1x authentication mode on the switch. |
| Syntax | **config 802.1x auth_mode {port_based \| mac_based]** |
| Description | The config 802.1x authentication mode command is used to enable either the port-based or MAC-based 802.1x authentication feature on the switch. |
| Parameters | port_based \| mac_based ports – The switch allows you to authenticate 802.1x by either port or MAC address. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To configure 802.1x authentication by MAC address:

```
DES-3526:4#config 802.1x auth_mode mac_based
Command: config 802.1x auth_mode mac_based

Success.

DES-3526:4#
```

| config 802.1x reauth | |
|---|---|
| Purpose | Used to configure the 802.1x re-authentication feature of the switch. |
| Syntax | **config 802.1x reauth {port_based ports [<portlist> \| all] \| mac_based [ports] [<portlist> \| all] {mac_address <macaddr>}]** |
| Description | The config 802.1x reauth command is used to re-authenticate a previously authenticated device based on port number. |
| Parameters | port_based – This instructs the switch to re-authorize 802.1x functions based only on the port number. Ports approved for re-authorization can then be specified.<br><br>mac_based ports – This instructs the switch to re-authorize 802.1x functions based only on the MAC address. MAC addresses approved for re-authorization can then be specified.<br><br><portlist> – Specifies a port or range of ports to be re-authorized.<br><br>mac_address <macaddr> - Enter the MAC address to be re-authorized.<br><br>all – Specifies all of the ports on the switch. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To configure 802.1x reauthentication for ports 1-18:

```
DES-3526:4#config 802.1x reauth port_based ports 1-18
Command: config 802.1x reauth port_based ports 1-18

Success.

DES-3526:4#
```

## 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 1-65535> \| acct_port <udp_port_number 1-65535>}]** |
| Description | The **config radius add** command is used to configure the settings the switch will use to communicate with a RADIUS server. |
| Parameters | <server_index 1-3> – Assigns a number to the current set of RADIUS server settings. Up to 3 groups of RADIUS server settings can be entered on the switch.<br><br><server_ip> – The IP address of the RADIUS server.<br><br>key – Specifies that a password and encryption key will be used between the switch and the Radius server.<br><br><passwd 32> – The shared-secret key used by the RADIUS server and the switch. Up to 32 characters can be used.<br><br>default – Uses the default udp port number in both the “auth_port” and “acct_port” settings.<br><br>auth_port <udp_port_number> – The UDP port number for authentication requests. The default is 1812.<br><br>acct_port <udp_port_number> – The UDP port number for accounting requests. The default is 1813. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To configure the RADIUS server communication setttings:

```
DES-3526:4#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-3526:4#
```

| 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-3526:4#config radius delete 1
Command: config radius delete 1

Success.

DES-3526:4#
```

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

| config radius | |
|---|---|
| | accounting requests. The default is 1813. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To configure the RADIUS settings:

```
DES-3526:4#config radius 1 10.48.74.121 key dlink default
Command: config radius 1 10.48.74.121 key dlink default

 Success.

DES-3526:4#
```

| 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-3526:4#show radius
Command: show radius

Idx  IP Address       Auth-Port   Acct-Port   Status      Key
                      No.         No.
-----  ---------------  ---------  ---------  ----------  ----------
1      10.1.1.1         1812       1813       Active      switch
2      20.1.1.1         1800       1813       Active      des3226
3      30.1.1.1         1812       1813       Active      dlink

Total Entries : 3

DES-3526:4#
```

# 21

# ACCESS CONTROL LIST (ACL) COMMANDS

The DES-3526 implements Access Control Lists that enable the switch to deny network access to specific devices or device groups based on IP settings or MAC address.

| Command | Parameters |
|---|---|
| create access_profile | [ ethernet{ vlan \| source_mac <macmask> \| destination_mac <macmask> \| 802.1p \| ethernet_type}\| ip { vlan \| source_ip_mask <netmask> \| destination_ip_mask <netmask> \| dscp \| [ icmp {type \| code } \| igmp {type } \| tcp {src_port_mask <hex 0x0-0xffff> \| dst_port_mask <hex 0x0-0xffff>\| flag_mask [all \| {urg \| ack \| psh \| rst \| syn \| fin}]} \| udp {src_port_mask <hex 0x0-0xffff> \| dst_port_mask <hex 0x0-xffff>} \| protocol_id_mask <hex0x0 - 0xFF> {user_define_mask <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff>} ]}\|packet_content_mask{offset_0-15 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> \| offset_16-31 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> \| offset_32-47 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> \| offset_48-63 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> \| offset_64-79 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff>}]{port[<portlist>\|all] \| profile_id <value 1-255> } |
| delete access_profile | <value 1-255> |
| config access_profile profile_id | <value 1-255>[ add access_id <value 1-255>[ ethernet {vlan <vlan_name 32> \| source_mac <macaddr> \| destination_mac <macaddr> \| 802.1p <value 0-7> \| ethernet_type <hex 0x0-0xffff> }\| ip {vlan <vlan_name 32> \| source_ip <ipaddr> \| destination_ip <ipaddr> \| dscp <value 0-63> \|[ icmp {type <value 0-255> code <value 0-255>} \| igmp {type <value 0-255>} \| tcp {src_port <value 0-65535> \| dst_port <value 0-65535> \| flag_mask [all \| {urg \| ack \| psh \| rst \| syn \| fin}]} \| udp {src_port <value 0-65535> \| dst_port <value 0-65535>} \| protocol_id <value 0 - 255> {user_define <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff>}]} \| packet_content_mask{offset_0-15 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> \| offset_16-31 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> \| offset_32-47 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> \| offset_48-63 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> \| offset_64-79 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff>}][ permit{replace_priority_with <value 0-7> \| replace_dscp_with <value 0-63> } \| deny] \| delete access_id <value 1-255> ] |
| show access_profile | {profile_id <value 1-255>} |

Due to a chipset limitation, the switch currently supports a maximum of 9 access profiles, each containing a maximum of 50 rules – with the additional limitation of 50 rules total for all 9 access profiles.

Access profiles allow you to establish criteria to determine whether or not the switch will forward packets based on the information contained in each packet's header. These criteria can be specified on a VLAN-by-VLAN basis.

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

**create access_profile ip source_ip_mask 255.255.255.0 profile_id 1**

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

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

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

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

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

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

## create access_profile

| | |
|---|---|
| Purpose | Used to create an access profile on the switch and to define which parts of each incoming frame's header the switch will examine. Masks can be entered that will be combined with the values the switch finds in the specified frame header fields. Specific values for the rules are entered using the **config access_profile** command, below. |
| Syntax | **[ 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-xffff>} \| protocol_id_mask <hex0x0 -0xFF> {user_define_mask <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff>} ]} \| packet_content_mask{offset_0-15 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> \| offset_16-31 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> \| offset_32-47 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> <hex 0x0-0xffffffff> \| offset_48-63 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> \| offset_64-79 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff>}] {port [<portlist>\|all] \| profile_id <value 1-255> }** |
| 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. |

## create access_profile

Parameters

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

- vlan – Specifies that the switch will examine the VLAN part of each packet header.
- source_mac <macmask> – Specifies a MAC address mask for the source MAC address. This mask is entered in the following hexadecimal format:
- destination_mac <macmask> – Specifies a MAC address mask for the destination MAC address.
- 802.1p – Specifies that the switch will examine the 802.1p priority value in the frame's header.
- ethernet_type – Specifies that the switch will examine the Ethernet type value in each frame's header.

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

- vlan – Specifies a VLAN mask.
- source_ip_mask <netmask> – Specifies an IP address mask for the source IP address.
- destination_ip_mask <netmask> – Specifies an IP address mask for the destination IP address.
- dscp – Specifies that the switch will examine the DiffServ Code Point (DSCP) field in each frame's header.
  - icmp – Specifies that the switch will examine the Internet Control Message Protocol (ICMP) field in each frame's header.
  - type – Specifies that the switch will examine each frame's ICMP Type field.
  - code – Specifies that the switch will examine each frame's ICMP Code field.
- igmp – Specifies that the switch will examine each frame's Internet Group Management Protocol (IGMP) field.
  - type – Specifies that the switch will examine each frame's IGMP Type field.
- tcp – Specifies that the switch will examine each frames Transport Control Protocol (TCP) field.
  - src_port_mask <hex 0x0-0xffff> – Specifies a TCP port mask for the source port.
  - dst_port_mask <hex 0x0-0xffff> – Specifies a TCP port mask for the destination port.
- flag_mask [ all | {urg | ack | psh | rst | syn | fin}] – Enter the

| create access_profile | |
|---|---|
| | appropriate flag_mask parameter. All incoming packets have TCP port numbers contained in them as the forwarding criterion. These numbers have flag bits asscociated 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 **all**, **urg** (urgent), **ack** (acknowledgement), **psh** (push), **rst** (reset), **syn** (synchronize) and **fin** (finish).<br><br>• udp – Specifies that the switch will examine each frame's Universal Datagram Protocol (UDP) field.<br><br>• src_port_mask <hex 0x0-0xffff> – Specifies a UDP port mask for the source port.<br><br>• dst_port_mask <hex 0x0-0xffff> – Specifies a UDP port mask for the destination port.<br><br>• protocol_id – Specifies that the switch will examine each frame's Protocol ID field.<br><br>• user_define_mask <hex 0x0-0xffffffff> – Specifies that the rule applies to the IP protocol ID and the mask options behind the IP header.<br><br>• packet_content_mask – Specifies that the switch will mask the packet header beginning with the offset value specified as follows:<br><br>• offset_0-15 – Enter a value in hex form to mask the packet from the beginning of the packet to the 16th byte.<br><br>• offset_16-31 - Enter a value in hex form to mask the packet from byte 16 to byte 31.<br><br>• offset_32-47 - Enter a value in hex form to mask the packet from byte 32 to byte 47.<br><br>• offset_48-63 - Enter a value in hex form to mask the packet from byte 48 to byte 63.<br><br>• offset_64-79- Enter a value in hex form to mask the packet from byte 64 to byte 79.<br><br>port<portlist> - Specifies a port or range of ports to be configured.<br><br>all – denotes all ports on the switch.<br><br>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 list rules:

```
DES-3526:4#create access_profile ip vlan
source_ip_mask 20.0.0.0 destination_ip_mask 10.0.0.0
dscp icmp type code permit profile_id 101

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


Success.


DES-3526:4#
```

## 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-3526:4# delete access_profile profile_id 1

Command: delete access_profile profile_id 1


Success.


DES-3526:4#
```

## 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. Specific values for the rules are entered using the **config access_profile** command, below. |
| Syntax | <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 |

## config access_profile

| | |
|---|---|
| | {src_port <value 0-65535> \| dst_port <value 0-65535> \| flag_mask [all \| {urg \| ack \| psh \| rst \| syn \| fin}]} \| udp {src_port <value 0-65535> \| dst_port <value 0-65535>} \| protocol_id <value 0 - 255> {user_define <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex0x0-0xffffffff>}]} \| packet_content_mask {offset_0-15 <hex0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> \| offset_16-31 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> \| offset_32-47 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> \| offset_48-63 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff> \| offset_64-79 <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex0x0-0xffffffff>}][ permit {replace_priority_with <value 0-7> \| replace_dscp_with <value 0-63> } \| deny] \| delete access_id <value 1-255> ] |
| Description | The **config access_profile** command is used to configure an access profile on the switch and to enter specific values that will be combined, using a logical AND operation, with masks entered with the **create access_profile** command, above. |
| Parameters | profile_id <value 1-255> – an integer between 1 and 8 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.<br><br>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.<br><br>ethernet – Specifies that the switch will look only into the layer 2 part of each packet.<br><br>• vlan <vlan_name 32> – Specifies that the access profile will apply to only to this VLAN.<br><br>• source_mac <macaddr> – Specifies that the access profile will apply to only packets with this source MAC address.<br><br>• destination_mac <macaddr> – Specifies that the access profile will apply to only packets with this destination MAC address.<br><br>• 802.1p <value 0-7> – Specifies that the access profile will apply only to packets with this 802.1p priority value.<br><br>• 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.<br><br>ip – Specifies that the switch will look into the IP fields in each packet.<br><br>• vlan <vlan_name 32> – – Specifies that the access profile will apply to only to this VLAN.<br><br>• source_ip <ipaddr> – Specifies that the access profile will apply to only packets with this source IP address. |

## config access_profile

- 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.
- priority <value 0-7> – Specifies that the access profile will apply to packets that contain this value in their 802.1p priority field of their header.
- dscp <value 0-63> – Allows you to specify a value to be written to the DSCP field of an incoming packet.
- 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.
- flag_mask – Enter the type of TCP flag to be masked. The choices are:
  - all: all flags are selected.
  - urg: TCP control flag (urgent)
  - ack: TCP control flag (acknowledgement)
  - psh: TCP control flag (push)
  - rst: TCP control flag (reset)
  - syn: TCP control flag (synchronize)
  - fin: TCP control flag (finish)

## config access_profile

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

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

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

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

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

- packet_content_mask – Specifies that the switch will mask the packet header beginning with the offset value specified as follows:

  - offset_0-15 – Enter a value in hex form to mask the packet from the beginning of the packet to the 15$^{th}$ byte.

  - offset_16-31 - Enter a value in hex form to mask the packet from byte 16 to byte 32.

  - offset_32-47 - Enter a value in hex form to mask the packet from byte 32 to byte 47.

  - offset_48-63 - Enter a value in hex form to mask the packet from byte 48 to byte 63.

- offset_64-79- Enter a value in hex form to mask the packet from byte 64 to byte 79.

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

- replace_priority with (0-7) – This parameter is specified if you want to change the 802.1p user priority of a packet that meets the specified criteria. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being transmitted from the switch.

replace_dscp with <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.

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

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

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

Example usage:

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

```
DES-3526:4# config access_profile profile_id 2 add access_id 1
ip source_ip 10.42.73.1 deny
Command: config access_profile profile_id 1 add access_id 1 ip
source_ip 10.42.73.1 deny

Success.

DES-3526:4#
```

| 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-3526:4#show access_profile
Command: show access_profile

Access Profile Table

Access Profile ID : 4
Type    : IP Frame Filter
Ports   : All
Masks   : VLAN
        ----------

ID  Mode
--- ------ ----------
1   Permit default
```

```
Access Profile ID : 246
Type    : IP Frame Filter
Ports   : All
Masks   : Source IP Addr
          ---------------
          255.0.0.0
ID  Mode
--- ------ ---------------

Access Profile ID : 247
Type    : Ethernet Frame Filter
Ports   : All
Masks   : 802.1p
          ------

ID  Mode
--- ------ ------

Access Profile ID : 248
Type    : Ethernet Frame Filter
Ports   : All
Masks   : VLAN
          ----------------

ID  Mode
--- ------ ----------------

Access Profile ID : 249
Type    : Packet Content Filter
Ports   : All
Masks   : Offset 0-15  : 0x00000000 00000000 00000000 00000000
          Offset 16-31 : 0x00000000 00000000 00000000 00000000
          Offset 32-47 : 0x00000000 00000000 00000000 00000000
          Offset 48-63 : 0x00000000 00000000 00000000 00000000
          Offset 64-79 : 0x00000000 00000000 00000000 00000000

ID  Mode
--- ------ ----------------------------------------------------

Access Profile ID : 250
Type    : Ethernet Frame Filter
Ports   : All
Masks   : VLAN
```

```
        ----------------

ID  Mode
--- ------ ----------------

Access Profile ID : 251
Type    : Ethernet Frame Filter
Ports   : All
Masks   : VLAN
        ----------------

ID  Mode
--- ------ ----------------

Access Profile ID : 252
Type    : Ethernet Frame Filter
Ports   : All
Masks   : VLAN
        ----------------

ID  Mode
--- ------ ----------------

Access Profile ID : 253
Type    : Ethernet Frame Filter
Ports   : All
Masks   : VLAN
        ----------------

ID  Mode
--- ------ ----------------

Total Entries : 1

DES-3526:4#
```

# 22

# 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 | <portlist> – Specifies a port or range of ports that will be configured for traffic segmentation.<br><br>forward_list – Specifies a range of ports that will receive forwarded frames from the ports specified in the portlist, above.<br><br>null – no ports are specified<br><br><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). |
| 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-3526:4# config traffic_segmentation 1-10 forward_list 11-15
Command: config traffic_segmentation 1-10 forward_list 11-15

Success.

DES-3526:4#
```

## show traffic_segmentation

| | |
|---|---|
| Purpose | Used to display the current traffic segmentation configuration on the switch. |

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

Example usage:

To display the current traffic segmentation configuration on the switch.

```
DES-3526:4#show traffic_segmentation
Command: show traffic_segmentation

Traffic Segmentation Table

Port   Forward Portlist
----   ----------------------------
1      1-26
2      1-26
3      1-26
4      1-26
5      1-26
6      1-26
7      1-26
8      1-26
9      1-26
10     1-26
11     1-26
12     1-26
13     1-26
14     1-26
15     1-26
16     1-26
17     1-26
18     1-26

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

# 23

# TIME AND SNTP COMMANDS

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

| Command | Parameters |
|---|---|
| config sntp | {primary <ipaddr> \| secondary <ipaddr> \| poll-interval <int 30-99999>} |
| 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 | primary – This is the primary server the SNTP information will be taken from.<br><br><ipaddr> – The IP address of the primary server.<br><br>secondary – This is the secondary server the SNTP information will be taken from in the event the primary server is unavailable.<br><br><ipaddr> – The IP address for the secondary server.<br><br>poll-interval – This is the interval between requests for updated SNTP information.<br><br><int 30-99999> – The polling interval ranges from 30 to 99,999 seconds. |

| config sntp | |
|---|---|
| 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-3526:4#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-3526:4#
```

| 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:

```
DES-3526:4#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-3526:4#
```

| 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 |

| enable sntp | |
|---|---|
| | 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-3526:4#enable sntp
Command: enable sntp

Success.

DES-3526:4#
```

| 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-3526:4#disable sntp
Command: disable sntp

Success.

DES-3526:4#
```

| config time | |
|---|---|
| Purpose | Used to manually configure system time and date settings. |
| Syntax | **config time <date ddmmmyyyy> <time hh:mm:ss>** |
| Description | This will configure the system time and date settings. These will be overridden if SNTP is configured and enabled. |

| config time | |
|---|---|
| Parameters | 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.<br><br>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. |
| 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-3526:4#config time 30jun2003 16:30:30
Command: config time 30jun2003 16:30:30

Success.

DES-3526:4#
```

| 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 | operator – Choose to add (+) or subtract (-) time to adjust for time zone relative to GMT.<br><br>hour – Select the number hours different from GMT.<br><br>min – Select the number of minutes difference added or subtracted to adjust the time zone. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To configure time zone settings:

```
DES-3526:4#config time_zone operator + hour 2 min 30
Command: config time_zone operator + hour 2 min 30

Success.

DES-3526:4#
```

## config dst

| | |
|---|---|
| Purpose | Used to enable and configure time adjustments to allow for the use of Daylight Savings Time (DST). |
| Syntax | **config dst [disable \| repeating {s_week <start_week 1-4,last> \| s_day <start_day sun-sat> \| s_mth <start_mth 1-12> \| s_time start_time hh:mm> \| e_week <end_week 1-4,last> \| e_day <end_day 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]}]** |
| 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 | disable -Disable the DST seasonal time adjustment for the switch.<br><br>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.<br><br>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.<br><br>s-week - Configure the week of the month in which DST begins.<br><br><start_week 1-4,last> - The number of the week during the month in which DST begins where 1 is the first week, 2 is the second week and so on, last is the last week of the month.<br><br>e-week - Configure the week of the month in which DST ends.<br><br><end_week 1-4,last> - The number of the week during the month in which DST ends where 1 is the first week, 2 is the second week and so on, last is the last week of the month.<br><br>s-wday – Configure the day of the week in which DST begins.<br><br><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)<br><br>e-wday - Configure the day of the week in which DST ends. |

| config dst | |
|---|---|
| | <end_weekday sun-sat> - The day of the week in which DST ends expressed using a three character abbreviation (sun, mon, tue, wed, thu, fri, sat)<br><br>s-mth - Configure the month in which DST begins.<br><br><start_mth 1-12> - The month to begin DST expressed as a number.<br><br>e-mth - Configure the month in which DST ends.<br><br><end_mth 1-12> - The month to end DST expressed as a number.<br><br>s-time – Configure the time of day to begin DST. Time is expressed using a 24-hour clock.<br><br>e-time - Configure the time of day to end DST. Time is expressed using a 24-hour clock.<br><br>s-date - Configure the specific date (day of the month) to begin DST. The date is expressed numerically.<br><br>e-date - Configure the specific date (day of the month) to begin DST. The date is expressed numerically.<br><br>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. |

Example usage:

To configure daylight savings time on the switch:

```
DES-3526:4#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-3526:4#
```

| 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. |

| show time | |
|---|---|
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

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

```
DES-3526:4#show time
Command: show time

Current Time Source : System Clock
Current Time        : 10 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  : 12 Oct 00:00

DES-3526:4#
```

# 24

# ARP COMMANDS

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

| Command | Parameters |
|---|---|
| create arpentry | <ipaddr> <macaddr> |
| config arpentry | <ipaddr> <macaddr> |
| delete arpentry | {[<ipaddr> \| all]} |
| show arpentry | {ipif <ipif_name 12> \| ipaddress <ipaddr> \| [static \| local]} |
| config arp_aging time | <value 0-65535> |
| clear arptable | |

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

## create arpentry

| | |
|---|---|
| Purpose | Used to make a static entry into the ARP table. |
| Syntax | **create arpentry <ipaddr> <macaddr>** |
| Description | This command is used to enter an IP address and the corresponding MAC address into the switch's ARP table. |
| Parameters | <ipaddr> – The IP address of the end node or station.<br><br><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-3526:4#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-3526:4#
```

## config arpentry

| | |
|---|---|
| Purpose | Used to configure a static entry in the ARP table. |
| Syntax | **config arpentry <ipaddr> <macaddr>** |
| Description | This command is used to configure a static entry in the ARP Table. The user may specify the IP address and the corresponding MAC address of an entry in the switch's ARP table. |

| config arpentry | |
|---|---|
| Parameters | <ipaddr> – The IP address of the end node or station.<br><br><macaddr> – The MAC address corresponding to the IP address above. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To configure a static arp entry for the IP address 10.48.74.12 and MAC address 00:50:BA:00:07:36:

```
DES-3526:4#config arpentry 10.48.74.12 00-50-BA-00-07-36
Command: config arpentry 10.48.74.12 00-50-BA-00-07-36

 Success.

DES-3526:4#
```

| 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.<br><br>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-3526:4#delete arpentry 10.48.74.121
Command: delete arpentry 10.48.74.121

 Success.

DES-3526:4#
```

| config arp_aging time | |
|---|---|
| Purpose | Used to configure the age-out timer for ARP table entries on the switch. |

| config arp_aging time | |
|---|---|
| Syntax | **config arp_aging time <value 0-65535>** |
| Description | This command sets the maximum amount of time, in minutes, that an ARP entry can remain in the switch's ARP table, without being accessed, before it is dropped from the table. |
| Parameters | time <value> – The ARP age-out time, in minutes. The value may be set in the range of 0-65535 minutes with a default setting of 20 minutes. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To configure ARP aging time:

```
DES-3526:4#config arp_aging time 30
Command: config arp_aging time 30

 Success.

DES-3526:4#
```

| show arpentry | |
|---|---|
| Purpose | Used to display the ARP table. |
| Syntax | **show arpentry {ipif <ipif_name 12> \| ipaddress <ipaddr> \| [static \| local]}** |
| Description | This command is used to display the current contents of the switch's ARP table. |
| Parameters | <ipif_name> – The name of the IP interface the end node or station for which the ARP table entry was made, resides on.<br><br><ipaddr> – The network address corresponding to the IP interface name above.<br><br>static – Displays the static entries to the ARP table.<br><br>local – Displays the local entries in the ARP table. |
| Restrictions | none. |

Example Usage:

To display the ARP table**:**

```
DES-3526:4#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-3526:4#
```

## 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-3526:4#clear arptable
Command: clear arptable

 Success.

DES-3526:4#
```

# 25

# ROUTING TABLE COMMANDS

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

| Command | Parameters |
|---|---|
| create iproute default | <ipaddr> {<metric 1-65535>} |
| delete iproute default | <network_address> |
| show iproute | {<network_address>} {static} |

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

## create iproute default

| | |
|---|---|
| Purpose | Used to create IP route entries to the switch's IP routing table. |
| Syntax | **create iproute default <ipaddr> {<metric 1-65535>}** |
| Description | This command is used to create a default static IP route entry to the switch's IP routing table. |
| Parameters | <ipaddr> – The gateway IP address for the next hop router.<br><br><metric> – Allows the entry of a routing protocol metric entry representing the number of routers between the Switch and the IP address above.The default setting is 1. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

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

```
DES-3526:4#create iproute default 10.48.74.121 1
Command: create iproute default 10.48.74.121 1

Success.

DES-3526:4#
```

## delete iproute default

| | |
|---|---|
| Purpose | Used to delete a default IP route entry from the switch's IP routing table. |
| Syntax | **delete iproute default** |
| Description | This command will delete an existing default entry from the switch's IP routing table. |
| Parameters | none |

| delete iproute default | |
|---|---|
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To delete the default IP route 10.53.13.254:

```
DES-3526:4#delete iproute default 10.53.13.254
Command: delete iproute default 10.53.13.254

 Success.

DES-3526:4#
```

| show iproute | |
|---|---|
| Purpose | Used to display the switch's current IP routing table. |
| Syntax | **show iproute {<network_address>} {static}** |
| Description | This command will display the switch's current IP routing table. |
| Parameters | <network_address> – IP address and netmask of the IP interface that is the destination of the route. You can specify the address and mask information using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8).<br><br>static – use this to display static iproute entries. |
| Restrictions | none. |

Example Usage:

To display the contents of the IP routing table:

```
DES-3526:4#show iproute
Command: show iproute

Routing Table

IP Address/Netmask    Gateway          Interface       Hops   Protocol
---------------       ---------------  ---------------  ----  -----------
  0.0.0.0             10.1.1.254       System           1     Default
 10.0.0.0/8           10.48.74.122     System           1     Local

Total Entries: 2

DES-3526:4#
```

# 26

# MAC NOTIFICATION COMMANDS

The MAC Notification Commands in the Command Line Interface (CLI) are listed, in the following table, along with their appropriate parameters.

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

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

| enable mac_notification | |
|---|---|
| Purpose | Used to enable global MAC address table notification on the switch. |
| Syntax | **enable mac_notification** |
| Description | This command is used to enable MAC Address Notification without changing configuration. |
| Parameters | None. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To enable MAC notification without changing basic configuration:

```
DES-3526:4#enable mac_notification
Command: enable mac_notification

Success.

DES-3526:4#
```

| disable mac_notification | |
|---|---|
| Purpose | Used to disable global MAC address table notification on the switch. |

## disable mac_notification

| | |
|---|---|
| Syntax | **disable mac_notification** |
| Description | This command is used to disable MAC Address Notification without changing configuration. |
| Parameters | None. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To disable MAC notification without changing basic configuration:

```
DES-3526:4#disable mac_notification
Command: disable mac_notification

Success.

DES-3526:4#
```

## config mac_notification

| | |
|---|---|
| Purpose | Used to configure MAC address notification. |
| Syntax | **config mac_notification {interval <int 1-2147483647> \| historysize <int 1-500>** |
| Description | MAC address notificiation is used to monitor MAC addresses learned and entered into the FDB. |
| Parameters | interval <sec> - time in seconds between notifications. The user may choose an interval between 1 and 2,147,483,647 seconds.<br><br>historysize <1 - 500> - maximum number of entries listed in the history log used for notification. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To configure the switch's MAC address table notification global settings:

```
DES-3526:4#config mac_notification interval 1 historysize 500
Command: config mac_notification interval 1 historysize 500

Success.

DES-3526:4#
```

## config mac_notification ports

## config mac_notification ports

| | |
|---|---|
| Purpose | Used to configure MAC address notification status settings. |
| Syntax | config mac_notification ports [<portlist \| all] [enable \| disable] |
| Description | MAC address notificiation is used to monitor MAC addresses learned and entered into the FDB. |
| Parameters | <portlist> Specify a port or range of ports to be configured.<br>all – Entering this command will set all ports on the system.<br>enable / disable – These commands will enable or disable MAC address table notification on the switch. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To enable port 7 for MAC address table notification:

```
DES-3526:4#config mac_notification ports 7 enable
Command: config mac_notification ports 7 enable

Success.

DES-3526:4#
```

## show mac_notification

| | |
|---|---|
| Purpose | Used to display the switch's MAC address table notification global settings |
| Syntax | **show mac_notification** |
| Description | This command is used to display the switch's MAC address table notification global settings. |
| Parameters | None. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To view the switch's MAC address table notification global settings:

```
DES-3526:4#show mac_notification
Command: show mac_notification

Global Mac Notification Settings

State          : Enabled
```

```
Interval        : 1
History Size  : 1

Success.

DES-3526:4#
```

## show mac_notification ports

| | |
|---|---|
| Purpose | Used to display the switch's MAC address table notification status settings |
| Syntax | **show mac_notification ports <portlist>** |
| Description | This command is used to display the switch's MAC address table notification status settings. |
| Parameters | <portlist> - Specify a port or group of ports to be viewed.<br><br>Entering this command without the parameter will display the MAC notification table for all ports. |
| Restrictions | None |

Example usage:

To display all port's MAC address table notification status settings:

```
DES-3526:4#show mac_notification ports
Command: show mac_notification ports

Port #  MAC Address Table Notification State
------  ------------------------------------
1               Disabled
2               Disabled
3               Disabled
4               Disabled
5               Disabled
6               Disabled
7               Disabled
8               Disabled
9               Disabled
10              Disabled
11              Disabled
12              Disabled
13              Disabled
14              Disabled
15              Disabled
16              Disabled
```

| | |
|---|---|
| **17** | **Disabled** |
| **18** | **Disabled** |
| **19** | **Disabled** |
| **20** | **Disabled** |
| **CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh** | |

# 27

# ACCESS AUTHENTICATION CONTROL COMMANDS

The TACACS / XTACACS / TACACS+ commands let you secure access to the switch using the TACACS / XTACACS / TACACS+ protocols. When a user logs in to the switch or tries to access the administrator level privelege, he or she is prompted for a password. If TACACS / XTACACS / TACACS+ authentication is enabled on the switch, it will contact a TACACS / XTACACS / TACACS+ server to verify the user. If the user is verified, he or she is granted access to the switch.

There are currently three versions of the TACACS security protocol, each a separate entity. The switch's software supports the following versions of TACACS:

- TACACS (Terminal Access Controller Access Control System) —Provides password checking and authentication, and notification of user actions for security purposes utilizing via one or more centralized TACACS servers, utilizing the UDP protocol for packet transmission.

- Extended TACACS (XTACACS) — An extension of the TACACS protocol with the ability to provide more types of authentication requests and more types of response condes than TACACS. This protocol also uses UDP to transmit packets.

- TACACS+ (Terminal Access Controller Access Control System plus) — Provides detailed access control for authentication for network devices. TACACS+ is facilitated through Authentication commands via one or more centralized servers. The TACACS+ protocol encrypts all traffic between the switch and the TACACS+ daemon, using the TCP protocol to ensure reliable delivery

In order for the TACACS / XTACACS / TACACS+ security function to work properly, a TACACS / XTACACS / TACACS+ server must be configured on a device other than the switch, called a *server host* and it must include usernames and passwords for authentication. When the user is prompted by the switch to enter usernames and passwords for authentication, the switch contacts the TACACS / XTACACS / TACACS+ server to verify, and the server will respond with one of three messages:

A) The server verifies the username and password, and the user is granted normal user priviledges on the switch.

B) The server will not accept the username and password and the user is denied access to the switch.

C) The server doesn't respond to the verification query. At this point, the switch receives the timeout from the server and then moves to the next method of verification configured in the method list.

The switch has three built-in *server groups*, one for each of the TACACS, XTACACS and TACACS+ protocols. These built-in *server groups* are used to authenticate users trying to access the switch. The users will set *server hosts* in a preferable order in the built-in *server group* and when a user tries to gain acess to the switch, the switch will ask the first *server host* for authentication. If no authentication is made, the second *server host* in the list will be queried, and so on. The built-in *server group* can only have hosts that are running the specified protocol. For example, the TACACS *server group* can only have TACACS *server hosts*.

The administrator for the switch may set up 5 different authentication techniques per user-defined *method list* (TACACS / XTACACS / TACACS+ / local / none) for authentication. These techniques will be listed in an order preferable, and defined by the user for normal user authentication on the switch, and may contain up to eight authentication techniques. When a user attempts to access the switch, the switch will select the first technique listed for authentication. If the first technique goes through its *server hosts* and no authentication is returned, the switch will then go to the next technique listed in the server group for authentication, until the authentication has been verified or denied, or the list is exhausted.

Please note that user granted access to the switch will be granted normal user privileges on the switch. To gain acess to admin level priveledges, the user must enter the `enable admin` command and then enter a password, which was previously configured by the administrator of the switch.

**NOTE:** TACACS, XTACACS and TACACS+ are separate entities and are not compatible. The switch and the server must be configured exactly the same, using the same protocol. (For example, if the switch is set up for TACACS authentication, so must be the host server.)

The TACACS (Terminal Access Controller Access Control System) commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

| Command | Parameters |
|---|---|
| enable authen_policy | |
| disable authen_policy | |
| show authen_policy | |
| create authen_login method_list_name | <string 15> |
| config authen_login | [default \| method_list_name <string 15>] method {tacacs \| xtacacs \| tacacs+ \| server_group <string 15> \| local \| none} |
| delete authen_login method_list_name | <string 15> |
| show authen_login | {default \| method_list_name <string 15> \| all} |
| create authen_enable method_list_name | <string 15> |
| config authen_enable | [default \| method_list_name <string 15>] method {tacacs \| xtacacs \| tacacs+ \| server_group <string 15> \| local_enable \| none} |
| delete authen_enable method_list_name | <string 15> |
| show authen_enable | [default \| method_list_name <string 15> \| all] |
| config authen application | {console \| telnet \| http \| all] [login \| enable] [default \| method_list_name <string 15>] |
| show authen application | |
| create authen server_group | <string 15> |
| config authen server_group | [tacacs \| xtacacs \| tacacs+ \| <string 15>] [add \| delete] server_host <ipaddr> protocol [tacacs \| xtacacs \| tacacs+] |
| delete authen server_group | <string 15> |
| show authen server_group | <string 15> |
| create authen server_host | <ipaddr> protocol [tacacs \| xtacacs \| tacacs+] {port <int 1-65535> \| key [<key_string 254> \| none] \| timeout <int 1-255> \| retransmit <int 1-255>} |
| config authen server_host | <ipaddr> protocol [tacacs \| xtacacs \| tacacs+] {port <int 1-65535> \| key [<key_string 254> \| none] \| timeout <int 1-255> \| retransmit <int 1-255>} |
| delete authen server_host | <ipaddr> protocol [tacacs \| xtacacs \| tacacs+] |
| show authen server_host | |
| config authen parameter response_timeout | <int 1-255> |

| Command | Parameters |
|---|---|
| config authen parameter attempt | <int 1-255> |
| show authen parameter | |
| enable admin | |
| config admin local_enable | <password 15> |

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

## enable authen_policy

| | |
|---|---|
| Purpose | Used to enable system access authentication policy. |
| Syntax | **enable authen_policy** |
| Description | This command will enable an administrator-defined authentication policy for users trying to access the switch. When enabled, the device will check the method list and choose a technique for user authentication upon login. |
| Parameters | None. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To enable the system access authentication policy:

```
DES-3526:4#enable authen_policy
Command: enable authen_policy

Success.

DES-3526:4#
```

## disable authen_policy

| | |
|---|---|
| Purpose | Used to disable system access authentication policy. |
| Syntax | **disable authen_policy** |
| Description | This command will disable the administrator-defined authentication policy for users trying to access the switch. When disabled, the switch will access the local user account database for username and password verification. In addition, the switch will now accept the local enable password as the authentication for normal users attempting to access administrator level priveledges. |
| Parameters | None. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To disable the system access authentication policy:

```
DES-3526:4#disable authen_policy
Command: disable authen_policy

Success.

DES-3526:4#
```

| show authen_policy | |
|---|---|
| Purpose | Used to display the system access authentication policy status on the switch. |
| Syntax | **show authen_policy** |
| Description | This command will show the current status of the access authentication policy on the switch |
| Parameters | None. |
| Restrictions | None. |

Example usage:

To display the system access authentication policy:

```
DES-3526:4#show authen_policy
Command: show authen_policy

Authentication Policy: Enabled

DES-3526:4#
```

| create authen_login method_list_name | |
|---|---|
| Purpose | Used to create a user defined method list of authentication methods for users logging on to the switch. |
| Syntax | **create authen_login method_list_name <string 15>** |
| Description | This command is used to create a list for authentication techniques for user login. The switch can support up to eight method lists, but one is reserved as a default and cannot be deleted. Multiple method lists must be created and configured separately. |
| Parameters | <string 15> Enter an alphanumeric string of up to 15 characters to define the given *method list*. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To create the method list “Trinity.”:

```
DES-3526:4#create authen_login method_list_name Trinity
Command: create authen_login method_list_name Trinity

Success.

DES-3526:4#
```

## config authen_login

| | |
|---|---|
| Purpose | Used to configure a user-defined or default *method list* of authentication methods for user login. |
| Syntax | **config authen_login [default \| method_list_name <string 15>] method {tacacs \| xtacacs \| tacacs+ \| server_group <string 15> \| local \| none}** |
| Description | This command will configure a user-defined or default *method list* of authentication methods for users logging on to the switch. The sequence of methods implemented in this command will affect the authentication result. For example, if a user enters a sequence of methods like *tacacs – xtacacs – local,* the switch will send an authentication request to the first *tacacs* host in the server group. If no response comes from the server host, the switch will send an authentication request to the second *tacacs* host in the server group and so on, until the list is exhausted. At that point, the switch will restart the same sequence with the following protocol listed, *xtacacs*. If no authentication takes place using the *xtacacs* list, the *local* account database set in the switch is used to authenticate the user. When the local method is used, the priviledge level will be dependant on the local account priveledge configured on the switch.<br><br>Successful login using any of these methods will give the user a "user" priviledge only. If the user wishes to upgrade his or her status to the administrator level, the user must implement the *enable admin* command, followed by a previously configured password. (*See the **enable admin** part of this section for more detailed information, concerning the **enable admin** command.)* |
| Parameters | default – The default method list for access authentication, as defined by the user. The user may choose one or a combination of up to four (4) of the following authentication methods:<br><br>▪ tacacs – Adding this parameter will require the user to be authenticated using the *tacacs* protocol from the remote tacacs *server hosts* of the tacacs *server group* list.<br><br>▪ xtacacs – Adding this parameter will require the user to be authenticated using the x*tacacs* protocol from the remote xtacacs *server hosts* of the xtacacs *server group* list.<br><br>▪ tacacs+ – Adding this parameter will require the user to be authenticated using the *tacacs* protocol from the remote tacacs+ *server hosts* of the tacacs+ *server group* list.<br><br>▪ server_group <string 15> - Adding this parameter will require the user to be authenticated using a user-defined server group previously configured on the switch. |

| config authen_login | |
|---|---|
| | ▪ local - Adding this parameter will require the user to be authenticated using the local *user account* database on the switch.<br><br>▪ none – Adding this parameter will require no authentication to access the switch.<br><br>method_list_name – Enter a previously implemented method list name defined by the user. The user may add one, or a combination of up to four (4) of the following authentication methods to this method list:<br><br>▪ tacacs – Adding this parameter will require the user to be authenticated using the *tacacs* protocol from a remote tacacs server.<br><br>▪ xtacacs – Adding this parameter will require the user to be authenticated using the x*tacacs* protocol from a remote xtacacs server.<br><br>▪ tacacs+ – Adding this parameter will require the user to be authenticated using the *tacacs* protocol from a remote tacacs server.<br><br>▪ server_group <string 15> - Adding this parameter will require the user to be authenticated using a user-defined server group previously configured on the switch.<br><br>▪ local - Adding this parameter will require the user to be authenticated using the local *user account* database on the switch.<br><br>▪ none – Adding this parameter will require no authentication to access the switch.<br><br>  **NOTE:** Entering *none* or *local* as an authentication protocol will override any other authentication that follows it on a method list or on the default method list. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To configure the user defined method list “Trinity” with authentication methods tacacs, xtacacs and local, in that order.

```
DES-3526:4#config authen_login method_list_name Trinity
method tacacs xtacacs local

Command: config authen_login method_list_name Trinity
method tacacs xtacacs local


Success.


DES-3526:4#
```

Example usage:

To configure the default method list with nauthentication methods xtacacs, tacacs+ and local, in that order:

```
DES-3526:4#config authen_login default method xtacacs
tacacs+ local
Command: config authen_login default method xtacacs
tacacs+ local

Success.

DES-3526:4#
```

## delete authen_login method_list_name

| | |
|---|---|
| Purpose | Used to delete a previously configured user defined method list of authentication methods for users logging on to the switch. |
| Syntax | **delete authen_login method_list_name <string 15>** |
| Description | This command is used to delete a list for authentication methods for user login. |
| Parameters | <string 15> Enter an alphanumeric string of up to 15 characters to define the given *method list* the user wishes to delete. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To delete the method list name “Trinity”:

```
DES-3526:4#delete authen_login method_list_name Trinity
Command: delete authen_login method_list_name Trinity

Success.

DES-3526:4#
```

## show authen_login

| | |
|---|---|
| Purpose | Used to display a previously configured user defined method list of authentication methods for users logging on to the switch. |
| Syntax | **show authen_login [default \| method_list_name <string 15> \| all]** |
| Description | This command is used to show a list of authentication methods for user login. |
| Parameters | default – Entering this parameter will display the default method list for users logging on to the switch.<br><br>method_list_name <string 15> Enter an alphanumeric string of up to 15 characters to define the given *method list* the user wishes to view.<br><br>all – Entering this parameter will display all the authentication login methods currewntly configured on the switch. |

## show authen_login

The window will display the following parameters:

- Method List Name – The name of a previously configured method list name.
- Priority – Defines which order the method list protocols will be queried for authentication when a user attempts to log on to the switch. Priority ranges from 1(highest) to 4 (lowest).
- Method Name – Defines which security protocols are implemeted, per method list name.
- Comment – Defines the type of Method. *User-defined Group* refers to server group defined by the user. *Built-in Group* refers to the tacacs, xtracacs and tacacs+ security protocols which are permanently set in the switch. *Keyword* refers to authentication using a technique INSTEAD of TACACS/XTACACS/TACACS+ which are local (authentication through the user account on the switch) and none (no authentication necessary to access any function on the switch).

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

```
DES-3526:4#show authen_login method_list_name Trinity
Command: show authen_login method_list_name Trinity

Method List Name  Priority   Method Name      Comment
----------------  --------   ---------------  ---------
Trinity           1          tacacs+          Built-in Group
                  2          tacacs           Built-in Group
                  3          Darren           User-defined Group
                  4          local            Keyword


DES-3526:4#
```

## create authen_enable method_list_name

Purpose: Used to create a user-defined method list of authentication methods for promoting normal user level privileges to Administrator level privileges on the switch.

Syntax: **create authen_enable method_list_name <string 15>**

Description: This command is used to promote users with normal level priveleges to Administrator level priviledges using authentication methods on the switch. Once a user acquires normal user level privileges on the switch, he or she must be authenticated by a method on the switch to gain administrator privileges on the switch, which is defined by the Administrator. A maximum of eight (8)

| create authen_enable method_list_name | |
|---|---|
| | enable method lists can be implemented on the switch. |
| Parameters | <string 15> Enter an alphanumeric string of up to 15 characters to define the given *enable method list* the user wishes to create. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To create a user-defined method list, named "Permit" for promoting user privileges to Adminstrator privileges:

```
DES-3526:4#create authen_enable method_list_name Permit
Command: show authen_login method_list_name Permit

Success.

DES-3526:4#
```

| config authen_enable | |
|---|---|
| Purpose | Used to configure a user-defined method list of authentication methods for promoting normal user level priveledges to Administrator level priveledges on the switch. |
| Syntax | **config authen_enable [default \| method_list_name <string 15>] method {tacacs \| xtacacs \| tacacs+ \| server_group <string 15> \| local_enable \| none}** |
| Description | This command is used to promote users with normal level priveleges to Administrator level priviledges using authentication methods on the switch. Once a user acquires normal user level privileges on the switch, he or she must be authenticated by a method on the switch to gain administrator privileges on the switch, which is defined by the Administrator. A maximum of eight (8) enable method lists can be implemented on the switch.<br><br>The sequence of methods implemented in this command will affect the authentication result. For example, if a user enters a sequence of methods like *tacacs – xtacacs – local_enable,* the switch will send an authentication request to the first *tacacs* host in the server group. If no verification is found, the switch will send an authentication request to the second *tacacs* host in the server group and so on, until the list is exhausted. At that point, the switch will restart the same sequence with the following protocol listed, *xtacacs*. If no authentication takes place using the *xtacacs* list, the *local_enable* password set in the switch is used to authenticate the user.<br><br>Successful authentication using any of these methods will give the user a "Admin" priviledge. |
| Parameters | default – The default method list for adminstration rights authentication, as defined by the user. The user may choose one or a combination of up to four (4) of the following authentication methods:<br><br>▪ tacacs – Adding this parameter will require the user to be |

| config authen_enable | |
|---|---|
| | authenticated using the *tacacs* protocol from the remote tacacs *server hosts* of the tacacs *server group* list.<br><br>▪ xtacacs – Adding this parameter will require the user to be authenticated using the x*tacacs* protocol from the remote xtacacs *server hosts* of the xtacacs *server group* list.<br><br>▪ tacacs+ – Adding this parameter will require the user to be authenticated using the *tacacs* protocol from the remote tacacs+ *server hosts* of the tacacs+ *server group* list.<br><br>▪ server_group <string 15> - Adding this parameter will require the user to be authenticated using a user-defined server group previously configured on the switch.<br><br>▪ local_enable - Adding this parameter will require the user to be authenticated using the local *user account* database on the switch.<br><br>▪ none – Adding this parameter will require no authentication to access the switch.<br><br>method_list_name – Enter a previously implemented method list name defined by the user (*create authen_enable*). The user may add one, or a combination of up to four (4) of the following authentication methods to this method list:<br><br>▪ tacacs – Adding this parameter will require the user to be authenticated using the *tacacs* protocol from a remote tacacs server.<br><br>▪ xtacacs – Adding this parameter will require the user to be authenticated using the x*tacacs* protocol from a remote xtacacs server.<br><br>▪ tacacs+ – Adding this parameter will require the user to be authenticated using the *tacacs* protocol from a remote tacacs server.<br><br>▪ server_group <string 15> - Adding this parameter will require the user to be authenticated using a user-defined server group previously configured on the switch.<br><br>▪ local_enable - Adding this parameter will require the user to be authenticated using the local *user account* database on the switch. The local enable password of the device can be configured using the "*config admin local_password*" command.<br><br>▪ none – Adding this parameter will require no authentication to access the administration level privileges on the switch. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To configure the user defined method list "Permit" with authentication methods tacacs, xtacacs and local, in that order.

```
DES-3526:4#config authen_enable method_list_name Trinity
method tacacs xtacacs local
```

```
Command: config authen_enable method_list_name Trinity
method tacacs xtacacs local

Success.

DES-3526:4#
```

Example usage:

To configure the default method list with authentication methods xtacacs, tacacs+ and local, in that order:

```
DES-3526:4#config authen_enable default method xtacacs
tacacs+ local
Command: config authen_enable default method xtacacs
tacacs+ local

Success.

DES-3526:4#
```

## delete authen_enable method_list_name

| | |
|---|---|
| Purpose | Used to delete a user-defined method list of authentication methods for promoting normal user level priveledges to Administrator level priveledges on the switch. |
| Syntax | **delete authen_enable method_list_name <string 15>** |
| Description | This command is used to delete a user-defined method list of authentication methods for promoting user level privileges to Adminstrator level privileges. |
| Parameters | <string 15> Enter an alphanumeric string of up to 15 characters to define the given *enable method list* the user wishes to delete. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To delete the user-defined method list “Permit”

```
DES-3526:4#delete authen_enable method_list_name Permit
Command: delete authen_enable method_list_name Permit

Success.

DES-3526:4#
```

## show authen_enable

| | |
|---|---|
| Purpose | Used to display the method list of authentication methods for promoting normal user level privileges to Administrator level privileges |

| show authen_enable | |
|---|---|
| | on the switch. |
| Syntax | **show authen_enable [default \| method_list_name <string 15> \| all]** |
| Description | This command is used to delete a user-defined method list of authentication methods for promoting user level privileges to Adminstrator level privileges. |
| Parameters | default – Entering this parameter will display the default method list for users attempting to gain access to Administrator level privileges on the switch.<br><br>method_list_name <string 15> Enter an alphanumeric string of up to 15 characters to define the given *method list* the user wishes to view.<br><br>all – Entering this parameter will display all the authentication login methods currently configured on the switch.<br><br>The window will display the following parameters:<br><br>▪ Method List Name – The name of a previously configured method list name.<br><br>▪ Priority – Defines which order the method list protocols will be queried for authentication when a user attempts to log on to the switch. Priority ranges from 1(highest) to 4 (lowest).<br><br>▪ Method Name – Defines which security protocols are implemeted, per method list name.<br><br>▪ Comment – Defines the type of Method. *User-defined Group* refers to *server groups* defined by the user. *Built-in Group* refers to the tacacs, xtracacs and tacacs+ security protocols which are permanently set in the switch. *Keyword* refers to authentication using a technique INSTEAD of TACACS/XTACACS/TACACS+ which are local (authentication through the *local_enable* password on the switch) and none (no authentication necessary to access any function on the switch). |
| Restrictions | None |

Example usage:

To display all method lists for promoting user level privileges to administrator level privileges.

```
DES-3526:4#show authen_enable all
Command: show authen_enable all

Method List Name  Priority   Method Name  Comment
----------------  --------   -----------  -------------------
Permit            1          tacacs+      Built-in Group
                  2          tacacs       Built-in Group
                  3          Darren       User-defined Group
                  4          local        Keyword
```

| | | | |
|---|---|---|---|
| **default** | **1** | **tacacs+** | **Built-in Group** |
| | **2** | **local** | **Keyword** |

**Total Entries : 2**

**DES-3526:4#**

## config authen application

| | |
|---|---|
| Purpose | Used to configure various applications on the switch for authentication using a previously configured method list. |
| Syntax | **config authen application [console \| telnet \| http \| all] [login \| enable] [default \| method_list_name <string 15>]** |
| Description | This command is used to configure switch configuration applications(console, telnet, web) for login at the user level and at the administration level (*authen_enable*) utilizing a previously configured method list. |
| Parameters | Application – choose the application to configure. The user may choose one of the following four applications to configure.<br>▪ console – choose this parameter to configure the command line interface login method.<br>▪ telnet – choose this parameter to configure the telnet login method.<br>▪ http – choose this parameter to configure the web interface login method.<br>▪ all – choose this parameter to configure all applications (console, telnet, web) login method.<br>login – Use this parameter to configure an application for normal login on the user level, using a previously configured method list.<br>enable - Use this parameter to configure an application for upgrading a normal user level to administrator privileges, using a previously configured method list.<br>default – Use this parameter to configure an application for user authentication using the default method list.<br>method_list_name <string 15> - Use this parameter to configure an application for user authentication using a prevoisly configured method list. Enter a alphanumeric string of up to 15 characters to define a previously configured method list. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To configure the default method list for the web interface:

**DES-3526:4#config authen application http login default**

```
Command: config authen application http login default

Success.

DES-3526:4#
```

## show authen application

| | |
|---|---|
| Purpose | Used to display authentication methods for the various applications on the switch. |
| Syntax | **show authen application** |
| Description | This command will display all of the authentication method lists (login, enable administrator privileges) for switch configuration applications(console, telnet, web) currently configured on the switch. |
| Parameters | None. |
| Restrictions | None. |

Example usage:

To display the login and enable method list for all applications on the switch:

```
DES-3526:4#show authen application
Command: show authen application

Application   Login Method List   Enable Method List
-----------   -----------------   ------------------------
Console       default             default
Telnet        Trinity             default
HTTP          default             default

DES-3526:4#
```

## create authen server_host

| | |
|---|---|
| Purpose | Used to create an authentication server host. |
| Syntax | **create authen server_host <ipaddr> protocol [tacacs \| xtacacs \| tacacs+] {port <int 1-65535> \| key [<key_string 254> \| none] \| timeout <int 1-255> \| retransmit < 1-255>}** |
| Description | This command will create an authentication server host for the tacacs/xtacacs/tacacs+ security protocols on the switch. When a user attempts to access the switch with authentication protocol enabled, the switch will send authentication packets to a remote tacacs/xtacacs/tacacs+ server host on a remote host. The tacacs/xtacacs/tacacs+ server host will then verify or deny the request and return the appropriate message to the switch. More than one authentication protocol can be run on the same physical server host but, remember that tacacs/xtacacs/tacacs+ are |

| create authen server_host | |
|---|---|
| | separate entities and are not compatible with each other. The maximum supported number of server hosts is 16. |
| Parameters | server_host <ipaddr> - The IP address of the remote server host the user wishes to add.<br><br>protocol – The protocol used by the server host. The user may choose one of the following:<br><br>▪ tacacs – Enter this parameter if the server host utilizes the tacacs protocol.<br><br>▪ xtacacs - Enter this parameter if the server host utilizes the xtacacs protocol.<br><br>▪ tacacs+ - Enter this parameter if the server host utilizes the tacacs+ protocol.<br><br>port <int 1-65535> Enter a number between 1 and 65535 to define the virtual port number of the authentication protocol on a server host. The default port number is 49 for tacacs/xtacacs/tacacs+ servers but the user may set a unique port number for higher security.<br><br>key <key_string 254> - Authentication key to be shared with a configured TACACS+ server only. Specify an alphanumeric string up to 254 characters.<br><br>timeout <int 1-255> - Enter the time in seconds the switch will wait for the server host to reply to an authentication request. The default value is 5 seconds.<br><br>retransmit <int 1-255> - Enter the value in the retransmit field to change how many times the device will resend an authentication request when the TACACS server does not respond. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To create a TACACS+ authentication server host, with port number 1234, a timeout value of 10 seconds and a retransmit count of 5.

```
DES-3526:4#create authen server_host 10.1.1.121 protocol
tacacs+ port 1234 timeout 10 retransmit 5

Command: create authen server_host 10.1.1.121 protocol tacacs+
port 1234 timeout 10 retransmit 5


Success.


DES-3526:4#
```

| config authen server_host | |
|---|---|
| Purpose | Used to configure a user-defined authentication server host. |

## config authen server_host

| | |
|---|---|
| Syntax | **create authen server_host <ipaddr> protocol [tacacs \| xtacacs \| tacacs+] {port <int 1-65535> \| key [<key_string 254> \| none] \| timeout <int 1-255> \| retransmit < 1-255>}** |
| Description | This command will configure a user-defined authentication server host for the tacacs/xtacacs/tacacs+ security protocols on the switch. When a user attempts to access the switch with authentication protocol enabled, the switch will send authentication packets to a remote tacacs/xtacacs/tacacs+ server host on a remote host. The tacacs/xtacacs/tacacs+ server host will then verify or deny the request and return the appropriate message to the switch. More than one authentication protocol can be run on the same physical server host but, remember that tacacs/xtacacs/tacacs+ are separate entities and are not compatible with each other. The maximum supported number of server hosts is 16. |
| Parameters | server_host <ipaddr> - The IP address of the remote server host the user wishes to alter.<br><br>protocol – The protocol used by the server host. The user may choose one of the following:<br><br>▪ tacacs – Enter this parameter if the server host utilizes the tacacs protocol.<br><br>▪ xtacacs - Enter this parameter if the server host utilizes the xtacacs protocol.<br><br>▪ tacacs+ - Enter this parameter if the server host utilizes the tacacs+ protocol.<br><br>port <int 1-65535> Enter a number between 1 and 65535 to define the virtual port number of the authentication protocol on a server host. The default port number is 49 for tacacs/xtacacs/tacacs+ servers but the user may set a unique port number for higher security.<br><br>key <key_string 254> - Authentication key to be shared with a configured TACACS+ server only. Specify an alphanumeric string up to 254 characters or choose none.<br><br>timeout <int 1-255> - Enter the time in seconds the switch will wait for the server host to reply to an authentication request. The default value is 5 seconds.<br><br>retransmit <int 1-255> - Enter the value in the retransmit field to change how many times the device will resend an authentication request when the TACACS server does not respond. This field is inoperable for the tacacs+ protocol. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To configure a TACACS+ authentication server host, with port number 4321, a timeout value of 12 seconds and a retransmit count of 4.

```
DES-3526:4#config authen server_host 10.1.1.121 protocol
tacacs+ port 4321 timeout 12 retransmit 4
```

```
Command: config authen server_host 10.1.1.121 protocol tacacs+
port 4321 timeout 12 retransmit 4

Success.

DES-3526:4#
```

## delete authen server_host

| | |
|---|---|
| Purpose | Used to delete a user-defined authentication server host. |
| Syntax | **delete authen server_host <ipaddr> protocol [tacacs \| xtacacs \| tacacs+]** |
| Description | This command is used to delete a user-defined authentication server host previously created on the switch. |
| Parameters | server_host <ipaddr> - The IP address of the remote server host the user wishes to delete.<br><br>protocol – The protocol used by the server host the user wishes to delete. The user may choose one of the following:<br><br>▪ tacacs – Enter this parameter if the server host utilizes the tacacs protocol.<br><br>▪ xtacacs - Enter this parameter if the server host utilizes the xtacacs protocol.<br><br>▪ tacacs+ - Enter this parameter if the server host utilizes the tacacs+ protocol. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To delete a user-defined TACACS+ authentication server host:

```
DES-3526:4#delete authen server_host 10.1.1.121 protocol
tacacs+
Command: delete authen server_host 10.1.1.121 protocol tacacs+

Success.

DES-3526:4#
```

## show authen server_host

| | |
|---|---|
| Purpose | Used to view a user-defined authentication server host. |
| Syntax | **show authen server_host** |
| Description | This command is used to view user-defined authentication server hosts previously created on the switch. |

| show authen server_host | |
|---|---|
| | The following parameters are displayed:<br><br>IP address – The IP address of the authentication server host.<br><br>Protocol – he protocol used by the server host. Possible results will include tacacs, xtacacs and tacacs+.<br><br>Port – The virtual port number on the server host. The default value is 49.<br><br>Timeout - The time in seconds the switch will wait for the server host to reply to an authentication request.<br><br>Retransmit - The value in the retransmit field denotes how many times the device will resend an authentication request when the TACACS server does not respond. This field is inoperable for the tacacs+ protocol.<br><br>Key - Authentication key to be shared with a configured TACACS+ server only. |
| Parameters | None. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To view authenticaion server hosts currently set on the switch:

```
DES-3526:4#show authen server_host
Command: show authen server_host

IP Address    Protocol    Port  Timeout  Retransmit  Key
---------------  --------     -----  -------     ---------------  --------
10.53.13.94   TACACS    49    5          2             No Use

Total Entries : 1

DES-3526:4#
```

| create authen server_group | |
|---|---|
| Purpose | Used to create a user-defined authentication server group. |
| Syntax | **create authen server_group <string 15>** |
| Description | This command will create an authentication server group. A server group is a technique used to group tacacs/xtacacs/tacacs+ server hosts into user defined categories for authentication using method lists. The user may add up to eight (8) authentication server hosts to this group using the **config authen server_group** command. |
| Parameters | <string 15> Enter an alphanumeric string of up to 15 characters to define the newly created server group. |

## create authen server_group

| | |
|---|---|
| | define the newly created server group. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To create the server group "group_1":

```
DES-3526:4#create server_group group_1
Command: create server_group group_1

Success.

DES-3526:4#
```

## config authen server_group

| | |
|---|---|
| Purpose | Used to create a user-defined authentication server group. |
| Syntax | **config authen server_group [tacacs \| xtacacs \| tacacs+ \| <string 15>] [add \| delete] server_host <ipaddr> protocol [tacacs \| xtacacs \| tacacs+]** |
| Description | This command will configure an authentication server group. A server group is a technique used to group tacacs/xtacacs/tacacs+ server hosts into user defined categories for authentication using method lists. The user may define the type of server group by protocol or by previously defined server group. Up to eight (8) authentication server hosts may be added to any particular group |
| Parameters | server_group - The user may define the group by protocol groups built into the switch(tacacs/xtacacs/tacacs+), or by a user-defined group previously created using the create authen server_group command.<br>▪ tacacs – Use this parameter to utilize the built-in tacacs server protocol on the switch. Only server hosts utilizing the tacacs protocol may be added to this group.<br>▪ xtacacs – Use this parameter to utilize the built-in xtacacs server protocol on the switch. Only server hosts utilizing the xtacacs protocol may be added to this group.<br>▪ tacacs+ – Use this parameter to utilize the built-in tacacs+ server protocol on the switch. Only server hosts utilizing the tacacs+ protocol may be added to this group.<br>▪ <string 15> Enter an alphanumeric string of up to 15 characters to define the previously created server group. This group may add any combination of server hosts to it, regardless of protocol.<br>add/delete – Enter the correct parameter to add or delete a server host from a server group.<br>server_host <ipaddr> - Enter the IP address of the previously |

| config authen server_group | |
|---|---|
| | configured server host the user wishes to add or delete.<br><br>protocol – Enter the protocol utilized by the server host. There are three options:<br><br>▪ tacacs – Use this parameter to define the protocol if the server host is using the tacacs authentication protocol.<br><br>▪ xtacacs – Use this parameter to define the protocol if the server host is using the xtacacs authentication protocol.<br><br>▪ tacacs+ – Use this parameter to define the protocol if the server host is using the tacacs+ authentication protocol. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To add an authentication host to server group "group_1":

```
DES-3526:4# config authen server_group group_1
add server_host 10.1.1.121 protocol tacacs+

Command: config authen server_group group_1 add
server_host 10.1.1.121 protocol tacacs+


Success.


DES-3526:4#
```

| delete authen server_group | |
|---|---|
| Purpose | Used to delete a user-defined authentication server group. |
| Syntax | **delete authen server_group <string 15>** |
| Description | This command will delete an authentication server group. |
| Parameters | <string 15> Enter an alphanumeric string of up to 15 characters to define the previously created server group the user wishes to delete. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To delete the server group "group_1":

```
DES-3526:4#delete server_group group_1

Command: delete server_group group_1


Success.


DES-3526:4#
```

## show authen server_group

| | |
|---|---|
| Purpose | Used to view authentication server groups on the switch. |
| Syntax | **show authen server_group <string 15>** |
| Description | This command will display authentication server groups currently configured on the switch.<br><br>This command will display the following fields:<br><br>**Group Name**: The name of the server group currently configured on the switch, including built in groups and user defined groups.<br><br>**IP Address**: The IP address of the server host.<br><br>**Protocol**: The authentication protocol used by the server host. |
| Parameters | <string 15> Enter an alphanumeric string of up to 15 characters to define the previously created server group the user wishes to view.<br><br>Entering this command without the <string> parameter will display all authentication server groups on the switch. |
| Restrictions | None. |

```
DES-3526:4#show authen server_group
Command: show authen server_group

Group Name    IP Address                Protocol
--------------  ---------------         --------
Darren          10.53.13.2              TACACS
tacacs          10.53.13.94             TACACS
tacacs+         (This group has no entry)
xtacacs         (This group has no entry)

Total Entries : 4

DES-3526:4#
```

## config authen parameter response_timeout

| | |
|---|---|
| Purpose | Used to configure the amount of time the switch will wait for a user to enter authentication before timing out. |
| Syntax | **config authen parameter response_timeout <int 1-255>** |
| Description | This command will set the time the switch will wait for a response of authentication from the user. |
| Parameters | response_timeout <int 1-255> - Set the time, in seconds, the switch will wait for a response of authentication from the user attempting to |

| config authen parameter response_timeout | |
|---|---|
| | log in from the command line interface or telnet interface. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To configure the response timeout for 60 seconds:

```
DES-3526:4# config authen parameter response_timeout 60
Command: config authen parameter response_timeout 60

Success.

DES-3526:4#
```

| config authen parameter attempt | |
|---|---|
| Purpose | Used to configure the maximum number of times the switch will accept authentication attempts. |
| Syntax | **config authen parameter attempt <int 1-255>** |
| Description | This command will configure the maximum number of times the switch will accept authentication attempts. Users failing to be authenticated after the set amount of attempts will be denied access to the switch and will be locked out of further authentication attempts. Command line interface users will have to wait 60 seconds before another authentication attempt. Telnet users will be disconnected from the switch. |
| Parameters | parameter attempt <int 1-255> - Set the maximum number of attempts the user may try to become authenticated by the switch, before being locked out. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To set the maximum number of authentication attempts at 5:

```
DES-3526:4# config authen parameter attempt 5
Command: config authen parameter attempt 5

Success.

DES-3526:4#
```

| show authen parameter | |
|---|---|
| Purpose | Used to display the authentication parameters currently configured on the switch. |

## show authen parameter

| | |
|---|---|
| Syntax | **show authen parameter** |
| Description | This command will display the authentication parameters currently configured on the switch, including the response timeout and user authentication attempts.<br><br>This command will display the following fields:<br><br>Response timeout – The configured time allotted for the switch to wait for a response of authentication from the user attempting to log in from the command line interface or telnet interface.<br><br>User attempts: The maximum number of attempts the user may try to become authenticated by the switch, before being locked out. |
| Parameters | None. |
| Restrictions | None. |

```
DES-3526:4#show authen parameter
Command: show authen parameter

Response timeout: 60 seconds
User attempts     : 5

DES-3526:4#
```

## enable admin

| | |
|---|---|
| Purpose | Used to promote user level privileges to administrator level privileges |
| Syntax | **enable admin** |
| Description | This command is for users who have logged on to the switch on the normal user level, to become promoted to the administrator level. After logging on to the switch users, will have only user level privileges. To gain acess to administrator level privileges, the user will enter this command and will have to enter an authentication password. Possible authentication methods for this function include tacacs, xtacacs, tacacs+, user defined server groups, local enable (local account on the switch), or no authentication(none). Because xtacacs and tacacs do not support the enable function, the user must create a special account on the server host which has the username “enable”, and a password configured by the administrator that will support the “enable” function. This function becomes inoperable when the authentication policy is disabled. |
| Parameters | None. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To enable administrator privileges on the switch:

```
DES-3526:4#enable admin
Password: ******

DES-3526:4#
```

| config admin local_enable | |
|---|---|
| Purpose | Used to configure the local enable password for administrator level privileges. |
| Syntax | **config admin local_enable** |
| Description | This command will configure the locally enabled password for the *enable admin* command. When a user chooses the "*local_enable*" method to promote user level privileges to administrator privileges, he or she will be prompted to enter the password configured here, that is set locally on the switch. |
| Parameters | <password 15> - After entering this command, the user will be prompted to enter the old password, then a new password in an alphanumeric string of no more than 15 characters, and finally prompted to enter the new password again to confirm. See the example below. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To configure the password for the "local_enable" authentication method.

```
DES-3526:4#config admin local_enable
Command: config admin local_ebable

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

DES-3526:4#
```

# 28

# SINGLE IP MANAGEMENT COMMANDS

Simply put, Single IP Management is a concept that will stack switches together over Ethernet instead of using stacking ports or modules. Switches using Single IP Management(labeled here as SIM) must conform to the following rules:

- SIM is an optional feature on the switch and can easily be enabled or disabled. SIM grouping has no effect on the normal operation of the switch in the user's network.
- There are three classifications for switches using SIM. The **Commander Switch(CS)**, which is the master switch of the group, **Member Switch(MS)**, which is a switch that is recognized by the CS a member of a SIM group, and a **Candidate Switch(CaS)**, which is a switch that has a physical link to the SIM group but has not been recognized by the CS as a member of the SIM group.
- A SIM group can only have one Commander Switch(CS).
- All switches in a particular SIM group must be in the same IP subnet(broadcast domain). Members of a SIM group cannot cross a router.
- A SIM group accepts up to 32 switches (numbered 0-31), including the Commander Switch(numbered 0).
- There is no limit to the number of SIM groups in the same IP subnet (broadcast domain), however a single switch can only belong to one group.
- If multiple VLANs are configured, the SIM group will only utilize the default VLAN on any switch.
- SIM allows intermediate devices that do not support SIM. This enables the user to manage a switch that are more than one hop away from the CS.

The SIM group is a group of switches that are managed as a single entity. The DES-3526 may take on three different roles:

**Commander Switch(CS)** – This is a switch that has been manually configured as the controlling device for a group, and takes on the following characteristics:

- It has an IP Address.
- It is not a command switch or member switch of another Single IP group.
- It is connected to the member switches through its management VLAN.

**Member Switch(MS)** – This is a switch that has joined a single IP group and is accessible from the CS, and it takes on the following characteristics:

- It is not a CS or MS of another IP group.
- It is connected to the CS through the CS management VLAN.

**Candidate Switch(CaS)** – This is a switch that is ready to join a SIM group but is not yet a member of the SIM group. The Candidate Switch may join the SIM group through an automatic function of the DES-3526, or by manually configuring it to be a MS of a SIM group. A switch configured as a CaS is not a member of a SIM group and will take on the following characteristics:

- It is not a CS or MS of another Single IP group.
- It is connected to the CS through the CS management VLAN

The following rules also apply to the above roles:

1. Each device begins in a Commander state.
2. CS's must change their role to CaS and then to MS, to become a MS of a SIM group. Thus the CS cannot directly be converted to a MS.
3. The user can manually configure a CS to become a CaS.
4. A MS can become a CaS by:
   a. Being configured as a CaS through the CS.
   b. If report packets from the CS to the MS time out.
5. The user can manually configure a CaS to become a CS

6. The CaS can be configured through the CS to become a MS.

After configuring one switch to operate as the CS of a SIM group, additional DES-3526 switches may join the group by either an automatic method or by manually configuring the switch to be a MS. The CS will then serve as the in band entry point for access to the MS. The CS's IP address will become the path to all MS's of the group and the CS's Administrator's password, and/or authentication will control access to all MS's of the SIM group.

With SIM enabled, the applications in the CS will redirect the packet instead of executing the packets. The applications will decode the packet from the administrator, modify some data, then send it to the MS. After execution, the CS may receive a response packet from the MS, which it will encode and send it back to the administrator.

When a CS becomes a MS, it automatically becomes a member of first SNMP community (include read/write and read only) to which the CS belongs. However if a MS has its own IP address, it can belong to SNMP communities to which other switches in the group, including the CS, do not belong.

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

| Command | Parameters |
|---|---|
| enable sim | |
| disable sim | |
| show sim | {[candidates{<candidate_id 1-32>} \| members{ <member_id 1-32> } \| group commander_mac <macaddr>}] \| neighbor_table} |
| reconfig | {member_id <value 1-32> \| exit} |
| config sim_group | [ add <candidate_id 1-32> {<password>} \| delete <member_id 1-32> ] |
| config sim | [{[ commander { group_name <groupname 64> \| candidate] \| dp_interval <sec 30-60> \| hold_time <sec 100-300>} |
| download sim_ms | [ firmware <ipaddr> <path_filename 64> {section_id <int 1-2>} \| configuration <ipaddr> <path_filename 64> {increment}] |
| upload sim_ms configuration | <ipaddr> <path_filename 64> <member_id 1-32> |

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

| enable sim | |
|---|---|
| Purpose | Used to enable Single IP Management(SIM) on the switch |
| Syntax | **enable sim** |
| Description | This command will enable SIM globally on the switch. SIM features and functions will not function properly unless this function is enabled. |
| Parameters | None. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To enable SIM on the switch:

```
DES-3526:4#enable sim
Command: enable sim

Success.
```

```
DES-3526:4#
```

## disable sim

| | |
|---|---|
| Purpose | Used to disable Single IP Management(SIM) on the switch |
| Syntax | **disable sim** |
| Description | This command will disable SIM globally on the switch.. |
| Parameters | None. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To disable SIM on the switch:

```
DES-3526:4#disable sim
Command: disable sim

Success.

DES-3526:4#
```

## show sim

| | |
|---|---|
| Purpose | Used to view the current information regarding the SIM group on the switch. |
| Syntax | **show sim {[candidates{<candidate_id 1-32>} \| members{ <member_id 1-32>} \| group commander_mac <macaddr>} ] neighbor}** |
| Description | This command will display the current information regarding the SIM group on the switch, including the following:<br><br>SIM Version - Displays the current Single IP Management version on the switch.<br><br>Firmware Version - Displays the current Firmware version on the switch.<br><br>Device Name - Displays the user-defined device name on the switch.<br><br>MAC Address - Displays the MAC Address of the switch.<br><br>Capabilities – Displays the type of switch, be it Layer 2 (L2) or Layer 3 (L3).<br><br>Platform – Switch Description including name and model number.<br><br>SIM State –Displays the current Single IP Management State of the switch, whether it be enabled or disabled. |

| show sim | |
|---|---|
| | Role State – Displays the current role the switch is taking, including Commander, Member or Candidate. A Stand-alone switch will always have the commander role.<br><br>Discovery Interval - Time in seconds the switch will send discovery packets out over the network.<br><br>Hold time – Displays the time in seconds the switch will hold discovery results before dropping it or utilizing it. |
| Parameters | candidates <candidate_id 1-32> - Entering this parameter will display information concerning candidates of the SIM group. To view a specific candidate, include that candidate's id number, listed from 1 to 32.<br><br>members <member_id 1-32> Entering this parameter will display information concerning members of the SIM group. To view a specific member, include that member's id number, listed from 1 to 32.<br><br>group commander_mac <macaddr>- Entering this parameter will display information concerning the SIM group. To view a specific group, include the commander's MAC address of the group.<br><br>neighbor – Entering this parameter will display neighboring devices of the switch. A SIM neighbor is defined as a switch that is physically connected to the switch but is not part of the SIM group. This screen will produce the following results:<br><br>Port – Displays the physical port number of the commander switch where the uplink to the neighbor switch is located.<br><br>MAC Address – Displays the MAC Address of the neighbor switch.<br><br>Role – Displays the role(CS, CaS, MS) of the neighbor switch. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To show the SIM information in detail:

```
DES-3526:4#show sim
Command: show sim

SIM Version          : VER-1
Firmware Version     : Build 1.00-B13
Device Name          :
MAC Address          : 00-35-26-11-11-00
Capabilities         : L3
Platform             : DES-3526 Fast-Ethernet Switch
SIM State            : Enabled
```

```
Role State              : Commander
Discovery Interval      : 60 sec
Hold Time               : 180 sec

DES-3526:4#
```

To show the candidate information in summary, if the candidate id is specified:

```
DES-3526:4#show sim candidate
Command: show sim candidate

ID  MAC Address         Platform /              Hold    Firmware    Device Name
                        Capability              Time    Version
--- ----------------    ----------------------  -----   ---------   ----------------
 1  00-01-02-03-04-00   DES-3526 L2 Switch      40      1.00-B06    The Man

 2  00-55-55-00-55-00   DES-3526 L2 Switch      140     1.00-B06    default master

Total Entries: 2

DES-3526:4#
```

To show the member information in summary, if the member id is specified:

```
DES-3526:4#show sim  member
Command: show sim  member

ID   MAC Address        Platform /              Hold    Firmware    Device Name
                        Capability              Time    Version
---  ----------------   ----------------------  ----    ---------   ----------------
 1  00-01-02-03-04-00   DES-3526 L2 Switch      40      1.00-B06     The Man

 2  00-55-55-00-55-00   DES-3526 L2 Switch      140     1.00-B06    default master

Total Entries: 2

DES-3526:4#
```

To show other groups information in summary, if group is specified:

```
DES-3526:4#show sim group
Command: show sim group

SIM Group Name : default

ID  MAC Address         Platform /              Hold    Firmware    Device Name
                        Capability              Time    Version
--- ----------------    ----------------------  -----   ---------   ----------------
```

```
*1  00-01-02-03-04-00  DES-3526 L2 Switch    40       1.00-B06       Trinity
 2  00-55-55-00-55-00   DES-3526 L2 Switch    140      1.00-B06       default master

SIM Group Name : SIM2

ID  MAC Address        Platform /            Hold     Firmware    Device Name
                       Capability            Time     Version
--- -----------------  ----------------------  - -----  ---------  ----------------
*1  00-01-02-03-04-00   DES-3526 L2 Switch    40       1.00-B06       Neo
 2  00-55-55-00-55-00    DES-3526 L2 Switch    140      1.00-B06       default master

'*' means commander switch.

DES-3526:4#
```

Example usage:

To view SIM neighbors:

```
DES-3526:4#show sim neighbor
Command: show sim neighbor

Neighbor Info Table

Port    MAC Address       Role
------   -----------------      ---------
23      00-35-26-00-11-99   Commander
23      00-35-26-00-11-91   Member
24      00-35-26-00-11-90   Candidate

Total Entries: 3

DES-3526:4#
```

## reconfig

| | |
|---|---|
| Purpose | Used to connect to a member switch, through the commander switch using telnet. |
| Syntax | **reconfig {member_id <value 1-32 \| exit}** |
| Description | This command is used to reconnect to a member switch using telnet. |
| Parameters | member_id <value 1-32> - Select the id number of the member switch the user desires to configure.<br><br>exit – This command is used to exit from managing the member switch and will return to managing the commander switch. |

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

Example usage:

To connect to the MS, with member id 2, through the CS, using the command line interface:

```
DES-3526:4#reconfig  member_id 2
Command: reconfig  member_id 2


DES-3526:4#
Login:
```

| config sim_group | |
|---|---|
| Purpose | Used to add candidates and delete members from the SIM group. |
| Syntax | **config sim [add <candidate_id 1-32> {<password>} \| delete <member_id 1-32>]** |
| Description | This command is used to add candidates and delete members from the SIM group by id number. |
| Parameters | add <candidate_id> <password> - Use this parameter to change a candidate switch(CaS) to a member switch(MS) of a SIM group. The CaS may be defined by its ID number and a password (if necessary).<br><br>delete <member_id 1-32> - Use this parameter to delete a member switch of a SIM group. The member switch should be defined by it ID number. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To add a member:

```
DES-3526:4#config sim_group add 2
Command: config sim_group add 2


Please wait for ACK...
GM Config Success !!!


Success.


DES-3526:4#
```

To delete a member:

```
DES-3526:4# config sim delete 1
Command: config sim delete 1
```

```
Please wait for ACK...
Success.

DES-3526:4#
```

## config sim

| | |
|---|---|
| Purpose | Used to configure role parameters for the SIM protocol on the switch. |
| Syntax | **config sim [{[ commander {group_name <groupname 64> \| candidate ] \| dp_interval <30-90> \| hold_time <sec 100-300>}]** |
| Description | This command is used to configure parameters of switches of the SIM. |
| Parameters | commander – Use this parameter to configure the commander switch for the following parameters:<br>▪ group_name <groupname 64> - Used to update the name of the group. Enter an alphanumeric string of up to 64 characters to rename the SIM group.<br>▪ dp_interval – The user may set the discovery protocol interval, in seconds that the switch will send out discovery packets. Returning information to the commander switch will include information about other switches connected to it. (Ex. MS, CaS). The user may set the dp interval from 30 to 90 seconds.<br>▪ hold time – Using this parameter, the user may set the time, in seconds, the switch will hold information sent to it from other switches, utilizing the discovery interval protocol. The user may set the hold time from 100 to 300 seconds.<br>candidate – Used to change the role of a commander switch to a candidate switch.<br>▪ dp_interval – The user may set the discovery protocol interval, in seconds that the switch will send out discovery packets. Returning information to the commander switch will include information about other switches connected to it. (Ex. MS, CaS). The user may set the dp interval from 30 to 90 seconds.<br>▪ hold time – Using this parameter, the user may set the time, in seconds, the switch will hold information sent to it from other switches, utilizing the discovery interval protocol. The user may set the hold time from 100 to 300 seconds. |
| Restrictions | Only administrator-level users can issue this command. |

To change the time interval of the discovery protocol:

```
DES-3526:4# config sim commander dp_interval 30
Command: config sim commander dp_interval 30
```

```
Success.

DES-3526:4#
```

To change the hold time of the discovery protocol:

```
DES-3526:4# config sim commander hold_time 120
Command: config sim commander hold_time 120

Success.

DES-3526:4#
```

To transfer the commander switch to be a candidate:

```
DES-3526:4# config sim_role candidate
Command: config sim_role candidate

Success.

DES-3526:4#
```

To transfer the switch to be a commander:

```
DES-3526:4# config sim commander
Command: config sim commander

Success.

DES-3526:4#
```

To update the name of a group:

```
DES-3526:4# config sim commander group_name Trinity
Command: config sim commander group_name Trinity

Success.

DES-3526:4#
```

## download sim

| | |
|---|---|
| Purpose | Used to download firmware or configuration file to an indicated device. |
| Syntax | **download sim [ firmware \| configuration] <ipaddr> <path_filename 64> {members <mslist> \| all}** |
| Description | This command will download a firmware file or configuration file to a specified device from a TFTP server. |
| Parameters | firmware – Specify this parameter if the user wishes to download firmware to members of a SIM group. |

| download sim | |
|---|---|
| | firmware to members of a SIM group.<br><br>configuration - Specify this parameter if the user wishes to download a switch configuration to members of a SIM group.<br><br>ipaddr – Enter the IP address of the TFTP server.<br><br>path_filename – Enter the path and the filename of the firmware or switch on the TFTP server.<br><br>members – Enter this parameter to specify the members the user prefers to download firmware or switch configuation files to. The user may specify a member or members by adding one of the following:<br><br>▪ <mslist> - Enter a value, or values to specify which members of the SIM group will receive the firmware or switch configuration.<br><br>▪ all – Add this parameter to specify all members of the SIM group will receive the firmware or switch configuration. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To download firmware:

```
DES-3526:4# download sim firmware 10.53.13.94 c:/des3526.had
members all

Command: download sim firmware 10.53.13.94 c:/des3526.had
members all


This device is updating firmware.  Please wait...


Download Status :


ID   MAC Address       Result
---  ----------------  ----------------
 1   00-01-02-03-04-00 Success
 2   00-07-06-05-04-03 Success
 3   00-07-06-05-04-03 Success


DES-3526:4#
```

To download configuration files:

```
DES-3526:4# download sim configuration 10.53.13.94
c:/des3526.txt members all

Command: download sim firmware 10.53.13.94 c:/des3526.txt
members all


This device is updating configuation.  Please wait...
```

```
Download Status :

ID   MAC Address       Result
---  ----------------  ----------------
 1   00-01-02-03-04-00 Success
 2   00-07-06-05-04-03 Success
 3   00-07-06-05-04-03 Success

DES-3526:4#
```

## upload sim_ms

| | |
|---|---|
| Purpose | User to upload a configuration file to a TFTP server froma specified member of a SIM group. |
| Syntax | **upload sim_ms <ipaddr> <path_filename> <member_id 1-32>** |
| Description | This command will upload a configuration file to a TFTP server froma specified member of a SIM group. |
| Parameters | <ipaddr> Enter the IP address of the TFTP server the user wishes to upload a configuration file to.<br><br><path_filename> – Enter a user-defined path and file name on the TFTP server the user wishes to upload configuration files to.<br><br><member_id 1-32> Enter this parameter to specify the member the user prefers to upload a switch configuation file to. The user may specify a member or members by adding the ID number of the specified member. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To upload configuration files to a TFTP server:

```
DES-3526:4# upload sim_ms configuration 10.55.47.1
D:\configuration.txt 1

Command: upload sim_ms configuration 10.55.47.1
D:\configuration.txt 1


Success.



DES-3526:4#
```

# 29

# COMMAND HISTORY LIST

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

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

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-3526:4#?
..
?
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 admin local_enable
config arp_aging time
config arpentry
config authen application
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

| dir | |
|---|---|
| Purpose | Used to display all commands in the Command Line Interface (CLI). |
| Syntax | **dir** |
| 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 commands:

```
DES-3526:4#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 admin local_enable
config arp_aging time
```

```
config arpentry
config authen application
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

## config command_history

| | |
|---|---|
| Purpose | Used to configure the command history. |
| Syntax | **config command_history <value 1-40>** |
| Description | This command is used to configure the command history. |
| Parameters | <value 1-40> – 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-3526:4#config command_history 20
Command: config command_history 20

 Success.

DES-3526:4#
```

## 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-3526:4#show command_history
Command: show command_history

?
? show
show vlan
show command history

DES-3526:4#
```

# A

## TECHNICAL SPECIFICATIONS

| Physical and Environmental | |
|---|---|
| AC input & External Redundant power Supply: | 100 - 240 VAC, 50-60 Hz (internal universal power supply)<br><br>Redundant power supply – will take over when internal power supply fails. |
| Power Consumption: | 90 watts maximum |
| DC fans: | 2 built-in 40 x 40 x10 mm fans |
| Operating Temperature: | 0 to 40 degrees Celsius |
| Storage Temperature: | -40 to 70 degrees Celsius |
| Humidity: | Operating: 5% to 95% RH non-condensing; Storage: 0% to 95% RH non-condensing |
| Dimensions: | 441 mm x 207 mm x 44 mm (1U), 19 inch rack-mount width |
| Weight: | 3.15 kg |
| EMC: | CE Class A<br><br>FCC Class A<br><br>C-Tick<br><br>VCCI Class A |
| Safety: | CSA International |

| General | |
|---|---|
| Standards: | IEEE 802.3u 100BASE-TX Fast Ethernet<br><br>IEEE 802.3ab 1000BASE-T Gigabit Ethernet<br><br>IEEE 802.1D Spanning Tree<br><br>IEEE 802.1W Rapid Spanning Tree<br><br>IEEE 802.1 P/Q VLAN<br><br>IEEE 802.1p Priority Queues<br><br>IEEE 802.3ad Link Aggregation Control |

| | |
|---|---|
| | IEEE 802.3x Full-duplex Flow Control<br>IEEE 802.3 Nway auto-negotiation |
| Protocols: | CSMA\|CD |
| Data Transfer Rates:<br>Ethernet<br>Fast Ethernet<br>Gigabit Ethernet<br><br><br><br>Fiber Optic | Half-duplex Full-duplex<br>10 Mbps 20Mbps<br>100Mbps 200Mbps<br>n\|a 2000Mbps<br>SFP (Mini GBIC) Support<br>IEEE 802.3z 1000BASE-LX (DEM-310GT transceiver)<br>IEEE 802.3z 1000BASE-SX (DEM-311GT transceiver)<br>IEEE 802.3z 1000BASE-LH (DEM-314GT transceiver)<br>IEEE 802.3z 1000BASE-ZX (DEM-315GT transceiver) |
| Network Cables:<br><br>10BASE-T:<br><br><br>100BASE-TX: | UTP Cat.5, Cat.5 Enhanced for 1000Mbps<br>UTP Cat.5 for 100Mbps<br>UTP Cat.3, 4, 5 for 10Mbps<br>EIA/TIA-568 100-ohm screened twisted-pair (STP)(100m) |
| Number of Ports: | 24 x 10\|100 Mbps NWay ports<br>2 Gigabit Ethernet |

| Performance | |
|---|---|
| Transmission Method: | Store-and-forward |
| RAM Buffer: | 16 MB per device |

| Performance | |
|---|---|
| Filtering Address Table: | 8K MAC address per device |
| Packet Filtering / Forwarding Rate: | Full-wire speed for all connections.<br>148,810 pps per port (for 100Mbps)<br>1,488,100 pps per port (for 1000Mbps) |
| MAC Address Learning: | Automatic update. |
| Forwarding Table Age Time: | Max age: 10 - 1000000 seconds.<br>Default = 300. |