D-Link®

DGS-3324SR

High-density Layer 3 Intelligent Switch

Command Line Interface Reference Manual

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.

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 ©2003 D-Link Corporation.
Contents subject to change without prior notice.
D-Link is a registered trademark of D-Link Corporation/D-Link Systems, Inc. All other trademarks belong to their respective proprietors.

Copyright Statement

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

FCC Warning

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

CE Mark Warning

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

VCCI Warning

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

Table of Contents

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:

- **115200 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.

```
         DGS-3324SR  Stackable Ethernet Switch
                 Command Line Interface

                 Firmware: Build 2.00-B19
      Copyright(C) 2000-2003 D-Link Corporation. All rights reserved.
UserName:
```
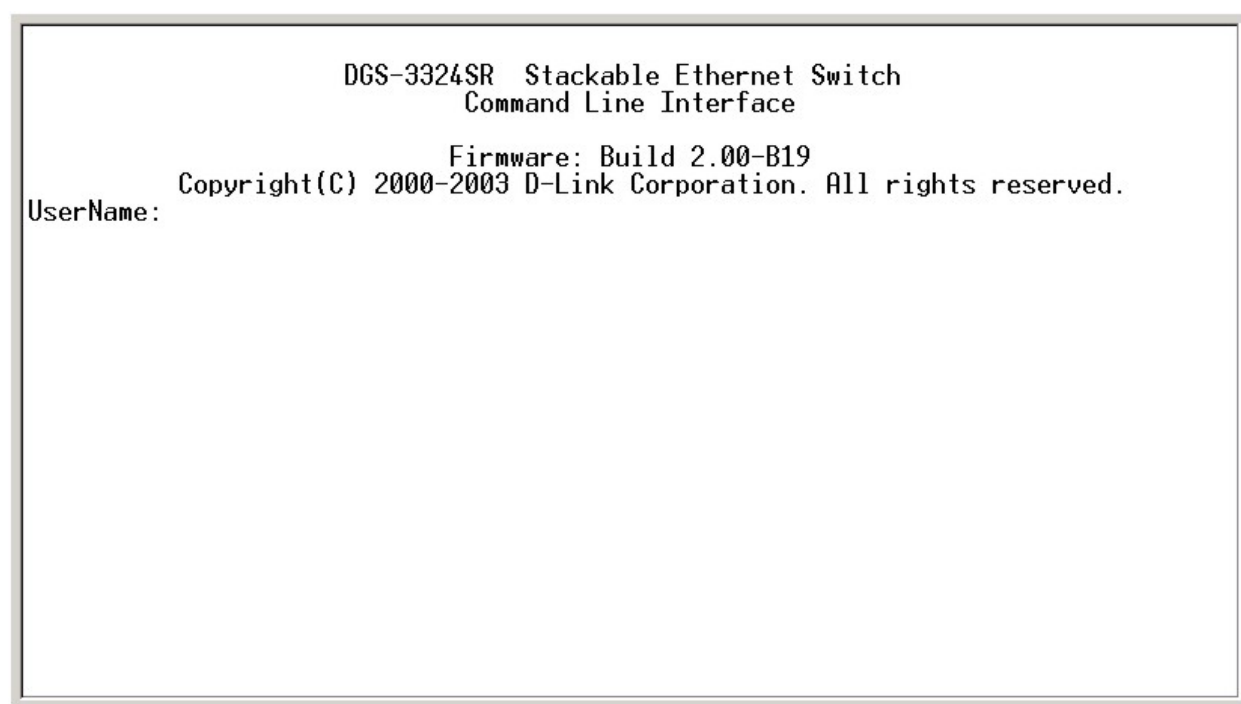
Figure 1-1. Initial CLI screen

There is no initial username or password. Just press the **Enter** key twice to display the CLI input cursor – **DGS-3324SR: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.

```
 Boot Procedure                                                    2.00.001
 ---------------------------------------------------------------------------
 Power On Self Test ................................... 100 %

 MAC Address   : 00-01-02-03-04-00
 H/W Version   : 2B1

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




```
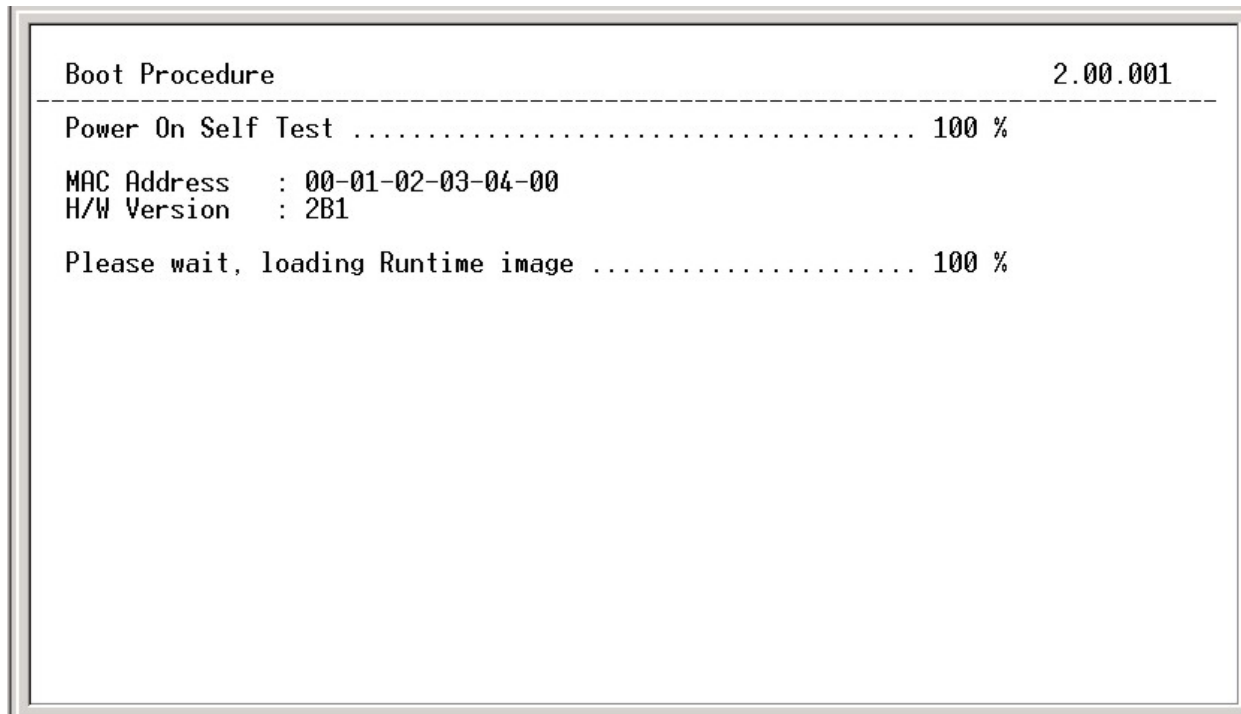
Figure 1-2. Boot Screen

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

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

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

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

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

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

```
                DGS-3324SR   Stackable Ethernet Switch
                       Command Line Interface

                       Firmware: Build 2.00-B19
          Copyright(C) 2000-2003 D-Link Corporation. All rights reserved.
UserName:
PassWord:

DGS-3324SR:4#config ipif System ipaddress 10.53.13.144/8
Command: config ipif System ipaddress 10.53.13.144/8

Success.

DGS-3324SR:4#
```

Figure 1-3. Assigning an IP Address

In the above example, the Switch was assigned an IP address of 10.53.13.144/8 with a subnet mask of 255.0.0.0. The system message **Success** indicates that the command was executed successfully. The Switch can now be configured and managed via Telnet and the CLI or via the Web-based management agent using the above IP address to connect to the Switch.

USING THE CONSOLE CLI

The DGS-3324SR 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**
- **115200 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:

```
                DGS-3324SR  Stackable Ethernet Switch
                      Command Line Interface

                      Firmware: Build 2.00-B19
         Copyright(C) 2000-2003 D-Link Corporation. All rights reserved.
UserName:
```
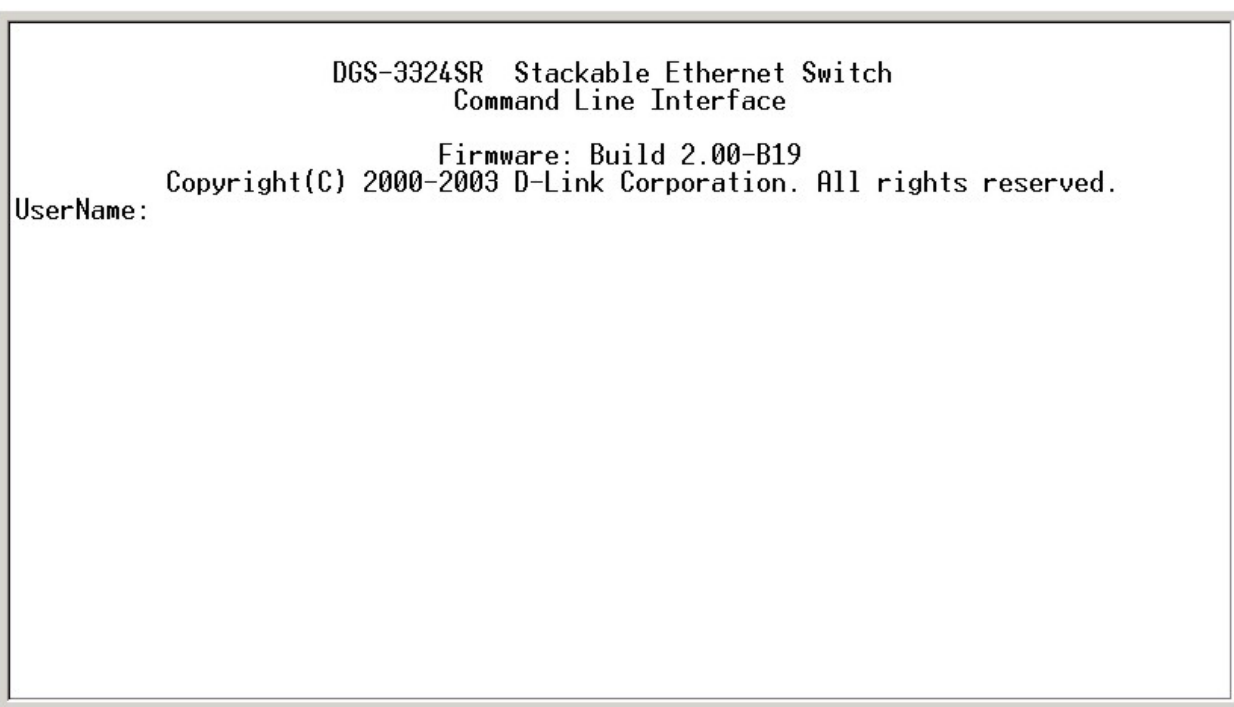
Figure 2-1. Initial Console Screen

Commands are entered at the command prompt, **DGS-3324SR: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.

```
;.
?
clear
clear arptable
clear counters
clear fdb
clear log
config 802.1p default_priority
config 802.1p user_priority
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 all_boxes_id
config arp_aging time
config bandwidth_control
config bootp_relay
config bootp_relay add ipif
config bootp_relay delete ipif
 CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

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.

```
DGS-3324SR:4#config account
Command: config account
Next possible completions:
        <username>

DGS-3324SR:4#
```

Figure 2-3. Example Command Parameter Help

In this case, the command **config account** was entered with the parameter **<username>**. The CLI will then prompt you to enter the **<username>** with the message, **Next possible completions:**. Every command in the CLI has this feature, and complex commands have several layers of parameter prompting.

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

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

```
DGS-3324SR:4#config account
Command: config account
Next possible completions:
        <username>

DGS-3324SR:4#config account
Command: config account
Next possible completions:
        <username>

DGS-3324SR:4#
```
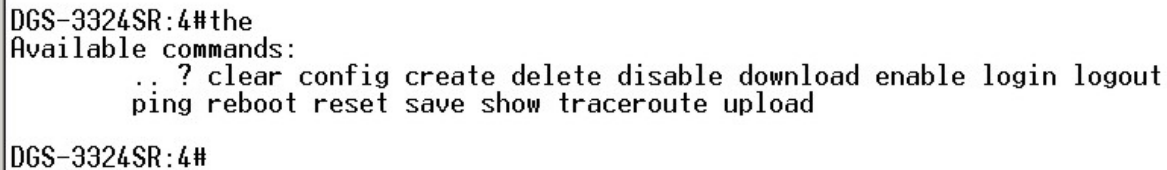
Figure 2-4. Using the Up Arrow to Re-enter a Command

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.

```
DGS-3324SR:4#the
Available commands:
        .. ? clear config create delete disable download enable login logout
        ping reboot reset save show traceroute upload

DGS-3324SR: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.

```
DGS-3324SR:4#show
Command: show
Next possible completions:
        802.1p 802.1x access_profile account acct_client arpentry auth_client
        auth_diagnostics auth_session_statistics auth_statistics
        bandwidth_control bootp_relay command_history device_status dnsr dvmrp
        error fdb gvrp hol_prevention igmp igmp_snooping ipfdb ipif ipmc
        iproute jumbo_frame lacp_port link_aggregation log md5 mirror
        multicast_fdb ospf packet pim port_security ports radius rip route
        router_ports scheduling scheduling_mechanism serial_port session snmp
        sntp stack_information stp switch switch_mode syslog time traffic
        traffic_segmentation trusted_host utilization vlan

DGS-3324SR:4#
```

Figure 2-6. Next possible completions: Show Command

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

COMMAND SYNTAX

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

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

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

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

| vertical bar	
Purpose	Separates two or more mutually exclusive items in a list, one of which must be entered.
Syntax	**show snmp [community|detail]**
Description	In the above syntax example, you must specify either **community,** or **detail**. Do not type the backslash.
Example Command	**show snmp community**

{braces}	
Purpose	Encloses an optional value or set of optional arguments.
Syntax	**reset {[config|system]}**
Description	In the above syntax example, you have the option to specify **config** or **detail**. It is not necessary to specify either optional value, however the effect of the system reset is dependent on which, if any, value is specified. Therefore, with this example there are three possible outcomes of

{braces}	
	performing a system reset. See the following chapter, Basic Commands for more details about the reset command.
Example command	**reset config**

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

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

BASIC SWITCH COMMANDS

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

Command	Parameters
create account	[admin|user] <username 15>
config account	<username 15>
show account	
delete account	<username 15>
show session	
show switch	
show switch_mode	
show device status	
show serial_port	
config serial_port	baud_rate [115200] auto_logout [never|2_minutes|5_minutes |10_minutes|15_minutes]
enable clipaging	
disable clipaging	
enable telnet	<tcp_port_number 1-65535>
disable telnet	
enable web	<tcp_port_number 1-65535>
disable web	
save	[log|all]
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> User <username>

create account

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

Example usage:

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

```
DGS-3324SR:4#create account admin dlink
Command: create account admin dlink

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

 Success.

DGS-3324SR:4#
```

config account

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

Example usage:

To configure the user password of "dlink" account:

```
DGS-3324SR: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.

DGS-3324SR:4#
```

show account

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

Example usage:

To display the accounts that have been created:

```
DGS-3324SR:4#show account
Command: show account

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

DGS-3324SR: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>

delete account

Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the user account "System":

```
DGS-3324SR:4#delete account System
Command: delete account System


 Success.


DGS-3324SR:4#
```

show session

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

Example usage:

To display the way that the users logged in:

```
DGS-3324SR:4#show session
Command: show session


ID  Live Time    From         Level   Name
--   ---------    -------------    -----  ---------------
*8  03:36:27  Serial  Port    4    Anonymous
Total Entries: 1
```

show switch

Purpose	Used to display information about the switch.
Syntax	show switch
Description	This command displays information about the switch.

show switch

Parameters	None.
Restrictions	None.

Example usage:

To display the switch information:

```
DGS-3324SR:4#show switch
Command: show switch

Device Type       : DGS-3324SR Stackable Ethernet Switch
Unit ID           : 1
MAC Address       : DA-10-21-00-00-01
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 1.00-B03
Firmware Version  : Build 2.00-B19
Hardware Version  : 2A1
Device S/N        :
System Name       : DGS-3324SR_#3
System Location   : 7th_flr_east_cabinet
System Contact    : Julius_Erving_212-555-6666
Spanning Tree     : Disabled
GVRP              : Disabled
IGMP Snooping     : Disabled
RIP               : Disabled
DVMRP              : Disabled
PIM-DM            : Disabled
OSPF               : Disabled
TELNET            : Enabled (TCP 23)
WEB               : Enabled (TCP 80)
RMON              : Enabled

DGS-3324SR:4#
```

show switch_mode

Purpose	Used to display the current switch mode.
Syntax	**show switch_mode**
Description	This command displays the current mode of operation of the switch.
Parameters	None.
Restrictions	None

Example usage:

To view the current switch mode:

```
DGS-3324SR:4#show switch_mode
Command: show switch_mode


Switch is in Layer 3 mode


DGS-3324SR:4#
```

show device status

Purpose	Used to display the current status of the hardware of the switch.
Syntax	**show device status**
Description	This command displays the current status of the switch's elements.
Parameters	None.
Restrictions	None

Example usage:

To show the current hardware status of the switch:

```
DGS-3324SR:4#show device_status
Command: show device_status


ID  Internal Power  External power  Side Fan   Back Fan
--- ---------------  ---------------   ----------  ----------
2   Active          Fail            OK         OK



DGS-3324SR: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:

```
DGS-3324SR:4#show serial_port
Command: show serial_port


 Baud Rate      : 115200
 Data Bits      : 8
 Parity Bits    : None
 Stop Bits      : 1
 Auto-Logout    : 10 mins


DGS-3324SR:4#
```

config serial_port

Purpose	Used to configure the serial port.
Syntax	**config serial_port {baud_rate [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[115200] – The serial bit rate that will be used to communicate with the management host. never – No time limit on the length of time the console can be open with no user input. 2_minutes – The console will log out the current user if there is no user input for 2 minutes. 5_minutes – The console will log out the current user if there is no user input for 5 minutes. 10_minutes – The console will log out the current user if there is no user input for 10 minutes. 15_minutes – The console will log out the current user if there is no user input for 15 minutes.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure baud rate:

```
DGS-3324SR:4#config serial_port baud_rate 115200
Command: config serial_port baud_rate 115200

 Success.

DGS-3324SR:4#
```

17

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:

```
DGS-3324SR:4#enable clipaging
Command: enable clipaging


 Success.


DGS-3324SR: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:

```
DGS-3324SR:4#disable clipaging
Command: disable clipaging

 Success.

DGS-3324SR: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:

```
DGS-3324SR:4#enable telnet 23
Command: enable telnet 23

 Success.

DGS-3324SR: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:

```
DGS-3324SR:4#disable telnet
Command: disable telnet


 Success.


DGS-3324SR:4#
```

enable web

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

Example usage:

To enable HTTP and configure port number:

```
DGS-3324SR:4#enable web 80
Command: enable web 80


 Success.


DGS-3324SR: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:

```
DGS-3324SR:4#disable web
Command: disable web

 Success.

DGS-3324SR:4#
```

save	
Purpose	Used to save changes in the switch's configuration to non-volatile RAM.
Syntax	**save [log|all]**
Description	This command is used to enter the current switch configuration into non-volatile RAM. The saved switch configuration will be loaded into the switch's memory each time the switch is restarted.
Parameters	Entering just the **save** command will save only the switch configuration to NV-Ram **log** – Entering the **log** parameter will save only the log file to NV-RAM. **all** - Entering the **all** command will save both the log file and the switch configuration to NV-RAM.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DGS-3324SR:4#save
Command: save

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

DGS-3324SR:4#
```

reboot	
Purpose	Used to restart the switch.
Syntax	**reboot**

reboot

Description	This command is used to restart the switch.
Parameters	None.
Restrictions	None.

Example usage:

To restart the switch:

```
DGS-3324SR: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. 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. 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:

```
DGS-3324SR:4#reset config
Command: reset config

 Success.
```

```
DGS-3324SR: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:

```
DGS-3324SR: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:

```
DGS-3324SR:4#logout
```

SWITCH PORT COMMANDS

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

Command	Parameters
config ports	[<portlist | all> {speed [auto | 10_half | 10_full |100_half | 100_full | 1000_full [master |slave]} | flow_control [enabled | disabled] | learning [enabled | disabled] state [enabled | disabled]}
show ports	<portlist>

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

config ports

Purpose	Used to configure the Switch's Ethernet port settings.
Syntax	[<portlist | all> {speed [auto | 10_half | 10_full |100_half | 100_full | 1000_full [master |slave]} | flow_control [enabled | disabled] | learning [enabled | disabled] state [enabled | disabled]
Description	This command allows for the configuration of the switch's Ethernet ports. Only the ports listed in the <portlist> will be affected.
Parameters	all − Configure all ports on the switch. <portlist> − Specifies a range of ports to be configured. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, **3** specifies port 3. **4** specifies port 4. **3-4** specifies all of the ports between port 3 and port 4 − in numerical order. auto − 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.

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

Example usage:

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

```
DGS-3324SR: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.
DGS-3324SR:4#
```

show ports

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

Example usage:

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

```
DGS-3324SR:4#show ports
Command show ports:

Port   Port      Settings                    Connection              Address
       State     Speed/Duplex/FlowCtrl  Speed/Duplex/FlowCtrl  Learning
------  --------  --------------------  --------------------   --------
1:1     Enabled   Auto/Enabled              Link Down              Enabled
1:2     Enabled   Auto/Enabled              Link Down              Enabled
1:3     Enabled   Auto/Enabled              Link Down              Enabled
1:4     Enabled   Auto/Enabled              Link Down              Enabled
1:5     Enabled   Auto/Enabled              Link Down              Enabled
1:6     Enabled   Auto/Enabled              Link Down              Enabled
1:7     Enabled   Auto/Enabled              Link Down              Enabled
1:8     Enabled   Auto/Enabled              Link Down              Enabled
1:9     Enabled   Auto/Enabled              Link Down              Enabled
1:10    Enabled   Auto/Enabled              100M/Full/802.3x       Enabled
1:11    Enabled   Auto/Enabled              Link Down              Enabled
1:12    Enabled   Auto/Enabled              Link Down              Enabled
1:13    Enabled   Auto/Disabled             Link Down              Enabled
1:14    Enabled   Auto/Disabled             Link Down              Enabled
1:15    Enabled   Auto/Disabled             Link Down              Enabled
1:16    Enabled   Auto/Disabled             Link Down              Enabled
1:17    Enabled   Auto/Disabled             Link Down              Enabled
1:18    Enabled   Auto/Disabled             Link Down              Enabled
1:19    Enabled   Auto/Disabled             Link Down              Enabled
1:20    Enabled   Auto/Disabled             Link Down              Enabled
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

PORT SECURITY COMMANDS

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

Command	Parameters
config port_security ports	[<portlist>| all] {admin_state [enabled| disabled] |max_learning_addr <max_lock_no 0-64>	lock_address_mode [DeleteOnTimeout	DeleteOnReset]}
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	**[<portlist>| all] {admin_state [enabled| disabled] |max_learning_addr <max_lock_no 0-64>	lock_address_mode [DeleteOnTimeout	DeleteOnReset]}**
Description	This command allows for the configuration of the port security feature. Only the ports listed in the <portlist> are effected.
Parameters	portlist – specifies a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are seperated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.

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

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

max_learning_addr <max_lock_no 0-64> - use this to limit the number of MAC addresses dynamically listed in the FDB for the ports.

lock_address_mode[DeleteOnTimout | DeleteOnReset] – delete FDB dynamic entries for the ports on timeout of the FDB (see Forwarding Database Commands). Specify DeleteOnReset to delete all FDB entries, including static entries upon system reset or rebooting. |

config port_security ports

Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the port security:

```
DGS-3324SR:4#config port_security ports 5:1-5:5 admin_state
enabled max_learning_addr 5 lock_address_mode
DeleteOnReset
Command: config port_security ports 5:1-5:5 admin_state
enable max_learning_addr 5 lock_address_mode DeleteOnReset

Success

DGS-3324SR: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 range of ports to be viewed. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are seperated by a dash. For example, **1:3** specifies switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.
Restrictions	None.

Example usage:

To display the port security configuration:

```
DGS-3324SR:4#show port_security ports 1:1-1:24
Command: show port_security ports 1:1-1:24

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

28

1:4	Disabled	1	DeleteOnReset
1:5	Disabled	1	DeleteOnReset
1:6	Disabled	1	DeleteOnReset
1:7	Enabled	10	DeleteOnReset
1:8	Disabled	1	DeleteOnReset
1:9	Disabled	1	DeleteOnReset
1:10	Disabled	1	DeleteOnReset
1:11	Disabled	1	DeleteOnReset
1:12	Disabled	1	DeleteOnReset
1:13	Disabled	1	DeleteOnReset
1:14	Disabled	1	DeleteOnReset
1:15	Disabled	1	DeleteOnReset
1:16	Disabled	1	DeleteOnReset
1:17	Disabled	1	DeleteOnReset
1:18	Disabled	1	DeleteOnReset
1:19	Disabled	1	DeleteOnReset
1:20	Disabled	1	DeleteOnReset
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh			

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 DGS-3324SR supports the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. You can specify which version of the SNMP you want to use to monitor and control the switch. The three versions of SNMP vary in the level of security provided between the management station and the network device. The following table lists the security features of the three SNMP versions:

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

Command	Parameters
create snmp user	create snmp user <SNMP_name 32> <groupname 32> {encrypted(1) [by_password(1) auth [md5(2) <auth_password 8-16 > | sha(3) <auth_password 8-20 >] priv [none(1) | des(2) <priv_password 8-16>] |by_key(2) auth [md5(2) <auth_key 32-32>| sha(3) <auth_key 40-40>] priv [none(1) | des(2) <priv_key 32-32>]]}
delete snmp user	<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 taps	
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	

Command	Parameters
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 <SNMP_name 32> <groupname 32> {encrypted(1) [by_password(1) auth [md5(2) <auth_password 8-16 > | sha(3) <auth_password 8-20 >] priv [none(1) | des(2) <priv_password 8-16>]|by_key(2) auth [md5(2) <auth_key 32-32>| sha(3) <auth_key 40-40>] priv [none(1) | des(2) <priv_key 32-32>]]}**
Description	The **create snmp user** command creates a new SNMP user and adds the user to an SNMP group that is also created by this command.
Parameters	<SNMP_name 32> − An alphanumeric name of up to 32 characters that will identify the new SNMP user.

<groupname 32> − An alphanumeric name of up to 32 characters that will identify the SNMP group the new SNMP user will be associated with.

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.

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.

Message integrity − ensures that packets have not been tampered with during transit.

Authentication − determines if an SNMP message is from a valid source.

Encryption − scrambles the contents of messages to prevent it being viewed by an unauthorized source.

encrypted – Specifies that the password will be in an encrypted format.

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

create snmp user

	setting session. **md5** − Specifies that the HMAC-MD5-96 authentication level will be used. **sha** − Specifies that the HMAC-SHA-96 authentication level will be used. <auth_password 8-20> − An alphanumeric sting of between 8 and 20 characters that will be used to authorize the agent to receive packets for the host. 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:

```
DGS-3324SR: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.


DGS-3324SR: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 <SNMP_name 32>**
Description	The **delete snmp user** command removes an SNMP user from its SNMP group and then deletes the associated SNMP group.
Parameters	<SNMP_name 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:

```
DGS-3324SR:4#delete snmp user dlink
Command: delete snmp user dlink

 Success.

DGS-3324SR: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:

```
DGS-3324SR:4#show snmp user
Command: show snmp user

 Username          Group Name       VerAuthPriv
 ---------------   --------------   ------------
 initial           initial          V3 None None

Total Entries: 1

DGS-3324SR: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

create snmp view

	view that will be created.
	<oid> − The object ID that identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager.
	included − Include this object in the list of objects that an SNMP manager can access.
	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:

```
DGS-3324SR:4#create snmp view dlinkview 1.3.6 view_type
included
Command: create snmp view dlinkview 1.3.6 view_type included

 Success.

DGS-3324SR:4#
```

delete snmp view

Purpose	Used to remove an SNMP view entry previously created on the switch.
Syntax	**delete snmp view <view_name 32> [all | <oid>]**
Description	The **delete snmp view** command is used to remove an SNMP view previously created on the switch.
Parameters	<view_name 32> − An alphanumeric string of up to 32 characters that identifies the SNMP view to be deleted.
	all − Specifies that all of the SNMP views on the switch will be deleted.
	<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:

```
DGS-3324SR:4#delete snmp view dlinkview all
Command: delete snmp view dlinkview all


 Success.


DGS-3324SR: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:

```
DGS-3324SR: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

DGS-3324SR: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

create snmp community

	the community string: An Access List of IP addresses of SNMP managers that are permitted to use the community string to gain access to the switch's SNMP agent. An MIB view that defines the subset of all MIB objects that will be accessible to the SNMP community. Read|write or read-only level permission for the MIB objects accessible to the SNMP community.
Syntax	**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. <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. 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. 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:"

37

```
DGS-3324SR: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:"

```
DGS-3324SR:4#delete snmp community dlink
Command: delete snmp community dlink


 Success.


DGS-3324SR: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

show snmp community

	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:

```
DGS-3324SR:4#show snmp community
Command: show snmp community

 SNMP Community Table

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

Total Entries: 3
```

config snmp engineID

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

Example usage:

To give the SNMP agent on the switch the name "0035636666"

```
DGS-3324SR:4#config snmp 0035636666
Command: config snmp engineID 0035636666

 Success.


DGS-3324SR:4#
```

show snmp engineID

Purpose	Used to display the identification of the SNMP engine on the switch.
Syntax	**show snmp engineID**
Description	The **show snmp engineID** command displays the identification of the SNMP engine on the switch.
Parameters	None.
Restrictions	None.

Example usage:

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

```
DGS-3324SR:4#show snmp engineID
Command: show snmp engineID

SNMP Engine ID : 0035636666

DGS-3324SR: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. v1 – Specifies that SNMP version 1 will be used. The Simple Network Management Protocol

create snmp group

(SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices.

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.

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:

Message integrity − ensures that packets have not been tampered with during transit.

Authentication − determines if an SNMP message is from a valid source.

Encryption − scrambles the contents of messages to prevent it being viewed by an unauthorized source.

noauth_nopriv − Specifies that there will be no authorization and no encryption of packets sent between the switch and a remote SNMP manager.

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.

auth_priv − Specifies that authorization will be required, and that packets sent between the switch and a remote SNMP manger will be encrypted.

read_view – Specifies that the SNMP group being created can request SNMP messages.

write_view – Specifies that the SNMP group being created has write privileges.

<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.

notify_view − Specifies that the SNMP group being created can receive SNMP trap messages generated by the switch's SNMP agent.

create snmp group

Restrictions	Only administrator-level users can issue this command.

Example usage:

To create an SNMP group named "sg1:"

```
DGS-3324SR: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.


DGS-3324SR: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".

```
DGS-3324SR:4#delete snmp group sg1
Command: delete snmp group sg1


 Success.


DGS-3324SR: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.

show snmp groups

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:

```
DGS-3324SR: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

DGS-3324SR: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>]**
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.

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 |

create snmp host

control network devices.

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.

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:

Message integrity − ensures that packets have not been tampered with during transit.

Authentication − determines if an SNMP message is from a valid source.

Encryption − scrambles the contents of messages to prevent it being viewed by an unauthorized source.

noauth_nopriv − Specifies that there will be no authorization and no encryption of packets sent between the switch and a remote SNMP manager.

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.

auth_priv − Specifies that authorization will be required, and that packets sent between the switch and a remote SNMP manger will be encrypted.

<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:

```
DGS-3324SR: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.

DGS-3324SR: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:

```
DGS-3324SR:4#delete snmp host 10.48.74.100
Command: delete snmp host 10.48.74.100

 Success.

DGS-3324SR: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:

```
DGS-3324SR: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


DGS-3324SR: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:

```
DGS-3324SR:4#create trusted_host 10.48.74.121
Command: create trusted_host 10.48.74.121


Success.


DGS-3324SR: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**
Description	This command is used to display a list of trusted hosts entered on the switch using the **create trusted_host** command above.
Parameters	none.
Restrictions	none.

Example Usage:

To display the list of trust hosts:

```
DGS-3324SR:4#show trusted_host
Command: show trusted_host


 Management Stations


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

Total Entries: 1


DGS-3324SR: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:

```
DGS-3324SR:4#delete trusted_host 10.48.74.121
Command: delete trusted_host 10.48.74.121


Success.
DGS-3324SR:4#
```

enable snmp traps

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

Example usage:

To enable SNMP trap support on the switch:

```
DGS-3324SR:4#enable snmp traps
Command: enable snmp traps


Success.


DGS-3324SR: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:

```
DGS-3324SR:4#enable snmp authenticate_traps
Command: enable snmp authenticate_traps


 Success.


DGS-3324SR: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.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To view the current SNMP trap support:

```
DGS-3324SR:4#show snmp traps
Command: show snmp traps


SNMP Traps          : Enabled
Authenticate Traps  : Enabled


DGS-3324SR: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:

```
DGS-3324SR:4#disable snmp traps
Command: disable snmp traps

Success.

DGS-3324SR: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:

```
DGS-3324SR:4#disable snmp authenticate_traps
Command: disable snmp authenticate_traps

 Success.

DGS-3324SR: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**":

```
DGS-3324SR:4#config snmp system_contact MIS Department II
Command: config snmp system_contact MIS Department II

Success.

DGS-3324SR: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**":

```
DGS-3324SR:4#config snmp system_location HQ 5F
Command: config snmp system_location HQ 5F

Success.

DGS-3324SR: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

config snmp system_name

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

Example usage:

To configure the switch name for "**DGS-3324SR Stackable Switch**":

```
DGS-3324SR:4#config snmp system_name DGS-3324SR
Stackable Switch
Command: config snmp system_name DGS-3324SR Stackable
Switch

Success.

DGS-3324SR: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:

```
DGS-3324SR:4#enable rmon
Command: enable rmon

 Success.

DGS-3324SR:4#
```

disable rmon

Purpose	Used to disable RMON on the switch.
Syntax	**disable rmon**

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:

```
DGS-3324SR:4#disable rmon
Command: disable rmon


 Success.


DGS-3324SR:4#
```

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_fromTFTP <ipaddr> <path_filename 64> {unit [all	<unitid 1-12>]}	cfg_fromTFTP <ipaddr> <path_filename 64> {increment}]
upload	[cfg_toTFTP	log_toTFTP] <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	[firmware_fromTFTP <ipaddr> <path_filename 64> {unit [all|<unitid 1-12>]}	cfg_fromTFTP <ipaddr> <path_filename 64> {increment}]
Description	This command is used to download a new firmware or a switch configuration file from a TFTP server.
Parameters	firmware – Download and install new firmware on the switch from a TFTP server.

configuration (cfg)– Download a switch configuration file from a TFTP server.

<ipaddr> – The IP address of the TFTP server.

<path_filename> – The DOS path and filename of the firmware or switch configuration file on the TFTP server. For example, C:\3226S.had.

unit [all|<unitid>] – all specifies all units (switches), <unitid> is the unit id of the switch that will receive the download.

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. |

download

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:

```
DGS-3324SR:4#download cfg_to TFTP 10.48.74.121
c:\cfg\setting.txt
Command: download cfg_to TFTP 10.48.74.121 c:\cfg\setting.txt


Connecting to server................... Done.
Download configuration............. Done.


DGS-3324SR:4#
```

upload

Purpose	Used to upload the current switch settings or the switch history log to a TFTP.
Syntax	**upload [cfg_toTFTP | log_toTFTP] <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 (cfg) − Specifies that the switch's current settings will be uploaded to the TFTP server. log − Specifies that the switch history log will be uploaded to the TFTP server. <ipaddr> − The IP address of the TFTP server. The TFTP server must be on the same IP subnet as the switch. <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:

```
DGS-3324SR:4#upload cfg_toTFTP 10.48.74.121 c:\cfg\log.txt
Command: upload cfg_to TFTP 10.48.74.121 c:\cfg\log.txt

 Connecting to server................... Done.
 Upload configuration...................Done.

DGS-3324SR: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.
	times - The number of individual ICMP echo messages to be sent.
	A value of 0 will send an infinite ICMP echo messages. The maximum value is 255. The default is 0.
	timeout - Defines the time-out period while waiting for a response from the remote device.
	A value of 1 to 99 seconds can be specified. The default is 1 second
Restrictions	None.

```
DGS-3324SR: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

DGS-3324SR:4#
```

traceroute

Purpose	Used to trace the routed path between the switch and a destination endstation.
Syntax	**traceroute <ipaddr> {ttl <value 1-60>	port <value 30000-64900>	timeout <sec 1-65535>	probe <value <1-9>**
Description	The traceroute command allows you to trace a route between the switch and a give host on the network.
Parameters	<ipaddr> - Specifies the IP address of the host.
	ttl <value 1-60> - The time to live value of the trace route request. This is the maximum number of routers the traceroute command will cross while seeking the network path between two devices.
	probe <value 1-9> - The probe value is the number of times the switch will send probe packets to the next hop on the intended traceroute path. The default is 1.
	port <value 30000-64900> The port number. Must be above 1024.The value range is from 30000 to 64900 .
	timeout - Defines the time-out period while waiting for a response from the remote device.An entry between 1 ans 65535 seconds.
Restrictions	None.

Example usage:

To trace the routed path between the switch and 10.48.74.121.

```
DGS-3324SR:4#traceroute 10.48.74.121 probe 3
Command: traceroute 10.48.74.121 probe 3


1 <10ms 10.254.254.251
2 <10ms 10.254.254.251
3 <10ms 10.254.254.251
4 <10ms 10.55.25.35
5 <10ms 10.55.25.35
6 <10ms 10.55.25.35
7 <10ms 10.22.35.1
8 <10ms 10.22.35.1
9 <10ms 10.22.35.1
10 <10ms 10.48.74.121


Trace Complete


DGS-3324SR:4#
```

NETWORK MONITORING COMMANDS

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

Command	Parameters
show packet ports	<portlist>
show error ports	<portlist>
show utilitzation	
clear counters	ports <portlist>
clear log	
show log	index <value_list>
enable syslog	
disable syslog	
show syslog	
create syslog host	<index 1-4> {severity [informational | warning | all] | facility [local0|local1|local2|local3|local4|local5|local6|local7] |udp_port <udp_port_number> | ipaddress <ipaddr> | state [enabled | disabled]}
config syslog host	<index 1-4> {severity [informational | warning |all] |facility [local0|local1|local2|local3|local4|local5|local6|local7] |udp_port <udp_port_number> | ipaddress <ipaddr> | state [enabled | disabled]}
config syslog host all	[severity[informational|warning|all] |facility[local0|local1|local2|local3|local4|local5|local6|local7] | udp_port <udp_port_number> | state [enabled|disabled]]
delete syslog host	<index 1-4> all
show syslog host	<index 1-4>

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

show packet ports

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

show packet ports

	lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separeted by a colon) are specified. The beginning and end of the port list range are seperated by a dash. For example, **1:3** specifies switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 − in numerical order.
Restrictions	None.

Example usage:

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

```
DGS-3324SR:4#show packet port 2:7

Port number : 2:7

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


DGS-3324SR: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 range of ports to be displayed. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, **1:3** specifies switch number 1, port 3. **2:4** specifies switch

show error ports

	number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.
Restrictions	None.

Example usage:

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

```
DGS-3324SR:4#show errors port 1:3
                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


DGS-3324SR:4#
```

show utilization

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

Example usage:

To display the port utilization statistics:

```
DGS-3324SR:4#show utilization
Port   TX/sec   RX/sec   Util    Port   TX/sec   RX/sec   Util
----   ----------   ----------   ----    ----   ----------   ----------   ----
1:1        0        0        0    1:22       0        0        0
1:2        0        0        0    1:23       0        0        0
1:3        0        0        0    1:24       0        0        0
1:4        0        0        0    1:25       0        0        0
1:5        0        0        0    1:26      19       49        1
1:6        0        0        0    2:1        0        0        0
1:7        0        0        0    2:2        0        0        0
1:8        0        0        0    2:3        0        0        0
1:9        0        0        0    2:4        0        0        0
1:10       0        0        0    2:5        0        0        0
1:11       0        0        0    2:6        0        0        0
1:12       0        0        0    2:7        0       30        1
1:13       0        0        0    2:8        0        0        0
1:14       0        0        0    2:9       30        0        1
1:15       0        0        0    2:10       0        0        0
1:16       0        0        0    2:11       0        0        0
1:17       0        0        0    2:12       0        0        0
1:18       0        0        0    2:13       0        0        0
1:19       0        0        0    2:14       0        0        0
1:20       0        0        0    2:15       0        0        0
1:21       0        0        0    2:16       0        0        0


DGS-3324SR: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 range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To clear the counters for ports 7-9 on unit 2:

```
DGS-3324SR:4#clear counters ports 2:7-2:9
Command: clear counters ports 2:7-2:9


 Success.
DGS-3324SR: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:

```
DGS-3324SR:4#clear log
Command: clear log


 Success.


DGS-3324SR:4#
```

show log

Purpose	Used to display the switch history log.
Syntax	**show log {index <value_list>}**
Description	This command will display the contents of the switch's history log.
Parameters	index <value_list> – Enter a value that corresponds to an entry made in the log. Multiple entries may be made in the form of *x-x* where x is the number of an entry in the log. The smallest number (and therefore the earlier entry) will be first.
Restrictions	None.

Example usage:

To display the switch history log:

```
DGS-3324SR:4#show log index 1-4
Command: show log index 1-4


Index Date       Time      Log Text
-----  ----------  --------  ------------------------------------------------
4      2000-03-02 01:54:53  Port 1:13 link up, 100Mbps FULL duplex
3      2000-03-02 01:54:53  Spanning Tree Protocol is enabled
2      2000-03-02 01:54:53  Unit 1, System started up
1      2000-02-28 06:06:09  Spanning Tree Protocol is disabled


DGS-3324SR: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.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To the syslog function on the switch:

```
DGS-3324SR:4#enable syslog
Command: enable syslog


 Success.


DGS-3324SR: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.

disable syslog

Restrictions	Only administrator-level users can issue this command.

Example usage:

To disable the syslog function on the switch:

```
DGS-3324SR:4#disable syslog
Command: disable syslog

 Success.

DGS-3324SR: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:

```
DGS-3324SR:4#show syslog
Command: show syslog

Syslog Global State: Enabled

DGS-3324SR:4#
```

create syslog host

Purpose	Used to create a new syslog host.
Syntax	**create syslog host [all|<index 1-4>] {severity [informational|warning|all]| facility[local0|local1|local2|local3| local4|local5|local6|local7]|udp_port<int>| ipaddress <ipaddr>| state[enabled|disabled]**
Description	The **create syslog host** command is used to create a new syslog host.

create 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 the facility values that the switch currently supports.

Numerical Code	Facility
0	kernel messages

create syslog host

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)**

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

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

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

create syslog host

	local3 − Specifies that local use 3 messages will be sent to the remote host. This corresponds to number 19 from the list above.
	local4 − Specifies that local use 4 messages will be sent to the remote host. This corresponds to number 20 from the list above.
	local5 − Specifies that local use 5 messages will be sent to the remote host. This corresponds to number 21 from the list above.
	local6 − Specifies that local use 6 messages will be sent to the remote host. This corresponds to number 22 from the list above.
	local7 − Specifies that local use 7 messages will be sent to the remote host. This corresponds to number 23 from the list above.
	udp_port <int> − Specifies the UDP port number that the syslog protocol will use to send messages to the remote host.
	ipaddress <ipaddr> − Specifies the IP address of the remote host where syslog messages will be sent.
	state [enabled	disabled] − 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:

```
DGS-3324SR:4#create syslog host 1 severity all facility local0
Command: create syslog host 1 severity all facility local0

 Success.

DGS-3324SR:4#
```

config syslog host

Purpose	Used to configure the syslog protocol to send system log data to a remote host.
Syntax	**config syslog host <index 1-4> {severity [informational	warning	all]	facility [local0|local1|local2|local3| local4|local5|local6|local7]	udp_port<int> |**

config syslog host

	**ipaddress <ipaddr>	state[enabled	disabled]**
Description	The **config syslog host** command is used to configure the syslog protocol to send system log information to a remote 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.
	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 Severity
Code

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 Facility
Code

0	kernel messages
1	user-level messages
2	mail system
3	system daemons

config syslog host

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)**

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

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

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

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

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

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

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

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

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

ipaddress <ipaddr> − Specifies the IP address

config syslog host

	of the remote host where syslog messages will be sent.
	state [enabled	disabled] − 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:

```
DGS-3324SR:4#config syslog host 1 severity all facility local0
Command: config syslog host all severity all facility local0
 Success.
DGS-3324SR:4#
```

config syslog host all

Purpose	Used to configure the syslog protocol to send system log data to all hosts.
Syntax	**config syslog host all [severity [informational|warning|all] |facility[local0|local1|local2|local3|local4|local5|local6|local7]	udp_port <udp_port_number>	state [enabled|disabled]]**
Description	The **config syslog host all** command is used to configure the syslog protocol to send system log information to all hosts.
Parameters	all − Specifies that the command will be applied to all hosts.
	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 Severity
	Code
	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

config syslog host all

6 from the list above.

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

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

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

Numerical   Facility
Code

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)**

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

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

config syslog host all

	local2 – Specifies that local use 2 messages will be sent to the remote host. This corresponds to number 18 from the list above.
	local3 – Specifies that local use 3 messages will be sent to the remote host. This corresponds to number 19 from the list above.
	local4 – Specifies that local use 4 messages will be sent to the remote host. This corresponds to number 20 from the list above.
	local5 – Specifies that local use 5 messages will be sent to the remote host. This corresponds to number 21 from the list above.
	local6 – Specifies that local use 6 messages will be sent to the remote host. This corresponds to number 22 from the list above.
	local7 – Specifies that local use 7 messages will be sent to the remote host. This corresponds to number 23 from the list above.
	udp_port <int> – Specifies the UDP port number that the syslog protocol will use to send messages to the remote host.
	state [enabled	disabled] – 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 for all hosts:

```
DGS-3324SR:4#config syslog host all severity all facility local0
Command: config syslog host all severity all facility local0
 Success.
DGS-3324SR:4#
```

delete syslog host

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

delete syslog host

Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete a previously configured syslog host:

```
DGS-3324SR:4#delete syslog host 4
Command: delete syslog host 4


 Success.


DGS-3324SR: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:

```
DGS-3324SR: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


DGS-3324SR:4#
```

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 [enabled | disabled]}
config stp ports	[all | <portlist>] {cost [auto | <value 1-200000000>] | priority <value0-240>|migrate [yes | no] |edge [true | false]|p2p [true | false | auto] |state [enabled | disabled]}
enable stp	
disable stp	
show stp	
show stp ports	<portlist>

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

config stp	
Purpose	Used to 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 [enabled | disabled]}**
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.
	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.
	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.
	priority <value> – A numerical value between 0

config stp

	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.

version [rstp \| stp] - select the Spanning Tree Protocol version used for the switch.

- stp – Selct this parameter for IEEE 802.1d STP and for IEEE 802.1w STP compatibility mode.

- rstp - Select this paramter for IEEE 802.1w Rapid STP mode.

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

fbpdu [enabled \| disabled] – Allows the forwarding of STP BPDU packets from other network devices when STP is disabled on the switch. The default is enabled. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To configure STP with maxage 18 and hellotime 4:

```
DGS-3324SR:4#config stp maxage 18 hellotime 4
Command: config stp maxage 18 hellotime 4


 Success.


DGS-3324SR: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 [enabled | disabled]**
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

config stp ports

chosen to forward packets.

Default port cost: 100Mbps port = 200000
Gigabit port = 20000

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.

<portlist> − Specifies a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, **1:3** specifies switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 − in numerical order.

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

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.

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*.

state [enabled | disabled] − Allows STP to be

config stp ports

	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 module 1.

```
DGS-3324SR:4#config stp ports 1:1-1:5 cost 19 priority 16 state
enabled
Command: config stp ports 1:1-1:5 cost 19 priority 16 state
enabled


Success.


DGS-3324SR: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:

```
DGS-3324SR:4#enable stp
Command: enable stp


 Success.


DGS-3324SR: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.

disable stp	
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To disable STP on the switch:

```
DGS-3324SR:4#disable stp
Command: disable stp

 Success.

DGS-3324SR: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

```
DGS-3324SR:4#show stp
Command: show stp

STP Status     : Enabled
Max Age        : 20
Hello Time     : 2
Forward Delay  : 15
Priority       : 32768
Default Path Cost:  802.1T
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

```
DGS-3324SR:4#show stp
Command: show stp

STP Status     : Disabled
Max Age        : 20
Hello Time     : 2
Forward Delay  : 15
Priority       : 32768
Default Path Cost: 802.1T
STP Version    : STP compatible
TX Hold Count  : 3
Forwarding BPDU : Enabled


DGS-3324SR:4#
```

show stp ports

Purpose	Used to display the switch's current per-port group STP configuration.
Syntax	**show stp ports <portlist>**

show stp ports

Description	This command displays the switch's current per-port group STP configuration.
Parameters	<portlist> – Specifies a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are seperated by a dash. For example, **1:3** specifies switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.
Restrictions	None

Example usage:

To display STP state of port 1-9 of module 1:

```
DGS-3324SR:4#show stp ports

Command: show ports

Port   Connection        State  Cost        Pri   Edge   P2P   Status      Role

------ ------------------ -----  ----------  ----  ----   ---   ----------  ----------

1:1    Link Down          Yes    *20000      128   No     Yes   Disabled  Disabled
1:2    Link Down          Yes    *20000      128   No     Yes   Disabled  Disabled
1:3    Link Down          Yes    *20000      128   No     Yes   Disabled  Disabled
1:4    Link Down          Yes    *20000      128   No     Yes   Disabled  Disabled
1:5    Link Down          Yes    *20000      128   No     Yes   Disabled  Disabled
1:6    Link Down          Yes    *20000      128   No     Yes   Disabled  Disabled
1:7    Link Down          Yes    *20000      128   No     Yes   Disabled  Disabled
1:8    Link Down          Yes    *20000      128   No     Yes   Disabled  Disabled
1:9    Link Down          Yes    *20000      128   No     Yes   Disabled  Disabled
1:10   100M/Full/None     Yes    *200000     128   No     Yes   Forwarding NonStp
1:11   Link Down          Yes    *20000      128   No     Yes   Disabled  Disabled
1:12   Link Down          Yes    *20000      128   No     Yes   Disabled  Disabled
1:13   Link Down          Yes    *20000      128   No     Yes   Disabled  Disabled
1:14   Link Down          Yes    *20000      128   No     Yes   Disabled  Disabled
1:15   Link Down          Yes    *20000      128   No     Yes   Disabled  Disabled
1:16   Link Down          Yes    *20000      128   No     Yes   Disabled  Disabled
1:17   Link Down          Yes    *20000      128   No     Yes   Disabled  Disabled
1:18   Link Down          Yes    *20000      128   No     Yes   Disabled  Disabled
1:19   Link Down          Yes    *20000      128   No     Yes   Disabled  Disabled
1:20   Link Down          Yes    *20000      128   No     Yes   Disabled  Disabled
1:21   Link Down          Yes    *20000      128   No     Yes   Disabled  Disabled


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

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}
show ipfdb	<ipaddr>

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

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

Example usage:

To create a unicast MAC FDB entry**:**

```
DGS-3324SR:4#create fdb default 00-00-00-00-01-02 port 2:5
Command: create fdb default 00-00-00-00-01-02 port 2:5


 Success.
DGS-3324SR:4#
```

create multicast_fdb

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

Example usage:

To create multicast MAC forwarding**:**

```
DGS-3324SR:4#create multicast_fdb default 01-00-00-00-00-01
Command: create multicast_fdb default 01-00-00-00-00-01


Success.


DGS-3324SR: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. <macaddr> − The MAC address that will be added to the multicast forwarding table.

config multicast_fdb

	[add | delete] − Add will add ports to the forwarding table. Delete will remove ports from the multicast forwarding table.
	<portlist> − Specifies a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, **1:3** specifies switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 − in numerical order.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To add multicast MAC forwarding:

```
DGS-3324SR:4#config multicast_fdb default 01-00-00-00-00-01
Command: config multicast_fdb default 01-00-00-00-00-01 add
1:1-1:5


Success.


DGS-3324SR: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

config fdb aging_time

Parameters	which case the switch will broadcast the packet to all ports, negating many of the benefits of having a switch. <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:

```
DGS-3324SR:4#config fdb aging_time 300
Command: config fdb aging_time 300


Success.


DGS-3324SR:4#
```

delete fdb

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

Example usage:

To delete a permanent FDB entry:

```
DGS-3324SR:4#delete fdb default 00-00-00-00-01-02
Command: delete fdb default 00-00-00-00-01-02


 Success.


DGS-3324SR:4#
```

Example usage:

To delete a multicast fdb entry:

```
DGS-3324SR:4#delete fdb default 01-00-00-00-01-02
Command: delete fdb default 01-00-00-00-01-02


 Success.


DGS-3324SR:4#
```

clear fdb

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

Example usage:

To clear all FDB dynamic entries:

```
DGS-3324SR:4#clear fdb all
Command: clear fdb all

 Success.


DGS-3324SR:4#
```

show multicast_fdb	
Purpose	Used to display the contents of the switch's multicast forwarding database.
Syntax	**show mulitcast_fdb [vlan <vlan_name 32> | mac_address <macaddr>]**
Description	This command is used to display the current contents of the switch's multicast MAC address forwarding database.
Parameters	<vlan_name 32> − The name of the VLAN on which the MAC address resides. <macaddr> − The MAC address that is present in the forwarding database table.
Restrictions	None.

Example usage:

To display multicast MAC address table:

```
DGS-3324SR: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   : 1:1-1:5,1:26,2:26
 Mode           : Static


 Total Entries  : 1


DGS-3324SR: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. <vlan_name 32> − The name of the VLAN on which the MAC address resides. <macaddr> − The MAC address that is present in the forwarding database table. static − Displays the static MAC address entries. aging_time − Displays the aging time for the MAC address forwarding database.
Restrictions	None.

Example usage:

To display unicast MAC address table:

```
DGS-3324SR: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

show ipfdb

Purpose	Used to display the current IP address forwarding database table.
Syntax	**show ipfdb <ipaddr>**
Description	This command will display the current contents of the switch's IP forwarding database.
Parameters	<ipaddr> The user may enter an IP address to view the table by.
Restrictions	None.

Example usage:

To view the IP forwarding database table:

```
DGS-3324SR:4#show ipfdb
Command: show ipfdb

Interface    IP Address      Port    Learned
------------  --------------   ----    ---------
System       10.0.0.1        1:13    Dynamic
System       10.0.0.2        1:13    Dynamic
System       10.0.0.3        1:13    Dynamic
System       10.0.0.4        1:13    Dynamic
System       10.0.0.7        1:13    Dynamic
System       10.0.0.30       1:13    Dynamic
System       10.0.34.1       1:13    Dynamic
System       10.0.51.1       1:13    Dynamic
System       10.0.58.4       1:13    Dynamic
System       10.0.85.168     1:13    Dynamic
System       10.1.1.1        1:13    Dynamic
System       10.1.1.99       1:13    Dynamic
System       10.1.1.101      1:13    Dynamic
System       10.1.1.102      1:13    Dynamic
System       10.1.1.103      1:13    Dynamic
System       10.1.1.152      1:13    Dynamic
System       10.1.1.157      1:13    Dynamic
System       10.1.1.161      1:13    Dynamic
System       10.1.1.162      1:13    Dynamic
System       10.1.1.163      1:13    Dynamic
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

BROADCAST STORM CONTROL COMMANDS

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

Command	Parameters
config traffic control	[<storm_grouplist> | all] { broadcast [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 [enabled | disabled] | multicast [enabled | disabled] | dlf [enabled | disabled] | threshold <value 0-255>**
Description	This command is used to configure broadcast storm control.
Parameters	<storm_grouplist> – Used to specify a broadcast storm control group. This is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, **1:3** specifies switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.

all – Specifies all broadcast storm control groups on the switch.

broadcast [enabled \| disabled] – Enables or disables broadcast storm control.

multicast [enabled \| disabled] – Enables or disables multicast storm control.

dlf [enabled \| disabled] – Enables or disables dlf traffic control.

threshold <value> – The upper threshold at which the specified traffic control is switched on. The <value> is the number of |

config traffic control

	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:

```
DGS-3324SR:4#config traffic control all broadcast enabled
Command: config traffic control all broadcast enabled

Success.

DGS-3324SR: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 listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, **1:3** specifies switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.
Restrictions	None.

Example usage:

To display traffic control setting:

```
DGS-3324SR:4#show traffic control 1:1-1:5

Command: show traffic control 1:1-1:5


Traffic Control

                                  Broadcast   Multicast   Destination
Module  Group [ports]  Threshold  Storm       Storm       Lookup Fail
------  -------------  ---------  ---------   ---------   --------
1       1              128        Disabled    Disabled    Disabled
1       2              128        Disabled    Disabled    Disabled
1       3              128        Disabled    Disabled    Disabled
1       4              128        Disabled    Disabled    Disabled
1       5              128        Disabled    Disabled    Disabled


Total Entries: 5


DGS-3324SR:4#
```

QOS COMMANDS

The DGS-3324SR switch supports 802.1p priority queuing. The switch has 7 priority queues. These priority queues are numbered from 6 (Class 6) — 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 Q2 queue.

- Priority 1 is assigned to the Switch's Q0 queue.

- Priority 2 is assigned to the Switch's Q1 queue.

- Priority 3 is assigned to the Switch's Q3 queue.

- Priority 4 is assigned to the Switch's Q4 queue.

- Priority 5 is assigned to the Switch's Q5 queue.

- Priority 6 is assigned to the Switch's Q6 queue.

- Priority 7 is assigned to the Switch's Q6 queue.

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

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

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

To use implement weight fair priority, the switch's eight priority queues can be configured to reduce the buffer in a wighted round-robin (**WRR**) fashion - beginning with the highest priority queue, and proceeding to the lowest priority queue before returning to the highest priority queue.

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

The possible range for maximum packets is: 0 to 15 packets.

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>	all] {rx_rate [no_limit	<value 1-999>]	tx_rate [no_limit<value 1-999>]}
show bandwidth_control	<portlist>
config scheduling	<class_id 0-6> max_packet <value 0-15>
show scheduling	
config 802.1p user_priority	<priority 0-7> <class_id 0-6>
show 802.1p user_priority	
config 802.1p	<portlist>

Command	Parameters
default_priority	[all | <priority 0-7>]
show 802.1p default_priority	<portlist>
config scheduling_mechanism	[strict | weight_fair]
show scheduling_mechanism	
enable hol_prevention	
disable hol_prevention	
show hol_prevention	

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> | all]{rx_rate [no_limit | <value 1-999>] | tx_rate [no_limit | <value 1-999>]}**
Description	The **config bandwidth_control** command is used to configure bandwidth on a by-port basis.
Parameters	<portlist> – Specifies a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, **1:3** specifies switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.
	rx_rate – Specifies that one of the parameters below (**no_limit** or **<value 1-999>**) will be applied to the rate at which the above specified ports will be allowed to receive packets
	no_limit – Specifies that there will be no limit on the rate of packets received by the above specified ports.
	<value 1-999> – Specifies the packet limit, in Mbps, that the above ports will be allowed to receive.
	tx_rate – Specifies that one of the parameters below (**no_limit** or **<value 1-999>**) will be applied to the rate at which the above specified ports will be allowed to transmit packets.
	no_limit – Specifies that there will be no limit on

config bandwidth_control

	the rate of packets received by the above specified ports.
	<value 1-999> – Specifies the packet limit, in Mbps, that the above ports will be allowed to receive..
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure bandwidth control:

```
DGS-3324SR:4#config bandwidth_control 1:1-1:10 tx_rate 10
Command: config bandwidth_control 1:1-1:10 tx_rate 10

 Success.

DGS-3324SR:4#
```

show bandwidth_control

Purpose	Used to display the bandwidth control configuration on the switch.
Syntax	**show bandwidth_control {<portlist>}**
Description	The **show bandwidth_control** command displays the current bandwidth control configuration on the switch, on a port-by-port basis.
Parameters	<portlist> – Specifies a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, **1:3** specifies switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.
Restrictions	None.

Example usage:

To display bandwidth control settings:

```
DGS-3324SR:4#show bandwidth_control  1:1-1:10

Command: show bandwidth_control 1:1-1:10


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


DGS-3324SR:4#
```

config scheduling

Purpose	Used to configure traffic scheduling for each of the switch's QoS queues.
Syntax	**config scheduling <class_id 0-6> {max_packet <value 0-15>}**
Description	The switch contains eight hardware priority queues per device. The switch's default settings draw down seven hardware queues in order, from the highest priority (Class 0) to the lowest priority (Class 6). Starting with the highest priority queue (Class 0), the highest priority queue will transmit all of the packets and empty its buffer before allowing the next lower priority queue to transmit its packets. The next highest priority queue will empty before proceeding to the next queue and so on. Lower priority queues are allowed to transmit only if the higher priority queue(s) in the buffer are completely emptied. Packets in the higher priority queues are always emptied before any in the lower priority queues.

The default settings for QoS scheduling employ this strict priority scheme to empty priority queues.

The **config scheduling** command can be used to specify the weighted round-robin (*WRR*) rotation by which these eight hardware priority queues are reduced. To use a weighted round- |

config scheduling

robin (*WRR*) scheme, the *max_packets* parameters must not have a value of zero (*0*). (See **Combination Queue** below.)

The **max_packet** parameter allows you to specify the maximum number of packets a given priority queue can transmit per weighted round-robin (*WRR*) scheduling cycle. This provides for a controllable CoS behavior while allowing for other queues to empty as well. A value between 0 and 15 packets can be specified per priority queue.

Entering a *0* into the *<value 0-15>* field of the *max_packet* parameter allows for the creation of a **Combination Queue** for the forwarding of packets. This **Combination Queue** allows for a combination of strict and weight-fair (weighted round-robin *"WRR"*) scheduling. Priority queues that have a *0* in the *max_packet* field will forward packets with strict priority scheduling. The remaining queues, that do not have a *0* in their *max_packet* field, will follow a weighted round-robin (*WRR*) method of forwarding packets — as long as the priority queues with a *0* in their *max_packet* field are empty. When a packet arrives in a priority queue with a *0* in its *max_packet* field, this queue will automatically begin forwarding packets until it is empty. Once a priority queue with a *0* in its *max_packet* field is empty, the remaining priority queues will reset the weighted round-robin (*WRR*) cycle of forwarding packets, starting with the highest available priority queue. Priority queues with an equal level of priority and equal entries in their *max_packet* field will empty their fields based on hardware priority scheduling.

Parameters

<class_id> − Specifies which of the seven priority queues the **config scheduling** command will be applied to. The seven priority queues are identified by number − from 0 to 6 − with queue 0 being the highest priority.

max_packet <value 0-15> − Specifies the maximum number of packets the above specified priority queue will be allowed to transmit per weighted round-robin (*WRR*) cycle. A value between 0 and 15 packets can be specified. A zero (**0**) denotes strict priority scheduling for that priority queue.

Restrictions

Only administrator-level users can issue this command.

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

Example usage:

To configure traffic scheduling:

```
DGS-3324SR:4# config scheduling 0 max_packet 15
Command: config scheduling 0 max_packet 15


 Success.


DGS-3324SR:4#
```

Example usage:

To configure a Combination Queue with a Class 6 priority queue with strict priority and the remaining Classes as weighted round robin (WRR) scheduling:

```
DGS-3324SR:4# config scheduling 6 max_packet 0
Command: config scheduling 6 max_packet 0


 Success.


DGS-3324SR:4#
```

show scheduling

Purpose	Used to display the currently configured traffic scheduling on the switch.
Syntax	**show scheduling**
Description	The **show scheduling** command displays the current configuration for the maximum number of packets (**max_packets**) assigned to the eight priority queues on the switch. At this value, it will empty the eight hardware queues in order, from the highest priority (queue 6) to the lowest priority (queue 0).
Parameters	None.
Restrictions	None.

Example usage:

To display the current scheduling configuration with Class 1 as the strict priority queue of a Combination Queue:

```
DGS-3324SR:4# show scheduling
Command: show scheduling

QOS Output Scheduling

              MAX. Packets

              ------------------
Class-0          1
Class-1          2
Class-2          3
Class-3          4
Class-4          5
Class-5          6
Class-6          7


DGS-3324SR:4#
```

config 802.1p user_priority

Purpose	Used to map the 802.1p user priority of an incoming packet to one of the eight hadware queues available on the switch.
Syntax	**config 802.1p user_priority <priority 0-7> <class_id 0-6>**
Description	The **config 802.1p user_priority** command is used to configure the way the switch will map an incoming packet, based on its 802.1p user priority tag, to one of the eight hardware priority queues available on the switch. The switch's default is to map the incoming 802.1p priority values to the four hardware queues according to the following chart:

802.1p Value	Switch Priority Queue	Remark
0	2	
1	0	
2	1	
3	3	
4	4	
5	5	

config 802.1p user_priority

	6	6
	7	6
Parameters	<priority 0-7> − Specifies which of the 8 802.1p priority values (0 through 7) you want to map to one of the switch's hardware priority queues (<class_id>, 0 through 6).	
	<class_id 0-6> − Specifies which of the switch's hardware priority queues the 802.1p priority value (specified above) will be mapped to.	
Restrictions	Only administrator-level users can issue this command.	

Example usage:

To configure 802.1 user priority on the switch:

```
DGS-3324SR:4# config 802.1p user_priority 1 3
Command: config 802.1p user_priority 1 3

 Success.

DGS-3324SR: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 eight hardware priority queues.
Parameters	None.
Restrictions	None.

Example usage:

To show 802.1p user priority:

```
DGS-3324SR:4# show 802.1p user_priority
Command: show 802.1p user_priority

COS Class of Traffic

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

DGS-3324SR:4#
```

config 802.1p default_priority

Purpose	Used to specify how to map an incoming packet that has no 802.1p priority tag to one of the switch's eight hardware priority queues.
Syntax	**config 802.1p default_priority [<portlist> | all] <priority 0-7>**
Description	The **config 802.1p default_priority** command allows you to specify the 802.1p priority value an untagged, incoming packet will be assigned before being forwarded to its destination.
Parameters	<portlist> – Specifies a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, **1:3** specifies switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. all – Specifies that the **config 802.1p default_priority** command will be applied to all ports on the switch. <priority 0-7> – Specifies the 802.1p priority value that an untagged, incoming packet will be given before being forwarded to its destination.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure 802.1p default priority on the switch:

```
DGS-3324SR:4#config 802.1p default_priority all 5
Command: config 802.1p default_priority all 5

Success.

DGS-3324SR:4#
```

show 802.1 default_priority

Purpose	Used to display the currently configured 802.1p priority value that will be assigned to an incoming, untagged packet before being forwarded to its destination.
Syntax	**show 802.1p default_priority {<portlist>}**
Description	The **show 802.1p default_priority** command displays the currently configured 802.1p priority value that will be assigned to an incoming, untagged packet before being forwarded to its destination.
Parameters	<portlist> − Specifies a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, **1:3** specifies switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 − in numerical order.
Restrictions	None.

Example usage:

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

```
DGS-3324SR:4# show 802.1p default_priority
Command: show 802.1p default_priority

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

DGS-3324SR:4#
```

config scheduling_mechanism

Purpose	Used to configure the scheduling mechanism for the QoS function
Syntax	**config scheduling mechanism [strict | weight_fair]**
Description	The **config scheduling_mechanism** command allows the user to select between a **Weight Fair (WRR)** and a **Strict** mechanism for emptying the priority queues of the QoS function. The switch contains 8 hardware priority queues. Incoming packets must be mapped to one of these eight queues. This command is used to specify the rotation by which these eight hardware priority queues are emptied.
	The switch's default is to empty the 8 hardware priority queues in order – from the highest priority queue (hardware queue 1) to the lowest priority queue (hardware queue 6). 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.

config scheduling_mechanism

Parameters	strict – Entering the **strict** parameter indicates that the highest queue is the first to be processed. That is, the highest queue should finish emptying before the others begin. weight_fair – Entering the weight fair parameter indicates that the priority queues will empty packets in a weightd round-robin (*WRR*) order. That is to say that they will be emptied in an even distribution.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the traffic scheduling mechanism for each COS queue:

```
DGS-3324SR:4#config scheduling_mechanism strict
Command: config scheduling_mechanism strict

Success.

DGS-3324SR:4#
```

show scheduling_mechanism

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

Example Usage:

To show the scheduling mechanism:

```
DGS-3324SR:4#show scheduling_mechanism
Command: show scheduling_mechanism

QOS scheduling_mechanism
CLASS ID  Mechanism
--------      -----------
Class-0    strict
Class-1    strict
Class-2    strict
Class-3    strict
Class-4    strict
Class-5    strict
Class-6    strict


DGS-3324SR:4#
```

enable hol_prevention

Purpose	Used to enable HOL prevention.
Syntax	**enable hol_prevention**
Description	The enable hol_prevention command enables Head of Line prevention.
Parameters	none.
Restrictions	You must have administrator privileges.

Example Usage:

To enable HOL prevention:

```
DGS-3324SR:4#enable hol_prevention
Command: enable hol_prevention

Success.

DGS-3324SR:4#
```

disable hol_prevention

Purpose	Used to disable HOL prevention.
Syntax	**disable hol_prevention**
Description	The disable hol_prevention command disables Head of Line prevention.
Parameters	none.

disable hol_prevention

Restrictions	You must have administrator privileges.

Example Usage:

To disable HOL prevention:

```
DGS-3324SR:4#disable hol_prevention
Command: disable hol_prevention


Success.


DGS-3324SR:4#
```

show hol_prevention

Purpose	Used to show HOL prevention.
Syntax	**show hol_prevention**
Description	The show hol_prevention command displays the Head of Line prevention state.
Parameters	none.
Restrictions	none.

Example Usage:

To show HOL prevention:

```
DGS-3324SR:4#show hol_prevention
Command: show hol_prevention


Device HOL Prevention State Enabled


DGS-3324SR:4#
```

PORT MIRRORING COMMANDS

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

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

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

config mirror port	
Purpose	Used to configure a mirror port – source port pair on the switch.
Syntax	**config mirror port <port> add source ports <portlist> [rx | tx | both]**
Description	This command allows a range of ports to have all of their traffic also sent to a designated port, where a network sniffer or other device can monitor the network traffic. In addition, you can specify that only traffic received by or sent by one or both is mirrored to the Target port.
Parameters	<port> – This specifies the Target port (the port where mirrored packets will be sent). source ports – The port or ports being mirrored. This cannot include the Target port. <portlist> – This specifies a range of ports that will be mirrored. That is, the range of ports in which all traffic will be copied and sent to the Target port. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, **1:3** specifies switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. rx – Allows the mirroring of only packets received by (flowing into) the port or ports in the port list.

config mirror port

	tx – Allows the mirroring of only packets sent to (flowing out of) the port or ports in the port list.
	both – Mirrors all the packets received or sent by the port or ports in the port list.
Restrictions	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:

```
DGS-3324SR:4# config mirror port 1:7 add source ports 1:1-1:5
both
Command: config mirror port 1:7 add source ports 1:1-1:5 both

Success.

DGS-3324SR: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 sent).
	<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.
	rx – Allows the mirroring of only packets received by (flowing into) the port or ports in the port list.
	tx – Allows the mirroring of only packets sent to (flowing out of) the port or ports in the port list.
	both – Mirrors all the packets received or sent by the port or ports in the port list.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete the mirroring ports:

```
DGS-3324SR:4#config mirror port 1:7 delete source port 1:1-1:5
both
Command: config mirror 1:7 delete source 1:1-1:5 both

Success.

DGS-3324SR:4#
```

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

Example usage:

To enable mirroring configurations:

```
DGS-3324SR:4#enable mirror
Command: enable mirror

 Success.

DGS-3324SR: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:

```
DGS-3324SR:4#disable mirror
Command: disable mirror

 Success.

DGS-3324SR:4#
```

show mirror

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

Example usage:

To display mirroring configuration:

```
DGS-3324SR:4#show mirror
Command: show mirror

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

DGS-3324SR:4#
```

VLAN COMMANDS

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

Command	Parameters
create vlan	<vlan_name 32> {tag <vlanid 2-4094> | advertisement}
delete vlan	<vlan_name 32>
config vlan	<vlan_name 32> {[add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enabled | disabled]}
config gvrp	[<portlist> | all] {state [enabled | disabled] | ingress_checking [enabled | disabled] | 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 2-4094> | 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. <vlanid> – The VLAN ID of the VLAN to be created. Allowed values = 2-4094 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:

```
DGS-3324SR:4#create vlan v1 tag 2
Command: create vlan v1 tag 2


 Success.


DGS-3324SR: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":

```
DGS-3324SR:4#delete vlan v1
Command: delete vlan v1


 Success.


DGS-3324SR: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 [enabled	disabled]}**
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.
	add − Specifies all of the ports on the switch.

config vlan

	tagged − Specifies the additional ports as tagged.
	untagged − Specifies the additional ports as untagged.
	forbidden − Specifies the additional ports as forbidden.
	delete − Deletes the above specified VLAN from the switch.
	<portlist> − A range of ports to add to the VLAN. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, **1:3** specifies switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 − in numerical order.
	advertisement [enabled|disabled] − Enables or disables GVRP on the specified VLAN.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DGS-3324SR:4#config vlan v1 add tagged 2:4-2:8
Command: config vlan v1 add tagged 2:4-2:8


 Success.


DGS-3324SR:4#
```

config gvrp

Purpose	Used to configure GVRP on the switch.
Syntax	**config gvrp [<portlist> | all] {state [enabled | disabled] | ingress_checking [enabled | disabled] | 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

116

config gvrp

	VLAN ID (PVID).
Parameters	<portlist> – A range of ports for which you want ingress checking. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, **1:3** specifies switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. all – Specifies all of the ports on the switch. state [enabled | disabled] – Enables or disables GVRP for the ports specified in the port list. ingress_checking [enabled | disabled] – Enables or disables ingress checking for the specified port list. 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. 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 :

```
DGS-3324SR:4#config gvrp 1:1-1:4 state enabled
ingress_checking enabled acceptable_frame tagged_only pvid 2
Command: config gvrp 1:1-1:4 state enabled ingress_checking
enabled acceptable_frame tagged_only pvid 2


Success.


DGS-3324SR: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):

```
DGS-3324SR:4#enable gvrp
Command: enable gvrp


 Success.


DGS-3324SR: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):

```
DGS-3324SR:4#disable gvrp
Command: disable gvrp


 Success.


DGS-3324SR: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:

```
DGS-3324SR:4#show vlan
Command: show vlan

VID             : 1              VLAN Name       : default
VLAN TYPE       : static         Advertisement   : Enabled
Member ports    : 1:1-1:24,2:1-2:24
 Static ports   : 1:1-1:24,2:1-2:24
Untagged ports  : 1:1-1:24,2:1-2:24
Forbidden ports :
VID             : 2              VLAN Name       : v1
VLAN TYPE       : static         Advertisement   : Disabled
Member ports    : 1:24,2:24
 Static ports   : 1:24,2:24
Untagged ports  :
Forbidden ports :


 Total Entries : 2


DGS-3324SR: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

show gvrp

Parameters	<portlist> – Specifies a range of ports for which the GVRP status is to be displayed. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, **1:3** specifies switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.
Restrictions	None.

Example usage:

To display GVRP port status:

```
DGS-3324SR: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

DGS-3324SR:4#
```

LINK AGGREGATION COMMANDS

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

Command	Parameters
create link_aggregation	group_id <value 1-32> {type[lacp|static]}
delete link_aggregation	group_id <value 1-32>
config link_aggregation	group_id <value1-32> {master_port <port> | ports <portlist> state [enabled | disabled]}
config link_aggregation algorithm	[mac_source | mac_destination |mac_source_dest | ip_source | ip_destination | ip_source_dest]
show link_aggregation	group_id <value 1-32> 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 1-32> {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 32 link aggregation groups to be configured. The group number identifies each of the groups.
	type – Specify the type of link aggregation used for the group. If the type is not specified the default type is static.
	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.
	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

create link_aggregation

	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:

```
DGS-3324SR:4#create link_aggregation group_id 1
Command: create link_aggregation group_id 1


 Success.


DGS-3324SR:4#
```

delete link_aggregation group_id

Purpose	Used to delete a previously configured link aggregation group.
Syntax	**delete link_aggregation group_id <value 1-32>**
Description	This command is used to delete a previously configured link aggregation group.
Parameters	<value> – Specifies the group id. The switch allows up to 32 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:

```
DGS-3324SR:4#delete link_aggregation group_id 6
Command: delete link_aggregation group_id 6


 Success.


DGS-3324SR:4#
```

config link_aggregation

Purpose	Used to configure a previously created link aggregation group.

config link_aggregation

Syntax	**config link_aggregation group_id <value 1-32> {master_port <port>	ports <portlist>	state [enabled	disabled]**
Description	This command allows you to configure a link aggregation group that was created with the **create link_aggregation** command above. The DGS-3324SR 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 32 link aggregation groups to be configured. The group number identifies each of the groups. 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 with the master port. ports<portlist> – Specifies a range of ports that will belong to the link aggregation group. Ports are specified by entering the lowest port number in a group, and then the highest port number in a group, separated by a dash such as **1-3**. Additional ports can be individually entered by their port number, separated by commas. So, a port group including the switch ports 1, 2, and 3 would be entered as **1-3**. Ports that are not contained within a group are specified by entering their port number, separated by a comma. So, the port group 1-3 and port 24 would be entered as **1-3,24**. Ports may be listed in only one port aggregation group, that is, link aggregation groups may not overlap. state [enabled	disabled] – 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 of module 1 with group members ports 5-7 plus port 9:

```
DGS-3324SR:4#config link_aggregation group_id 1 master_port 1:5 ports
1:5-1:7, 1:9
Command: config link_aggregation group_id 1 master_port 1:5 ports 1:5-
1:7, 1:9


Success.


DGS-3324SR: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. mac_destination – Indicates that the switch should examine the MAC destination address. mac_source_dest – Indicates that the switch should examine the MAC source and destination addresses ip_source – Indicates that the switch should examine the IP source address. ip_destination – Indicates that the switch should examine the IP destination address. ip_source_dest – Indicates that the switch should examine the IP source address and the destination address.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DGS-3324SR:4#config link_aggregation algorithm
mac_source_dest
Command: config link_aggregation algorithm mac_source_dest


 Success.


DGS-3324SR:4#
```

show link_aggregation

Purpose	Used to display the current link aggregation configuration on the switch.
Syntax	**show link_aggregation {group_id <value 1-32>	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 32 link aggregation groups to be configured. The group number identifies each of the groups.
	algorithm – Allows you to specify the display of link aggregation by the algorithm in use by that group.
Restrictions	None.

Example usage:

To display Link Aggregation configuration:

```
DGS-3324SR:4#show link_aggregation
Command: show link_aggregation


Link Aggregation Algorithm = MAC-source-dest
Group ID     : 1
Master Port   : 2:17
Member Port   : 1:5-1:10,2:17
Active Port:
Status       : Disabled
Flooding Port : 1:5
```

config lacp_ports

Purpose	Used to configure settings for LACP compliant ports.

config lacp_ports

Syntax	**config lacp_ports <portlist> mode [active | passive]**
Description	This command is used to configure ports that have been previously designated as LACP ports (see create link_aggregation).
Parameters	<portlist> − Specifies a range of ports to be configured. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 specifies port 3. **4** specifies port 4. **3-4** specifies all of the ports between port 3 and port 4 − in numerical order. mode – Select the mode to determine if LACP ports will initially send LACP control frames. 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. passive – LACP ports that are designated as passive cannot initially send 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:

```
DGS-3324SR:4#config lacp_port 1:1-1:12 mode active
Command: config lacp_port 1:1-1:12 mode active

Success.

DGS-3324SR:4#
```

show lacp_port

Purpose	Used to display current LACP port mode settings.

show lacp_port

Syntax	**show lacp_port {<portlist>}**
Description	This command will display the LACP mode settings as they are currently configured.
Parameters	<portlist> - Specifies a range of ports to be configured. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 specifies port 3. **4** specifies port 4. **3-4** specifies all of the ports between port 3 and port 4 − in numerical order.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To display LACP port mode settings:

```
DGS-3324SR:4#show lacp_port
Command: show lacp_port

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

DGS-3324SR:4#
```

BASIC IP COMMANDS

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

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

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

enable ipif	
Purpose	Used to enable an IP interface on the switch.
Syntax	**enable ipif {<ipif_name 12>	all}**
Description	This command will enable the IP interface function on the switch.
Parameters	<ipif_name> – The name for the IP interface to be created.
	all – Entering this parameter will delete all the IP interfaces currently configured on the switch.
Restrictions	none

Example usage:

To enable the ipif function on the switch:

```
DGS-3324SR:4#enable ipif s2
Command: enable ipif s2


Success.


DGS-3324SR:4#
```

create ipif	
Purpose	Used to create an IP interface on the switch.

create ipif

Syntax	**create ipif <ipif_name 12> <network_address> <vlan_name 32> {state [enabled	disabled]}**
Description	This command will create an IP interface.
Parameters	<ipif_name> − The name for the IP interface to be created. <vlan_name> − The name of the VLAN that will be associated with the above IP interface. <network_address> − IP address and netmask of the IP interface to be created. You can specify the address and mask information using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8). state [enabled	disabled] − Allows you to enable or disable the IP interface.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create an IP interface on the switch:

```
DGS-3324SR:4#create ipif System ipaddress 10.48.74.122/8 v2
state enabled
Command: create ipif System ipaddress 10.48.74.122/8 v2 state
enabled


 Success.

DGS-3324SR:4#
```

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	<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).

129

config ipif

	<vlan_name 32> – The name of the VLAN corresponding to the System IP interface.
	state [enabled | disabled] – Allows you to enable or disable the IP interface.
	bootp – Allows the selection of the BOOTP protocol for the assignment of an IP address to the switch's System IP interface.
	dhcp – Allows the selection of the DHCP protocol for the assignment of an IP address to the switch's System IP interface.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the IP interface System:

```
DGS-3324SR:4#config ipif System ipaddress 10.48.74.122/8
Command: config ipif System ipaddress 10.48.74.122/8

 Success.

DGS-3324SR: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.

```
DGS-3324SR: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  : 1:1-1:24


DGS-3324SR:4#
```

delete ipif

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

Example usage:

To delete the IP interface named s2:

```
DGS-3324SR:4#delete ipif s2
Command: delete ipif s2


Success.


DGS-3324SR:4#
```

disable ipif

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

disable ipif

	an IP interface on the switch.
Parameters	<ipif_name> – The name created for the IP interface. all – Entering this parameter will delete all the IP interfaces currently configured on the switch.
Restrictions	None.

Example usage:

To disable the IP interface named "s2":

```
DGS-3324SR:4#disable ipif s2
Command: disable ipif s2


Success.


DGS-3324SR:4#
```

IGMP SNOOPING COMMANDS

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

Command	Parameters
config igmp_snooping	[<vlan_name 32>	all] {host_timeout <sec 1-16711450>	router_timeout < sec 1-16711450>	leave_timer < sec 1-16711450>	state [enabled	disabled]}
config igmp_snooping querier	[<vlan_name 32>	all] {query_interval <sec 1-65535>	max_response_time <sec 1-25>	robustness_variable <value 1-255>	last_member_query_interval <sec 1-25>	state [enabled	disabled]
config router_ports	<vlan_name 32> [add	delete] <portlist>
config router_ports_forbidden	<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>}

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

config igmp_snooping	
Purpose	Used to configure IGMP snooping on the switch.
Syntax	**config igmp_snooping [<vlan_name 32>	all] {host_timeout <sec 1-16711450>	router_timeout < sec 1-16711450>	leave_timer < sec 1-16711450>	state [enabled	disabled]}**
Description	This command allows you to configure IGMP snooping on the switch.
Parameters	<vlan_name 32> − The name of the VLAN for which IGMP snooping is to be configured. host_timeout <sec> − 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. router_timeout <sec> − Specifies the maximum

config igmp_snooping

	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.
	leave_timer <sec> − Leave timer. The default is 2 seconds.
	state [enabled | disabled] − Allows you to enable or disable IGMP snooping for the specified VLAN.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the igmp snooping:

```
DGS-3324SR:4#config igmp_snooping default host_timeout 250
state enabled
Command: config igmp_snooping default host_timeout 250 state
enabled


 Success.


DGS-3324SR: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 [enabled | disabled]**
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. query_interval <sec> − Specifies the amount of time in seconds between general query transmissions. The default setting is 125 seconds. max_response_time <sec> − Specifies the

config igmp_snooping querier

	maximum time in seconds to wait for reports from members. The default setting is 10 seconds. 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: • Group member interval—Amount of time that must pass before a multicast router decides there are no more members of a group on a network. This interval is calculated as follows: (robustness variable x query interval) + (1 x query response interval). • Other querier present interval—Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: (robustness variable x query interval) + (0.5 x query response interval). • Last member query count—Number of group-specific queries sent before the router assumes there are no local members of a group. The default number is the value of the robustness variable. • By default, the robustness variable is set to 2. You might want to increase this value if you expect a subnet to be lossy. Although 1 is specified as a valid entry, the roubustness variable should not be one or problems may arise. 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. state [enabled | disabled] − Allows the switch to be specified as an IGMP Querier or Non-querier.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the igmp snooping:

```
DGS-3324SR:4#config igmp_snooping querier default
query_interval 125 state enabled


Command: config igmp_snooping querier default query_interval
125 state enabled


 Success.


DGS-3324SR: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. <portlist> − Specifies a range of ports that will be configured as router ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, **1:3** specifies switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 − in numerical order.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To set up static router ports:

```
DGS-3324SR:4#config router_ports default add 2:1-2:10
Command: config router_ports default add 2:1-2:10


 Success.


DGS-3324SR:4#
```

config router_ports_forbidden

Purpose	Used to configure ports as forbidden multicast router ports.
Syntax	**config router_ports_forbidden <vlan_name 32> [add | delete] <portlist>**
Description	This command allows you to designate a port or range of ports as being forbidden to multicast-enabled routers. This will ensure that multicast packets will not be forwarded to this port − regardless of protocol, etc.
Parameters	<vlan_name 32> − The name of the VLAN on which the router port resides. <portlist> − Specifies a range of ports that will be configured as forbidden router ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, **1:3** specifies switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 − in numerical order.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To set up forbidden router ports:

```
DGS-3324SR:4#config router_ports_forbidden default
add 2:1-2:10

Command: config router_ports_forbidden default add 2:1-
2:10


 Success.


DGS-3324SR: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

enable igmp_snooping

	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:

```
DGS-3324SR:4#enable igmp_snooping
Command: enable igmp_snooping


 Success.
DGS-3324SR:4#
```

disable igmp_snooping

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

Example usage:

To disable IGMP snooping on the switch:

```
DGS-3324SR:4#disable igmp_snooping
Command: disable igmp_snooping


 Success.


DGS-3324SR:4#
```

show igmp_snooping

Purpose	Used to show the current status of IGMP snooping on the switch.

show igmp_snooping

	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:

```
DGS-3324SR: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

DGS-3324SR: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>}**

show igmp_snooping group

	\<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:

```
DGS-3324SR:4#show igmp_snooping group
Command: show igmp_snooping group

 VLAN Name    : default
 Multicast group: 224.0.0.2
 MAC address   : 01-00-5E-00-00-02
 Reports       : 1
 Port Member   : 1:26,2:7

 VLAN Name    : default
 Multicast group: 224.0.0.9
 MAC address   : 01-00-5E-00-00-09
 Reports       : 1
 Port Member   : 1:26,2:7
 VLAN Name    : default
 Multicast group: 234.5.6.7
 MAC address   : 01-00-5E-05-06-07
 Reports       : 1
 Port Member   : 1:26,2:9

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

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

 VLAN Name    : default
 Multicast group: 239.255.255.254
 MAC address   : 01-00-5E-7F-FF-FE
 Reports       : 1
 Port Member   : 1:26,2:7
```

```
 Total Entries   : 6

DGS-3324SR: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	forbidden}**
Description	This command will display the router ports currently configured on the switch.
Parameters	<vlan_name 32> – The name of the VLAN on which the router port resides. static – Displays router ports that have been statically configured. dynamic – Displays router ports that have been dynamically configured. forbidden –Displays router ports that have been labeled as forbidden.
Restrictions	None.

Example usage:

To display the router ports.

```
DGS-3324SR:4#show router_ports
Command: show router_ports

VLAN Name        : default
Static router port     : 2:1-2:10
Dynamic router port   :
Forbidden Router Port:

VLAN Name        : vlan2
Static router port     :
Dynamic router port   :
Forbidden Router Port:

 Total Entries: 2

DGS-3324SR: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>}**

show igmp_snooping forwarding

Description	This command will display the current IGMP snooping forwardingtable 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":

```
DGS-3324SR: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    : 1:17


 Total Entries: 1


 DGS-3324SR:4#
```

802.1X COMMANDS

The DGS-3324SR 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	
create 802.1x user	<username 15>
show 802.1x user	
delete 802.1x user	
show 802.1x auth_state	ports [<portlist>	all]
show 802.1x auth_configuration	ports [<portlist>	all]
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	[local	radius eap]
config 802.1x init	{port_based ports [<portlist>	all]}
config 802.1x reauth	{port_based ports [<portlist>	all]}
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	
show acct_client	
show auth_client	
show auth_diagnostics	{ports<portlist>}
show auth_session statistics	{ports<portlist>}
show	{ports<portlist>}

Command	Parameters
auth_statistics	

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

Example usage:

To enable 802.1x switch wide:

```
DGS-3324SR:4#enable 802.1x
Command: enable 802.1x


 Success.


DGS-3324SR: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:

```
DGS-3324SR:4#disable 802.1x
Command: disable 802.1x


 Success.


DGS-3324SR:4#
```

create 802.1x user

Purpose	Used to create a new 802.1x user.
Syntax	**create 802.1x user <username 15>**
Description	The create 802.1x user command is used to create new 802.1x users.
Parameters	<username 15> − A username can be as many as 15 alphanumeric characters.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To create an 802.1x user:

```
DGS-3324SR:4#create 802.1x user dtremblett
Command: create 802.1x user dtremblett


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


DGS-3324SR:4#
```

show 802.1x user

Purpose	Used to display the 802.1x user accounts on the switch.
Syntax	**show 802.1x user <username 15>**
Description	The **show 802.1x user** command is used to display the 802.1x Port-based Network Access control local users currently configured on the switch.
Parameters	<username 15> − A username can be as many as 15 alphanumeric characters.
Restrictions	None.

Example usage:

To view 802.1X users currently configured on the Switch:

```
DGS-3324SR:4#show 802.1x user
Command: show 802.1x user
Current Accounts:
Username          Password
--------------     --------------
Darren            Trinity


Total entries: 1


DGS-3324SR:4#
```

delete 802.1x user

Purpose	Used to delete an 802.1x user account on the switch.
Syntax	**delete 802.1x user <username 15>**
Description	The **delete 802.1x user** command is used to display the 802.1x Port-based Network Access control local users currently configured on the switch.
Parameters	<username 15> – A username can be as many as 15 alphanumeric characters.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete 802.1x users:

```
DGS-3324SR:4#delete 802.1x user
Command: delete 802.1x user dtremblett



Success.

DGS-3324SR: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>| all]}**
Description	The show 802.1x command is used to display the current configuration of the 802.1x Port-

show 802.1x auth_configuration

	based Network Access Control server application on the switch.
Parameters	ports

- <portlist> − Specifies a range of ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 − in numerical order.

- all – denotes all ports on the Switch.

The following details what is displayed:

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

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

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

Capability: 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.

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.

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.

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.

show 802.1x auth_configuration

	QuietPeriod – Shows the time interval between authentication failure and the start of a new authentication attempt.
	TxPeriod – Shows the time to wait for a response from a supplicant (user) to send EAP Request|Identiy packets.
	SuppTimeout – Shows the time to wait for a response from a supplicant (user) for all EAP packets, except for the Request|Identity packets.
	ServerTimeout – Shows the length of time to wait for a response from a Radius server.
	MaxReq – Shows the maximum number of times to retry sending packets to the supplicant.
	ReAuthPeriod – shows the time interval between successive re-authentications.
	ReAuthenticate: Enabled|Disabled – Shows whether or not to re-authenticate.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DGS-3324SR: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 | all>}**
Description	The show 802.1x auth_state command is used to display the current authentication state of the 802.1x Port-based Network Access Control server application on the switch.
Parameters	ports • <portlist> – Specifies a range of ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.

show 802.1x auth_state

- all – denotes all ports on the Switch

The following details what is displayed:

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

Auth PAE State: Initalize|Disconnected|Connecting| Authenticating|Authenticated|Held |ForceAuth|ForceUnauth – Shows the current state of the Authenticator PAE.

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

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

Restrictions	Only administrator-level users can issue this command.

Example usage:

To display the 802.1x auth state:

```
DGS-3324SR:4#show 802.1x auth_state
Command: show 802.1x auth_state


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

config 802.1x capability

Purpose	Used to configure the 802.1x capability of a range of ports on the switch.
Syntax	**config 802.1x capability ports [<portlist>	all] [authenticator	none]**
Description	The **config 802.1x** command has four capabilities that can be set for each port. Authenticator, Supplicant, Authenticator and Supplicant, and None.
Parameters	<portlist> – Specifies a range of ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, **1:3** specifies switch number 1, port 3. **2:4**

config 802.1x capability

	specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 − in numerical order.
	all − Specifies all of the ports on the switch.
	authenticator − A user must pass the authentication process to gain access to the network.
	none − The port is not controlled by the 802.1x functions.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DGS-3324SR:4#config 802.1x capability ports 1:1 – 1:10
authenticator
Command: config 802.1x capability ports 1-10 authenticator


 Success.


DGS-3324SR: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 range of ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are

config 802.1x auth_parameter

specified. The beginning and end of the port list range are separated by a dash. For example, **1:3** specifies switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.

all – Specifies all of the ports on the switch.

default – Returns all of the ports in the specified range to their 802.1x default settings.

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

port_control – Configures the administrative control over the authentication process for the range of ports.The user has the following authentication options:

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

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

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

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

tx_period <sec 1-65535> - Configures the time to wait for a response from a supplicant (user) to send EAP Request/Identity packets.

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.

server_timeout <sec 1-65535> - Configure the length of time to wait for a response from a Radius server.

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

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

config 802.1x auth_parameter

	authentications.
	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:

```
DGS-3324SR:4#config 802.1x auth_parameter ports 1:1 – 1:20
direction both
Command: config 802.1x auth_parameter ports 1:1-1:20 direction
both


 Success.


DGS-3324SR:4#
```

config 802.1x auth_protocol

Purpose	Used to configure the 802.1x authentication protocol on the switch.
Syntax	**config 802.1x auth_protocol [local | radius_eap]**
Description	The config 802.1x auth_protocol command enables you to configure the authentication protocol.
Parameters	Local | radius_eap – 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:

```
DGS-3324SR:4# config 802.1x auth_protocol local
Command: config 802.1x auth_protocol local


 Success.


DGS-3324SR: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>] }**
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. <portlist> – Specifies a range of ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, **1:3** specifies switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. 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:

```
DGS-3324SR:4# config 802.1x init port_based ports all
Command: config 802.1x init port_based ports all

Success.

DGS-3324SR: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>}**
Description	The config 802.1x reauth command is used to re-authenticate a previously authenticated

config 802.1x reauth

	device based on port number.
Parameters	port_based – This instructs the switch to re-authorize 802.1x function based only on the port number. Ports approved for re-authorization can then be specified. ports <portlist> – Specifies a range of ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, **1:3** specifies switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. 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:

```
DGS-3324SR:4#config 802.1x reauth port_based ports 1-18
Command: config 802.1x reauth port_based ports 1-18

Success.

DGS-3324SR: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.

config radius add

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.
	<server_ip> − The IP address of the RADIUS server.
	key − Specifies that a password and encryption key will be used between the switch and the Radius server.
	<passwd 32> − The shared-secret key used by the RADIUS server and the switch. Up to 32 characters can be used.
	default − Uses the default udp port number in both the "auth_port" and "acct_port" settings.
	auth_port <udp_port_number> − The UDP port number for authentication requests. The default is 1812.
	acct_port <udp_port_number> − The UDP port number for accounting requests. The default is 1813.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the RADIUS server communication setttings:

```
DGS-3324SR: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.
DGS-3324SR: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.

config radius delete

Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete previously configured RADIUS server communication settings:

```
DGS-3324SR:4#config radius delete 1
Command: config radius delete 1


 Success.


DGS-3324SR: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.
	<server_ip> – The IP address of the Radius server.
	key – Specifies that a password and encryption key will be used between the switch and the RADIUS server.
	<passwd 32> – The shared-secret key used by the RADIUS server and the switch. Up to 32 characters can be used.
	default – Uses the default udp port number in both the "auth_port" and "acct_port" settings.
	auth_port <udp_port_number> – The UDP port number for authentication requests. The default is 1812.
	acct_port <udp_port_number> – The UDP port number for accounting requests. The default is 1813.

config radius

Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the RADIUS settings:

```
DGS-3324SR:4#config radius 1 10.48.74.121 key dlink default
Command: config radius 1 10.48.74.121 key dlink default

 Success.

DGS-3324SR: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:

```
DGS-3324SR: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

DGS-3324SR:4#
```

show acct_client

Purpose	Used to display the current RADIUS accounting client.
Syntax	**show acct_client**
Description	The show radius acct_client command is used to display the current RADIUS accounting client currently configured on the switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the current RADIUS accounting client:

```
DGS-3324SR:4#show acct_client
Command: show acct_client


 radiusAcctClient ==>
 radiusAcctClientIdentifier          D-Link


 radiusAuthServerEntry ==>
 radiusAccServerIndex : 1


 radiusAccServerAddress           10.53.13.199
 radiusAccClientServerPortNumber       32
 radiusAccClientRoundTripTime          0
 radiusAccClientRequests           0
 radiusAccClientRetransmissions        0
 radiusAccClientResponses          0
 radiusAccClientMalformedResponses      0
 radiusAccClientBadAuthenticators       0
 radiusAccClientPendingRequests        0
 radiusAccClientTimeouts           0
 radiusAccClientUnknownTypes          0
 radiusAccClientPacketsDropped         0
 CTRL+C ESC q Quit SPACE n Next Page Enter Next Entry a All
```

show auth_client

Purpose	Used to display the current RADIUS authentication client.
Syntax	**show auth_client**

show auth_client

Description	The show radius auth_client command is used to display the current RADIUS authentication client currently configured on the switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the current RADIUS authentication client:

```
DGS-3324SR:4#show auth_client
Command: show auth_client


radiusAuthClient ==>
radiusAuthClientInvalidServerAddresses   0
radiusAuthClientIdentifier          D-Link


radiusAuthServerEntry ==>
radiusAuthServerIndex :1


radiusAuthServerAddress              10.53.13.199
radiusAuthClientServerPortNumber        25
radiusAuthClientRoundTripTime          0
radiusAuthClientAccessRequests         0
radiusAuthClientAccessRetransmissions   0
radiusAuthClientAccessAccepts          0
radiusAuthClientAccessRejects          0
radiusAuthClientAccessChallenges        0
radiusAuthClientMalformedAccessResponses 0
radiusAuthClientBadAuthenticators       0
radiusAuthClientPendingRequests         0
radiusAuthClientTimeouts               0
radiusAuthClientUnknownTypes            0
radiusAuthClientPacketsDropped          0
CTRL+C ESC q Quit SPACE n Next Page Enter Next Entry a All
```

show auth_diagnostics

Purpose	Used to display the current authentication diagnostics.
Syntax	**show auth_diagnostics {ports <portlist>}**
Description	The show auth_diagnostics command is used to display the current authentication diagnostics of

show auth_diagnostics

	the switch on a per port basis.
Parameters	ports <portlist> – Specifies a range of ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, **1:3** specifies switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. If no parameter is entered, all ports will be shown.
Restrictions	None.

Example usage:

To display the current authentication diagnostics for port 16:

```
GS-3324SR:4#show auth_diagnostics ports 16
Command: show auth_diagnostics ports 1:16


 Port number : 1:16


 EntersConnecting                0
 EapLogoffsWhileConnecting            0
 EntersAuthenticating              0
 SuccessWhileAuthenticating          0
 TimeoutsWhileAuthenticating         0
 FailWhileAuthenticating          0
 ReauthsWhileAuthenticating          0
 EapStartsWhileAuthenticating        0
 EapLogoffWhileAuthenticating         0
 ReauthsWhileAuthenticated          0
 EapStartsWhileAuthenticated         0
 EapLogoffWhileAuthenticated          0
 BackendResponses               0
 BackendAccessChallenges           0
 BackendOtherRequestsToSupplicant     0
 BackendNonNakResponsesFromSupplicant  0
 BackendAuthSuccesses             0
 BackendAuthFails             0


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

show auth_session_statistics

Purpose	Used to display the current authentication session statistics.
Syntax	**show auth_session_statistics {ports <portlist>}**
Description	The show auth_session statistics command is used to display the current authentication session statistics of the switch on a per port basis.
Parameters	ports <portlist> – Specifies a range of ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example,

show auth_session_statistics

	1:3 specifies switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. If no parameter is entered, all ports will be shown.
Restrictions	None.

Example usage:

To display the current authentication session statistics for port 16:

```
DGS-3324SR:4#show auth_session_statistics ports 16
Command: show auth_session_statistics ports 1:16


 Port number : 1:16


 SessionOctetsRx            0
 SessionOctetsTx            0
 SessionFramesRx             0
 SessionFramesTx            0
 SessionId
 SessionAuthenticMethod     Remote Authentication Server
 SessionTime                0
 SessionTerminateCause      SupplicantLogoff
 SessionUserName


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

show auth_statistics

Purpose	Used to display the current authentication statistics.
Syntax	**show auth_statistics {ports <portlist>}**
Description	The show auth_statistics command is used to display the current authentication statistics of the switch on a per port basis.
Parameters	ports <portlist> – Specifies a range of ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, **1:3** specifies switch number 1, port 3. **2:4**

show auth_statistics

	specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. If no parameter is entered, all ports will be shown.
Restrictions	None.

Example usage:

To display the current authentication statistics for port 16:

```
DGS-3324SR:4#show auth_statistics ports 16
Command: show auth_statistics ports 1:16


 Port number : 1:16


 EapolFramesRx              0
 EapolFramesTx              0
 EapolStartFramesRx           0
 EapolReqIdFramesTx             0
 EapolLogoffFramesRx             0
 EapolReqFramesTx             0
 EapolRespIdFramesRx             0
 EapolRespFramesRx             0
 InvalidEapolFramesRx           0
 EapLengthErrorFramesRx            0


 LastEapolFrameVersion           0
 LastEapolFrameSource            00-00-00-00-00-00


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

ACCESS CONTROL LIST (ACL) COMMANDS

The DGS-3324SR 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 0x0-0xffff>} | protocol_id{user_mask <hex 0x0-0xffffffff>}]}]{port [<portlist>| all]} profile_id <value 1-8>
delete access_profile	profile_id <value 1-8>
config access_profile profile_id	<value 1-8>[add access_id <value 1-50>[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> | urg | ack | psh | rst | syn | fin } | udp {src_port <value 0-65535> | dst_port <value 0-65535>} | protocol_id <value 0 - 255> {user_define <hex 0x0-0xffffffff>}]}][permit { priority <value 0-7> { replace_priority} | replace_dscp <value 0-63> } |deny]| delete <value 1-50>]
show access_profile	{profile_id <value 1-8>}

Due to a chipset limitation, the switch currently supports a maximum of 8 access profiles, each containing a maximum of 50 rules − with the additional limitation of 50 rules total for all 8 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	**create access_profile [ethernet{ vlan	source_mac <macmask>	destination_mac <macmask>	802.1p	ethernet_type}| ip { vlan	source_ip_mask <netmask>	destination_ip_mask <netmask>	dscp	[icmp {type	code }	igmp {type }	tcp {src_port_mask <hex 0x0-0xffff>	dst_port_mask <hex 0x0-0xffff>|flag_mask [all	{urg	ack	psh	rst	syn	fin}] }	udp {src_port_mask <hex 0x0-0xffff>	dst_port_mask <hex 0x0-0xffff>}	protocol_id{user_mask <hex 0x0-0xffffffff>}]}]{port [<portlist>| all]} profile_id <value 1-8>**
Description	The **create access_profile** command is used to create an access profile on the switch and to define which parts of each incoming frame's header the switch will examine. Masks can be entered that will be combined with the values the switch finds in the specified frame header fields. Specific values for the rules are entered using the **config access_profile** command, below.
Parameters	ethernet – Specifies that the switch will examine the layer 2 part of each packet header.
	• vlan – Specifies that the switch will examine the VLAN part of each packet header.
	• source_mac <macmask> – Specifies a MAC address mask for the source MAC

create access_profile

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> −

168

create access_profile

	Specifies a TCP port mask for the destination port.
	• flag_mask [all	{urg	ack	psh	rst	syn	fin}] – Enter the appropriate flag_mask parameter. All incoming packets have TCP port numbers contained in them as the forwarding 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).
	• udp – Specifies that the switch will examine each frame's Universal Datagram Protocol (UDP) field.
	• src_port_mask <hex 0x0-0xffff> – Specifies a UDP port mask for the source port.
	• dst_port_mask <hex 0x0-0xffff> – Specifies a UDP port mask for the destination port.
	• protocol_id – Specifies that the switch will examine each frame's Protocol ID field.
	• user_mask <hex 0x0-0xffffffff> – Specifies that the rule applies to the IP protocol ID and the mask options behind the IP header.
	port<portlist> - Specifies a range of ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, **1:3** specifies switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.
	profile_id <value 1-8> – 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:

169

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

```
DGS-3324SR:4# create access_profile ip source_ip_mask
255.255.255.0 profile_id 1

Command: create access_profile ip source_ip_mask
255.255.255.0 profile_id 1


Success.


DGS-3324SR:4#
```

delete access_profile

Purpose	Used to delete a previously created access profile.
Syntax	**delete access_profile [profile_id <value 1-8>]**
Description	The **delete access_profile** command is used to delete a previously created access profile on the switch.
Parameters	profile_id <value 1-8> – 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.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DGS-3324SR:4# delete access_profile profile_id 1
Command: delete access_profile profile_id 1


Success.


DGS-3324SR: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**

config access_profile

Syntax	**config access_profile profile_id <value 1-8>[add access_id <value 1-50>[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>	urg	ack	psh	rst	syn	fin }	udp {src_port <value 0-65535>	dst_port <value 0-65535>}	protocol_id <value 0 - 255> {user_define <hex 0x0-0xffffffff>}]}]][permit { priority <value 0-7> { replace_priority}	replace_dscp <value 0-63> } |deny]| delete <value 1-50>]**
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 1-8> − an integer between 1 and 8 that is used to identify the access profile that will be configured using this command. This value is assigned to the access profile when it is created with the **create access_profile** command.
	add access_id <value 1-50> − Adds an additional rule to the above specified access profile. The value specifies the relative priority of the additional rule. The lower access ID, the higher the priority the rule will be given.
	ethernet − Specifies that the switch will look only into the layer 2 part of each packet.
	• vlan <vlan_name 32> − Specifies that the access profile will apply to only to this VLAN.
	• source_mac <macaddr> − Specifies that the access profile will apply to only packets with this source MAC address.
	• destination_mac <macaddr> − Specifies that the access profile will apply to only packets with this destination MAC address.
	• 802.1p <value 0-7> − Specifies that the access profile will apply only to packets

config access_profile

with this 802.1p priority value.

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

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

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

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

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

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

- 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.

- replace_priority − 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 <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.

- 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.

config access_profile

- 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.

- 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)

- 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

config access_profile

	found in the frame header using a logical AND operation.
	permit – Specifies that packets that match the access profile are permitted to be forwarded by the switch.
	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 <value 1-50> – Specifies the access ID of a rule you want to delete.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DGS-3324SR: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.


DGS-3324SR: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:

```
DGS-3324SR:4#show access_profile
Command: show access_profile


Access Profile Table


Access Profile ID: 1                         TYPE : Ethernet
Ports: 1:1
================================================================
MASK Option :
VLAN


-----------


Access ID : 1    Mode: Deny
-----------
0
================================================================


Access Profile ID: 2                         TYPE : IP
Ports: 1:1-1:24,2:1-2:24
================================================================
MASK Option :
Source IP MASK
255.255.255.0
-------------- ----------------
================================================================


Total Entries: 1


DGS-3324SR:4#
```

TRAFFIC SEGMENTATION COMMANDS

Traffic segmentation allows you to further sub-divide VLANs into smaller groups of ports that will help to reduce traffic on the VLAN. The VLAN rules take precedence, and then the traffic segmentation rules are applied.

Command	Parameters
config traffic_segmentation	[<portlist>| all] forward_list [null	all	<portlist>]
show traffic_segmentation	<portlist>

config traffic_segmentation

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

```
DGS-3324SR:4# config traffic_segmentation 1:1-1:10 forward_list
1:11-1:15
Command: config traffic_segmentation 1:1-1:10 forward_list 1:11-
1:15


Success.


DGS-3324SR:4#
```

show traffic_segmentation

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

Example usage:

To display the current traffic segmentation configuration on the switch.

```
DGS-3324SR:4#show traffic_segmentation
Command: show traffic_segmentation

Traffic Segmentation Table

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

```
2:13   1:1-1:24,2:1-2:24
2:14   1:1-1:24,2:1-2:24
2:15   1:1-1:24,2:1-2:24
2:16   1:1-1:24,2:1-2:24
2:17   1:1-1:24,2:1-2:24
2:18   1:1-1:24,2:1-2:24
2:19   1:1-1:24,2:1-2:24
2:20   1:1-1:24,2:1-2:24
2:21   1:1-1:24,2:1-2:24
2:22   1:1-1:24,2:1-2:24
2:23   1:1-1:24,2:1-2:24
2:24   1:1-1:24,2:1-2:24


DGS-3324SR:4#
```

STACKING COMMANDS

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

Command	Parameters
config box_priority	current_box_id <value 1-12> priority <value 1-16>
config box_id	current_box_id <value 1-12> new_box_id [auto|1|2|3|4|5|6|7|8|9|10|11|12]
config box_type	current_box_id <value 1-12> type [DGS-3324SR	BOX_NOTEXIST]
config all_boxes_id	[static_mode	auto_mode]
show stack_information	

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

config box_priority	
Purpose	Used to configure box priority, which determines which box becomes master. Lower numbers have higher priority..
Syntax	**config box_priority {current_box_id <value 1-12> priority <value 1-16>}**
Description	This command configures box (switch) priority.
Parameters	current_box_id – identifies the switch being configured. Range is 1-12.
	priority – assigns a priority value to the box, with lower numbers having higher priority. Range is 1-16.
Restrictions	Administrator privileges are needed to issue this command.

Usage Example:

To configure box priority:

```
DGS-3324SR:4#config box_priority current_box_id 1 priority 1
Command: config box_priority current_box_id 1 priority 1


 Success.


DGS-3324SR:4#
```

config box_id

Purpose	Used to configure box ID. Users can use this command to reassign box Ids.
Syntax	**config box_id {current_box_id <value 1-12> new_box_id [auto|1|2|3|4|5|6|7|8|9|10|11|12]}**
Description	This command will assign box Ids to switches in a stack.
Parameters	current_box_id – identifies the switch being configured. Range is 1-12. new_box_id – the new Id being assigned to the box. Range is 1-12. auto – allows the box ID to be assigned automatically.
Restrictions	Administrator privileges are needed to issue this command.

Usage Example:

To change a box ID:

```
DGS-3324SR:4#config box_id current_box_id 1 new_box_id 2
Command: config box_id current_box_id 1 new_box_id 2

 Success.

DGS-3324SR:4#
```

config box_type

Purpose	Used to configure box type.
Syntax	**config box_type {current_box_id <value 1-12> type [DGS-3324SR | BOX_NOTEXIST]}**
Description	This command will pre-assign the box type of switches in a stack.
Parameters	current_box_id – identifies the switch being configured. Range is 1-12. DGS-3324SR – Name of a switch that can be set in the stack. BOX_NOTEXIST – identifies a switch which may be added to the stack in future. A box_type may be assigned to this box, in effect to pre-configure it, as it is added to the stack. If box_type is not assigned, box is identified as BOX_NOTEXIST and box type will be identified

181

config box_type

	automatically.
Restrictions	Administrator privileges are needed to issue this command.

Usage Example:

To configure box type:

```
DGS-3324SR:4#config box_type current_box_id 3 type
BOX_NOTEXIST
Command: config box_type current_box_id 3 type
BOX_NOTEXIST


 Success.


DGS-3324SR:4#
```

config all_boxes_id

Purpose	Used to configure box IDs for switches in a stack.
Syntax	**config all_boxes _id [static_mode | auto_mode]**
Description	This command will determine the mode of assigning box IDs.
Parameters	static_mode –box IDs assigned by the user
	auto_mode – box IDs are assigned automatically
Restrictions	Administrator privileges are needed to issue this command.

Usage Example:

To configure box type:

```
DGS-3324SR:4#config all_boxes_id auto_mode
Command: config all_boxes_id auto_mode


 Success.


DGS-3324SR:4#
```

show stack_information

Purpose	Used to display the stack information table.
Syntax	**show stack_information**
Description	This command display stack information.
Parameters	None.
Restrictions	None.

Usage Example:

To display stack information:

```
DGS-3324SR:4#show stack_information
Command: show stack_information

 Box    User                          Prio- Prom      Runtime    H/W
 ID     Set   Type          Exist     rity  version   version    version
 ---    ----  -----------   -----     ----- --------  --------   --------
  1      1    DGS-3324SR    exist     16    1.00-B03  2.00-B19   2A1
  2      -    USR-NOT-CFG   no
  3      -    USR-NOT-CFG   no
  4      -    USR-NOT-CFG   no
  5      -    USR-NOT-CFG   no
  6      -    USR-NOT-CFG   no
  7      -    USR-NOT-CFG   no
  8      -    USR-NOT-CFG   no
  9      -    USR-NOT-CFG   no
 10      -    USR-NOT-CFG   no
 11      -    USR-NOT-CFG   no
 12      -    USR-NOT-CFG   no
 --------------------------------------------------------------
Topology    : DUPLEX_CHAIN
My Box ID   :1
Current state:MASTER
Box Count   :1

DGS-3324SR:4#
```

TIME AND *SNTP COMMANDS*

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

Command	Parameters
config sntp	{primary <ipaddr> | secondary <ipaddr> | poll-interval <int 30-99999>}(1)
show sntp	
enable sntp	
disable sntp	
config time	<date ddmthyyyy > <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.
	<ipaddr> − The IP address of the primary server.
	secondary − This is the secondary server the SNTP information will be taken from in the event the primary server is unavailable.
	<ipaddr> − The IP address for the secondary server.
	poll-interval − This is the interval between

config sntp

	requests for updated SNTP information.
	<int 30-99999> – The polling interval ranges from 30 to 99,999 seconds.
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:

```
DGS-3324SR: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.

DGS-3324SR: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:

```
DGS-3324SR: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

DGS-3324SR:4#
```

enable sntp

Purpose	Enables SNTP service support.
Syntax	**enable sntp**
Description	This will enable SNTP support. SNTP service must be separately configured (see config sntp).Enabling and configuring SNTP support will override any manually configured system time settings.
Parameters	None.
Restrictions	Only administrator-level users can issue this command. SNTP settings must be configured for SNTP to function (config sntp).

Example usage:

To enable the SNTP function:

```
DGS-3324SR:4#enable sntp
Command: enable sntp


Success.


DGS-3324SR:4#
```

disable sntp

Purpose	Disables SNTP service 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:

```
DGS-3324SR:4#disable sntp
Command: disable sntp


Success.


DGS-3324SR:4#
```

config time

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

```
DGS-3324SR:4#config time 30jun2003 16:30:30
Command: config time 30jun2003 16:30:30


Success.


DGS-3324SR: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.

config time_zone

	hour – Select the number hours different from GMT.
	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:

```
DGS-3324SR:4#config time_zone operator + hour 2 min 30
Command: config time_zone operator + hour 2 min 30

Success.

DGS-3324SR: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.
	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

config dst

on Sunday during the last week of October.

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.

s-week - Configure the week of the month in which DST begins.

<start_week 1-4,last> - The number of the week during the month in which DST begins where 1 is the first month, 2 is the second month and so on, last is the last week of the month.

e-week - Configure the week of the month in which DST ends.

<end_week 1-4,last> - The number of the week during the month in which DST ends where 1 is the first week of the month, 2 is the second week of the month and so on, last is the last week of the month.

s-wday – Configure the day of the week in which DST begins.

<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)

e-wday - Configure the day of the week in which DST ends.

<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)

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

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

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

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

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

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

s-date - Configure the specific date (day of the

config dst

	month) to begin DST. The date is expressed numerically.
	e-date - Configure the specific date (day of the month) to begin DST. The date is expressed numerically.
	offset - Indicates number of minutes to add 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:

```
 DGS-3324SR: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.


DGS-3324SR:4#
```

show time

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

Example usage:

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

```
DGS-3324SR:4#show time
Command: show time

Current Time Source : System Clock
Boot Time           : 2 Jul 2003 10:59:59
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   : 012 Oct 00:00


DGS-3324SR:4#
```

ARP COMMANDS

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

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

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

create arpentry

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

Example Usage:

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

```
DGS-3324SR: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.


DGS-3324SR:4#
```

delete arpentry

Purpose	Used to delete a static entry into the ARP table.
Syntax	**delete arpentry {<ipaddr>	all}**

delete arpentry

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

Example Usage:

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

```
DGS-3324SR:4#delete arpentry 10.48.74.121
Command: delete arpentry 10.48.74.121


 Success.


DGS-3324SR:4#
```

config arp_aging time

Purpose	Used to configure the age-out timer for ARP table entries on the switch.
Syntax	**config arp_aging time <value 0-65535>**
Description	This command sets the maximum amount of time, in minutes, that an ARP entry can remain in the switch's ARP table, without being accessed, before it is dropped from the table.
Parameters	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:

```
DGS-3324SR:4#config arp_aging time 30
Command: config arp_aging time 30

 Success.

DGS-3324SR:4#
```

show arpentry

Purpose	Used to display the ARP table.
Syntax	**show arpentry {ipif <ipif_name 12> | ipaddress <ipaddr> | static}**
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. <ipaddr> − The network address corresponding to the IP interface name above. static − Displays the static entries to the ARP table.
Restrictions	none.

Example Usage:

To display the ARP table**:**

```
DGS-3324SR: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

DGS-3324SR: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:

```
DGS-3324SR:4#clear arptable
Command: clear arptable


 Success.


DGS-3324SR:4#
```

ROUTING TABLE COMMANDS

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

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

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

create iproute

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

Example Usage:

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

```
DGS-3324SR:4#create iproute 10.48.74.121/255.0.0.0 10.1.1.254 1
Command: create iproute 10.48.74.121/8 10.1.1.254 1


 Success.
DGS-3324SR:4#
```

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. <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:

```
DGS-3324SR:4#create iproute default 10.48.74.121 1
Command: create iproute default 10.48.74.121 1

Success.

DGS-3324SR:4#
```

delete iproute

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

198

delete iproute

	example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8).
	<ipaddr> The gateway IP address for the next hop router.
	primary | backup - The user may choose between *Primary* and *Backup.* If the Primary Static/Default Route fails, the Backup Route will support the entry. Please take note that the Primary and Backup entries cannot have the same Gateway.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

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

```
DGS-3324SR:4#delete iproute 10.48.74.121/8 10.1.1.254
Command: delete iproute 10.48.74.121/8 10.1.1.254


 Success.


DGS-3324SR:4#
```

delete iproute default

Purpose	Used to delete a default IP route entry from the switch's IP routing table.
Syntax	**delete iproute default <ipaddr>**
Description	This command will delete an existing default entry from the switch's IP routing table.
Parameters	<ipaddr> The gateway IP address for the next hop router.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete the default IP route 10.53.13.254:

```
DGS-3324SR:4#delete iproute default 10.53.13.254
Command: delete iproute default 10.53.13.254


 Success.


DGS-3324SR:4#
```

show iproute

Purpose	Used to display the switch's current IP routing table.
Syntax	**show iproute {<network_address>} {static | rip | ospf}**
Description	This command will display the switch's current IP routing table.
Parameters	<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). static – use this to display static iproute entries. rip – use this to display RIP iproute entries. ospf – use this to display OSPF iproute entries.
Restrictions	none.

Example Usage:

To display the contents of the IP routing table:

```
DGS-3324SR:4#show iproute
Command: show iproute


IP Address/Netmask    Gateway        Interface      Cost   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

DGS-3324SR:4#
```

ROUTE REDISTRIBUTION COMMANDS

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

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

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

create route redistribute dst ospf src	
Purpose	Used to add route redistribution settings for the exchange of RIP routes to OSPF routes on the switch.
Syntax	**create route redistribute dst ospf src [static | rip | local] {mettype [1 | 2] | metric <value>}**
Description	This command will redistribute routing information between the OSPF and RIP routing protocols to all routers on the network that are running OSPF or RIP. Routing information entered into the Static Routing Table on the local DGS-3324SR switch is also redistributed.
Parameters	src [static | rip | local] − Allows for the selection of the protocol for the source device. mettype [1 | 2] − Allows for the selection of one of two methods of calculating the metric value. Type-1 calculates (for RIP to OSPF) by adding the destination's interface cost to the metric entered in the Metric field. Type-2 uses the metric entered in the Metric field without change. this field applies only when the destination field is OSPF. metric <value> − Allows the entry of an OSPF interface cost. This is analogous to a Hop Count

create route redistribute dst ospf src

	in the RIP routing protocol.
Restrictions	Only administrator-level users can issue this command.

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

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

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

Example Usage:

To add route redistribution settings:

```
DGS-3324SR:4#create route redistribute dst ospf src rip
Command: create route redistribute dst ospf src rip

 Success.

DGS-3324SR:4#
```

create route redistribute dst rip src

Purpose	Used to add route redistribution settings for the exchange of OSPF routes to RIP routes on the switch.
Syntax	**create route redistribute dst rip src [local | static | ospf [all | internal | external |type_1 |type_2 | inter+e1| inter+e2]]{metric <value>}**
Description	This command will redistribute routing information between the OSPF and Rip routing protocols to all routers on the network that are running OSPF or RIP. Routing information entered into the Static Routing Table on the local DGS-3324SR switch is also redistributed
Parameters	src {local |static |ospf [all | internal | external | type_1 | type_2 | inter+e1 | inter+e2]} – Allows the selection of the protocol of the source device. metric <value> – Allows the entry of an OSPF interface cost. this is analogous to a HOP Count in the RIP routing protocol.

create route redistribute dst rip src

Restrictions	Only administrator-level users can issue this command.

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

Route Source	Metric	Type
OSPF	0 to 16	all type_1 type_2 inter+e1 inter+e2 external internal
Static	0 to 16	not applicable

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

Entering the metric **0** specifies transparency.

Example Usage:

To add route redistribution settings:

```
DGS-3324SR:4#create route redistribute dst rip src ospf all metric 2
Command: create route redistribute dst rip src ospf all metric 2

 Success.

DGS-3324SR:4#
```

config route redistribute dst ospf src

Purpose	Used configure route redistribution settings for the exchange of RIP routes to OSPF routes on the switch.
Syntax	**config route redistribute dst ospf src [static | rip | local] {mettype [1 | 2] | metric <value>}**
Description	Route redistribution allows routers on the network – that are running different routing protocols to exchange routing information. this is accomplished by comparing the routes stored in the various router's routing tables and assigning appropriate metrics. This information is then exchanged among the various routers according to the individual routers current routing protocol. The switch can redistribute routing information between the OSPF and RIP routing protocols to

config route redistribute dst ospf src

	all routers on the network that are running OSPF or RIP. Routing information entered into the Static Routing Table on the local switch is also redistributed.
Parameters	src [static | rip | local] – Allows the selection of the protocol of the source device. mettype – allows the selection of one of the methods for calculating the metric value. Type-a calculates the metric (for RIP to OSPF) by adding the destination's interface cost to the metric entered in the Metric field. Type-2 uses the metric entered in the Metric field without change. This field applies only when the destination field is OSPF. metric <value> – Allows the entry of an OSPF interface cost. This is analogous to a Hop Count in the RIP routing protocol.
Restrictions	Only administrator-level users can issue this command.

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

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

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

Example Usage:

To configure route redistributions:

```
DGS-3324SR:4#config route redistribute dst ospf src all metric 2
Command: config route redistribute dst ospf src all metric 2


Success.


DGS-3324SR:4#
```

config route redistribute dst rip src

Purpose	Used configure route redistribution settings for the exchange of RIP routes to OSPF routes on the switch.
Syntax	**config route redistribute dst rip src [local | static | ospf [all | internal | external |type_1 | type_2 | inter+e1 | inter+e2]] {metric <value>}**
Description	Route redistribution allows routers on the network – that are running different routing protocols to exchange routing information. this is accomplished by comparing the routes stored in the various router's routing tables and assigning appropriate metrics. this information is then exchanged among the various routers according to the individual routers current routing protocol. The switch can redistribute routing information between the OSPF and RIP routing protocols to all routers on the network that are running OSPF or RIP. Routing information entered into the Static Routing Table on the local switch is also redistributed.
Parameters	src {local | static | ospf [all | internal | external | type_1 | type_2 | inter+e1 | inter+e2]} – Allows the selection of the protocol of the source device. metric <value> – Allows the entry of an OSPF interface cost. This is analogous to a Hop Count in the RIP routing protocol.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure route redistributions:

```
DGS-3324SR:4#config route redistribute dst ospf src rip mettype type_1
metric 2
Command: config route redistribute dst ospf src rip mettype type_1
metric 2


Success.


DGS-3324SR:4#
```

delete route redistribute

Purpose	Used to delete an existing route redistribute configuration on the switch.
Syntax	**delete route redistribute {dst [rip | ospf] src [rip | static | local | ospf]}**

delete route redistribute

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

Example Usage:

To delete route redistribution settings:

```
DGS-3324SR:4#delete route redistribute dst rip src ospf
Command: delete route redistribute dst rip src ospf

 Success.

DGS-3324SR:4#
```

show route redistribute

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

Example Usage:

To display route redistributions:

```
DGS-3324SR:4#show route redistribute
Command: show route redistribute


Source      Destination     Type        Metric
Protocol    Protocol

--------    ------------    --------    --------
STATIC      RIP             All         1
LOCAL       OSPF            Type-2      20


Total Entries : 2


DGS-3324SR:4#
```

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

Command	Parameters
config igmp	[ipif <ipif_name 12> | all] {version <value 1-2> | query_interval <1-65535 sec> | max_response_time <1-25 sec> | robustness_variable <value 1-255> | last_member_query_interval <value 1-25> | state [enabled | disabled]}
show igmp	ipif <ipif_name 12>
show igmp group	{group <group> | ipif <ipif_name 12>}

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

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

config igmp	
	between Group-Specific Query messages. The default is 1 second
	state [enabled | disabled] – Enables or disables IGMP for the specified IP interface.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure the IGMP for the IP interface System:

```
DGS-3324SR:4#config igmp all version 1 state enabled
Command: config igmp all version 1 state enabled

 Success.

DGS-3324SR:4#
```

show igmp	
Purpose	Used to display the IGMP configuration for the switch of for a specified IP interface.
Syntax	show igmp {ipif <ipif_name 12>}
Description	This command will display the IGMP configuration for the switch if no IP interface name is specified. If an IP interface name is specified, the command will display the IGMP configuration for that IP interface.
Parameters	<ipif_name> – The name of the IP interface for which the IGMP configuration will be displayed.
Restrictions	none.

Example Usage:

To display IGMP configurations:

```
DGS-3324SR:4#show igmp
Command: show igmp

IGMP Interface Connections

Interface   IP Address      Ver-  Query  Maximum   Robust-  Last Member   State
                            sion         Response  ness     Query
                                         Time      Value
                                                   Interval

------------  ---------------  ----  ------  --------  -------  -----  -------
System      10.90.90.90/8    1    125    10        2        1      Enabled
Develop       20.1.1.1/8     1    125    10        2        1      Enabled

Total Entries: 2

DGS-3324SR:4#
```

show igmp group

Purpose	Used to display the switch's IGMP group table.
Syntax	**show igmp group {group <group>} {ipif <ipif_name 12>}**
Description	This command will display the IGMP group configuration.
Parameters	group <group> − The multicast group ID.
	<ipif_name> − The name of the IP interface the IGMP group is part of.
Restrictions	none.

Example Usage:

To display IGMP group table:

```
DGS-3324SR:4#show igmp group
Command: show igmp group

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

Total Entries: 5

DGS-3324SR:4#
```

BOOTP RELAY COMMANDS

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

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

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

config bootp_relay	
Purpose	Used to configure the BOOTP relay feature of the switch.
Syntax	**config bootp_relay {hops <value 1-16>} {time <sec 0-65535>}**
Description	This command is used to configure the BOOTP relay feature.
Parameters	hops <value> – Specifies the maximum number of relay agent hops that the BOOTP packets can cross. time <sec> – If this time is exceeded, the switch will relay the BOOTP packet.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure bootp relay status.

```
DGS-3324SR:4#config bootp_relay hops 4 time 2
Command: config bootp_relay hops 4 time 2

Success.

DGS-3324SR:4#
```

config bootp_relay add

Purpose	Used to add an IP destination address to the switch's BOOTP relay table.
Syntax	**config bootp_relay add ipif <ipif_name 12> <ipaddr>**
Description	This command adds an IP address as a destination to forward (relay) BOOTP packets to.
Parameters	<ipif_name> − The name of the IP interface in which BOOTP relay is to be enabled. <ipaddr> − The BOOTP server IP address.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To add a BOOTP relay.

```
DGS-3324SR:4#config bootp_relay add ipif System 10.43.21.12
Command: config bootp_relay add ipif System 10.43.21.12


Success.


DGS-3324SR:4#
```

config bootp_relay delete

Purpose	Used to delete an IP destination addresses from the switch's BOOTP relay table.
Syntax	**config bootp_relay delete ipif <ipif_name 12> <ipaddr>**
Description	This command is used to delete an IP destination addresses in the switch's BOOTP relay table.
Parameters	<ipif_name> − The name of the IP interface that contains the IP address below. <ipaddr> − The BOOTP server IP address.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete a BOOTP relay:

```
DGS-3324SR:4#config bootp_relay delete ipif System 10.43.21.12
Command: config bootp_relay delete ipif System 10.43.21.12

Success.

DGS-3324SR:4#
```

enable bootp_relay

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

Example Usage:

To enable the BOOTP relay function:

```
DGS-3324SR:4#enable bootp_relay
Command: enable bootp_relay

Success.

DGS-3324SR:4#
```

disable bootp_relay

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

Example Usage:

To disable the BOOTP relay function:

```
DGS-3324SR:4#disable bootp_relay
Command: disable bootp_relay

Success.

DGS-3324SR:4#
```

show bootp_relay

Purpose	Used to display the current BOOTP relay configuration.
Syntax	**show bootp_relay {ipif <ipif_name 12>}**
Description	This command will display the current BOOTP relay configuration for the switch, or if an IP interface name is specified, the BOOTP relay configuration for that IP interface.
Parameters	<ipif_name> – The name of the IP interface for which you what to display the current BOOTP relay configuration.
Restrictions	none.

Example Usage:

To display bootp relay status:

```
DGS-3324SR:4#show bootp_relay
Command: show bootp_relay

Bootp Relay Status: Disabled
Bootp Hops Count Limit: 4
Bootp Relay Time Threshold: 0


Interface    Server 1        Server 2        Server 3        Server 4
------------ --------------- --------------- --------------- --------------
System       10.48.74.122  10.23.12.34    10.12.34.12   10.48.75.121


Total Entries: 1

DGS-3324SR:4#
```

DNS RELAY COMMANDS

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

Command	Parameters
config dnsr	{[primary | secondary] nameserver <ipaddr> | [add | delete] static <domain_name 32> <ipaddr>}
enable dnsr	{cache | static}
disable dnsr	{cache | static}
show dnsr	static

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

config dnsr

Purpose	Used to configure the DNS relay function.
Syntax	**config dnsr {[primary | secondary] nameserver <ipaddr> | [add | delete] static <domain_name 32> <ipaddr>}**
Description	This command is used to configure the DNS relay function on the switch.
Parameters	primary − Indicates that the IP address below is the address of the primary DNS server. secondary − Indicates that the IP address below is the address of the secondary DNS server. nameserver <ipaddr> − The IP address of the DNS nameserver. add|delete – Indicates if the user wishes to add or delete the dns relay function. <domain_name> − The domain name of the entry. <ipaddr> − The IP address of the entry.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To set IP address 10.43.21.12 of primary.

```
DGS-3324SR:4#config dnsr primary 10.43.21.12
Command: config dnsr primary 10.43.21.12


Success


DGS-3324SR:4#
```

Example Usage:

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

```
DGS-3324SR:4#config dnsr add static dns1 10.43.21.12
Command: config dnsr add static dns1 10.43.21.12


Success.
DGS-3324SR:4#
```

Example Usage:

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

```
DGS-3324SR:4#config dnsr delete static dns1 10.43.21.12
Command: config dnsr delete static dns1 10.43.21.12


Success.


DGS-3324SR:4#
```

enable dnsr

Purpose	Used to enable DNS relay.
Syntax	**enable dnsr {cache	static}**
Description	This command is used, in combination with the **disable dnsr** command below, to enable and disable DNS Relay on the switch.
Parameters	cache – This parameter will allow the user to enable the cache lookup for the DNS rely on the switch. static - This parameter will allow the user to enable the static table lookup for the DNS rely on the switch.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable status of DNS relay:

```
DGS-3324SR:4#enable dnsr
Command: enable dnsr

Success.

DGS-3324SR:4#
```

Example Usage:

To enable cache lookup for DNS relay.

```
DGS-3324SR:4#enable dnsr cache
Command: enable dnsr cache

Success.

DGS-3324SR:4#
```

Example Usage:

To enable static table lookup for DNS relay.

```
DGS-3324SR:4#enable dnsr static
Command: enable dnsr static

Success.

DGS-3324SR:4#
```

disable dnsr

Purpose	Used to disable DNS relay on the switch.
Syntax	**disable dnsr {cache | static}**
Description	This command is used, in combination with the **enable dnsr** command above, to enable and disable DNS Relay on the switch.
Parameters	cache – This parameter will allow the user to disable the cache lookup for the DNS rely on the switch. static - This parameter will allow the user to disable the static table lookup for the DNS rely on the switch.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To disable status of DNS relay.

```
DGS-3324SR:4#disable dnsr
Command: disable dnsr


Success.


DGS-3324SR:4#
```

Example Usage:

To disable cache lookup for DNS relay.

```
DGS-3324SR:4#disable dnsr cache
Command: disable dnsr cache


Success.


DGS-3324SR:4#
```

Example Usage:

To disable static table lookup for DNS relay.

```
DGS-3324SR:4#disable dnsr static
Command: disable dnsr static


Success.


DGS-3324SR:4#
```

show dnsr

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

Example Usage:

To display DNS relay status:

```
DGS-3324SR:4#show dnsr
Command: show dnsr


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


DNS Relay Static Table

Domain Name              IP Address

------------------------------------  --------------

www.123.com.tw           10.12.12.123
  bbs.ntu.edu.tw          140.112.1.23


Total Entries: 2


DGS-3324SR:4#
```

RIP COMMANDS

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

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

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

config rip	
Purpose	Used to configure RIP on the switch.
Syntax	**config rip [ipif <ipif_name 12> | all] {authentication [enabled <password 16> | disabled] | tx_mode [disabled | v1_only | v1_compatible | v2_only] | rx_mode [v1_only | v2_only | v1_or_v2 | disabled] state [enabled | disabled]}**
Description	This command is used to configure RIP on the switch.
Parameters	<ipif_name 12> − The name of the IP interface. all – To configure all RIP receiving mode for all IP interfaces. rx_mode − Determines how received RIP packets will be interpreted – as RIP version **V1 only, V2 Only,** or **V1 or V2.** This entry specifies which version of the RIP protocol will be used to receive RIP packets. The Disabled entry prevents the reception of RIP packets. tx_mode − Determines how received RIP packets will be interpreted – as RIP version **V1 only, V2 Only,** or **V1 Compatible (V1 and V2).** This entry specifies which version of the RIP protocol will be used to transfer RIP packets. The Disabled entry prevents the reception of RIP packets. disable − Prevents the reception of RIP packets. v1_only − Specifies that only RIP v1 packets will

221

config rip

	be accepted.
	v2_only − Specifies that only RIP v2 packets will be accepted.
	v1_or_v2 − Specifies that RIP v1 or v2 packets will be accepted.
	authentication [enabled | disabled] − Enables or disables authentication for RIP on the switch.
	<password> − Allows the specification of a case-sensitive password.
	state [enabled | disabled] − Allows RIP to be enabled and disabled on the switch.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

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

```
DGS-3324SR:4#config rip ipif System rx_mode v1_only
Command: config rip ipif System rx_mode v1_only

Success.

DGS-3324SR:4#
```

enable rip

Purpose	Used to enable RIP.
Syntax	**enable rip**
Description	This command is used to enable RIP on the switch.
Parameters	none.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable RIP:

```
DGS-3324SR:4#enable rip
Command: enable rip

Success.

DGS-3324SR:4#
```

disable rip

Purpose	Used to disable RIP.
Syntax	**disable rip**
Description	This command is used to disable RIP on the switch.
Parameters	none.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To disable rip:

```
DGS-3324SR:4#disable rip
Command: disable rip

Success.

DGS-3324SR:4#
```

show rip

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

Example Usage:

To display RIP configuration:

```
DGS-3324SR:4#show rip
Command: show rip

RIP Global State : Disabled

  Settings


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

Total Entries : 1

DGS-3324SR:4#
```

DVMRP COMMANDS

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

Command	Parameters
config dvmrp	[ipif <ipif_name 12>	all] {metric <value 1-31>	probe <sec 1-65535> |neighbor_timeout <sec 1-65535>	state [enabled	disabled]}
enable dvmrp	
disable dvmrp	
show dvmrp neighbor	{ipif <ipif_name 12>	ipaddress <network_address>}
show dvmrp nexthop	{ipaddress <network_address>	ipif <ipif_name 12>}
show dvmrp routing_table	{ipaddress <network_address>}
show dvmrp	ipif <ipif_name 12>

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

config dvmrp	
Purpose	Used to configure DVMRP on the switch.
Syntax	**config dvmrp [ipif <ipif_name 12>	all] {metric <value 1-31>	probe <sec 1-65535> |neighbor_timeout <sec 1-65535>	state [enabled	disabled]}**
Description	This command is used to configure DVMRP on the switch.
Parameters	<ipif_name> – The name of the IP interface for which DVMRP is to be configured. all – Specifies that DVMRP is to be configured for all IP interfaces on the switch. metric <value> – Allows the assignment of a DVMRP route cost to the above IP interface. A DVMRP route cost is a relative number that represents the real cost of using this route in the construction of a multicast delivery tree. It is similar to, but not defined as, the hope count in RIP. The default is 1. probe <second> – DVMRP defined an extension to IGMP that allows routers to inform other routers that it is currently operational. This is referred to as a 'probe'. These probes are used by DVMRP routers to identify and locate each

config dvmrp

	other, determine capabilities and to"keep-alive" in order to detect when a neighbor is lost. This entry will set an intermittent DVMRP probe (in seconds) on the device that will transmit dvmrp probe packets, depending on the time specified.The default value is 10 seconds. neighbor_timeout <second> − The time period for which DVMRP will hold Neighbor Router reports before issuing poison route messages. The default value is 35 seconds. state [enabled | disabled] − Allows DVMRP to be enabled or disabled.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure DVMRP configurations of IP interface System:

```
DGS-3324SR:4#config dvmrp ipif System neighbor_timeout 30 metric
1 probe 5
Command: config dvmrp ipif System neighbor_timeout 30 metric 1
probe 5


Success


DGS-3324SR:4#
```

enable dvmrp

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

Example Usage:

To enable DVMRP:

```
DGS-3324SR:4#enable dvmrp

Command: enable dvmrp


Success.


DGS-3324SR:4#
```

disable dvmrp

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

Example Usage:

To disable DVMRP:

```
DGS-3324SR:4#disable dvmrp

Command: disable dvmrp


Success.


DGS-3324SR:4#
```

show dvmrp routing_table

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

Example Usage:

To display DVMRP routing table:

```
DGS-3324SR:4#show dvmrp routing_table
Command: show dvmrp routing_table


DVMRP Routing Table
Source Address  Netmask      Next Hop Router    Hop  Learned   Interface    Expire
---------------   _____     ---------------    ----  -------   ------------  ------
   10.0.0.0/8    255.0.0.0   10.90.90.90         2    Local     System       -
   20.0.0.0/8    255.0.0.0   20.1.1.1            2    Local     ip2          117
   30.0.0.0/8    255.0.0.0   30.1.1.1            2    Dynamic   ip3          106


Total Entries: 3


DGS-3324SR:4#
```

show dvmrp neighbor

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

Example Usage:

To display DVMRP neighbor table:

```
DGS-3324SR:4#show dvmrp neighbor
Command: show dvmrp neighbor
DVMRP Neighbor Address Table


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


Total Entries: 1


DGS-3324SR:4#
```

show dvmrp nexthop

Purpose	Used to display the current DVMRP routing next hop table.
Syntax	**show dvmrp nexthop {ipaddress <network_address> | ipif <ipif_name 12>}**
Description	This command will display the DVMRP routing next hop table.
Parameters	<ipif_name> – The name of the IP interface for which you want to display the current DVMRP routing next hop table. ipaddress <network_address> – The IP address and netmask of the destination. You can specify the IP address and netmask information using the traditional format or the CIDR format. For example, 10.1.2.3/255.255.0.0 or 10.2.3.4/16.
Restrictions	none.

Example Usage:

To display DVMRP routing next hop table:

```
DGS-3324SR:4#show dvmrp nexthop
Command: show dvmrp nexthop

Source IP Address  Netmask        Interface Name    Type
-----------------  --------------  ---------------  ------
    10.0.0.0/8      255.0.0.0           ip2           Leaf
    10.0.0.0/8      255.0.0.0           ip3           Leaf
    20.0.0.0/8      255.0.0.0         System          Leaf
    20.0.0.0/8      255.0.0.0           ip3           Leaf
    30.0.0.0/8      255.0.0.0         System          Leaf
    30.0.0.0/8      255.0.0.0           ip2           Leaf

Total Entries: 6

DGS-3324SR:4#
```

show dvmrp

Purpose	Used to display the current DVMRP configurations.
Syntax	**show dvmrp {ipif <ipif_name 12>}**
Description	The command will display the current DVMRP configurations on the switch.
Parameters	<ipif_name> − The name of the IP interface for which you want to view DVMRP configurations.
Restrictions	none.

Example Usage:

To show DVMRP configurations:

```
DGS-3324SR:4#show dvmrp
Command: show dvmrp

DVMRP Global State : Disabled

Interface IP Address/Netmask Neighbor Timeout Probe Metric State
-----------  ---------------     --------------- -----  ------  -------
 System    10.90.90.90/8             35           10     1     Disabled

Total Entries: 1

DGS-3324SR:4#
```

PIM COMMANDS

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

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

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

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

config pim	
	Note that PIM settings must also be enabled globally for the switch with the **enable pim** described below for PIM to operate on any configured IP interfaces.
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To configure PIM settings for IP interface "System":

```
DGS-3324SR:4#config pim ipif System hello 35 jp_interval 70 state enabled
Command: config pim ipif System hello 35 jp_interval 70 state enabled

Success.

DGS-3324SR:4#
```

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

Usage Example:

To enable PIM as previously configured on the switch:

```
DGS-3324SR:4#enable pim
Command: enable pim

Success.

DGS-3324SR:4#
```

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

disable pim	
	time with the **enable pim**.
Parameters	None.
Restrictions	Only administrator-level users can use this command.

Usage Example:

To disable PIM on the switch:

```
DGS-3324SR:4#disable pim
Command: disable pim


Success.


DGS-3324SR:4#
```

show pim neighbor	
Purpose	Used to display PIM neighbor router table entries.
Syntax	**show pim neighbor {ipif <ipif_name 12>	ipaddress <network_address>}**
Description	This command will list current entries in the PIM neighbor table for a specified IP interface or destination router IP address.
Parameters	ipif – The name of an IP interface for which you want to view the PIM neighbor router table. ipaddress - The IP address and netmask of the destination routing device for which you want to view the neighbor raouter table. You can specify the IP address and netmask information usnig the traditional format or the CIDR format. For example, 10.1.2.3/255.255.0.0 or 10.2.3.4/16. If no parameters are specified, all PIM neighbor router tables are displayed.
Restrictions	None.

Usage Example:

To display PIM settings as configured on the switch:

```
DGS-3324SR:4#show pim neighbor
Command: show pim neighbor

PIM Neighbor Address Table

Interface Name   Neighbor Address  Expire Time
---------------  ----------------  -----------
System           10.48.74.122      5

Total Entries : 1

DGS-3324SR:4#
```

show pim

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

Usage Example:

To display PIM settings as configured on the switch:

```
DGS-3324SR:4#show pim
Command: show pim

PIM Global State : Disabled

PIM-DM Interface Table
                        Hello    Join/Prune
Interface  IP Address   Interval Interval    State
---------- ------------- -------- ---------- --------
System     10.90.90.90/8 35       0          Enabled

Total Entries : 1

DGS-3324SR:4#
```

IP MULTICASTING COMMANDS

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

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

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

show ipmc cache	
Purpose	Used to display the current IP multicast forwarding cache.
Syntax	**show ipmc cache {group <group>} {ipaddress <network_address>}**
Description	This command will display the current IP multicast forwarding cache.
Parameters	<group> − The multicast group ID. <network_address> − The IP address and netmask of the destination. You can specify the IP address and netmask information using the traditional format or the CIDR format. For example, 10.1.2.3/255.255.0.0 or 10.2.3.4/16.
Restrictions	none.

Usage Example:

To display the current IP multicast forwarding cache:

```
DGS-3324SR:4#show ipmc cache
Command: show ipmc cache
Multicast       Source Address/      Upstream         Expire      Routing
  Group            Netmask           Neighbor          Time       Protocol
------------------   ----------------   ---------------   -----------   ---------
224.1.1.1       10.48.74.121/32      10.48.75.63        30         dvmrp
224.1.1.1       20.48.74.25 /32     20.48.75.25         20         pim-dm
224.1.2.3        10.48.75.3 /3       10.48.76.6         30         dvmrp


Total Entries: 3


DGS-3324SR:4#
```

show ipmc

Purpose	Used to display the IP multicast interface table.
Syntax	**show ipmc {ipif <ipif_name 12>	protocol dvmrp}**
Description	This command will display the current IP multicast interface table.
Parameters	<ipif_name> – The name of the IP interface for which you want to display the IP multicast interface table for. protocol dvmrp – Allows the user to specify whether or not to use the DVMRP protocol to display the IP multicast interface table. For example, if DVMRP is specified, the table will display only those entries that are related to the DVMRP protocol.
Restrictions	none.

Usage Example

To display the current IP multicast interface table by DVMRP entry:

```
DGS-3324SR:4#show ipmc ipif System protocol dvmrp
Command: show ipmc ipif System protocol dvmrp

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

Total Entries: 1

DGS-3324SR:4#
```

MD5 CONFIGURATION COMMANDS

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

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

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

config md5 key

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

Usage Example

To configure an MD5 Key password:

```
DGS-3324SR:4#config md5 key 1 dlink
Command: config md5 key 1 dlink


Success.


DGS-3324SR:4#
```

create md5 key

Purpose	Used to create a new entry in the MD5 key table.
Syntax	**create md5 key <key_id 1-255> <password 1-16>**

create md5 key

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

Usage Example

To create an entry in the MD5 key table:

```
DGS-3324SR:4# create md5 key 1 dlink
Command: create md5 key 1 dlink

Success.

DGS-3324SR:4#
```

delete md5 key

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

Usage Example

The delete an entry in the MD5 key table:

```
DGS-3324SR:4# delete md5 key 1
Command: delete md5 key 1

Success.

DGS-3324SR:4#
```

show md5

Purpose	Used to display an MD5 key table.
Syntax	show md5 {key <key_id 1-255>}

238

show md5

Description	This command will display the current MD5 key table.
Parameters	<key_id> – The MD5 key ID.
Restrictions	none.

Usage Example

To display the current MD5 key:

```
DGS-3324SR:4#show md5
Command: show md5

MD5 Key Table

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

Total Entries: 4

DGS-3324SR:4#
```

OSPF CONFIGURATION COMMANDS

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

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

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

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

config ospf router_id

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

Usage Example

To configure the OSPF router ID:

```
DGS-3324SR:4#config ospf router_id 10.48.74.122
Command: config ospf router_id 10.48.74.122

Success.

DGS-3324SR:4#
```

enable ospf

Purpose	Used to enable OSPF on the switch.
Syntax	**enable ospf**
Description	This command, in combination with the **disable ospf** command below, is used to enable and disable OSPF on the switch.

enable ospf

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

Usage Example

To enable OSPF on the switch:

```
DGS-3324SR:4#enable ospf
Command: enable ospf

Success.

DGS-3324SR:4#
```

disable ospf

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

Usage Example

To disable OSPF on the switch:

```
DGS-3324SR:4#disable ospf
Command: disable ospf

Success.

DGS-3324SR:4#
```

show ospf

Purpose	Used to display the current OSPF state on the switch.
Syntax	**show ospf**
Description	This command will display the current state of OSPF on the switch, divided into the following categories:

show ospf

	General OSPF settings
	OSPF Interface settings
	OSPF Area settings
	OSPF Virtual Interface settings
	OSPF Area Aggregation settings
	OSPF Host Route settings
Parameters	none.
Restrictions	none.

Usage Example:

To show OSPF state:

```
DGS-3324SR:4#show ospf
Command: show ospf

OSPF Router ID : 10.1.1.2
State        : Enabled

OSPF Interface Settings

Interface  IP Address    Area ID      State      Link        Metric
                                                 Status
-----------  -----------------  ---------  --------  ---------  ---------
System    10.90.90.90/8  0.0.0.0    Disabled  Link DOWN      1
    ip2      20.1.1.1/8    0.0.0.0    Disabled  Link DOWN      1
    ip3      30.1.1.1/8    0.0.0.0    Disabled  Link DOWN      1
Total Entries : 3

OSPF Area Settings

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

Total Entries : 4
```

```
Virtual Interface Configuration

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

Total Entries : 2

OSPF Area Aggregation Settings

Area ID        Aggregated           LSDB    Advertise
               Network Address      Type
---------------    ------------------    --------  ---------
Total Entries : 0

OSPF Host Route Settings

Host Address   Metric        Area ID
---------------         ------    ---------------
   10.3.3.3              1        10.1.1.1
Total Entries : 1

DGS-3324SR:4#
```

create ospf area

Purpose	Used to configure OSPF area settings.
Syntax	**create ospf area <area_id> type [normal | stub {stub_summary [enabled | disabled] | metric <value 0-65535>}]**
Description	This command is used to create an OSPF area and configure its settings.
Parameters	<area_id> – The OSPF area ID. type – The OSPF area mode of operation – stub or normal. stub_summary – enables or disables the OSPF area to import summary LSA advertisements. <value> – The OSPF area cost between 0 and 65535. 0 denotes that the value will be automatically assigned. The default setting is 0.
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To create an OSPF area:

```
DGS-3324SR:4#create ospf area 10.48.74.122 type normal
Command: create ospf area 10.48.74.122 type normal


Success.


DGS-3324SR:4#
```

delete ospf area

Purpose	Used to delete an OSPF area.
Syntax	**delete ospf area <area_id>**
Description	This command is used to delete an OSPF area.
Parameters	<area_id> − A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To delete an OSPF area:

```
DGS-3324SR:4#delete ospf area 10.48.74.122
Command: delete ospf area 10.48.74.122


Success.


DGS-3324SR:4#
```

config ospf area

Purpose	Used to configure an OSPF area's settings.
Syntax	**config ospf area <area_id> type [normal	stub {stub_summary [enabled	disabled]	metric <value 0-65535>}]**
Description	This command is used to configure an OSPF area's settings.
Parameters	<area_id> − The OSPF area ID. type − Allows the specification of the OSPF mode of operation − stub or normal. stub_summary [enabled	disabled] − Allows the OSPF area import of LSA advertisements to be enabled or disabled. <value> − The OSPF area stub default cost.

config ospf area

Restrictions	Only administrator-level users can issue this command.

Usage Example

To configure an OSPF area's settings:

```
DGS-3324SR:4#config ospf area 10.48.74.122 type stub stub_summary enabled metric 1
Command: config ospf area 10.48.74.122 type stub stub_summary enabled metric 1

Success.

DGS-3324SR:4#
```

show ospf area

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

Usage Example

To display an OSPF area's settings:

```
DGS-3324SR:4#show ospf area
Command: show ospf area
  Area Id      Type     Stub    Import  Summary LSA  Stub    Default Cost
-------------- ----------- ---------- --------- ----------------- ----------- --------
    0.0.0.0    Normal   None                            None     None
10.48.74.122   Stub     Enabled                         Enabled   1

Total Entries: 2

DGS-3324SR:4#
```

create ospf host_route

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

create ospf host_route

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

Usage Example

To configure the OSPF host route settings:

```
DGS-3324SR:4#create ospf host_route 10.48.74.122 area 10.1.1.1
metric 2
Command: create ospf host_route 10.48.74.122 area 10.1.1.1
metric 2


Success.


DGS-3324SR:4#
```

delete ospf host_route

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

Usage Example

To delete an OSPF host route:

```
DGS-3324SR:4#delete ospf host_route 10.48.74.122
Command: delete ospf host_route 10.48.74.122


Success.


DGS-3324SR:4#
```

config ospf host_route

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

Usage Example

To configure an OSPF host route:

```
DGS-3324SR:4#config ospf host_route 10.48.74.122 area 10.1.1.1 metric 2
Command: config ospf host_route 10.48.74.122 area 10.1.1.1 metric 2
Success.

DGS-3324SR:4#
```

show ospf host_route

Purpose	Used to display the current OSPF host route table.
Syntax	**show ospf host_route {<ipaddr>}**
Description	This command will display the current OSPF host route table.
Parameters	<ipaddr> − The IP address of the host.
Restrictions	none.

Usage Example:

To display the current OSPF host route table:

```
DGS-3324SR:4#show ospf host_route
Command: show ospf host_route


Host Address        Metric         Area_ID

 ---------------    ---------------    -----------
10.48.73.21             2           10.1.1.1

10.48.74.122            1           10.1.1.1


Total Entries: 2


DGS-3324SR:4#
```

create ospf aggregation

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

Usage Example:

To create an OSPF area aggregation:

```
DGS-3324SR:4#create ospf aggregation 10.1.1.1 10.48.76.122/16 lsdb_type
summary advertise enabled
Command: create ospf aggregation 10.1.1.1 10.48.76.122/16 lsdb_type
summary advertise enabled


Success.


DGS-3324SR:4#
```

delete ospf aggregation

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

Usage Example

To configure the OSPF area aggregation settings:

```
DGS-3324SR:4#delete ospf aggregation 10.1.1.1 10.48.76.122/16
lsdb_type summary
Command:  delete ospf aggregation 10.1.1.1 10.48.76..122/16
lsdb_type summary


Success.


DGS-3324SR:4#
```

config ospf aggregation

Purpose	Used to configure the OSPF area aggregation settings.
Syntax	**config ospf aggregation <area_id> <network_address> lsdb_type summary {advertise [enabled | disabled]}**
Description	This command is used to configure the OSPF area aggregation settings.
Parameters	<area_id> − A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain. <network_address> − The 32-bit number in the form of an IP address that uniquely identifies the network that corresponds to the OSPF Area.

config ospf aggregation

	lsdb_type [summary] – Specifies the type of address aggregation.
	advertise [enabled | disabled] – Allows for the advertisement trigger to be enabled or disabled.
Restrictions	Only administrator-level users can issue this command.

Usage Example

To configure the OSPF area aggregation settings:

```
DGS-3324SR:4#config ospf aggregation 10.1.1.1 10.48.76.122/16
lsdb_type summary advertise enabled
Command: config ospf aggregation 10.1.1.1 10.48.76.122/16 lsdb_type
summary advertise enabled

Success.

DGS-3324SR:4#
```

show ospf aggregation

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

Usage Example

To display OSPF area aggregation settings:

```
DGS-3324SR:4#show ospf aggregation

Command: show ospf aggregation


OSPF Area Aggregation Settings


Area ID    Aggregated          LSDB           Advertise
           Network Address     Type

------------  --------------------   -------------   -------------
 10.1.1.1     10.0.0.0/8          Summary        Enabled
 10.1.1.1     20.2.0.0/16         Summary        Enabled


Total Entries: 2


DGS-3324SR:4#
```

show ospf lsdb

Purpose	Used to display the OSPF Link State Database (LSDB).
Syntax	**show ospf lsdb {area_id <area_id> | advertise_router <ipaddr> | type [rtrlink | netlink | summary | assummary | asextlink]}**
Description	This command will display the current OSPF Link State Database (LSDB).
Parameters	area_id <area_id> − A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain. advertise_router <ipaddr> − The router ID of the advertising router. type [rtrlink | netlink | summary | assummary | asextlink] − The type of link.
Restrictions	none.

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

Usage Example:

To display the link state database of OSPF:

```
DGS-3324SR:4#show ospf lsdb
Command: show ospf lsdb


 Area       LSDB          Advertising     Link State    Cost    Sequence
 ID         Type          Router ID       ID                    Number

----------  --------------  ----------------------------------------------------------
0.0.0.0     RTRLink       50.48.75.73     50.48.75.73    *      0x80000002
0.0.0.0     Summary       50.48.75.73     10.0.0.0/8     1      0x80000001
1.0.0.0     RTRLink       50.48.75.73     50.48.75.73    *      0x80000001
1.0.0.0     Summary       50.48.75.73     40.0.0.0/8     1      0x80000001
1.0.0.0     Summary       50.48.75.73     50.0.0.0/8     1      0x80000001
*           ASExtLink     50.48.75.73     1.2.0.0/16     20     0x80000001


Total Entries: 5


DGS-3324SR:4#
```

show ospf neighbor

Purpose	Used to display the current OSPF neighbor router table.
Syntax	**show ospf neighbor {<ipaddr>}**
Description	This command will display the current OSPF neighbor router table.
Parameters	<ipaddr> − the IP address of the neighbor router.
Restrictions	none.

Usage Example

To display the current OSPF neighbor router table:

```
DGS-3324SR:4#show ospf neighbor
Command: show ospf neighbor


IP Address of     Router ID of     Neighbor      Neighbor
Neighbor          Neighbor         Priority      State

---------------   ---------------  --------      ------------
10.48.74.122       10.2.2.2            1          Initial


DGS-3324SR:4#
```

show ospf virtual_neighbor

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

253

show ospf virtual_neighbor

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

Usage Example

To display the current OSPF virtual neighbor table:

```
DGS-3324SR:4#show ospf virtual_neighbor
Command: show ospf virtual_neighbor


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


DGS-3324SR:4#
```

config ospf ipif

Purpose	Used to configure the OSPF interface settings.
Syntax	**config ospf ipif <ipif_name> {area <area_id>	priority <value>	hello_interval <sec 1-65535>| dead_interval <sec 1-65535>	authentication [none	simple <password 8>	md5 <key_id 1-255>]	metric <value 1-65535>	state [enabled	disabled]}**
Description	This command is used to configure the OSPF interface settings.
Parameters	<ipif_name> – The name of the IP interface. priority <value> – The priority used in the election of the Designated Router (DR). A number between 0 and 255. metric <value> – The interface metric (1 to 65535). Entering a 0 will allow automatic calculation of the metric.

config ospf ipif

	hello_interval <sec> − Allows the specification of the interval between the transmission of OSPF Hello packets, in seconds. Between 1 and 65535 seconds can be specified. The Hello Interval, Dead Interval, Authorization Type, and Authorization Key should be the same for all routers on the same network.
	dead_interval <sec> − Allows the specification of the length of time between the receipt of Hello packets from a neighbor router before the selected area declares that router down. An interval between 1 and 65535 seconds can be specified. The Dead Interval must be evenly divisible by the Hello Interval.
	<password> − A case-sensitive password of no more than eight (8) characters.
	<key_id> − A previously configured MD5 key ID (1 to 255).
	metric <value> − This field allows the entry of a number between 1 and 65,535 that is representative of the OSPF cost of reaching the selected OSPF interface. The default metric is 1.
Restrictions	Only administrator-level users can issue this command.

Usage Example

To configure OSPF interface settings:

```
DGS-3324SR:4#config ospf ipif System priority 2 hello_interval 15
metric 2 state enabled
Command: config ospf ipif System priority 2 metric 2 state enabled
hello_interval 15


Success.


DGS-3324SR:4#
```

config ospf all

Purpose	Used to configure all of the OSPF interfaces on the switch at one time.
Syntax	**config ospf all {area <area_id>	priority <value>	hello_interval <sec 1-65535>	dead_interval <sec 1-65535>	authentication [none	simple <password 8>	md5 <key_id 1-255>]	metric <value 1-65535>	state [enabled	disabled]}**
Description	This command is used to configure all of the OSPF interfaces on the switch, using a single group of

config ospf all

	parameters, at one time.
Parameters	priority <value> − The priority used in the election of the Designated Router (DR). A number between 0 and 255.
	metric <value> − The interface metric (1 to 65535). Entering a 0 will allow automatic calculation of the metric.
	hello_interval <sec> − Allows the specification of the interval between the transmission of OSPF Hello packets, in seconds. Between 1 and 65535 seconds can be specified. The Hello Interval, Dead Interval, Authorization Type, and Authorization Key should be the same for all routers on the same network.
	dead_interval <sec> − Allows the specification of the length of time between the receipt of Hello packets from a neighbor router before the selected area declares that router down. An interval between 1 and 65535 seconds can be specified. The Dead Interval must be evenly divisible by the Hello Interval.
Parameters	<password> − A case-sensitive password.
	<key_id> − A previously configured MD5 key ID (1 to 255).
	metric <value> − This field allows the entry of a number between 1 and 65,535 that is representative of the OSPF cost of reaching the selected OSPF interface. The default metric is 1.
Restrictions	Only administrator-level users can issue this command.

Usage Example

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

```
DGS-3324SR:4#config ospf all state enabled
Command: config ospf all state enabled

Success.

DGS-3324SR:4#
```

show ospf ipif

Purpose	Used to display the current OSPF interface settings for the specified interface name.

show ospf ipif

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

Usage Example

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

```
DGS-3324SR:4#show ospf ipif ipif2
Command: show ospf ipif ipif2

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

Total Entries: 1

DGS-3324SR:4#
```

show ospf all

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

Usage Example:

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

```
DGS-3324SR:4#show ospf all

Command: show ospf all

Interface Name: System          IP Address:  10.42.73.10/8 (Link Up)

Network Medium Type: BROADCAST    Metric:  1

Area ID:  0.0.0.0                       Administrative State:  Enabled

Priority:  1                            DR State:  DR

DR Address:  10.42.73.10               Backup DR Address:  None

Hello Interval:  10                    Dead Interval:  40

Transmit Delay:  1                     Retransmit Time:  5

Authentication:  None


Interface Name:  ipif2          IP Address:  123.234.12.34/24 ((Link Up)

Network Medium Type: BROADCAST    Metric:  1

Area ID:  1.0.0.0                       Administrative State:  Enabled

Priority:  1                            DR State:  DR

DR Address:  123.234.12.34             Backup DR Address:  None

Hello Interval:  10                    Dead Interval:  40

Transmit Delay:  1                     Retransmit Time:  5

Authentication:  None


Total Entries: 2


DGS-3324SR:4#
```

config ospf virtual_link

Purpose	Used to configure the OSPF virtual interface settings.
Syntax	**config ospf virtual_link <area_id> <neighbor_id> {hello_interval <sec 1-65535> | dead_interval <sec 1-65535> | authentication [none | simple <password 8> | md5 <key_id 1-255>]}**
Description	This command is used to configure the OSPF virtual interface settings.
Parameters	<area_id> − A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.
	<neighbor_id> − The OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router.
	hello_interval <sec> − Allows the specification of the interval between the transmission of OSPF Hello packets, in seconds. Between 1 and 65535

config ospf virtual_link

	seconds can be specified. The Hello Interval, Dead Interval, Authorization Type, and Authorization Key should be the same for all routers on the same network.
	dead_interval <sec> − Allows the specification of the length of time between the receipt of Hello packets from a neighbor router before the selected area declares that router down. An interval between 1 and 65535 seconds can be specified. The Dead Interval must be evenly divisible by the Hello Interval.
	<password> − A case-sensitive password of no more than eight (8) characters.
	<key_id> − A previously configured MD5 key. A value between 1 and 255 seconds can be entered.
Restrictions	Only administrator-level users can issue this command.

Usage Example

To configure the OSPF virtual interface settings:

```
DGS-3324SR:4#config ospf virtual_link 10.1.1.2 20.1.1.1 hello_interval 10
Command: config ospf virtual_link 10.1.1.2 20.1.1.1 hello_interval 10

Success.

DGS-3324SR:4#
```

create ospf virtual_link

Purpose	Used to create an OSPF virtual interface.
Syntax	**create ospf virtual_link <area_id> <neighbor_id> {hello_interval <sec 1-65535> | dead_interval <sec 1-65535> | authentication [none | simple <password 8> | md5 <key_id 1-255>]}**
Description	This command is used to create an OSPF virtual interface.
Parameters	<area_id> − A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.
	<neighbor_id> − The OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router. The router ID of the neighbor router.
	hello_interval <sec> − Allows the specification

create ospf virtual_link

	of the interval between the transmission of OSPF Hello packets, in seconds. Between 1 and 65535 seconds can be specified. The Hello Interval, Dead Interval, Authorization Type, and Authorization Key should be the same for all routers on the same network.
Parameters	dead_interval <sec> − dead_interval <sec> − Allows the specification of the length of time between the receipt of Hello packets from a neighbor router before the selected area declares that router down. An interval between 1 and 65535 seconds can be specified. The Dead Interval must be evenly divisible by the Hello Interval. <password> − A case-sensitive password of no more than eight (8) characters. <key_id> − A previously configured MD5 key ID (1 to 255).
Restrictions	Only administrator-level users can issue this command.

Usage Example

To create an OSPF virtual interface:

```
DGS-3324SR:4#create ospf virtual_link 10.1.12 20.1.1.1
hello_interval 10
Command: create ospf virtual_link 10.1.12 20.1.1.1 hello_interval
10


Success.


DGS-3324SR:4#
```

delete ospf virtual_link

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

delete ospf virtual_link

	Border Router. The router ID of the neighbor router.
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To delete an OSPF virtual interface from the switch:

```
DGS-3324SR:4#delete ospf virtual_link 10.1.12 20.1.1.1
Command: delete ospf virtual_link 10.1.12 20.1.1.1


Success.


DGS-3324SR:4#
```

show ospf virtual_link

Purpose	Used to display the current OSPF virtual interface configuration.
Syntax	**show ospf virtual_link {<area_id> <neighbor_id>**
Description	This command will display the current OSPF virtual interface configuration.
Parameters	<area_id> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain. <neighbor_id> – The OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router. This is the router ID of the neighbor router.
Restrictions	none.

Usage Example:

To display the current OSPF virtual interface configuration:

```
DGS-3324SR:4#show ospf virtual_link

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

Total Entries: 1

DGS-3324SR:4#
```

JUMBO FRAME COMMANDS

Certain switches can support jumbo frames (frames larger than the standard Ethernet frame size of 1518 bytes). To transmit frames of up to 9K (and 9004 bytes tagged), the user can increase the maximum transmission unit (MTU) size from the default of 1522 by enabling the Jumbo Frame command.

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

Command	Parameters
enable jumbo_frame	
disable jumbo_frame	
show jumbo_frame	

enable jumbo_frame	
Purpose	Used to enable the jumbo frame function on the switch.
Syntax	**enable jumbo_frame**
Description	This command will allow ethernet frames larger than 1518 bytes to be processed by the switch. The maximum size of the jumbo frame may not exceed 9K.
Parameters	None.
Restrictions	None.

Example usage:

To enable the jumbo frame function on the switch:

```
DGS-3324SR:4#enable jumbo_frame
Command: enable jumbo_frame

 Success.

DGS-3324SR:4#
```

disable jumbo_frame	
Purpose	Used to disable the jumbo frame function on the switch.
Syntax	**disable jumbo_frame**
Description	This command will disable the jumbo frame function on the switch.

disable jumbo_frame

Parameters	None.
Restrictions	None.

Example usage:

To enable the jumbo frame function on the switch:

```
DGS-3324SR:4#disable jumbo_frame
Command: disable jumbo_frame


 Success.


DGS-3324SR:4#
```

show jumbo_frame

Purpose	Used to show the status of the jumbo frame function on the switch.
Syntax	**show jumbo_frame**
Description	This command will show the status of the jumbo frame function on the switch.
Parameters	None.
Restrictions	None.

Usage Example:

To show the jumbo frame status currently configured on the switch:

```
DGS-3324SR:4#show jumbo_frame
Command: show jumbo_frame


 Off.


DGS-3324SR:4#
```

COMMAND HISTORY LIST

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

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

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

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

Example usage

To display all of the commands in the CLI:

```
DGS-3324SR:4#?
..
?
clear
clear arptable
clear counters {ports <portlist2>}
clear fdb
clear log
config 802.1p default_priority
config 802.1p user_priority
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 all_boxes_id
config arp_aging time
config bandwidth_control
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

show command_history

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

Example usage

To display the command history:

```
DGS-3324SR:4#show command_history
Command: show command_history

?
? show
show vlan
config router_ports vlan2 add 1:1-1:10
config router_ports vlan2 add
config router_ports vlan2
config router_ports
show vlan
create vlan vlan2 tag 3
create vlan vlan2 tag 2
show router_ports
show router ports
login

DGS-3324SR:4#
```

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:

```
DGS-3324SR:4#config command_history 20
Command: config command_history 20


 Success.

DGS-3324SR:4#
```

TECHNICAL SPECIFICATIONS

Physical and Environmental	
AC input & External Redundant power Supply:	100 – 120; 200 - 240 VAC, 50|60 Hz (internal universal power supply)
Power Consumption:	90 watts maximum
DC fans:	2 built-in 40 x 40 x10 mm fans
Operating Temperature:	0 to 40 degrees Celsius
Storage Temperature:	-25 to 55 degrees Celsius
Humidity:	Operating: 5% to 95% RH non-condensing; Storage: 0% to 95% RH non-condensing
Dimensions:	441 mm x 207 mm x 44 mm (1U), 19 inch rack-mount width
Weight:	3.15 kg
EMC:	FCC Part 15 Class A / IECES-003 Class (Canada) EN55022 Class A / EN55024
Safety:	CSA International

General		
Standards:	IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.1 P/Q VLAN IEEE 802.3x Full-duplex Flow Control IEEE 802.3 Nway auto-negotiation	
Protocols:	CSMA|CD	
Data Transfer Rates: Ethernet Fast Ethernet Gigabit Ethernet	Half-duplex 10 Mbps 100Mbps n|a	Full-duplex 20Mbps 200Mbps 2000Mbps
Fiber Optic	SFP (Mini GBIC) Support IEEE 802.3z 1000BASE-LX (DEM-310GT	

General	
	transceiver)
	IEEE 802.3z 1000BASE-SX (DEM-311GT transceiver)
	IEEE 802.3z 1000BASE-LH (DEM-314GT transceiver)
	IEEE 802.3z 1000BASE-ZX (DEM-315GT transceiver)
Network Cables:	
10BASE-T:	UTP Cat.5, Cat.5 Enhanced for 1000Mbps
	UTP Cat.5 for 100Mbps
	UTP Cat.3, 4, 5 for 10Mbps
100BASE-TX:	EIA/TIA-568 100-ohm screened twisted-pair (STP)(100m)
Number of Ports:	24 x 10|100 Mbps NWay ports
	4 Gigabit Ethernet (optional)

Performance	
Transmission Method:	Store-and-forward
RAM Buffer:	2 MB per device
Filtering Address Table:	16K MAC address per device
Packet Filtering| Forwarding Rate:	Full-wire speed for all connections.
	148,810 pps per port (for 100Mbps)
	1,488,100 pps per port (for 1000Mbps)
MAC Address Learning:	Automatic update.
Forwarding Table Age Time:	Max age: 10 - 1000000 seconds.
	Default = 300.