BLADE OS™

Command Reference

RackSwitch™ G8124

Version 5.0

Part Number: BMD00142, November 2009

BLADE NETWORK TECHNOLOGIES

2350 Mission College Blvd.
Suite 600
Santa Clara, CA 95054
www.bladenetwork.net

Contents

Preface

The *BLADE OS 5.0 Command Reference* describes how to configure and use the BLADE OS 5.0 software with your RackSwitch G8124 (G8124). This guide lists each command, together with the complete syntax and a functional description, using the BLADE OS Command Line Interface (CLI).

For documentation on installing the switches physically, see the *Installation Guide* for your RackSwitch G8124. For details about configuration and operation of your G8124, see the *BLADE OS 5.0 Application Guide*.

Who Should Use This Book

This book is intended for network installers and system administrators engaged in configuring and maintaining a network. The administrator should be familiar with Ethernet concepts, IP addressing, the IEEE 802.1D Spanning Tree Protocol, and SNMP configuration parameters.

How This Book Is Organized

Chapter 1, "The Command Line Interface," describes how to connect to the switch and access the information and configuration menus.

Chapter 2, "First-Time Configuration," describes how to use the Setup utility for initial switch configuration and how to change the system passwords.

Chapter 3, "Menu Basics," provides an overview of the menu system, including a menu map, global commands, and menu shortcuts.

Chapter 4, "The Information Menu," shows how to view switch configuration parameters.

Chapter 5, "The Statistics Menu," shows how to view switch performance statistics.

Chapter 6, "The Configuration Menu," shows how to configure switch system parameters, ports, VLANs, Spanning Tree Protocol, SNMP, Port Mirroring, IP Routing, Port Trunking, and more.

Chapter 7, "The Operations Menu," shows how to use commands which affect switch performance immediately, but do not alter permanent switch configurations (such as temporarily disabling ports). The menu describes how to activate or deactivate optional software features.

Chapter 8, "The Boot Options Menu," describes the use of the primary and alternate switch images, how to load a new software image, and how to reset the software to factory defaults.

Chapter 9, "The Maintenance Menu," shows how to generate and access a dump of critical switch state information, how to clear it, and how to clear part or all of the forwarding database.

Appendix A, "BLADE OS Syslog Messages," shows a listing of syslog messages.

Appendix B, "BLADE OS SNMP Agent," lists the Management Interface Bases (MIBs) supported in the switch software.

"Index" includes pointers to the description of the key words used throughout the book.

Typographic Conventions

The following table describes the typographic styles used in this book.

Table 1 Typographic Conventions

Typeface or Symbol	Meaning	Example
`AaBbCc123`	This type is used for names of commands, files, and directories used within the text.	View the `readme.txt` file.
	It also depicts on-screen computer output and prompts.	`Main#`
`AaBbCc123`	This bold type appears in command examples. It shows text that must be typed in exactly as shown.	`Main#` **`sys`**
<AaBbCc123>	This italicized type appears in command examples as a parameter placeholder. Replace the indicated text with the appropriate real name or value when using the command. Do not type the brackets.	To establish a Telnet session, enter: `host#` **`telnet`** *<IP address>*
	This also shows book titles, special terms, or words to be emphasized.	Read your *User's Guide* thoroughly.
[ ]	Command items shown inside brackets are optional and can be used or excluded as the situation demands. Do not type the brackets.	`host#` **`ls`** [**`-a`**]

How To Get Help

If you need help, service, or technical assistance, call BLADE Network Technologies Technical Support:

US toll free calls: 1-800-414-5268

International calls: 1-408-834-7871

You also can visit our web site at the following address:

`http://www.bladenetwork.net`

Click the **Support** tab.

The warranty card received with your product provides details for contacting a customer support representative. If you are unable to locate this information, please contact your reseller. Before you call, prepare the following information:

- Serial number of the switch unit
- Software release version number
- Brief description of the problem and the steps you have already taken
- Technical support dump information (`# show tech-support`)

CHAPTER 1

The Command Line Interface

Your RackSwitch G8124 is ready to perform basic switching functions right out of the box. Some of the more advanced features, however, require some administrative configuration before they can be used effectively.

The extensive BLADE OS switching software included in your switch provides a variety of options for accessing and configuring the switch:

- A built-in, text-based command line interface and menu system for access via a Telnet session or serial-port connection
- SNMP support for access through network management software such as IBM Director or HP OpenView
- BLADE OS Browser-Based Interface (BBI)

The command line interface is the most direct method for collecting switch information and performing switch configuration. Using a basic terminal, you are presented with a hierarchy of menus that enable you to view information and statistics about the switch, and to perform any necessary configuration.

This chapter explains how to access the Command Line Interface (CLI) for the switch.

Connecting to the Switch

You can access the command line interface in any one of the following ways:

- Using a Telnet connection over the network
- Using an SSH connection
- Using a serial connection via the serial port on the G8124

Connecting to the Switch via Telnet

A Telnet connection offers the convenience of accessing the switch from any workstation connected to the network. Telnet access provides the same options for user access and administrator access as those available through the console port.

To configure the switch for Telnet access, the switch must have an IP address. The switch can get its IP address in one of two ways:

- Dynamically, from a DHCP server on your network
- Manually, when you configure the switch IP address

Once you have configured the switch with an IP address and gateway, you can access the switch from any workstation connected to the management network. Telnet access provides the same options for user and administrator access as those available through the console port.

By default, Telnet access is enabled. Use the following command to disable/enable Telnet access:

```
# /cfg/sys/access/tnet e|d
```

To establish a Telnet connection to the switch, you can run the Telnet program on your workstation and issue the Telnet command, followed by the switch IP address:

```
telnet <switch IP address>
```

Connecting to the Switch via SSH

Although a remote network administrator can manage the configuration of a G8124 via Telnet, this method does not provide a secure connection. The SSH (Secure Shell) protocol enables you to securely log into another device over a network to execute commands remotely. As a secure alternative to using Telnet to manage switch configuration, SSH ensures that all data sent over the network is encrypted and secure.

The switch can do only one session of key/cipher generation at a time. Thus, a SSH/SCP client will not be able to login if the switch is doing key generation at that time. Similarly, the system will fail to do the key generation if a SSH/SCP client is logging in at that time.

The supported SSH encryption and authentication methods are listed below.

- Server Host Authentication: Client RSA-authenticates the switch in the beginning of every connection.
- Key Exchange: RSA
- Encryption: 3DES-CBC, DES
- User Authentication: Local password authentication, RADIUS, TACACS+

The following SSH clients have been tested:

- OpenSSH_5.1p1 Debian-3ubuntu1
- SecureCRT 5.0 (Van Dyke Technologies, Inc.)
- Putty beta 0.60

Note – The BLADE OS implementation of SSH supports both versions 1.5 and 2.0 and supports SSH client version 1.5 - 2.x.

Using SSH to Access the Switch

Once the IP parameters are configured and the SSH service is enabled on the G8124 (it is disabled by default), you can access the command line interface using an SSH connection.

To establish an SSH connection with the switch, run the SSH program on your workstation by issuing the SSH command, followed by the switch IP address:

```
>> # ssh <switch IP address>
```

If SecurID authentication is required, use the following command:

```
>> # ssh -1 ace <switch IP address>
```

You will then be prompted to enter your user name and password.

Accessing the Switch

To enable better switch management and user accountability, three levels or *classes* of user access have been implemented on the G8124. Levels of access to CLI, Web management functions, and screens increase as needed to perform various switch management tasks. Conceptually, access classes are defined as follows:

- User interaction with the switch is completely passive—nothing can be changed on the G8124. Users may display information that has no security or privacy implications, such as switch statistics and current operational state information.
- Operators can only effect temporary changes on the G8124. These changes will be lost when the switch is rebooted/reset. Operators have access to the switch management features used for daily switch operations. Because any changes an operator makes are undone by a reset of the switch, operators cannot severely impact switch operation.

- Administrators are the only ones that may make permanent changes to the switch configuration—changes that are persistent across a reboot/reset of the switch. Administrators can access switch functions to configure and troubleshoot problems on the G8124. Because administrators can also make temporary (operator-level) changes as well, they must be aware of the interactions between temporary and permanent changes.

Access to switch functions is controlled through the use of unique surnames and passwords. Once you are connected to the switch via local Telnet, remote Telnet, or SSH, you are prompted to enter a password. The default user names/password for each access level are listed in the following table.

Note – It is recommended that you change default switch passwords after initial configuration and as regularly as required under your network security policies. For more information, see "Setting Passwords" on page 31.

Table 2 User Access Levels

User Account	Description and Tasks Performed	Password
User	The User has no direct responsibility for switch management. He or she can view all switch status information and statistics, but cannot make any configuration changes to the switch.	`user`
Operator	The Operator manages all functions of the switch. The Operator can reset ports, except the management ports.	`oper`
Administrator	The superuser Administrator has complete access to all menus, information, and configuration commands on the G8124, including the ability to change both the user and administrator passwords.	`admin`

Note – With the exception of the "admin" user, access to each user level can be disabled by setting the password to an empty value.

Setup vs. CLI

Once the administrator password is verified, you are given complete access to the switch. If the switch is still set to its factory default configuration, the system will ask whether you wish to run Setup (see Chapter 2, "First-Time Configuration"), a utility designed to help you through the first-time configuration process. If the switch has already been configured, the Main Menu of the CLI is displayed instead.

The following table shows the Main Menu with administrator privileges.

```
[Main Menu]
      info    - Information Menu
      stats   - Statistics Menu
      cfg     - Configuration Menu
      oper    - Operations Command Menu
      boot    - Boot Options Menu
      maint   - Maintenance Menu
      diff    - Show pending config changes  [global command]
      apply   - Apply pending config changes [global command]
      save    - Save updated config to FLASH [global command]
      revert  - Revert pending or applied changes [global command]
      exit    - Exit  [global command, always available]
```

Note – If you are accessing a user account, some menu options will not be available.

Command Line History and Editing

For a description of global commands, shortcuts, and command line editing functions, see "Menu Basics" on page 35."

Idle Timeout

By default, the switch will disconnect your Telnet session after 10 minutes of inactivity. This function is controlled by the idle timeout parameter, which can be set from 1 to 60 minutes. For information on changing this parameter, see "System Configuration Menu" on page 157.

CHAPTER 2

First-Time Configuration

To help with the initial process of configuring your switch, the BLADE OS software includes a Setup utility. The Setup utility prompts you step-by-step to enter all the necessary information for basic configuration of the switch. This chapter describes how to use the Setup utility and how to change system passwords. Before you run Setup, you must first connect to the switch (see Chapter 1, "Connecting to the Switch").

Using the Setup Utility

Whenever you log in as the system administrator under the factory default configuration, you are asked whether you wish to run the Setup utility. Setup can also be activated manually from the command line interface any time after login.

Information Needed for Setup

Setup requests the following information:

- Basic system information
  - Date & time
  - Whether to use Spanning Tree Group or not
- Optional configuration for each port
  - Speed, duplex, flow control, and negotiation mode (as appropriate)
  - Whether to use VLAN tagging or not (as appropriate)
- Optional configuration for each VLAN
  - Name of VLAN
  - Which ports are included in the VLAN

- Optional configuration of IP parameters
  - IP address, subnet mask, and VLAN for each IP interface
  - IP addresses for default gateway
  - Destination, subnet mask, and gateway IP address for each IP static route
  - Whether IP forwarding is enabled or not
  - Whether the RIP supply is enabled or not

Starting Setup When You Log In

The Setup prompt appears automatically whenever you login as the system administrator under the factory default settings.

1. Connect to the switch.

   After connecting, the login prompt will appear as shown below.

```
Enter Password:
```

2. Enter **admin** as the default administrator password.

   If the factory default configuration is detected, the system prompts:

```
Blade Network Technologies RackSwitch G8124
18:44:05 Wed Jan 3, 2009

The switch is booted with factory default configuration.
To ease the configuration of the switch, a "Set Up" facility which
will prompt you with those configuration items that are essential to
the operation of the switch is provided.
Would you like to run "Set Up" to configure the switch? [y/n]:
```

Note – If the default `admin` login is unsuccessful, or if the administrator Main Menu appears instead, the system configuration has probably been changed from the factory default settings. If you are certain that you need to return the switch to its factory default settings, see "Selecting a Configuration Block" on page 317.

3. Enter **y** to begin the initial configuration of the switch, or n to bypass the Setup facility.

Stopping and Restarting Setup Manually

Stopping Setup

To abort the Setup utility, press <Ctrl-C> during any Setup question. When you abort Setup, the system will prompt:

```
Would you like to run from top again? [y/n]
```

Enter **n** to abort Setup, or **y** to restart the Setup program at the beginning.

Restarting Setup

You can restart the Setup utility manually at any time by entering the following command at the administrator prompt:

```
# /cfg/setup
```

Setup Part 1: Basic System Configuration

When Setup is started, the system prompts:

```
"Set Up" will walk you through the configuration of
  System Date and Time, Spanning Tree, Port Speed/Mode,
  VLANs, and IP interfaces. [type Ctrl-C to abort "Set Up"]
```

1. Enter **y** if you will be configuring VLANs. Otherwise enter **n**.

   If you decide not to configure VLANs during this session, you can configure them later using the configuration menus, or by restarting the Setup facility. For more information on configuring VLANs, see the *BLADE OS Application Guide*.

   Next, the Setup utility prompts you to input basic system information.

2. Enter the year of the current date at the prompt:

   ```
   System Date:
   Enter year [2009]:
   ```

   Enter the four-digits that represent the year. To keep the current year, press <Enter>.

   The system displays the date and time settings:

   ```
   System clock set to 18:55:36 Wed Jan 28, 2009.
   ```

3. Enter the month of the current system date at the prompt:

```
System Date:
Enter month [1]:
```

Enter the month as a number from 1 to 12. To keep the current month, press <Enter>.

4. Enter the day of the current date at the prompt:

```
Enter day [3]:
```

Enter the date as a number from 1 to 31. To keep the current day, press <Enter>.

5. Enter the hour of the current system time at the prompt:

```
System Time:
Enter hour in 24-hour format [18]:
```

Enter the hour as a number from 00 to 23. To keep the current hour, press <Enter>.

6. Enter the minute of the current time at the prompt:

```
Enter minutes [55]:
```

Enter the minute as a number from 00 to 59. To keep the current minute, press <Enter>.

7. Enter the seconds of the current time at the prompt:

```
Enter seconds [37]:
```

Enter the seconds as a number from 00 to 59. To keep the current second, press <Enter>. The system then displays the date and time settings:

```
System clock set to 8:55:36 Wed Jan 28, 2009.
```

8. Turn Spanning Tree Protocol on or off at the prompt:

```
Spanning Tree:
Current Spanning Tree Group 1 setting: ON
Turn Spanning Tree Group 1 OFF? [y/n]
```

Enter **y** to turn off Spanning Tree, or enter **n** to leave Spanning Tree on.

Setup Part 2: Port Configuration

Note – When configuring port options for your switch, some prompts and options may be different.

1. Select the port to configure, or skip port configuration at the prompt:

```
Port Config:
Will you configure VLANs and VLAN tagging for ports? [y/n]
```

If you wish to change settings for VLANs, enter `y`, or enter `n` to skip VLAN configuration.

Note – The sample screens that appear in this document might differ slightly from the screens displayed by your system. Screen content varies based on the type of BladeCenter unit that you are using and the firmware versions and options that are installed.

2. Select the port to configure, or skip port configuration at the prompt:

```
Port Config:
Enter port (1-24, MGTA, MGTB):
```

If you wish to change settings for individual ports, enter the number of the port you wish to configure. To skip port configuration, press <Enter> without specifying any port and go to "Setup Part 3: VLANs" on page 26.

3. Configure Gigabit Ethernet port flow parameters.

If you selected a port that has a Gigabit Ethernet connector, the system prompts:

```
Gig Link Configuration:
Port Flow Control:
Current Port 1 flow control setting:    both
Enter new value ["rx"/"tx"/"both"/"none"]:
```

Enter **`rx`** to enable receive flow control, **`tx`** for transmit flow control, **`both`** to enable both, or **`none`** to turn flow control off for the port. To keep the current setting, press <Enter>.

4. Configure Gigabit Ethernet port autonegotiation mode.

If you selected a port that has a Gigabit Ethernet connector, the system prompts:

```
Port Auto Negotiation:
Current Port 1 autonegotiation:         on
Enter new value ["on"/"off"]:
```

Enter **`on`** to enable port autonegotiation, **`off`** to disable it, or press <Enter> to keep the current setting.

5. If configuring VLANs, enable or disable VLAN tagging for the port.

   If you have selected to configure VLANs back in Part 1, the system prompts:

```
Port VLAN tagging config (tagged port can be a member of multiple VLANs)
Current VLAN tag support:                disabled
Enter new VLAN tag support [d/e]:
```

   Enter **d** to disable VLAN tagging for the port or enter **e** to enable VLAN tagging for the port. To keep the current setting, press <Enter>.

6. The system prompts you to configure the next port:

```
Enter port (1-24, MGTA, MGTB):
```

   When you are through configuring ports, press <Enter> without specifying any port. Otherwise, repeat the steps in this section.

Setup Part 3: VLANs

If you chose to skip VLANs configuration back in Part 2, skip to "Setup Part 4: IP Configuration" on page 27.

1. Select the VLAN to configure, or skip VLAN configuration at the prompt:

```
VLAN Config:
Enter VLAN number from 2 to 4094, NULL at end:
```

   If you wish to change settings for individual VLANs, enter the number of the VLAN you wish to configure. To skip VLAN configuration, press <Enter> without typing a VLAN number and go to "Setup Part 4: IP Configuration" on page 27.

2. Enter the new VLAN name at the prompt:

```
Current VLAN name: VLAN 2
Enter new VLAN name:
```

   Entering a new VLAN name is optional. To use the pending new VLAN name, press <Enter>.

3. Enter the VLAN port numbers:

```
Define Ports in VLAN:
Current VLAN 2:  empty
Enter ports one per line, NULL at end:
```

   Enter each port, by port number or port alias, and confirm placement of the port into this VLAN. When you are finished adding ports to this VLAN, press <Enter> without specifying any port.

4. Configure Spanning Tree Group membership for the VLAN:

```
Spanning Tree Group membership:
Enter new Spanning Tree Group index [1-127]:
```

5. The system prompts you to configure the next VLAN:

```
VLAN Config:
Enter VLAN number from 2 to 4094, NULL at end:
```

Repeat the steps in this section until all VLANs have been configured. When all VLANs have been configured, press <Enter> without specifying any VLAN.

Setup Part 4: IP Configuration

The system prompts for IP parameters.

IP Interfaces

IP interfaces are used for defining subnets to which the switch belongs.

Up to 128 IP interfaces can be configured on the RackSwitch G8124. The IP address assigned to each IP interface provide the switch with an IP presence on your network. No two IP interfaces can be on the same IP subnet. The interfaces can be used for connecting to the switch for remote configuration, and for routing between subnets and VLANs (if used).

Note – Interfaces 127 and 128 are reserved for switch management.

1. Select the IP interface to configure, or skip interface configuration at the prompt:

```
IP Config:

IP interfaces:
Enter interface number: (1-128)
```

If you wish to configure individual IP interfaces, enter the number of the IP interface you wish to configure. To skip IP interface configuration, press <Enter> without typing an interface number and go to "Default Gateways" on page 28.

Note – Because interface 128 is reserved for switch management, if you change the IP address of IF 128, you can lose the connection to the management module. Use the management module to change the IP address of the G8124.

2. For the specified IP interface, enter the IP address in dotted decimal notation:

```
Current IP address:     0.0.0.0
Enter new IP address:
```

To keep the current setting, press <Enter>.

3. At the prompt, enter the IP subnet mask in dotted decimal notation:

```
Current subnet mask:            0.0.0.0
Enter new subnet mask:
```

To keep the current setting, press <Enter>.

4. If configuring VLANs, specify a VLAN for the interface.

This prompt appears if you selected to configure VLANs back in Part 1:

```
Current VLAN:     1
Enter new VLAN [1-4094]:
```

Enter the number for the VLAN to which the interface belongs, or press <Enter> without specifying a VLAN number to accept the current setting.

5. At the prompt, enter **y** to enable the IP interface, or **n** to leave it disabled:

```
Enable IP interface? [y/n]
```

6. The system prompts you to configure another interface:

```
Enter interface number: (1-128)
```

Repeat the steps in this section until all IP interfaces have been configured. When all interfaces have been configured, press <Enter> without specifying any interface number.

Default Gateways

1. At the prompt, select a default gateway for configuration, or skip default gateway configuration:

```
IP default gateways:
Enter default gateway number: (1-4)
```

Enter the number for the default gateway to be configured. To skip default gateway configuration, press <Enter> without typing a gateway number and go to "IP Routing" on page 29.

2. At the prompt, enter the IP address for the selected default gateway:

```
Current IP address:     0.0.0.0
Enter new IP address:
```

Enter the IP address in dotted decimal notation, or press <Enter> without specifying an address to accept the current setting.

3. At the prompt, enter **y** to enable the default gateway, or **n** to leave it disabled:

```
Enable default gateway? [y/n]
```

4. The system prompts you to configure another default gateway:

```
Enter default gateway number: (1-4)
```

Repeat the steps in this section until all default gateways have been configured. When all default gateways have been configured, press <Enter> without specifying any number.

IP Routing

When IP interfaces are configured for the various subnets attached to your switch, IP routing between them can be performed entirely within the switch. This eliminates the need to send inter-subnet communication to an external router device. Routing on more complex networks, where subnets may not have a direct presence on the G8124, can be accomplished through configuring static routes or by letting the switch learn routes dynamically.

This part of the Setup program prompts you to configure the various routing parameters.

1. At the prompt, enable or disable forwarding for IP Routing:

```
Enable IP forwarding? [y/n]
```

Enter **y** to enable IP forwarding. To disable IP forwarding, enter **n**. To keep the current setting, press <Enter>.

Setup Part 5: Final Steps

1. When prompted, decide whether to restart Setup or continue:

```
Would you like to run from top again? [y/n]
```

Enter **y** to restart the Setup utility from the beginning, or **n** to continue.

2. When prompted, decide whether you wish to review the configuration changes:

```
Review the changes made? [y/n]
```

Enter **y** to review the changes made during this session of the Setup utility. Enter **n** to continue without reviewing the changes. We recommend that you review the changes.

3. Next, decide whether to apply the changes at the prompt:

```
Apply the changes? [y/n]
```

Enter **y** to apply the changes, or **n** to continue without applying. Changes are normally applied.

4. At the prompt, decide whether to make the changes permanent:

```
Save changes to flash? [y/n]
```

Enter **y** to save the changes to flash. Enter **n** to continue without saving the changes. Changes are normally saved at this point.

5. If you do not apply or save the changes, the system prompts whether to abort them:

```
Abort all changes? [y/n]
```

Enter **y** to discard the changes. Enter **n** to return to the "`Apply the changes?`" prompt.

Note – After initial configuration is complete, it is recommended that you change the default passwords as shown in "Setting Passwords" on page 31.

Optional Setup for Telnet Support

Note – This step is optional. Perform this procedure only if you are planning on connecting to the G8124 through a remote Telnet connection.

---

1. Telnet is enabled by default. To change the setting, use the following command:

```
>> # /cfg/sys/access/tnet
```

2. Apply and save the configuration(s).

```
>> System# apply
>> System# save
```

Setting Passwords

It is recommended that you change the user and administrator passwords after initial configuration and as regularly as required under your network security policies.

To change the administrator password, you must login using the administrator password.

Note – If you forget your administrator password, call your technical support representative for help using the password fix-up mode.

Changing the Default Administrator Password

The administrator has complete access to all menus, information, and configuration commands, including the ability to change both the user and administrator passwords.

The default password for the administrator account is `admin`. To change the default password, follow this procedure:

1. Connect to the switch and log in using the `admin` password.
2. From the Main Menu, use the following command to access the Configuration Menu:

```
Main# /cfg
```

The Configuration Menu is displayed.

```
[Configuration Menu]
     sys       - System-wide Parameter Menu
     port      - Port Menu
     qos       - QOS Menu
     acl       - Access Control List Menu
     pmirr     - Port Mirroring Menu
     l2        - Layer 2 Menu
     l3        - Layer 3 Menu
     setup     - Step by step configuration set up
     dump      - Dump current configuration to script file
     ptcfg     - Backup current configuration to FTP/TFTP server
     gtcfg     - Restore current configuration from FTP/TFTP server
     cur       - Display current configuration
```

3. From the Configuration Menu, use the following command to select the System Menu:

```
>> Configuration# sys
```

The System Menu is displayed.

```
[System Menu]
     syslog   - Syslog Menu
     sshd     - SSH Server Menu
     radius   - RADIUS Authentication Menu
     tacacs+  - TACACS+ Authentication Menu
     ldap     - LDAP Authentication Menu
     ntp      - NTP Server Menu
     ssnmp    - System SNMP Menu
     access   - System Access Menu
     dst      - Custom DST Menu
     sflow    - sFlow Menu
     date     - Set system date
     time     - Set system time
     timezone - Set system timezone (daylight savings)
     dlight   - Set system daylight savings
     idle     - Set timeout for idle CLI sessions
     notice   - Set login notice
     bannr    - Set login banner
     hprompt  - Enable/disable display hostname (sysName) in CLI prompt
     dhcp     - Enable/disable use of DHCP on Mgmt interface
     reminder - Enable/disable Reminders
     rstctrl  - Enable/disable System reset on panic
     cur      - Display current system-wide parameters
```

4. From the System Menu, use the following command to select the System Access Menu:

```
>> System# access
```

The System Access Menu is displayed.

```
[System Access Menu]
     mgmt     - Management Network Definition Menu
     user     - User Access Control Menu (passwords)
     https    - HTTPS Web Access Menu
     snmp     - Set SNMP access control
     tnport   - Set Telnet server port number
     tport    - Set the TFTP Port for the system
     wport    - Set HTTP (Web) server port number
     http     - Enable/disable HTTP (Web) access
     tnet     - Enable/disable Telnet access
     tsbbi    - Enable/disable Telnet/SSH configuration from BBI
     userbbi  - Enable/disable user configuration from BBI
     cur      - Display current system access configuration
```

5. Select the administrator password.

```
System Access# user/admpw
```

6. Enter the current administrator password at the prompt:

```
Changing ADMINISTRATOR password; validation required...
Enter current administrator password:
```

Note – If you forget your administrator password, call your technical support representative for help using the password fix-up mode.

7. Enter the new administrator password at the prompt:

```
Enter new administrator password:
```

8. Enter the new administrator password, again, at the prompt:

```
Re-enter new administrator password:
```

9. Apply and save your change by entering the following commands:

```
System# apply
System# save
```

Changing the Default User Password

The user login has limited control of the switch. Through a user account, you can view switch information and statistics, but you can't make configuration changes.

The default password for the user account is `user`. This password can be changed from the user account. The administrator can change all passwords, as shown in the following procedure.

1. Connect to the switch and log in using the `admin` password.
2. From the Main Menu, use the following command to access the Configuration Menu:

```
Main# cfg
```

3. From the Configuration Menu, use the following command to select the System Menu:

```
>> Configuration# sys
```

4. From the System Menu, use the following command to select the System Access Menu:

```
>> System# access
```

5. Select the user password.

```
System# user/usrpw
```

6. Enter the current administrator password at the prompt.

   Only the administrator can change the user password. Entering the administrator password confirms your authority.

```
Changing USER password; validation required...
Enter current administrator password:
```

7. Enter the new user password at the prompt:

```
Enter new user password:
```

8. Enter the new user password, again, at the prompt:

```
Re-enter new user password:
```

9. Apply and save your changes:

```
System# apply
System# save
```

CHAPTER 3

Menu Basics

The RackSwitch G8124 Command Line Interface (CLI) is used for viewing switch information and statistics. In addition, the administrator can use the CLI for performing all levels of switch configuration.

To make the CLI easy to use, the various commands have been logically grouped into a series of menus and sub-menus. Each menu displays a list of commands and/or sub-menus that are available, along with a summary of what each command will do. Below each menu is a prompt where you can enter any command appropriate to the current menu.

This chapter describes the Main Menu commands, and provides a list of commands and shortcuts that are commonly available from all the menus within the CLI.

The Main Menu

The Main Menu appears after a successful connection and login. The following table shows the Main Menu for the administrator login. Some features are not available under the user login.

```
[Main Menu]
      info    - Information Menu
      stats   - Statistics Menu
      cfg     - Configuration Menu
      oper    - Operations Command Menu
      boot    - Boot Options Menu
      maint   - Maintenance Menu
      diff    - Show pending config changes  [global command]
      apply   - Apply pending config changes [global command]
      save    - Save updated config to FLASH [global command]
      revert  - Revert pending or applied changes [global command]
      exit    - Exit  [global command, always available]
```

Menu Summary

- **Information Menu**

  Provides sub-menus for displaying information about the current status of the switch: from basic system settings to VLANs, and more.

- **Statistics Menu**

  Provides sub-menus for displaying switch performance statistics. Included are port, IF, IP, ICMP, TCP, UDP, SNMP, routing, ARP, DNS, and VRRP statistics.

- **Configuration Menu**

  This menu is available only from an administrator login. It includes sub-menus for configuring every aspect of the switch. Changes to configuration are not active until explicitly applied. Changes can be saved to non-volatile memory.

- **Operations Menu**

  Operations-level commands are used for making immediate and temporary changes to switch configuration. This menu is used for bringing ports temporarily in and out of service, enabling or disabling FDB learning on a port, or sending NTP requests. It is also used for activating or deactivating optional software packages.

- **Boot Options Menu**

  This menu is used for upgrading switch software, selecting configuration blocks, and for resetting the switch when necessary.

- **Maintenance Menu**

  This menu is used for debugging purposes, enabling you to generate a dump of the critical state information in the switch, and to clear entries in the forwarding database and the ARP and routing tables.

Global Commands

Some basic commands are recognized throughout the menu hierarchy. These commands are useful for obtaining online help, navigating through menus, and for applying and saving configuration changes.

For help on a specific command, type `help`. You will see the following screen:

```
Global Commands: [can be issued from any menu]
help              up                print             pwd
lines             verbose           exit              quit
diff              apply             save              revert
revert apply
ping              traceroute        telnet            history
pushd             popd              who               chpass_p
chpass_s

The following are used to navigate the menu structure:
    .  Print current menu
   ..  Move up one menu level
    /  Top menu if first, or command separator
    !  Execute command from history
```

Table 3 Description of Global Commands

Command	Action
? *command* **or help**	Provides more information about a specific command on the current menu. When used without the *command* parameter, a summary of the global commands is displayed.
. or **print**	Display the current menu.
list	Lists the commands available at the current level. You may follow the list command with a text string, and list all of the available commands that match the string.
.. or **up**	Go up one level in the menu structure.
/	If placed at the beginning of a command, go to the Main Menu. Otherwise, this is used to separate multiple commands placed on the same line.
lines [*n***]**	Set the number of lines (*n*) that display on the screen at one time. The default is 24 lines. When used without a value, the current setting is displayed. Set lines to a value of 0 (zero) to disable pagination.
diff	Show any pending configuration changes.

Table 3 Description of Global Commands

Command	Action
apply	Apply pending configuration changes.
save	Write configuration changes to non-volatile flash memory.
revert	Remove pending configuration changes between "`apply`" commands. Use this command to remove any configuration changes made since last `apply`.
revert apply	Remove pending or applied configuration changes between "`save`" commands. Use this command to remove any configuration changes made since last `save`.
exit or **quit**	Exit from the command line interface and log out.
ping	Use this command to verify station-to-station connectivity across the network. The format is as follows: **ping** *<host name>* | *<IP address>* [*<tries (1-32)>* [*<msec delay>*]] **[-ma|-mgta|-mb|mgtb|-d|-data]** Where *IP address* is the hostname or IP address of the device, *tries* (optional) is the number of attempts (1-32), and *msec delay* (optional) is the number of milliseconds between attempts. By default, the **-ma** or **-mgta** option for management port A is used. To use data ports, specify the **-d** or **-data** option. The DNS parameters must be configured if specifying hostnames (see "Domain Name System Configuration" on page 293).
traceroute	Use this command to identify the route used for station-to-station connectivity across the network. The format is as follows: **traceroute** *<host name>*| *<IP address>* [*<max-hops (1-16)>* [*<msec delay>*]] Where *IP address* is the hostname or IP address of the target station, *max-hops* (optional) is the maximum distance to trace (1-16 devices), and *delay* (optional) is the number of milliseconds for wait for the response. As with `ping`, the DNS parameters must be configured if specifying hostnames.
pwd	Display the command path used to reach the current menu.

Table 3 Description of Global Commands

Command	Action
verbose *n*	Sets the level of information displayed on the screen: **0** = Quiet: Nothing appears except errors—not even prompts. **1** = Normal: Prompts and requested output are shown, but no menus. **2** = Verbose: Everything is shown. When used without a value, the current setting is displayed.
telnet	This command is used to telnet out of the switch. The format is as follows: **telnet** <*hostname*> | <*IP address*> [<*port*>] **[-ma|-mgta|-mb|-mgtb|-d|-data]** Where *IP address* is the hostname or IP address of the device. By default, the **-ma** or **-mgta** option for management port A is used. To use data ports, specify the **-d** or **-data** option.
history	This command displays the most recent commands.
pushd	Save the current menu path, so you can jump back to it using `popd`.
popd	Go to the menu path and position previously saved by using `pushd`.
who	Displays a list of users that are logged on to the switch.
chpass_p	Configures the password for the primary TACACS+ server.
chpass_s	Configures the password for the secondary TACACS+ server.

Command Line History and Editing

Using the command line interface, you can retrieve and modify previously entered commands with just a few keystrokes. The following options are available globally at the command line:

Table 4 Command Line History and Editing Options

Option	Description
`history`	Display a numbered list of the last 64 previously entered commands.
`!!`	Repeat the last entered command.
`!`*n*	Repeat the n^{th} command shown on the history list.
<Ctrl-p>	(Also the up arrow key.) Recall the *previous* command from the history list. This can be used multiple times to work backward through the last 64 commands. The recalled command can be entered as is, or edited using the options below.
<Ctrl-n>	(Also the down arrow key.) Recall the *next* command from the history list. This can be used multiple times to work forward through the last 64 commands. The recalled command can be entered as is, or edited using the options below.
<Ctrl-a>	Move the cursor to the beginning of command line.
<Ctrl-e>	Move cursor to the *end* of the command line.
<Ctrl-b>	(Also the left arrow key.) Move the cursor *back* one position to the left.
<Ctrl-f>	(Also the right arrow key.) Move the cursor *forward* one position to the right.
<Backspace>	(Also the Delete key.) Erase one character to the left of the cursor position.
<Ctrl-d>	*Delete* one character at the cursor position.
<Ctrl-k>	*Kill* (erase) all characters from the cursor position to the end of the command line.
<Ctrl-l>	Redraw the screen.
<Ctrl-u>	Clear the entire line.
Other keys	Insert new characters at the cursor position.

Command Line Interface Shortcuts

The following shortcuts allow you to enter commands quickly and easily.

CLI List and Range Inputs

For CLI commands that allow an individual item to be selected from within a numeric range, lists and ranges of items can now be specified. For example, the `/info/vlan` command permits the following options:

# /info/vlan	*(show all VLANs)*
# /info/vlan 1	*(show only VLAN 1)*
# /info/vlan 1,3,4095	*(show listed VLANs)*
# /info/vlan 1-20	*(show range 1 through 20)*
# /info/vlan 1-5,90-99,4090-4095	*(show multiple ranges)*
# /info/vlan 1-5,19,20,4090-4095	*(show a mix of lists and ranges)*

The numbers in a range must be separated by a dash: *<start of range>*-*<end of range>*

Multiple ranges or list items are permitted using a comma: *<range or item 1>*,*<range or item 2>*

Do not use spaces within list and range specifications.

Ranges can also be used to apply the same command option to multiple items. For example, to enable multiple ports with one command:

# /cfg/port 1-4/ena	*(Enable ports 1 though 4)*

Note – Port ranges accept only port numbers, not port aliases.

Command Stacking

As a shortcut, you can type multiple commands on a single line, separated by forward slashes (**/**). You can connect as many commands as required to access the menu option that you want. For example, the keyboard shortcut to access the Spanning Tree Port Configuration Menu from the `Main#` prompt is as follows:

```
Main# cfg/l2/stg 1/port
```

Command Abbreviation

Most commands can be abbreviated by entering the first characters which distinguish the command from the others in the same menu or sub-menu. For example, the command shown above could also be entered as follows:

```
Main# c/l2/stg 1/po
```

Tab Completion

By entering the first letter of a command at any menu prompt and hitting <Tab>, the CLI will display all commands or options in that menu that begin with that letter. Entering additional letters will further refine the list of commands or options displayed. If only one command fits the input text when <Tab> is pressed, that command will be supplied on the command line, waiting to be entered. If the <Tab> key is pressed without any input on the command line, the currently active menu will be displayed.

CHAPTER 4
The Information Menu

You can view configuration information for the switch in both the user and administrator command modes. This chapter discusses how to use the command line interface to display switch information.

/info
Information Menu

```
[Information Menu]
     sys      - System Information Menu
     l2       - Layer 2 Information Menu
     l3       - Layer 3 Information Menu
     qos      - QoS Menu
     acl      - Show ACL information
     link     - Show link status
     port     - Show port information
     transcvr - Show Port Transceiver status
     dump     - Dump all information
```

The information provided by each menu option is briefly described in Table 5, with pointers to detailed information.

Table 5 Information Menu Options

Command Syntax and Usage
sys Displays the System Information menu. For details, see page 46.
12 Displays the Layer 2 Information menu. For details, see page 60.
13 Displays the Layer 3 Information menu. For details, see page 80.

Table 5 Information Menu Options

Command Syntax and Usage
qos Displays the Quality of Service (QoS) Information menu. For details, see page 100.
acl Displays the current configuration profile for each Access Control List (ACL). For details, see page 102.
link Displays configuration information about each port, including: □ Port alias and number □ Port speed □ Duplex mode (half, full, or auto) □ Flow control for transmit and receive (no, yes, or both) □ Link status (up, down, or disabled) For details, see page 104.
port Displays port status information, including: □ Port alias and number □ Whether the port uses VLAN Tagging or not □ Port VLAN ID (PVID) □ Port name □ VLAN membership □ Fast Fowarding status □ FDB Learning status □ Flood Blocking status For details, see page 105.

Table 5 Information Menu Options

Command Syntax and Usage
transcvr Displays the status of the port transceiver module on each external port. For details, see page 106.
dump Dumps all switch information available from the Information menu (10K or more, depending on your configuration). If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.

/info/sys
System Information Menu

```
[System Menu]
     errdis    - Errdisable Menu
     snmpv3    - SNMPv3 Information Menu
     general   - Show general system information
     log       - Show syslog messages
     user      - Show current user status
     dump      - Dump all system information
```

The information provided by each menu option is briefly described in Table 6, with pointers to where detailed information can be found.

Table 6 System Information Options

Command Syntax and Usage
errdis Displays Error Disable and Recovery Information menu. To view the menu options, see page 47.
snmpv3 Displays SNMPv3 Information menu. To view the menu options, see page 48.
general Displays system information, including: □ System date and time □ Switch model name and number □ Switch name and location □ Time of last boot □ MAC address of the switch management processor □ IP address of management interface □ Hardware version and part number □ Software image file and version number □ Configuration name □ Log-in banner, if one is configured For details, see page 56.
log Displays most recent syslog messages. For details, see page 58.

Table 6 System Information Options

Command Syntax and Usage
user Displays configured user names and their status. For details, see page 59.
dump Dumps all switch information available from the Information menu (10K or more, depending on your configuration).

/info/sys/errdis
Error Disable and Recovery Information

```
[ErrDisable Information Menu]
     recovery - Show ErrDisable recovery information
     timers   - Show ErrDisable timer information
     dump     - Show all of the above
```

This menu allows you to display information about the Error Disable and Recovery feature for interface ports.

Table 7 Error Disable Information Options

Command Syntax and Usage
recovery Displays a list ports with their Error Recovery status.
timers Displays a list of active recovery timers, if applicable.
dump Displays all Error Disable and Recovery information.

/info/sys/snmpv3
SNMPv3 System Information

SNMP version 3 (SNMPv3) is an extensible SNMP Framework that supplements the SNMPv2 Framework by supporting the following:

- a new SNMP message format
- security for messages
- access control
- remote configuration of SNMP parameters

For more details on the SNMPv3 architecture please refer to RFC2271 to RFC2276.

```
[SNMPv3 Information Menu]
     usm       - Show usmUser table information
     view      - Show vacmViewTreeFamily table information
     access    - Show vacmAccess table information
     group     - Show vacmSecurityToGroup table information
     comm      - Show community table information
     taddr     - Show targetAddr table information
     tparam    - Show targetParams table information
     notify    - Show notify table information
     dump      - Show all SNMPv3 information
```

Table 8 SNMPv3 information Options

Command Syntax and Usage
usm Displays User Security Model (USM) table information. To view the table, see page 49.
view Displays information about view, sub-trees, mask and type of view. To view a sample, see page 50.
access Displays View-based Access Control information. To view a sample, see page 51.
group Displays information about the group that includes, the security model, user name, and group name. To view a sample, see page 52.
comm Displays information about the community table information. To view a sample, see page 52.

Table 8 SNMPv3 information Options

Command Syntax and Usage
taddr Displays the Target Address table information. To view a sample, see page 53.
tparam Displays the Target parameters table information. To view a sample, see page 54.
notify Displays the Notify table information. To view a sample, see page 54.
dump Displays all the SNMPv3 information. To view a sample, see page 55.

/info/sys/snmpv3/usm
SNMPv3 USM User Table Information

The User-based Security Model (USM) in SNMPv3 provides security services such as authentication and privacy of messages. This security model makes use of a defined set of user identities displayed in the USM user table. The USM user table contains the following information:

- the user name
- a security name in the form of a string whose format is independent of the Security Model
- an authentication protocol, which is an indication that the messages sent on behalf of the user can be authenticated
- the privacy protocol

```
usmUser Table:
User Name                       Protocol
------------------------------- --------------------------------
adminmd5                        HMAC_MD5, DES PRIVACY
adminsha                        HMAC_SHA, DES PRIVACY
v1v2only                        NO AUTH,  NO PRIVACY
```

Table 9 USM User Table Information

Field	Description
User Name	This is a string that represents the name of the user that you can use to access the switch.
Protocol	This indicates whether messages sent on behalf of this user are protected from disclosure using a privacy protocol. BLADE OS supports DES algorithm for privacy. The software also supports two authentication algorithms: MD5 and HMAC-SHA.

/info/sys/snmpv3/view
SNMPv3 View Table Information

The user can control and restrict the access allowed to a group to only a subset of the management information in the management domain that the group can access within each context by specifying the group's rights in terms of a particular MIB view for security reasons.

```
View Name            Subtree                Mask           Type
-----------------    ------------------   --------------  --------
iso                  1.3                                  included
v1v2only             1.3                                  included
v1v2only             1.3.6.1.6.3.15                       excluded
v1v2only             1.3.6.1.6.3.16                       excluded
v1v2only             1.3.6.1.6.3.18                       excluded
```

Table 10 SNMPv3 View Table Information

Field	Description
View Name	Displays the name of the view.
Subtree	Displays the MIB subtree as an OID string. A view subtree is the set of all MIB object instances which have a common Object Identifier prefix to their names.
Mask	Displays the bit mask.
Type	Displays whether a family of `view subtrees` is included or excluded from the MIB view.

/info/sys/snmpv3/access
SNMPv3 Access Table Information

The access control sub system provides authorization services.

The vacmAccessTable maps a group name, security information, a context, and a message type, which could be the read or write type of operation or notification into a MIB view.

The View-based Access Control Model defines a set of services that an application can use for checking access rights of a group. This group's access rights are determined by a read-view, a write-view and a notify-view. The read-view represents the set of object instances authorized for the group while reading the objects. The write-view represents the set of object instances authorized for the group when writing objects. The notify-view represents the set of object instances authorized for the group when sending a notification.

```
Group Name Model   Level         ReadV      WriteV     NotifyV
---------- ------- ------------- ---------- ---------- ----------
v1v2grp    snmpv1  noAuthNoPriv iso         iso        v1v2only
admingrp   usm     authPriv     iso         iso        iso
```

Table 11 SNMPv3 Access Table Information

Field	Description
Group Name	Displays the name of group.
Model	Displays the security model used, for example, SNMPv1, or SNMPv2 or USM.
Level	Displays the minimum level of security required to gain rights of access. For example, `noAuthNoPriv`, `authNoPriv`, or `authPriv`.
ReadV	Displays the MIB view to which this entry authorizes the read access.
WriteV	Displays the MIB view to which this entry authorizes the write access.
NotifyV	Displays the Notify view to which this entry authorizes the notify access.

/info/sys/snmpv3/group
SNMPv3 Group Table Information

A group is a combination of security model and security name that defines the access rights assigned to all the security names belonging to that group. The group is identified by a group name.

```
Sec Model    User Name                       Group Name
----------   ------------------------------  --------------------
snmpv1       v1v2only                        v1v2grp
usm          adminmd5                        admingrp
usm          adminsha                        admingrp
```

Table 12 SNMPv3 Group Table Information

Field	Description
Sec Model	Displays the security model used, which is any one of: USM, SNMPv1, SNMPv2, and SNMPv3.
User Name	Displays the name for the group.
Group Name	Displays the access name of the group.

/info/sys/snmpv3/comm
SNMPv3 Community Table Information

This command displays the community table information stored in the SNMP engine.

```
Index      Name       User Name            Tag
---------- ---------- -------------------- ----------
trap1      public     v1v2only             v1v2trap
```

Table 13 SNMPv3 Community Table Information

Field	Description
Index	Displays the unique index value of a row in this table
Name	Displays the community string, which represents the configuration.
User Name	Displays the User Security Model (USM) user name.
Tag	Displays the community tag. This tag specifies a set of transport endpoints from which a command responder application accepts management requests and to which a command responder application sends an SNMP trap.

/info/sys/snmpv3/taddr
SNMPv3 Target Address Table Information

This command displays the SNMPv3 target address table information, which is stored in the SNMP engine.

```
Name        Transport Addr  Port Taglist    Params
----------- --------------- ---- ---------- ---------------
trap1       47.81.25.66     162  v1v2trap   v1v2param
```

Table 14 SNMPv3 Target Address Table Information

Field	Description
Name	Displays the locally arbitrary, but unique identifier associated with this `snmpTargetAddrEntry`.
Transport Addr	Displays the transport addresses.
Port	Displays the SNMP UDP port number.
Taglist	This column contains a list of tag values which are used to select target addresses for a particular SNMP message.
Params	The value of this object identifies an entry in the `snmpTargetParamsTable`. The identified entry contains SNMP parameters to be used when generating messages to be sent to this transport address.

/info/sys/snmpv3/tparam
SNMPv3 Target Parameters Table Information

```
Name            MP Model   User Name          Sec Model  Sec Level
--------------- --------   --------------     ---------  ---------
v1v2param       snmpv2c    v1v2only           snmpv1     noAuthNoPriv
```

Table 15 SNMPv3 Target Table Information

Field	Description
Name	Displays the locally arbitrary, but unique identifier associated with this `snmpTargeParamsEntry`.
MP Model	Displays the Message Processing Model used when generating SNMP messages using this entry.
User Name	Displays the `securityName`, which identifies the entry on whose behalf SNMP messages will be generated using this entry.
Sec Model	Displays the security model used when generating SNMP messages using this entry. The system may choose to return an `inconsistentValue` error if an attempt is made to set this variable to a value for a security model which the system does not support.
Sec Level	Displays the level of security used when generating SNMP messages using this entry.

/info/sys/snmpv3/notify
SNMPv3 Notify Table Information

```
Name                Tag
------------------- -------------------
v1v2trap            v1v2trap
```

Table 16 SNMPv3 Notify Table Information

Field	Description
Name	The locally arbitrary, but unique identifier associated with this `snmpNotifyEntry`.
Tag	This represents a single tag value which is used to select entries in the `snmpTargetAddrTable`. Any entry in the `snmpTargetAddrTable` that contains a tag value equal to the value of this entry, is selected. If this entry contains a value of zero length, no entries are selected.

/info/sys/snmpv3/dump
SNMPv3 Dump Information

```
usmUser Table:
User Name                       Protocol
------------------------------- --------------------------------
adminmd5                        HMAC_MD5, DES PRIVACY
adminsha                        HMAC_SHA, DES PRIVACY
v1v2only                        NO AUTH,  NO PRIVACY

vacmAccess Table:
Group Name Model   Level        ReadV      WriteV     NotifyV
---------- ------- ------------ ---------- ---------- ----------
v1v2grp    snmpv1  noAuthNoPriv iso        iso        v1v2only
admingrp   usm     authPriv     iso        iso        iso

vacmViewTreeFamily Table:
View Name            Subtree           Mask            Type
-------------------- ---------------  ------------    --------------
iso                  1.3                               included
v1v2only             1.3                               included
v1v2only             1.3.6.1.6.3.15                    excluded
v1v2only             1.3.6.1.6.3.16                    excluded
v1v2only             1.3.6.1.6.3.18                    excluded

vacmSecurityToGroup Table:
Sec Model  User Name                       Group Name
---------- -------------------------------  ------------------------
snmpv1     v1v2only                        v1v2grp
usm        adminmd5                        admingrp
usm        adminsha                        admingrp

snmpCommunity Table:
Index      Name       User Name            Tag
---------- ---------- -------------------- ----------

snmpNotify Table:
Name                 Tag
-------------------- --------------------

snmpTargetAddr Table:
Name       Transport Addr  Port Taglist    Params
---------- --------------- ---- ---------- ---------------

snmpTargetParams Table:
Name                 MP Model User Name           Sec Model Sec Level
-------------------- -------- ------------------  --------- -------
```

/info/sys/general
General System Information

```
System Information at 13:41:04 Fri Jan 20, 2009
Time zone: America/Barbados
Daylight Savings Time Status: Disabled

Blade Network Technologies RackSwitch G8124

Switch has been up for 0 days, 17 hours, 10 minutes and 45 seconds.
Last boot: 20:41:01 Thu Jan 19, 2000 (power cycle)

MAC address: 00:25:03:49:83:00    IP (If 1) address: 0.0.0.0
MGMT-A Port MAC Address: 00:25:03:49:83:ee
MGMT-A Port IP Address (if 127): 172.16.2.45
MGMT-B Port MAC Address: 00:25:03:49:83:ef
MGMT-B Port IP Address (if 128):
Revision: 1
Switch Serial No: CH49380010
Hardware Part No: BAC-00045-02        Spare Part No: BAC-00045-02
Manufacturing date: 09/40
Software Version 5.0.0 (FLASH image1), active configuration.

Fans are in Forward AirFlow, Warning at 85 C and Recover at 100 C

Temperature Sensor 1: 28.0 C
Temperature Sensor 2: 33.0 C
Temperature Sensor 3: 37.75 C
Temperature Sensor 4: 42.75 C
Temperature Sensor 5: 36.50 C

Speed of Fan 1:   8231 RPM
Speed of Fan 2:   8294 RPM
Speed of Fan 3:   8256 RPM
Speed of Fan 4:   8231 RPM
Speed of Fan 5:   8411 RPM
Speed of Fan 6:   8530 RPM

State of Power Supply 1:   Off
State of Power Supply 2:   On
```

Note – The display of temperature will come up only if the temperature of any of the sensors exceeds the temperature threshold. There will be a warning from the software if any of the sensors exceeds this temperature threshold. The switch will shut down if the power supply overheats.

System information includes:

- System date and time
- Switch model
- Switch name and location
- Time of last boot
- MAC address of the switch management processor
- Software image file and version number, and configuration name.
- IP address of the management interface
- Hardware version and part number
- Log-in banner, if one is configured

/info/sys/log
Show Recent Syslog Messages

```
Date     Time       Criticality level       Message
Jul   8  17:25:41    NOTICE       system: link up on port 1
Jul   8  17:25:41    NOTICE       system: link up on port 8
Jul   8  17:25:41    NOTICE       system: link up on port 7
Jul   8  17:25:41    NOTICE       system: link up on port 2
Jul   8  17:25:41    NOTICE       system: link up on port 1
Jul   8  17:25:41    NOTICE       system: link up on port 4
Jul   8  17:25:41    NOTICE       system: link up on port 3
Jul   8  17:25:41    NOTICE       system: link up on port 6
Jul   8  17:25:41    NOTICE       system: link up on port 5
Jul   8  17:25:41    NOTICE       system: link up on port 4
Jul   8  17:25:41    NOTICE       system: link up on port 1
Jul   8  17:25:41    NOTICE       system: link up on port 3
Jul   8  17:25:41    NOTICE       system: link up on port 2
Jul   8  17:25:41    NOTICE       system: link up on port 3
Jul   8  17:25:42    NOTICE       system: link up on port 2
Jul   8  17:25:42    NOTICE       system: link up on port 4
Jul   8  17:25:42    NOTICE       system: link up on port 3
Jul   8  17:25:42    NOTICE       system: link up on port 6
Jul   8  17:25:42    NOTICE       system: link up on port 5
Jul   8  17:25:42    NOTICE       system: link up on port 1
Jul   8  17:25:42    NOTICE       system: link up on port 6
```

Each syslog message has a criticality level associated with it, included in text form as a prefix to the log message. One of eight different prefixes is used, depending on the condition that the administrator is being notified of, as shown below.

- `EMERG`: indicates the system is unusable
- `ALERT`: Indicates action should be taken immediately
- `CRIT`: Indicates critical conditions
- `ERR`: indicates error conditions or errored operations
- `WARNING`: indicates warning conditions
- `NOTICE`: indicates a normal but significant condition
- `INFO`: indicates an information message
- `DEBUG`: indicates a debug-level message

/info/sys/user
User Status Information

```
Usernames:
  user      - enabled - offline
  oper      - disabled - offline
  admin     - Always Enabled - online 1 session
Current User ID table:
  1: name paul    , dis, cos user     , password valid, offline
Current strong password settings:
  strong password status: disabled
```

This command displays the status of the configured usernames.

/info/l2
Layer 2 Information Menu

```
[Layer 2 Menu]
     fdb       - Forwarding Database Information Menu
     lacp      - Link Aggregation Control Protocol Menu
     failovr   - Show Failover information
     hotlink   - Show Hot Links information
     stp       - Show STP information
     cist      - Show CIST information
     trunk     - Show Trunk Group information
     vlan      - Show VLAN information
     prvlan    - Show private-vlan information
     dump      - Dump all layer 2 information
```

The information provided by each menu option is briefly described in Table 17, with pointers to where detailed information can be found.

Table 17 Layer 2 Information Options

Command Syntax and Usage
fdb Displays the Forwarding Database (FDB) Information menu. For details, see page 63.
lacp Displays the Link Aggregation Control Protocol menu. For details, see page 65.
failovr Displays the Layer 2 Failover Information menu. For details, see page 66.
hotlink Displays the Hot Links Information menu. For details, see page 68.

Table 17 Layer 2 Information Options

Command Syntax and Usage
stp Displays Spanning Tree information, including the status (on or off), Spanning Tree mode (STP/PVST+, RSTP, PVRST, or MSTP), and VLAN membership. In addition to seeing if STG is enabled or disabled, you can view the following STG bridge information: □ Priority □ Hello interval □ Maximum age value □ Forwarding delay □ Aging time You can also see the following port-specific STG information: □ Port alias and priority □ Cost □ State □ Port Fast Forwarding state For details, see page 69.
cist Displays Common Internal Spanning Tree (CIST) information, including the MSTP digest and VLAN membership. CIST bridge information includes: □ Priority □ Hello interval □ Maximum age value □ Forwarding delay □ Root bridge information (priority, MAC address, path cost, root port) CIST port information includes: □ Port number and priority □ Cost □ State For details, see page 75.

Table 17 Layer 2 Information Options

Command Syntax and Usage
trunk When trunk groups are configured, you can view the state of each port in the various trunk groups. For details, see page 77.
vlan Displays VLAN configuration information, including: □ VLAN Number □ VLAN Name □ Status □ Port membership of the VLAN □ Private VLAN information For details, see page 78.
pvlan Displays Protocol VLAN information.
prvlan Displays Private VLAN information.
dump Dumps all switch information available from the Layer 2 menu (10K or more, depending on your configuration). If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.

/info/l2/fdb
FDB Information

```
[Forwarding Database Menu]
      find    - Show a single FDB entry by MAC address
      port    - Show FDB entries on a single port
      vlan    - Show FDB entries on a single VLAN
      state   - Show FDB entries by state
      dump    - Show all FDB entries
```

The forwarding database (FDB) contains information that maps the media access control (MAC) address of each known device to the switch port where the device address was learned. The FDB also shows which other ports have seen frames destined for a particular MAC address.

Note – The master forwarding database supports up to 16K MAC address entries on the MP per switch.

Table 18 FDB Information Options

Command Syntax and Usage
find *<MAC address>* [*<VLAN>*] Displays a single database entry by its MAC address. You are prompted to enter the MAC address of the device. Enter the MAC address using the format, `xx:xx:xx:xx:xx:xx`. For example, `08:00:20:12:34:56` You can also enter the MAC address using the format, `xxxxxxxxxxxx`. For example, `080020123456`
port *<port number or alias>* Displays all FDB entries for a particular port.
trunk *<trunk number>* Displays all FDB entries for a particular trunk.
vlan *<VLAN number>* Displays all FDB entries on a single VLAN.
state unknown|**forward**|**trunk** Displays all FDB entries of a particular state.
dump Displays all entries in the Forwarding Database. For more information, see page 64.

/info/l2/fdb/dump
Show All FDB Information

```
    MAC address       VLAN  Port  Trnk  State  Permanent
-----------------  ----  ----  ----  -----  ---------
00:04:38:90:54:18     1  4             FWD
00:09:6b:9b:01:5f     1  13            FWD
00:09:6b:ca:26:ef  4095  1             FWD
00:0f:06:ec:3b:00  4095  1             FWD
00:11:43:c4:79:83     1  4             FWD       P
```

An address that is in the forwarding (FWD) state, means that it has been learned by the switch. When in the trunking (TRK) state, the port field represents the trunk group number. If the state for the port is listed as unknown (UNK), the MAC address has not yet been learned by the switch, but has only been seen as a destination address.

When an address is in the unknown state, no outbound port is indicated, although ports which reference the address as a destination will be listed under “Reference ports.”

Clearing Entries from the Forwarding Database

To clear the entire FDB, refer to “Forwarding Database Maintenance” on page 322.

/info/l2/lacp
Link Aggregation Control Protocol Information

```
[LACP Menu]
     aggr      - Show LACP aggregator information for the port
     port      - Show LACP port information
     dump      - Show all LACP ports information
```

Use these commands to display Link Aggregation Protocol (LACP) status information about each port on the switch.

Table 19 LACP Information Options

Command Syntax and Usage
aggr *<port alias or number>* Displays detailed information about the LACP aggregator used by the selected port.
port Displays LACP information about the selected port.
dump Displays a summary of LACP information. For details, see page 66.

/info/l2/lacp/dump
Show All LACP Information

```
port   mode      adminkey  operkey  selected   prio   aggr   trunk  status
------------------------------------------------------------------------------
1      active          30       30     yes     32768    17      19     up
2      active          30       30     yes     32768    17      19     up
3      off              3        3     no      32768    --      --     --
4      off              4        4     no      32768    --      --     --
...
```

LACP dump includes the following information for each external port in the G8124:

- `mode` Displays the port's LACP mode (active, passive, or off).
- `adminkey` Displays the value of the port's *adminkey*.
- `operkey` Shows the value of the port's operational key.
- `selected` Indicates whether the port has been selected to be part of a Link Aggregation Group.
- `prio` Shows the value of the port priority.
- `aggr` Displays the aggregator associated with each port.
- `trunk` This value represents the LACP trunk group number.
- `status` Displays the status of LACP on the port (up or down).

/info/l2/failovr
Layer 2 Failover Information

```
[Failover Info Menu]
     trigger  - Show Trigger information
```

Table 20 describes the Layer 2 Failover information options.

Table 20 Layer 2 Failover Information Options

Command Syntax and Usage
trigger *<trigger number>* Displays detailed information about the selected Layer 2 Failover trigger.

/info/l2/failovr/trigger <trigger number>
Show Layer 2 Failover Information

```
Trigger 1 Auto Monitor: Enabled
Trigger 1 limit: 0
Monitor State: Up
Member      Status
---------   -----------
trunk 1
 2          Operational
 3          Operational

Control State: Auto Disabled
Member      Status
---------   -----------
 1          Operational
 2          Operational
 3          Operational
 4          Operational
...
```

A monitor port's Failover status is `Operational` only if all the following conditions hold true:

- Port link is up.
- If Spanning-Tree is enabled, the port is in the `Forwarding` state.
- If the port is a member of an LACP trunk group, the port is aggregated.

If any of the above conditions are not true, the monitor port is considered to be failed.

A control port is considered to be operational if the monitor trigger state is `Up`. Even if a port's link status is `Down`, Spanning-Tree status is `Blocking`, and the LACP status is `Not Aggregated`, from a teaming perspective the port status is `Operational`, since the trigger is `Up`.

A control port's status is displayed as `Failed` only if the monitor trigger state is `Down`.

/info/l2/hotlink
Hot Links Information

```
[Hot Links Info Menu]
     trigger  - Show Trigger information
```

Table 21 Hot Links Information Options

Command Syntax and Usage
trigger Displays status and configuration information for each Hot Links trigger. To view a sample display, see page 68.

/info/l2/hotlink/trigger
Hotlinks Trigger Information

```
Hot Links Info: Trigger

Current global Hot Links setting: ON
bpdu disabled
sndfdb disabled

Current Trigger 1 setting: enabled
name "Trigger 1", preempt enabled, fdelay 1 sec

Active state: None

Master settings:
port 1
Backup settings:
port 2
```

Hot Links trigger information includes the following:

- Hot Links status (on or off)
- Status of BPDU flood option
- Status of FDB send option
- Status and configuration of each Hot Links trigger

/info/l2/stp
Spanning Tree Information

```
------------------------------------------------------------------
upfast disabled, update 40
Pvst+ compatibility mode enabled
------------------------------------------------------------------
Spanning Tree Group 1: On (PVRST)
VLANs:  1

Current Root:            Path-Cost  Port Hello MaxAge FwdDel
 8000 00:22:00:ee:cc:00     2000       1    2     20     15

Parameters:  Priority  Hello  MaxAge  FwdDel  Aging
              32769      2      20      15     300

Port  Prio  Cost     State  Role Designated Bridge      Des Port Type
----- ---- --------- -----  ---- ---------------------- -------- ----
1      128     2000!  FWD    ROOT 8000-00:22:00:ee:cc:00     8001  P2P
2      128     2000!  DISC   ALTN 8000-00:22:00:ee:cc:00     8002  P2P
3      128     2000!  DISC   ALTN 8000-00:22:00:ee:cc:00     8003  P2P
10     128     2000!  DISC   DESG 8001-00:22:00:7d:5f:00     800a  P2P
11     128     2000!  DISC   DESG 8001-00:22:00:7d:5f:00     800b  P2P
! = Automatic path cost.

------------------------------------------------------------------
Spanning Tree Group 128: Off (PVRST), FDB aging timer 300
VLANs:  4095

Port  Prio  Cost     State  Role Designated Bridge      Des Port Type
----- ---- --------- -----  ---- ---------------------- -------- ----
MGTA     0        0   FWD *

* = STP turned off for this port.
```

The switch software uses the IEEE 802.1D Spanning Tree Protocol (STP). If IEEE 802.1w Rapid Spanning Tree Protocol (RSTP), the IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), or Per VLAN Rapid Spanning Tree Protocol (PVRST) are turned on, see "RSTP/MSTP Information" on page 72.

When STP is used, in addition to seeing if STG is enabled or disabled, you can view the following STG bridge information:

Table 22 Spanning Tree Parameter Descriptions

Parameter	Description
Current Root	The Current Root shows information about the root bridge for the Spanning Tree. Information includes the priority (in hexadecimal notation) and MAC address of the root.
Priority (bridge)	The bridge priority parameter controls which bridge on the network will become the STG root bridge.
Hello	The hello time parameter specifies, in seconds, how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value.
MaxAge	The maximum age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigure the STG network.
FwdDel	The Forward Delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from listening to learning and from learning state to forwarding state.
Aging	The aging time parameter specifies, in seconds, the amount of time the bridge waits without receiving a packet from a station before removing the station from the Forwarding Database.
Priority (port)	The port priority parameter helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.
Cost	The port path cost parameter is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. A setting of 0 indicates that the cost will be set to the appropriate default after the link speed has been auto negotiated.
FastFwd	The FastFwd shows whether the port is in Fast Forwarding mode or not, which permits the port that participates in Spanning Tree to bypass the Listening and Learning states and enter directly into the Forwarding state.
State	The state field shows the current state of the port. The state field can be either `BLOCKING`, `LISTENING`, `LEARNING`, `FORWARDING`, or `DISABLED`.

Table 22 Spanning Tree Parameter Descriptions (continued)

Parameter	Description
Designated Bridge	The Designated Bridge shows information about the bridge connected to each port, if applicable. Information includes the priority (in hexadecimal notation) and MAC address of the Designated Bridge.
Designated Port	The identifier of the port on the Designated Bridge to which this port is connected.

/info/l2/stp
RSTP/MSTP Information

```
------------------------------------------------------------------
upfast disabled, update 40
Pvst+ compatibility mode enabled
------------------------------------------------------------------
Spanning Tree Group 1: On (RSTP)
VLANs:  1

Current Root:            Path-Cost  Port Hello MaxAge FwdDel
 0000 00:16:60:ba:6c:01     2026       1    2     20     15

Parameters:  Priority  Hello  MaxAge  FwdDel  Aging
              32768      2      20      15     300

Port  Prio  Cost     State  Role Designated Bridge      Des Port Type
----- ---- --------- -----  ---- ---------------------- -------- ----
1      128     2000!  FWD    ROOT fffe-00:13:0a:4f:7d:d0     8013  P2P
23     128     2000!  FWD    DESG 8000-00:13:0a:4f:7e:10     8017  P2P
24     128     2000!  FWD    DESG 8000-00:13:0a:4f:7e:10     8018  P2P

------------------------------------------------------------------
Spanning Tree Group 128: Off (RSTP), FDB aging timer 300
VLANs:  4095

Port  Prio  Cost     State  Role Designated Bridge      Des Port Type
----- ---- --------- -----  ---- ---------------------- -------- ----
MGTA     0        0   FWD *

* = STP turned off for this port.
! = Automatic path cost.
```

The switch software can be set to use the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) or the IEEE 802.1s Multiple Spanning Tree Protocol (MSTP). If RSTP/MSTP is turned on (see page 222), you can view RSTP/MSTP bridge information for the Spanning Tree Group and port-specific RSTP information.

The following table describes the STP parameters in RSTP or MSTP mode.

Table 23 RSTP/MSTP Parameter Descriptions

Parameter	Description
Current Root	The Current Root shows information about the root bridge for the Spanning Tree. Information includes the priority (in hexadecimal notation) and MAC address of the root.
Priority (bridge)	The bridge priority parameter controls which bridge on the network will become the STP root bridge.
Hello	The hello time parameter specifies, in seconds, how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value.
MaxAge	The maximum age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the STP network.
FwdDel	The Forward Delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from listening to learning and from learning state to forwarding state.
Aging	The aging time parameter specifies, in seconds, the amount of time the bridge waits without receiving a packet from a station before removing the station from the Forwarding Database.
Prio (port)	The port priority parameter helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.
Cost	The port path cost parameter is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. A setting of 0 indicates that the cost will be set to the appropriate default after the link speed has been auto negotiated.
State	The State field shows the current state of the port. The State field in RSTP or MSTP mode can be one of the following: Discarding (`DISC`), Learning (`LRN`), Forwarding (`FWD`), or Disabled (`DSB`).
Role	The Role field shows the current role of this port in the Spanning Tree. The port role can be one of the following: Designated (`DESG`), Root (`ROOT`), Alternate (`ALTN`), Backup (`BKUP`), Disabled (`DSB`), Master (`MAST`).

Table 23 RSTP/MSTP Parameter Descriptions (continued)

Parameter	Description
Designated Bridge	The Designated Bridge shows information about the bridge connected to each port, if applicable. Information includes the priority (in hexadecimal notation) and MAC address of the Designated Bridge.
Designated Port	The port ID of the port on the Designated Bridge to which this port is connected.
Type	Type of link connected to the port, and whether the port is an edge port. Link type values are `AUTO`, `P2P`, or `SHARED`.

/info/l2/cist
Common Internal Spanning Tree Information

```
Mstp Digest: 0xac36177f50283cd4b83821d8ab26de62

Common Internal Spanning Tree:

VLANs MAPPED:  1-4094
VLANs:  1 2 4095

Current Root:             Path-Cost  Port MaxAge FwdDel
 8000 00:11:58:ae:39:00      2026     0     20     15

Cist Regional Root:       Path-Cost
 8000 00:11:58:ae:39:00        0

Parameters:  Priority  MaxAge  FwdDel  Hops
              32768      20      15    20

Port  Prio  Cost     State  Role Designated Bridge      Des Port Hello Type
----- ---- --------- -----  ---- ---------------------- -------- ----- ----
1     128     2000!  FWD  ROOT fffe-00:13:0a:4f:7d:d0    8011   2    P2P#
23    128     2000!  DISC ALTN fffe-00:22:00:24:46:00    8012   2    P2P#
MGTA    0        0   FWD *

* = STP turned off for this port.
! = Automatic path cost.
# = PVST Protection enabled for this port.
```

In addition to seeing if Common Internal Spanning Tree (CIST) is enabled or disabled, you can view CIST bridge and port-specific information. The following table describes the CIST parameters.

Table 24 CIST Parameter Descriptions

Parameter	Description
CIST Root	The CIST Root shows information about the root bridge for the Common Internal Spanning Tree (CIST). Values on this row of information refer to the CIST root.
CIST Regional Root	The CIST Regional Root shows information about the root bridge for this MSTP region. Values on this row of information refer to the regional root.
Priority (bridge)	The bridge priority parameter controls which bridge on the network will become the STP root bridge.

Table 24 CIST Parameter Descriptions

Parameter	Description
Hello	The hello time parameter specifies, in seconds, how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value.
MaxAge	The maximum age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigure the STP network.
FwdDel	The forward delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from learning state to forwarding state.
Priority (port)	The port priority parameter helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.
Cost	The port path cost parameter is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. A setting of 0 indicates that the cost will be set to the appropriate default after the link speed has been auto negotiated.
State	The state field shows the current state of the port. The state field can be either Discarding (`DISC`), Learning (`LRN`), or Forwarding (`FWD`).
Role	The Role field shows the current role of this port in the Spanning Tree. The port role can be one of the following: Designated (`DESG`), Root (`ROOT`), Alternate (`ALTN`), Backup (`BKUP`), Disabled (`DSB`), Master (`MAST`), or Unknown (`UNK`).
Designated Bridge	The Designated Bridge shows information about the bridge connected to each port, if applicable. Information includes the priority (in hexadecimal notation) and MAC address of the Designated Bridge.
Designated Port	The port ID of the port on the Designated Bridge to which this port is connected.
Type	Type of link connected to the port, and whether the port is an edge port. Link type values are `AUTO`, `P2P`, or `SHARED`.

/info/l2/trunk
Trunk Group Information

```
Trunk group 1: Enabled
Protocol - Static
Port state:
  1: STG  1 forwarding
  2: STG  1 forwarding
```

When trunk groups are configured, you can view the state of each port in the various trunk groups.

Note – If Spanning Tree Protocol on any port in the trunk group is set to `forwarding`, the remaining ports in the trunk group will also be set to `forwarding`.

/info/l2/vlan
VLAN Information

```
VLAN                Name                 Status            Ports
----  -------------------------------  ------  -----------------------
1     Default VLAN                     ena     1-20
2     VLAN 2                           dis     21-22

4095  Mgmt VLAN                        ena     MGTA MGTB

Private-VLAN    Type       Mapped-To           Status       Ports
------------  ---------  ------------------  ---------- ---------------
100           primary    200 300             ena         2 3 10
200           community  100                 ena         12
300           isolated   100                 ena         14
```

This information display includes all configured VLANs and all member ports that have an active link state. Port membership is represented in slot/port format.

VLAN information includes:

- VLAN Number
- VLAN Name
- Status
- Port membership of the VLAN
- Private VLAN information (if available)

/info/l2/prvlan
Private VLAN Information

```
Private-VLAN  Type       Mapped-To  Status     Ports
------------ --------- ---------- ---------- -----------------
100          primary    110 120     ena         1
110          community  100         ena         2
120          isolated   100         ena         3
```

Private VLAN information includes:

- Private-VLAN Number
- PrivateVLAN Type
- Private VLAN mapping
- Private VLANs Status
- Port membership of the Private-VLAN

/info/l3

Layer 3 Information Menu

```
[Layer 3 Menu]
     route     - IP Routing Information Menu
     arp       - ARP Information Menu
     ospf      - OSPF Routing Information Menu
     rip       - RIP Routing Information Menu
     ecmp      - Show ECMP static routes information
     ip        - Show IP information
     igmp      - Show IGMP Snooping Multicast Group information
     vrrp      - Show Virtual Router Redundancy Protocol information
     dump      - Dump all layer 3 information
```

The information provided by each menu option is briefly described in Table 25, with pointers to detailed information.

Table 25 Layer 3 Information Options

Command Syntax and Usage
route Displays the IP Routing menu. Using the options of this menu, the system displays the following for each configured or learned route: □ Route destination IP address, subnet mask, and gateway address □ Type of route □ Tag indicating origin of route □ Metric for RIP tagged routes, specifying the number of hops to the destination (1-15 hops, or 16 for infinite hops) □ The IP interface that the route uses For details, see page 82.
arp Displays the Address Resolution Protocol (ARP) Information menu. For details, see page 85.
ospf Displays OSPF routing Information menu. For details, see page 87.
rip Displays Routing Information Protocol menu. For details, see page 92.

Table 25 Layer 3 Information Options

Command Syntax and Usage
ecmp Displays ECMP route information. For details, see page 93.
ip Displays IP Information. For details, see page 94. IP information, includes: □ IP interface information: Interface number, IP address, subnet mask, VLAN number, and operational status. □ Default gateway information: Metric for selecting which configured gateway to use, gateway number, IP address, and health status □ IP forwarding settings, network filter settings, route map settings
igmp Displays IGMP Information menu. For details, see page 95.
vrrp Displays VRRP Information. For details, see page 99.
dump Dumps all switch information available from the Layer 3 Information menu (10K or more, depending on your configuration). If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.

/info/l3/route
IP Routing Information

```
[IP Routing Menu]
      find    - Show a single route by destination IP address
      gw      - Show routes to a single gateway
      type    - Show routes of a single type
      tag     - Show routes of a single tag
      if      - Show routes on a single interface
      dump    - Show all routes
```

Using the commands listed below, you can display all or a portion of the IP routes currently held in the switch.

Table 26 Route Information Options

Command Syntax and Usage
find *<IP address (such as 192.4.17.101)>* Displays a single route by destination IP address.
gw *<default gateway address (such as 192.4.17.44)>* Displays routes to a single gateway.
type indirect|direct|local|broadcast|martian|multicast Displays routes of a single type. For a description of IP routing types, see Table 27 on page 83.
tag fixed|static|addr|rip|ospf|broadcast|martian|multicast Displays routes of a single tag. For a description of IP routing types, see Table 28 on page 84.
if *<interface number>* Displays routes on a single interface.
dump Displays all routes configured in the switch. For more information, see page 83.

/info/l3/route/dump
Show All IP Route Information

```
Status code: * - best
    Destination          Mask           Gateway        Type       Tag     Metr If
  ---------------  --------------- --------------- --------- --------- ---- --
* 0.0.0.0          0.0.0.0         172.31.1.1      indirect  static           1
* 12.0.0.0         255.0.0.0       0.0.0.0         martian   martian
* 12.31.0.0        255.255.0.0     172.31.36.139   direct    fixed            1
* 12.31.36.139     255.255.255.255 172.31.36.139   local     addr             1
* 12.31.255.255    255.255.255.255 172.31.255.255  broadcast broadcast        1
* 224.0.0.0        224.0.0.0       0.0.0.0         martian   martian
* 224.0.0.0        240.0.0.0       0.0.0.0         multicast addr
* 255.255.255.255 255.255.255.255 255.255.255.255 broadcast broadcast
```

The following table describes the `Type` parameters.

Table 27 IP Routing Type Parameters

Parameter	Description
indirect	The next hop to the host or subnet destination will be forwarded through a router at the `Gateway` address.
direct	Packets will be delivered to a destination host or subnet attached to the switch.
local	Indicates a route to one of the switch's IP interfaces.
broadcast	Indicates a broadcast route.
martian	The destination belongs to a host or subnet which is filtered out. Packets to this destination are discarded.
multicast	Indicates a multicast route.

The following table describes the `Tag` parameters.

Table 28 IP Routing Tag Parameters

Parameter	Description
fixed	The address belongs to a host or subnet attached to the switch.
static	The address is a static route which has been configured on the G8124.
addr	The address belongs to one of the switch's IP interfaces.
rip	The address was learned by the Routing Information Protocol (RIP).
ospf	The address was learned by Open Shortest Path First (OSPF).
broadcast	Indicates a broadcast address.
martian	The address belongs to a filtered group.
multicast	Indicates a multicast address.

/info/l3/arp
ARP Information

```
[Address Resolution Protocol Menu]
      find    - Show a single ARP entry by IP address
      port    - Show ARP entries on a single port
      vlan    - Show ARP entries on a single VLAN
      addr    - Show ARP address list
      dump    - Show all ARP entries
```

The ARP information includes IP address and MAC address of each entry, address status flags (see Table 29 on page 85), VLAN and port for the address, and port referencing information.

Table 29 ARP Information Options

Command Syntax and Usage
find *<IP address (such as, 192.4.17.101>* Displays a single ARP entry by IP address.
port *<port alias or number>* Displays the ARP entries on a single port.
vlan *<VLAN number>* Displays the ARP entries on a single VLAN.
addr Displays the ARP address list: IP address, IP mask, MAC address, and VLAN flags.
dump Displays all ARP entries. including: □ IP address and MAC address of each entry □ Address status flag (see below) □ The VLAN and port to which the address belongs □ The ports which have referenced the address (empty if no port has routed traffic to the IP address shown) For more information, see page 86.

/info/l3/arp/addr
ARP Address List Information

```
Current ARP configuration:
 rearp 5

Current static ARP:
ip               mac                 interface
--------------   -----------------   ---------

IP Address       Flags     Hardware Address    Interface
--------------   ------    -----------------   ---------
127.20.1.1                 00:15:40:07:20:42    1
127.20.254.21    P         00:22:00:4d:b9:00    1
```

The `Port` field shows the target port of the ARP entry.

The `Flag` field is interpreted as follows:

Table 30 ARP Flag Parameters

Flag	Description
P	Permanent entry created for switch IP interface.
R	Indirect route entry.
U	Unresolved ARP entry. The MAC address has not been learned.

/info/l3/arp/dump
Show All ARP Entry Information

```
    IP address     Flags    MAC address     VLAN  Age Port
  ---------------- ----- ----------------- ----  --- ----
  10.100.130.1           00:0e:40:99:cc:5d    1  276 19
  10.100.130.12    P     00:22:00:d5:a8:00    1
```

/info/l3/ospf
OSPF Information

```
[OSPF Information Menu]
      general - Show general information
      aindex  - Show area(s) information
      if      - Show interface(s) information
      virtual - Show details of virtual links
      nbr     - Show neighbor(s) information
      dbase   - Database Menu
      sumaddr - Show summary address list
      nsumadd - Show NSSA summary address list
      routes  - Show OSPF routes
      dump    - Show OSPF information
```

Table 31 OSPF Information Options

Command Syntax and Usage
general Displays general OSPF information. See page 89 for a sample output.
aindex *<area index (0-2)>* Displays area information for a particular area index. If no parameter is supplied, it displays area information for all the areas.
if *<interface number>* Displays interface information for a particular interface. If no parameter is supplied, it displays information for all the interfaces. See page 89 for a sample output.
virtual Displays information about all the configured virtual links.
nbr *<nbr router-id (A.B.C.D)>* Displays the status of a neighbor with a particular router ID. If no router ID is supplied, it displays the information about all the current neighbors.
dbase Displays the OSPF database menu. To view menu options, see page 90.
sumaddr *<area index (0-2)>* Displays the list of summary ranges belonging to non-NSSA areas.

Table 31 OSPF Information Options

Command Syntax and Usage
nsumadd *<area index (0-2)>* Displays the list of summary ranges belonging to NSSA areas.
routes Displays OSPF routing table. See page 92 for a sample output.
dump Displays the OSPF information.

/info/l3/ospf/general
OSPF General Information

```
OSPF Version 2
Router ID: 10.10.10.1
Started at 1663 and the process uptime is 4626
Area Border Router: yes, AS Boundary Router: no
LS types supported are 6
External LSA count 0
External LSA checksum sum 0x0
Number of interfaces in this router is 2
Number of virtual links in this router is 1
16 new lsa received and 34 lsa originated from this router
Total number of entries in the LSDB 10
Database checksum sum 0x0
Total neighbors are 1, of which
                                  2 are >=INIT state,
                                  2 are >=EXCH state,
                                  2 are =FULL state
Number of areas is 2, of which 3-transit 0-nssa
        Area Id : 0.0.0.0
        Authentication : none
        Import ASExtern : yes
        Number of times SPF ran : 8
        Area Border Router count : 2
        AS Boundary Router count : 0
        LSA count : 5
        LSA Checksum sum : 0x2237B
        Summary : noSummary
```

/info/l3/ospf/if *<interface number>*
OSPF Interface Information

```
Ip Address 10.10.12.1, Area 0.0.0.1, Admin Status UP
   Router ID 10.10.10.1, State DR, Priority 1
   Designated Router (ID) 10.10.10.1, Ip Address 10.10.12.1
   Backup Designated Router (ID) 10.10.14.1, Ip Address 10.10.12.2
   Timer intervals, Hello 10, Dead 40, Wait 1663, Retransmit 5,
                Poll interval 0, Transit delay 1
   Neighbor count is 1   If Events 4, Authentication type none
```

/info/l3/ospf/dbase
OSPF Database Information

```
[OSPF Database Menu]
      advrtr  - LS Database info for an Advertising Router
      asbrsum - ASBR Summary LS Database info
      dbsumm  - LS Database summary
      ext     - External LS Database info
      nw      - Network LS Database info
      nssa    - NSSA External LS Database info
      rtr     - Router LS Database info
      self    - Self Originated LS Database info
      summ    - Network-Summary LS Database info
      all     - All
```

Table 32 OSPF Database Information Options

Command Syntax and Usage

advrtr *<router-id (A.B.C.D)>*

Takes advertising router as a parameter. Displays all the Link State Advertisements (LSAs) in the LS database that have the advertising router with the specified router ID, for example: 20.1.1.1.

asbrsum *<adv-rtr (A.B.C.D)>* | *<link_state_id (A.B.C.D>* | *<self>*

Displays ASBR summary LSAs. The usage of this command is as follows:

- `asbrsum adv-rtr 20.1.1.1`
  Displays ASBR summary LSAs having the advertising router 20.1.1.1.
- `asbrsum link-state-id 10.1.1.1`
  Displays ASBR summary LSAs having the link state ID 10.1.1.1.
- `asbrsum self`
  Displays the self advertised ASBR summary LSAs.
- `asbrsum` with no parameters displays all the ASBR summary LSAs.

dbsumm

Displays the following information about the LS database in a table format:

- Number of LSAs of each type in each area.
- Total number of LSAs for each area.
- Total number of LSAs for each LSA type for all areas combined.
- Total number of LSAs for all LSA types for all areas combined.

No parameters are required.

Table 32 OSPF Database Information Options

Command Syntax and Usage
ext *<adv-rtr (A.B.C.D)> | <link_state_id (A.B.C.D> | <self>* Displays the AS-external (type 5) LSAs with detailed information of each field of the LSAs. The usage of this command is the same as the usage of the command `asbrsum`.
nw *<adv-rtr (A.B.C.D)> | <link_state_id (A.B.C.D> | <self>* Displays the network (type 2) LSAs with detailed information of each field of the LSA.network LS database. The usage of this command is the same as the usage of the command `asbrsum`.
nssa *<adv-rtr (A.B.C.D)> | <link_state_id (A.B.C.D> | <self>* Displays the NSSA (type 7) LSAs with detailed information of each field of the LSAs. The usage of this command is the same as the usage of the command `asbrsum`.
rtr *<adv-rtr (A.B.C.D)> | <link_state_id (A.B.C.D> | <self>* Displays the router (type 1) LSAs with detailed information of each field of the LSAs. The usage of this command is the same as the usage of the command `asbrsum`.
self Displays all the self-advertised LSAs. No parameters are required.
summ *<adv-rtr (A.B.C.D)> | <link_state_id (A.B.C.D> | <self>* Displays the network summary (type 3) LSAs with detailed information of each field of the LSAs. The usage of this command is the same as the usage of the command `asbrsum`.
all Displays all the LSAs.

/info/l3/ospf/routes
OSPF Route Codes Information

```
Codes: IA - OSPF inter area,
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
 IA 10.10.0.0/16 via 200.1.1.2
 IA 40.1.1.0/28 via 20.1.1.2
 IA 80.1.1.0/24 via 200.1.1.2
 IA 100.1.1.0/24 via 20.1.1.2
 IA 140.1.1.0/27 via 20.1.1.2
 IA 150.1.1.0/28 via 200.1.1.2
 E2 172.18.1.1/32 via 30.1.1.2
 E2 172.18.1.2/32 via 30.1.1.2
 E2 172.18.1.3/32 via 30.1.1.2
 E2 172.18.1.4/32 via 30.1.1.2
 E2 172.18.1.5/32 via 30.1.1.2
 E2 172.18.1.6/32 via 30.1.1.2
 E2 172.18.1.7/32 via 30.1.1.2
 E2 172.18.1.8/32 via 30.1.1.2
```

/info/l3/rip
Routing Information Protocol Information

```
[RIP Information Menu]
     routes    - Show RIP routes
     dump      - Show RIP user's configuration
```

Use this menu to view information about the Routing Information Protocol (RIP) configuration and statistics.

Table 33 RIP Information Options

Command Syntax and Usage
routes Displays RIP routes. For more information, see page 93.
dump *<interface number or zero for all IFs)>* Displays RIP user's configuration. For more information, see page 93.

/info/l3/rip/routes
RIP Routes Information

```
>> IP Routing# /info/l3/rip/routes

30.1.1.0/24 directly connected
3.0.0.0/8 via 30.1.1.11 metric 4
4.0.0.0/16 via 30.1.1.11 metric 16
10.0.0.0/8 via 30.1.1.2 metric 3
20.0.0.0/8 via 30.1.1.2 metric 2
```

This table contains all dynamic routes learnt through RIP, including the routes that are undergoing garbage collection with metric = 16. This table does not contain locally configured static routes.

/info/l3/rip/dump *<interface number>*
RIP Interface Information

```
RIP USER CONFIGURATION :
        RIP on update 30
        RIP Interface 1 : 10.4.4.2,         enabled
        version 2, listen enabled, supply enabled, default none
        poison disabled, split horizon enabled, trigg enabled,
        mcast enabled, metric 1
        auth none,key none
```

/info/l3/ecmp
ECMP Static Route Information

```
Current ecmp static routes:
Destination     Mask            Gateway         If    GW Status
--------------- --------------- --------------- ----- -----------
10.10.1.1       255.255.255.255 100.10.1.1        1    up
                                200.20.2.2        1    down

10.20.2.2       255.255.255.255 10.233.3.3        1    up
10.20.2.2       255.255.255.255 10.234.4.4        1    up
10.20.2.2       255.255.255.255 10.235.5.5        1    up

ECMP health-check ping interval: 1
ECMP health-check retries number: 3
```

ECMP route information shows the status of each ECMP route configured on the switch.

/info/l3/ip
IP Information

```
IP information:
Interface information:
1: 127.16.2.45     255.255.0.0     127.16.255.255,  vlan 4095, up

Default gateway information: metric strict
  1: 127.16.1.1,      FAILED

Current BOOTP relay settings: OFF
Current primary BOOTP server: 0.0.0.0
Current secondary BOOTP server: 0.0.0.0

Current IP forwarding settings: ON, dirbr disabled

Current network filter settings:
  none

Current route map settings:
```

IP information includes:

- IP interface information: Interface number, IP address, subnet mask, broadcast address, VLAN number, and operational status.
- Default gateway information: Metric for selecting which configured gateway to use, gateway number, IP address, and health status
- BootP relay settings
- IP forwarding settings, including the forwarding status of directed broadcasts, and the status of ICMP re-directs
- Network filter settings
- Route map settings

/info/l3/igmp
IGMP Multicast Group Information

```
[IGMP Multicast Menu]
     querier  - Show IGMP Querier information
     mrouter  - Show IGMP Snooping Multicast Router Port information
     find     - Show a single group by IP group address
     vlan     - Show groups on a single vlan
     port     - Show groups on a single port
     trunk    - Show groups on a single trunk
     detail   - Show detail of a single group by IP group address
     dump     - Show all groups
```

Table 34 describes the commands used to display information about IGMP groups learned by the switch.

Table 34 IGMP Multicast Group Information Options

Command Syntax and Usage
querier Displays IGMP Querier information. For details, see page 96.
mrouter Displays IGMP Multicast Router menu. To view menu options, see page 97.
find *<IP address>* Displays a single IGMP multicast group by its IP address.
vlan *<VLAN number>* Displays all IGMP multicast groups on a single VLAN.
port *<port number or alias>* Displays all IGMP multicast groups on a single port.
trunk *<trunk number>* Displays all IGMP multicast groups on a single trunk group.
detail *<IP address>* Displays details about IGMP multicast groups, including source and timer information.
dump Displays information for all multicast groups. For details, see page 97

/info/l3/igmp/querier <VLAN number>
IGMP Querier Information

```
Current IGMP Querier information:
 IGMP Querier information for vlan 1:
 Other IGMP querier - none
 Switch-querier enabled, current state: Querier
 Switch-querier type: Ipv4, address 0.0.0.0,
 Switch-querier general query interval: 125 secs,
 Switch-querier max-response interval: 100 'tenths of secs',
 Switch-querier startup interval: 31 secs, count: 2
 Switch-querier robustness: 2
 IGMP configured version is v3
 IGMP Operating version is v3
```

IGMP Querier information includes:

- VLAN number
- Querier status
  - Other IGMP querier—none
  - IGMP querier present, address: (IP or MAC address)
    Other IGMP querier present, interval (minutes:seconds)
- Querier election type (IPv4 or MAC) and address
- Query interval
- Querier startup interval
- Maximum query response interval
- Querier robustness value
- IGMP version number

/info/l3/igmp/mrouter
IGMP Multicast Router Port Information

```
[IGMP Multicast Router Menu]
     vlan     - Show all multicast router ports on a single vlan
     dump     - Show all learned multicast router ports
```

Table 35 describes the commands used to display information about multicast routers (Mrouters) learned through IGMP Snooping.

Table 35 IGMP Mrouter Information Options

Command Syntax and Usage
vlan *<VLAN number>* Displays the multicast router ports configured or learned on the selected VLAN.
dump Displays information for all multicast groups learned by the switch.

/info/l3/igmp/mrouter/dump
IGMP Multicast Router Dump Information

```
SrcIP                VLAN    Port       Version   Expires   MRT       QRV   QQIC

-------------------- ------- -------    --------- --------  -------   ----  ----
10.1.1.1              2       21         V3        4:09      128       2     125
10.1.1.5              2       23         V2        4:09      125       -       -
10.10.10.43           9       24         V2       static     unknown   -       -
```

IGMP Mrouter information includes:

- Source IP address
- VLAN and port where the Mrouter is connected
- IGMP version
- Mrouter expiration
- Maximum query response time
- Querier's Robustness Variable (QRV)
- Querier's Query Interval Code (QQIC)

/info/l3/igmp/dump
IGMP Group Information

```
Note: Local groups (224.0.0.x) are not snooped/relayed and will not appear.
     Source          Group        VLAN    Port    Version   Mode  Expires  Fwd
 -------------- --------------- ------- ------ --------  ----- -------  ---
 10.1.1.1       232.1.1.1         2       4       V3       INC    4:16    Yes
 10.1.1.5       232.1.1.1         2       4       V3       INC    4:16    Yes
    *           232.1.1.1         2       4       V3       INC     -      No
 10.10.10.43    235.0.0.1         9       1       V3       INC    2:26    Yes
    *           236.0.0.1         9       1       V3       EXC     -      Yes
```

IGMP Group information includes:

- IGMP source address
- IGMP Group address
- VLAN and port
- IGMP version
- IGMPv3 filter mode
- Expiration timer value
- IGMP multicast forwarding state

/info/l3/vrrp
VRRP Information

Virtual Router Redundancy Protocol (VRRP) support on the G8124 provides redundancy between routers in a LAN. This is accomplished by configuring the same virtual router IP address and ID number on each participating VRRP-capable routing device. One of the virtual routers is then elected as the master, based on a number of priority criteria, and assumes control of the shared virtual router IP address. If the master fails, one of the backup virtual routers will assume routing authority and take control of the virtual router IP address.

```
VRRP information:
  1: vrid 2, 205.178.18.210, if  1, renter, prio 100, master
  2: vrid 1, 205.178.18.202, if  1, renter, prio 100, backup
  3: vrid 3, 205.178.18.204, if  1, renter, prio 100, master
```

When virtual routers are configured, you can view the status of each virtual router using this command. VRRP information includes:

- Virtual router number
- Virtual router ID and IP address
- Interface number
- Ownership status
  - `owner` identifies the preferred master virtual router. A virtual router is the owner when the IP address of the virtual router and its IP interface are the same.
  - `renter` identifies virtual routers which are not owned by this device.
- Priority value. During the election process, the virtual router with the highest priority becomes master.
- Activity status
  - `master` identifies the elected master virtual router.
  - `backup` identifies that the virtual router is in backup mode.
  - `init` identifies that the virtual router is waiting for a startup event.
    For example, once it receives a startup event, it transitions to master if its priority is 255, (the IP address owner), or transitions to backup if it is not the IP address owner.

/info/qos
Quality of Service Information Menu

```
[QoS Menu]
     8021p    - Show QOS 802.1p information
```

Table 36 QoS Information Options

Command Syntax and Usage
8021p Displays 802.1p information. For details, see page 100.

/info/qos/8021p
802.1p Information

```
Current priority to COS queue information:
Priority  COSq  Weight
--------  ----  ------
    0       0       1
    1       1       2
    2       2       3
    3       3       4
    4       4       5
    5       5       7
    6       6      15
    7       7       0

Current port priority information:
Port   Priority  COSq  Weight
-----  --------  ----  ------
1           0       0       1
2           0       0       1
3           0       0       1
4           0       0       1
5           0       0       1
6           0       0       1
7           0       0       1
8           0       0       1
9           0       0       1
10          0       0       1
...
```

The following table describes the IEEE 802.1p priority to COS queue information.

Table 37 802.1p Priority-to-COS Queue Parameter Descriptions

Parameter	Description
Priority	Displays the 802.1p priority level.
COSq	Displays the Class of Service queue.
Weight	Displays the scheduling weight of the COS queue.

The following table describes the IEEE 802.1p port priority information.

Table 38 802.1p Port Priority Parameter Descriptions

Parameter	Description
Port	Displays the port alias.
Priority	Displays the 802.1p priority level.
COSq	Displays the Class of Service queue.
Weight	Displays the scheduling weight.

/info/acl
Access Control List Information Menu

```
[ACL Information Menu]
     acl-list - Show ACL list
```

Table 39 ACL Information Options

Command Syntax and Usage
acl-list *<ACL number>* Displays ACL list information. For details, see page 102.

/info/acl/acl-list
Access Control List Information

```
Current ACL List information:
-------------------------
Filter 1 profile:
   Ethernet
     - SMAC       : 00:00:aa:aa:01:fe/ff:ff:ff:ff:ff:ff
     - DMAC       : 00:0d:60:9c:ec:d5/ff:ff:ff:ff:ff:ff
     - VID        : 10/0xfff
     - Ethertype  : IP (0x0800)
     - Priority   : 3
   Meter
     - Set to disabled
     - Set committed rate : 64
     - Set max burst size : 32
   Re-Mark
     - Set use of TOS precedence to disabled
   Packet Format
     - Ethernet format : None
     - Tagging format  : Any
     - IP format       : None
   Actions        : Deny
   Statistics   : enabled

Mirror Target Configuration:
        Mirror target destination: port
        Egress port for mirror target: 4
```

Access Control List (ACL) information includes configuration settings for each ACL.

Table 40 ACL List Parameter Descriptions

Parameter	Description
Filter x profile	Indicates the ACL number.
Ethernet	Displays the ACL Ethernet header parameters, if configured.
IPv4	Displays the ACL IPv4 header parameters, if configured.
TCP/UDP	Displays the ACL TCP/UDP header parameters, if configured.
Meter	Displays the ACL meter parameters.
Re-Mark	Displays the ACL re-mark parameters.
Packet Format	Displays the ACL Packet Format parameters, if configured.
Actions	Displays the configured action for the ACL.
Stastistics	Displays status of ACL statistics (enabled or disabled).
Mirror Target Configuration	Displays ACL port mirroring parameters.

/info/link
Link Status Information

```
Alias   Port   Speed    Duplex     Flow Ctrl      Link
-----   ----   -----   --------  --TX-----RX--   ------
1         1     any      any     yes    yes       up
2         2    1000     full     yes    yes       up
3         3     any      any     yes    yes      down
4         4     any      any     yes    yes      down
5         5     any      any     yes    yes      down
6         6     any      any     yes    yes      down
7         7     any      any     yes    yes      down
8         8     any      any     yes    yes      down
9         9     any      any     yes    yes      down
10       10     any      any     yes    yes      down
11       11     any      any     yes    yes      down
12       12     any      any     yes    yes      down
13       13     any      any     yes    yes      down
14       14     any      any     yes    yes      down
15       15     any      any     yes    yes      down
16       16     any      any     yes    yes      down
17       17     any      any     yes    yes      down
18       18     any      any     yes    yes      down
19       19   10000     full     yes    yes      down
20       20   10000     full     yes    yes      down
21       21   10000     full     yes    yes      down
22       22   10000     full     yes    yes      down
23       23   10000     full     yes    yes      down
24       24   10000     full     yes    yes      down
MGTA     25     100     full     yes    yes       up
MGTB     26      10     half     yes    yes      down
```

Use this command to display link status information about each port on a G8124 slot, including:

- Port alias and number
- Port speed
- Duplex mode (half, full, any)
- Flow control for transmit and receive (no, yes, or both)
- Link status (up, down, or disabled)

/info/port
Port Information

```
Alias Port Tag Lrn Fld PVID       NAME                 VLAN(s)
----- ---- --- --- --- ----- -------------- --------------------------
1     1     n   e   e     1                1
2     2     n   e   e     1                1
3     3     n   e   e     1                1
4     4     n   e   e     1                1
5     5     n   e   e     1                1
6     6     n   e   e     1                1
7     7     n   e   e     1                1
8     8     n   e   e     1                1
9     9     n   e   e     1                1
10    10    n   e   e     1                1
11    11    n   e   e     1                1
12    12    n   e   e     1                1
13    13    n   e   e     1                1
14    14    n   e   e     1                1
15    15    n   e   e     1                1
16    16    n   e   e     1                1
17    17    n   e   e     1                1
18    18    n   e   e     1                1
19    19    n   e   e     1                1
20    20    n   e   e     1                1
21    21    n   e   e     1                1
22    22    n   e   e     1                1
23    23    n   e   e     1                1
24    24    n   e   e     1                1
MGTA  25    n   e   e  4095             4095
MGTB  26    n   e   e  4095             4095

* = PVID is tagged.
```

Port information includes:

- Port alias and number
- Whether the port uses VLAN tagging or not (`y` or `n`)
- Whether the port has FDB learning enabled (**`Lrn`**)
- Whether the port has Port Flood Blocking enabled (**`Fld`**)
- Port VLAN ID (**`PVID`**)
- Port name
- VLAN membership

/info/transcvr
Port Transceiver Status

```
Ports :
  SFP1 SFP+: Is Present  NOT APPROVED
  SFP2 SFP+: Is Present  Is Approved
    Vendor:Blade Network    Part:BN-CKM-SP-SR     Rev:-SP-
    Laser:850nm Serial:AD0752E01KL      Date:071225
  SFP3 SFP+: Is Present  NOT APPROVED
  SFP4 SFP+: Is Present  NOT APPROVED
```

This command displays the status of the transceiver module on each external port.

/info/dump
Information Dump

Use the dump command to dump all switch information available from the Information menu (10K or more, depending on your configuration). This data is useful for tuning and debugging switch performance.

If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.

CHAPTER 5
The Statistics Menu

You can view switch performance statistics in both the user and administrator command modes. This chapter discusses how to use the command line interface to display switch statistics.

/stats
Statistics Menu

```
[Statistics Menu]
     port      - Port Stats Menu
     l2        - Layer 2 Stats Menu
     l3        - Layer 3 Stats Menu
     mp        - MP-specific Stats Menu
     acl       - ACL Stats Menu
     snmp      - Show SNMP stats
     ntp       - Show NTP stats
     clrmp     - Clear all MP related stats
     clrports - Clear stats for all ports
     dump      - Dump all stats
```

The information provided by each menu option is briefly described in Table 41, with pointers to detailed information.

Table 41 Statistics Menu Options

Command Syntax and Usage
port *<port alias or number>* Displays the Port Statistics menu for the specified port. Use this command to display traffic statistics on a port-by-port basis. Traffic statistics are included in SNMP Management Information Base (MIB) objects. To view menu options, see page 109.
l2 Displays the Layer 2 Statistics menu. To view menu options, see page 117.

Table 41 Statistics Menu Options

Command Syntax and Usage
l3 Displays the Layer 3 Stats menu. To view menu options, see page 121.
mp Displays the Management Processor Statistics menu. Use this command to view information on how switch management processes and resources are currently being allocated. To view menu options, see page 140.
acl Displays ACL Statistics menu. To view menu options, see page 145.
snmp Displays SNMP statistics. See page 146 for sample output.
ntp [**clear**] Displays Network Time Protocol (NTP) Statistics. See page 150 for a sample output and a description of NTP Statistics. You can use the `clear` option to delete all NTP statistics.
clrmp Clears all management processor statistics.
clrports Clears statistics counters for all ports.
dump Dumps all switch statistics. Use this command to gather data for tuning and debugging switch performance. If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump command. For details, see page 151.

/stats/port <port alias or number>

Port Statistics Menu

This menu allows you to display traffic statistics on a port-by-port basis. Traffic statistics include SNMP Management Information Base (MIB) objects.

```
[Port Statistics Menu]
     brg       - Show bridging ("dot1") stats
     ether     - Show Ethernet ("dot3") stats
     if        - Show interface ("if") stats
     ip        - Show Internet Protocol ("IP") stats
     link      - Show link stats
     maint     - Show port maintenance stats
     dump      - Show all port stats
     clear     - Clear all port stats
```

Table 42 Port Statistics Menu Options

Command Syntax and Usage
brg Displays bridging (“dot1”) statistics for the port. See page 110 for sample output.
ether Displays Ethernet (“dot3”) statistics for the port. See page 111 for sample output.
if Displays interface statistics for the port. See page 114 for sample output.
ip Displays IP statistics for the port. See page 116 for sample output.
link Displays link statistics for the port. See page 116 for sample output.
maint Displays detailed maintenance statistics for the port.
dump This command dumps all statistics for the selected port.
clear This command clears all the statistics on the selected port.

/stats/port <port alias or number>/brg
Bridging Statistics

This option displays the bridging statistics of the selected port.

```
Bridging statistics for port 1:
dot1PortInFrames:                    63242584
dot1PortOutFrames:                   63277826
dot1PortInDiscards:                         0
dot1TpLearnedEntryDiscards:                 0
dot1StpPortForwardTransitions:              0
```

Table 43 Bridging Statistics of a Port

Statistics	Description
dot1PortInFrames	The number of frames that have been received by this port from its segment. A frame received on the interface corresponding to this port is only counted by this object if and only if it is for a protocol being processed by the local bridging function, including bridge management frames.
dot1PortOutFrames	The number of frames that have been transmitted by this port to its segment. Note that a frame transmitted on the interface corresponding to this port is only counted by this object if and only if it is for a protocol being processed by the local bridging function, including bridge management frames.
dot1PortInDiscards	Count of valid frames received which were discarded (that is, filtered) by the Forwarding Process.
dot1TpLearnedEntry Discards	The total number of Forwarding Database entries, which have been or would have been learnt, but have been discarded due to a lack of space to store them in the Forwarding Database. If this counter is increasing, it indicates that the Forwarding Database is regularly becoming full (a condition which has unpleasant performance effects on the subnetwork). If this counter has a significant value but is not presently increasing, it indicates that the problem has been occurring but is not persistent.
dot1StpPortForward Transitions	The number of times this port has transitioned from the Learning state to the Forwarding state.

/stats/port <port alias or number>/ether
Ethernet Statistics

This option displays the ethernet statistics of the selected port

```
Ethernet statistics for port 1:
dot3StatsAlignmentErrors:                    0
dot3StatsFCSErrors:                          0
dot3StatsSingleCollisionFrames:              0
dot3StatsMultipleCollisionFrames:            0
dot3StatsLateCollisions:                     0
dot3StatsExcessiveCollisions:                0
dot3StatsInternalMacTransmitErrors:         NA
dot3StatsFrameTooLongs:                      0
dot3StatsInternalMacReceiveErrors:           0
```

Table 44 Ethernet Statistics for Port

Statistics	Description
dot3StatsAlignment Errors	A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the Frame Check Sequence (FCS) check. The count represented by an instance of this object is incremented when the `alignmentError` status is returned by the MAC service to the Logical Link Control (LLC) (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
dot3StatsFCSErrors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the Frame Check Sequence (FCS) check. The count represented by an instance of this object is incremented when the `frameCheckError` status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.

Table 44 Ethernet Statistics for Port

Statistics	Description
dot3StatsSingleCollision Frames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the `ifOutUcastPkts`, `ifOutMulticastPkts`, or `ifOutBroadcastPkts`, and is not counted by the corresponding instance of the `dot3StatsMultipleCollisionFrame` object.
dot3StatsMultiple CollisionFrames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the `ifOutUcastPkts`, `ifOutMulticastPkts`, or `ifOutBroadcastPkts`, and is not counted by the corresponding instance of the `dot3StatsSingleCollisionFrames` object.
dot3StatsLateCollisions	The number of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet. Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mbit/s system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics.
dot3StatsExcessive Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions.
dot3StatsInternalMac TransmitErrors	A count of frames for which transmission on a particular interface fails due to an internal MAC sub layer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the `dot3StatsLateCollisions` object, the `dot3StatsExcessiveCollisions` object, or the `dot3StatsCarrierSenseErrors` object. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of transmission errors on a particular interface that are not otherwise counted.

Table 44 Ethernet Statistics for Port

Statistics	Description
dot3StatsFrameTooLongs	A count of frames received on a particular interface that exceed the maximum permitted frame size. The count represented by an instance of this object is incremented when the `frameTooLong` status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
dot3StatsInternalMacReceiveErrors	A count of frames for which reception on a particular interface fails due to an internal MAC sub layer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the `dot3StatsFrameTooLongs` object, the `dot3StatsAlignmentErrors` object, or the `dot3StatsFCSErrors` object. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of received errors on a particular interface that are not otherwise counted.

/stats/port <port alias or number>/if
Interface Statistics

This option displays the interface statistics of the selected port.

```
Interface statistics for port 1:
                     ifHCIn Counters       ifHCOut Counters
Octets:                  51697080313            51721056808
UcastPkts:                  65356399               65385714
BroadcastPkts:                     0                   6516
MulticastPkts:                     0                      0
FlowCtrlPkts:                      0                      0
Discards:                          0                      0
Errors:                            0                  21187
```

Table 45 Interface Statistics for Port

Statistics	Description
ifInOctets	The total number of octets received on the interface, including framing characters.
ifInUcastPkts	The number of packets, delivered by this sub-layer to a higher sub-layer, which were not addressed to a multicast or broadcast address at this sub-layer.
ifInBroadcastPkts	The number of packets, delivered by this sub-layer to a higher sub-layer, which were addressed to a broadcast address at this sub-layer.
ifInMulticastPkts	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses.
ifInFlowControlPkts	The total number of flow control `pause` packets received on the interface.
ifInDiscards	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being delivered to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.

Table 45 Interface Statistics for Port

Statistics	Description
ifInErrors	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being delivered to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol.
ifOutOctets	The total number of octets transmitted out of the interface, including framing characters.
ifOutUcastPkts	The total number of packets that higher-level protocols requested to be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.
ifOutBroadcastPkts	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent. This object is a 64-bit version of `ifOutBroadcastPkts`.
ifOutMulticastPkts	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses. This object is a 64-bit version of `ifOutMulticastPkts`.
ifOutFlowControlPkts	The total number of flow control `pause` packets transmitted out of the interface.
ifOutDiscards	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
ifOutErrors	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.

/stats/port <port alias or number>/ip
Interface Protocol Statistics

This option displays the interface statistics of the selected port.

```
GEA IP statistics for port 1:
ipInReceives    :          0
```

Table 46 Interface Protocol Statistics of a Port

Statistics	Description
ipInReceives	The total number of input datagrams received from interfaces, including those received in error.

/stats/port <port alias or number>/link
Link Statistics

This option displays the link statistics of the selected port.

```
Link statistics for port 1:
linkStateChange:              1
```

Table 47 Link Statistics of a Port

Statistics	Description
linkStateChange	The total number of link state changes.

/stats/l2

Layer 2 Statistics Menu

```
[Layer 2 Statistics Menu]
     fdb       - Show FDB stats
     lacp      - Show LACP stats
     hotlink   - Show Hot Links stats
```

The Layer 2 statistics provided by each menu option are briefly described in Table 48, with pointers to detailed information.

Table 48 Layer 2 Statistics Menu Options

Command Syntax and Usage
fdb [**clear**] Displays FDB statistics. See page 118 for sample output. Use the `clear` option to delete all FDB statistics.
lacp [<*port alias or number*>|**clear**] Displays Link Aggregation Control Protocol (LACP) statistics for a specified port, or for all ports if no port is specified. See page 119 for sample output. Use the `clear` option to delete all LACP statistics.
hotlink Displays Hotlinks statistics. See page 120 for sample output.

/stats/l2/fdb [clear]
FDB Statistics

```
FDB statistics:
 current:            83   hiwat:              855
```

This option displays statistics about the use of the forwarding database, including the number of new entries, finds, and unsuccessful searches.

FDB statistics are described in the following table:

Table 49 Forwarding Database Statistics

Statistic	Description
current	Current number of entries in the Forwarding Database.
hiwat	Highest number of entries recorded at any given time in the Forwarding Database.

Use the `clear` option to delete all FDB statistics.

/stats/l2/lacp [<port alias or number>|clear]
LACP Statistics

```
Port 1:
 ---------------------------------------
 Valid LACPDUs received:          - 870
 Valid Marker PDUs received:      - 0
 Valid Marker Rsp PDUs received:  - 0
 Unknown version/TLV type:        - 0
 Illegal subtype received:        - 0
 LACPDUs transmitted:             - 6031
 Marker PDUs transmitted:         - 0
 Marker Rsp PDUs transmitted:     - 0
```

Link Aggregation Control Protocol (LACP) statistics are described in the following table:

Table 50 LACP Statistics

Statistic	Description
Valid LACPDUs received	Total number of valid LACP data units received.
Valid Marker PDUs received	Total number of valid LACP marker data units received.
Valid Marker Rsp PDUs received	Total number of valid LACP marker response data units received.
Unknown version/TLV type	Total number of LACP data units with an unknown version or type, length, and value (TLV) received.
Illegal subtype received	Total number of LACP data units with an illegal subtype received.
LACPDUs transmitted	Total number of LACP data units transmitted.
Marker PDUs transmitted	Total number of LACP marker data units transmitted.
Marker Rsp PDUs transmitted	Total number of LACP marker response data units transmitted.

Use the `clear` option to delete all LACP statistics.

/stats/l2/hotlink
Hotlinks Statistics

```
Hot Links Trigger Stats:

Trigger 1 statistics:
    Trigger Name: Trigger 1
    Master active:           0
    Backup active:           0
    FDB update:              0   failed: 0
```

The following table describes the Hotlinks statistics:

Table 51 Hotlinks Statistics

Statistic	Description
Master active	Total number of times the Master interface transitioned to the Active state.
Backup active	Total number of times the Backup interface transitioned to the Active state.
FDB update	Total number of FDB update requests sent.
failed	Total number of FDB update requests that failed.

/stats/l3

Layer 3 Statistics Menu

```
[Layer 3 Statistics Menu]
     ip        - Show IP stats
     route     - Show route stats
     arp       - Show ARP stats
     dns       - Show DNS stats
     icmp      - Show ICMP stats
     tcp       - Show TCP stats
     udp       - Show UDP stats
     igmp      - Show IGMP stats
     ospf      - OSPF stats
     vrrp      - Show VRRP stats
     rip       - Show RIP stats
     clrigmp   - Clear IGMP stats
     ipclear   - Clear IP stats
     clrvrrp   - Clear VRRP stats
     ripclear  - Clear RIP stats
     ospfclr   - Clear all OSPF stats
     dump      - Dump layer 3 stats
```

The Layer 3 statistics provided by each menu option are briefly described in Table 52, with pointers to detailed information.

Table 52 Layer 3 Statistics Menu Options

Command Syntax and Usage
ip Displays IP statistics. See page 123 for sample output.
route [**clear**] Displays route statistics. See page 125 for sample output. Use the `clear` option to delete all route statistics.
arp [**clear**] Displays Address Resolution Protocol (ARP) statistics. See page 125 for sample output.
dns [**clear**] Displays Domain Name System (DNS) statistics. See page 126 for sample output. Use the `clear` option to delete all DNS statistics.

Table 52 Layer 3 Statistics Menu Options

Command Syntax and Usage
icmp [**clear**] Displays ICMP statistics. See page 127 for sample output. Use the `clear` option to delete all ICMP statistics.
tcp [**clear**] Displays TCP statistics. See page 129 for sample output. Use the `clear` option to delete all TCP statistics.
udp [**clear**] Displays UDP statistics. See page 131 for sample output. Use the `clear` option to delete all UDP statistics.
igmp Displays IGMP statistics. See page 132 for sample output.
ospf Displays OSPF statistics. See page 133 for sample output.
vrrp When virtual routers are configured, you can display the protocol statistics for VRRP. See page 138 for sample output.
rip Displays Routing Information Protocol (RIP) statistics. See page 139 for sample output.
clrigmp Clears IGMP statistics.
ipclear Clears IPv4 statistics. Use this command with caution as it will delete all the IPv4 statistics.
clrvrrp Clears VRRP statistics.
ripclear Clears Routing Information Protocol (RIP) statistics.

Table 52 Layer 3 Statistics Menu Options

Command Syntax and Usage
ospfclear Clears Open Shortest Path First (OSPF) statistics.
dump Dumps all Layer 3 statistics. Use this command to gather data for tuning and debugging switch performance. If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump command.

/stats/l3/ip
IPv4 Statistics

```
IP statistics:
ipInReceives:               0   ipInHdrErrors:            0
ipInAddrErrors:             0
ipInUnknownProtos:          0   ipInDiscards:             0
ipInDelivers:               0   ipOutRequests:         1274
ipOutDiscards:              0
ipDefaultTTL:             255
```

Table 53 IP Statistics

Statistics	Description
ipInReceives	The total number of input datagrams received from interfaces, including those received in error.
ipInHdrErrors	The number of input datagrams discarded due to errors in their IP headers, including bad `checksums`, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so forth.
ipInAddrErrors	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity (the switch). This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
ipInUnknownProtos	The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.

Table 53 IP Statistics

Statistics	Description
ipInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
ipInDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
ipOutRequests	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in `ipForwDatagrams`.
ipOutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space). Note that this counter would include datagrams counted in `ipForwDatagrams` if any such packets met this (discretionary) discard criterion.
ipDefaultTTL	The default value inserted into the `Time-To-Live` (TTL) field of the IP header of datagrams originated at this entity (the switch), whenever a TTL value is not supplied by the transport layer protocol.

/stats/l3/route [clear]
Route Statistics

```
Route statistics:
ipRoutesCur:              11  ipRoutesHighWater:        11
ipRoutesMax:            4096
```

Table 54 Route Statistics

Statistics	Description
ipRoutesCur	The total number of outstanding routes in the route table.
ipRoutesHighWater	The highest number of routes ever recorded in the route table.
ipRoutesMax	The maximum number of routes that are supported.

Use the `clear` option to delete all route statistics.

/stats/l3/arp
ARP Statistics

This option displays Address Resolution Protocol (ARP) statistics.

```
ARP statistics:
arpEntriesCur:              3  arpEntriesHighWater:          4
arpEntriesMax:           2048
```

Table 55 ARP Statistics

Statistics	Description
arpEntriesCur	The total number of outstanding ARP entries in the ARP table.
arpEntriesHighWater	The highest number of ARP entries ever recorded in the ARP table.
arpEntriesMax	The maximum number of ARP entries that are supported.

/stats/l3/dns [clear]
DNS Statistics

This option displays Domain Name System (DNS) statistics.

```
DNS statistics:
dnsOutRequests:             0
dnsBadRequests:             0
```

Table 56 DNS Statistics

Statistics	Description
dnsOutRequests	The total number of DNS response packets that have been transmitted.
dnsBadRequests	The total number of DNS request packets received that were dropped.

Use the `clear` option to delete all DNS statistics.

/stats/l3/icmp [clear]
ICMP Statistics

```
ICMP statistics:
icmpInMsgs:              245802   icmpInErrors:              1393
icmpInDestUnreachs:          41   icmpInTimeExcds:              0
icmpInParmProbs:              0   icmpInSrcQuenchs:             0
icmpInRedirects:              0   icmpInEchos:                 18
icmpInEchoReps:          244350   icmpInTimestamps:             0
icmpInTimestampReps:          0   icmpInAddrMasks:              0
icmpInAddrMaskReps:           0   icmpOutMsgs:             253810
icmpOutErrors:                0   icmpOutDestUnreachs:         15
icmpOutTimeExcds:             0   icmpOutParmProbs:             0
icmpOutSrcQuenchs:            0   icmpOutRedirects:             0
icmpOutEchos:            253777   icmpOutEchoReps:             18
icmpOutTimestamps:            0   icmpOutTimestampReps:         0
icmpOutAddrMasks:             0   icmpOutAddrMaskReps:          0
```

Table 57 ICMP Statistics

Statistics	Description
icmpInMsgs	The total number of ICMP messages which the entity (the switch) received. Note that this counter includes all those counted by `icmpInErrors`.
icmpInErrors	The number of ICMP messages which the entity (the switch) received but determined as having ICMP-specific errors (bad ICMP `checksums`, bad length, and so forth).
icmpInDestUnreachs	The number of ICMP Destination Unreachable messages received.
icmpInTimeExcds	The number of ICMP Time Exceeded messages received.
icmpInParmProbs	The number of ICMP Parameter Problem messages received.
icmpInSrcQuenchs	The number of ICMP Source Quench (buffer almost full, stop sending data) messages received.
icmpInRedirects	The number of ICMP Redirect messages received.
icmpInEchos	The number of ICMP Echo (request) messages received.
icmpInEchoReps	The number of ICMP Echo Reply messages received.
icmpInTimestamps	The number of ICMP Timestamp (request) messages received.
icmpInTimestampReps	The number of ICMP Timestamp `Reply` messages received.

Table 57 ICMP Statistics

Statistics	Description
icmpInAddrMasks	The number of ICMP Address Mask Request messages received.
icmpInAddrMaskReps	The number of ICMP Address Mask Reply messages received.
icmpOutMsgs	The total number of ICMP messages which this entity (the switch) attempted to send. Note that this counter includes all those counted by `icmpOutErrors`.
icmpOutErrors	The number of ICMP messages which this entity (the switch) did not send due to problems discovered within ICMP such as a lack of buffer. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of errors that contribute to this counter's value.
icmpOutDestUnreachs	The number of ICMP Destination Unreachable messages sent.
icmpOutTimeExcds	The number of ICMP Time Exceeded messages sent.
icmpOutParmProbs	The number of ICMP Parameter Problem messages sent.
icmpOutSrcQuenchs	The number of ICMP Source Quench (buffer almost full, stop sending data) messages sent.
icmpOutRedirects	The number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
icmpOutEchos	The number of ICMP Echo (request) messages sent.
icmpOutEchoReps	The number of ICMP Echo Reply messages sent.
icmpOutTimestamps	The number of ICMP Timestamp (request) messages sent.
icmpOutTimestampReps	The number of ICMP Timestamp `Reply` messages sent.
icmpOutAddrMasks	The number of ICMP Address Mask Request messages sent.
icmpOutAddrMaskReps	The number of ICMP Address Mask Reply messages sent.

Use the `clear` option to delete all ICMP statistics.

/stats/l3/tcp [clear]
TCP Statistics

```
TCP statistics:
tcpRtoAlgorithm:        4   tcpRtoMin:              0
tcpRtoMax:         240000   tcpMaxConn:           512
tcpActiveOpens:    252214   tcpPassiveOpens:        7
tcpAttemptFails:      528   tcpEstabResets:         4
tcpInSegs:         756401   tcpOutSegs:        756655
tcpRetransSegs:         0   tcpInErrs:              0
tcpCurBuff:             0   tcpCurConn:             3
tcpOutRsts:           417
```

Table 58 TCP Statistics

Statistics	Description
tcpRtoAlgorithm	The algorithm used to determine the `timeout` value used for retransmitting unacknowledged octets.
tcpRtoMin	The minimum value permitted by a TCP implementation for the retransmission `timeout`, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission `timeout`. In particular, when the `timeout` algorithm is rsre(3), an object of this type has the semantics of the LBOUND quantity described in RFC 793.
tcpRtoMax	The maximum value permitted by a TCP implementation for the retransmission `timeout`, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission `timeout`. In particular, when the `timeout` algorithm is rsre(3), an object of this type has the semantics of the UBOUND quantity described in RFC 793.
tcpMaxConn	The limit on the total number of TCP connections the entity (the switch) can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1.
tcpActiveOpens	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
tcpPassiveOpens	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.

Table 58 TCP Statistics

Statistics	Description
tcpAttemptFails	The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.
tcpEstabResets	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
tcpInSegs	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
tcpOutSegs	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
tcpRetransSegs	The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
tcpInErrs	The total number of segments received in error (for example, bad TCP `checksums`).
tcpCurBuff	The total number of outstanding memory allocations from heap by TCP protocol stack.
tcpCurConn	The total number of outstanding TCP sessions that are currently opened.
tcpOutRsts	The number of TCP segments sent containing the RST flag.

Use the `clear` option to delete all TCP statistics.

/stats/l3/udp [clear]
UDP Statistics

```
UDP statistics:
udpInDatagrams:         54   udpOutDatagrams:         43
udpInErrors:             0   udpNoPorts:         1578077
```

Table 59 UDP Statistics

Statistics	Description
udpInDatagrams	The total number of UDP datagrams delivered to the switch.
udpOutDatagrams	The total number of UDP datagrams sent from this entity (the switch).
udpInErrors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
udpNoPorts	The total number of received UDP datagrams for which there was no application at the destination port.

Use the `clear` option to delete all UDP statistics.

/stats/l3/igmp <VLAN number>
IGMP Statistics

```
IGMP Snoop vlan 2 statistics:
-------------------------------------------------------------------------
rxIgmpValidPkts:                 0   rxIgmpInvalidPkts:                 0
rxIgmpGenQueries:                0   rxIgmpGrpSpecificQueries:         0
rxIgmpGroupSrcSpecificQueries:   0
rxIgmpLeaves:                    0   rxIgmpReports:                     0
txIgmpReports:                   0   txIgmpGrpSpecificQueries:         0
txIgmpLeaves:                    0   rxIgmpV3CurrentStateRecords:      0
rxIgmpV3SourceListChangeRecords:0    rxIgmpV3FilterChangeRecords:      0
txIgmpGenQueries:                     18
```

This option displays statistics about the use of the IGMP Multicast Groups. IGMP statistics are described in the following table:

Table 60 IGMP Statistics

Statistic	Description
rxIgmpValidPkts	Total number of valid IGMP packets received
rxIgmpInvalidPkts	Total number of invalid packets received
rxIgmpGenQueries	Total number of General Membership Query packets received
rxIgmpGrpSpecific Queries	Total number of Membership Query packets received from specific groups
rxIgmpGroupSrcSpecific Queries	Total number of Group Source-Specific Queries (GSSQ) received
rxIgmpLeaves	Total number of Leave requests received
rxIgmpReports	Total number of Membership Reports received
txIgmpReports	Total number of Membership reports transmitted
txIgmpGrpSpecific Queries	Total number of Membership Query packets transmitted to specific groups
txIgmpLeaves	Total number of Leave messages transmitted
rxIgmpV3CurrentState Records	Total number of Current State records received
rxIgmpV3SourceList ChangeRecords	Total number of Source List Change records received.

Table 60 IGMP Statistics

Statistic	Description
rxIgmpV3FilterChange Records	Total number of Filter Change records received.
txIgmpGenQueries	Total number of General Membership Query packets transmitted

/stats/l3/ospf
OSPF Statistics

```
[OSPF stats Menu]
      general - Show global stats
      aindex  - Show area(s) stats
      if      - Show interface(s) stats
```

Table 61 OSPF Statistics Options

Command Syntax and Usage
general Displays global statistics. See page 134 for sample output.
aindex Displays area statistics.
if Displays interface statistics.

/stats/l3/ospf/general
OSPF General Statistics

The OSPF General Statistics contain the sum total of all OSPF packets received on all OSPF areas and interfaces.

```
OSPF stats
----------
Rx/Tx Stats:          Rx            Tx
                    --------      --------
  Pkts                   0             0
  hello                 23           518
  database               4            12
  ls requests            3             1
  ls acks                7             7
  ls updates             9             7

Nbr change stats:                Intf change Stats:
  hello                   2            hello              4
  start                   0            down               2
  n2way                   2            loop               0
  adjoint ok              2            unloop             0
  negotiation done        2            wait timer         2
  exchange done           2            backup             0
  bad requests            0            nbr change         5
  bad sequence            0
  loading done            2
  n1way                   0
  rst_ad                  0
  down                    1

Timers kickoff
  hello                 514
  retransmit           1028
  lsa lock                0
  lsa ack                 0
  dbage                   0
  summary                 0
  ase export              0
```

Table 62 OSPF General Statistics (stats/l3/ospf/general)

Statistics	Description
Rx/Tx Stats:	
Rx Pkts	The sum total of all OSPF packets received on all OSPF areas and interfaces.
Tx Pkts	The sum total of all OSPF packets transmitted on all OSPF areas and interfaces.
Rx Hello	The sum total of all Hello packets received on all OSPF areas and interfaces.
Tx Hello	The sum total of all Hello packets transmitted on all OSPF areas and interfaces.
Rx Database	The sum total of all Database Description packets received on all OSPF areas and interfaces.
Tx Database	The sum total of all Database Description packets transmitted on all OSPF areas and interfaces.
Rx ls Requests	The sum total of all Link State Request packets received on all OSPF areas and interfaces.
Tx ls Requests	The sum total of all Link State Request packets transmitted on all OSPF areas and interfaces.
Rx ls Acks	The sum total of all Link State Acknowledgement packets received on all OSPF areas and interfaces.
Tx ls Acks	The sum total of all Link State Acknowledgement packets transmitted on all OSPF areas and interfaces.
Rx ls Updates	The sum total of all Link State Update packets received on all OSPF areas and interfaces.
Tx ls Updates	The sum total of all Link State Update packets transmitted on all OSPF areas and interfaces.
Nbr Change Stats:	
hello	The sum total of all Hello packets received from neighbors on all OSPF areas and interfaces.
Start	The sum total number of neighbors in this state (that is, an indication that Hello packets should now be sent to the neighbor at intervals of `HelloInterval` seconds.) across all OSPF areas and interfaces.

Table 62 OSPF General Statistics (stats/l3/ospf/general) (continued)

Statistics	Description
n2way	The sum total number of bidirectional communication establishment between this router and other neighboring routers.
adjoint ok	The sum total number of decisions to be made (again) as to whether an adjacency should be established/maintained with the neighbor across all OSPF areas and interfaces.
negotiation done	The sum total number of neighbors in this state wherein the Master/slave relationship has been negotiated, and sequence numbers have been exchanged, across all OSPF areas and interfaces.
exchange done	The sum total number of neighbors in this state (that is, in an adjacency's final state) having transmitted a full sequence of Database Description packets, across all OSPF areas and interfaces.
bad requests	The sum total number of Link State Requests which have been received for a link state advertisement not contained in the database across all interfaces and OSPF areas.
bad sequence	The sum total number of Database Description packets which have been received that either: a. Has an unexpected DD sequence number b. Unexpectedly has the init bit set c. Has an options field differing from the last Options field received in a Database Description packet. Any of these conditions indicate that some error has occurred during adjacency establishment for all OSPF areas and interfaces.
loading done	The sum total number of link state updates received for all out-of-date portions of the database across all OSPF areas and interfaces.
n1way	The sum total number of Hello packets received from neighbors, in which this router is not mentioned across all OSPF interfaces and areas.
rst_ad	The sum total number of times the Neighbor adjacency has been reset across all OPSF areas and interfaces.
down	The total number of Neighboring routers down (that is, in the initial state of a neighbor conversation.) across all OSPF areas and interfaces.

Table 62 OSPF General Statistics (stats/l3/ospf/general) (continued)

Statistics	Description
Intf Change Stats:	
hello	The sum total number of Hello packets sent on all interfaces and areas.
down	The sum total number of interfaces down in all OSPF areas.
loop	The sum total of interfaces no longer connected to the attached network across all OSPF areas and interfaces.
unloop	The sum total number of interfaces, connected to the attached network in all OSPF areas.
wait timer	The sum total number of times the Wait Timer has been fired, indicating the end of the waiting period that is required before electing a (Backup) Designated Router across all OSPF areas and interfaces.
backup	The sum total number of Backup Designated Routers on the attached network for all OSPF areas and interfaces.
nbr change	The sum total number of changes in the set of bidirectional neighbors associated with any interface across all OSPF areas.
Timers Kickoff:	
hello	The sum total number of times the Hello timer has been fired (which triggers the `send` of a Hello packet) across all OPSF areas and interfaces.
retransmit	The sum total number of times the Retransmit timer has been fired across all OPSF areas and interfaces.
lsa lock	The sum total number of times the Link State Advertisement (LSA) lock timer has been fired across all OSPF areas and interfaces.
lsa ack	The sum total number of times the LSA `Ack` timer has been fired across all OSPF areas and interfaces.
dbage	The total number of times the data base age (`Dbage`) has been fired.
summary	The total number of times the Summary timer has been fired.
ase export	The total number of times the Autonomous System Export (ASE) timer has been fired.

/stats/l3/vrrp
VRRP Statistics

Virtual Router Redundancy Protocol (VRRP) support on the RackSwitch G8124 (G8124) provides redundancy between routers in a LAN. This is accomplished by configuring the same virtual router IP address and ID number on each participating VRRP-capable routing device. One of the virtual routers is then elected as the master, based on a number of priority criteria, and assumes control of the shared virtual router IP address. If the master fails, one of the backup virtual routers will assume routing authority and take control of the virtual router IP address.

When virtual routers are configured, you can display the following protocol statistics for VRRP:

- Advertisements received (`vrrpInAdvers`)
- Advertisements transmitted (`vrrpOutAdvers`)
- Advertisements received, but ignored (`vrrpBadAdvers`)

The statistics for the VRRP LAN are displayed:

```
VRRP statistics:
vrrpInAdvers:              0   vrrpBadAdvers:            0
vrrpOutAdvers:             0
vrrpBadVersion:            0   vrrpBadVrid:              0
vrrpBadAddress:            0   vrrpBadData:              0
vrrpBadPassword:           0   vrrpBadInterval:          0
```

Table 63 VRRP Statistics

Statistics	Description
`vrrpInAdvers`	The total number of valid VRRP advertisements that have been received.
`vrrpBadAdvers`	The total number of VRRP advertisements received that were dropped.
`vrrpOutAdvers`	The total number of VRRP advertisements that have been sent.
`vrrpBadVersion`	The total number of VRRP advertisements received that had a bad version number.
`vrrpBadVrid`	The total number of VRRP advertisements received that had a bad virtual router ID.
`vrrpBadAddress`	The total number of VRRP advertisements received that had a bad address.
`vrrpBadData`	The total number of VRRP advertisements received that had bad data.

Table 63 VRRP Statistics

Statistics	Description
vrrpBadPassword	The total number of VRRP advertisements received that had a bad password.
vrrpBadInterval	The total number of VRRP advertisements received that had a bad interval.

/stats/l3/rip
Routing Information Protocol Statistics

```
RIP ALL STATS INFORMATION:
        RIP packets received  = 12
        RIP packets sent      = 75
        RIP request received  = 0
        RIP response recevied = 12
        RIP request sent      = 3
        RIP reponse sent      = 72
        RIP route timeout     = 0
        RIP bad size packet received = 0
        RIP bad version received       = 0
        RIP bad zeros received         = 0
        RIP bad src port received      = 0
        RIP bad src IP received        = 0
        RIP packets from self received = 0
```

/stats/mp

Management Processor Statistics Menu

```
[MP-specific Statistics Menu]
     thr       - Show STEM thread stats
     i2c       - Show I2C stats
     pkt       - Show Packet stats
     tcb       - Show All TCP control blocks in use
     ucb       - Show All UDP control blocks in use
     cpu       - Show CPU utilization
     mem       - Show Memory utilization stats
```

Table 64 Management Processor Statistics Menu Options

Command Syntax and Usage
thr Displays STEM thread statistics. This command is used by Technical Support personnel.
i2c Displays I2C statistics. This command is used by Technical Support personnel.
pkt Displays packet statistics, to check for leads and load. To view a sample output and a description of the stats, see page 141.
tcb Displays all TCP control blocks that are in use. To view a sample output and a description of the stats, see page 143.
ucb Displays all UDP control blocks that are in use. To view a sample output, see page 143.
cpu Displays CPU utilization for periods of up to 1, 4, and 64 seconds. To view a sample output and a description of the stats, see page 144.
mem Displays system memory statistics.

/stats/mp/pkt
MP Packet Statistics

```
Packet counts seen by MP:
 allocs:           859
 frees:            859
 failures:           0

  small packet buffers:
 ----------------------
   current:                 0
   hi-watermark:            4
   hi-water time:   17:56:35 Tue Jul 14, 2009

 medium packet buffers:
 ----------------------
   current:                 0
   hi-watermark:            1
   hi-water time:   17:56:16 Tue Jul 14, 2009

 jumbo packet buffers:
 ----------------------
   current:                 0
   hi-watermark:            0
```

Table 65 Packet Statistics

Statistics	Description
allocs	Total number of packet allocations from the packet buffer pool by the TCP/IP protocol stack.
frees	Total number of times the packet buffers are freed (released) to the packet buffer pool by the TCP/IP protocol stack.
failures	Total number of packet allocation failures from the packet buffer pool by the TCP/IP protocol stack.
small packet buffers	
current	Total number of packet allocations with size less than 128 bytes from the packet buffer pool by the TCP/IP protocol stack.
hi-watermark	The highest number of packet allocation with size less than 128 bytes from the packet buffer pool by the TCP/IP protocol stack.
hi-water time	Time stamp that indicates when the hi-watermark was reached.
medium packet buffers	

Table 65 Packet Statistics

Statistics	Description
current	Total number of packet allocations with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
hi-watermark	The highest number of packet allocation with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
hi-water time	Time stamp that indicates when the hi-watermark was reached.
jumbo packet buffers	
current	Total number of packet allocations with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
hi-watermark	The highest number of packet allocation with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.

/stats/mp/tcb
TCP Statistics

```
All TCP allocated control blocks:
10ad41e8:  0.0.0.0             0 <=> 0.0.0.0            80  listen
10ad5790:  47.81.27.5       1171 <=> 47.80.23.243       23  established
```

Table 66 MP Specified TCP Statistics

Statistics	Description
10ad41e8/10ad5790	Memory
0.0.0.0/47.81.27.5	Destination IP address
0/1171	Destination port
0.0.0.0/47.80.23.243	Source IP
80/23	Source port
listen/established	State

/stats/mp/ucb
UCB Statistics

```
All UDP allocated control blocks:
  161:  listen
```

/stats/mp/cpu
CPU Statistics

This option displays the CPU utilization statistics.

```
CPU utilization:
cpuUtil1Second:             53%
cpuUtil4Seconds:            54%
cpuUtil64Seconds:           54%
```

Table 67 CPU Statistics

Statistics	Description
cpuUtil1Second	The utilization of MP CPU over 1 second. It shows the percentage.
cpuUtil4Seconds	The utilization of MP CPU over 4 seconds. It shows the percentage.
cpuUtil64Seconds	The utilization of MP CPU over 64 seconds. It shows the percentage.

/stats/acl
ACL Statistics Menu

```
[ACL Menu]
     acl       - Display ACL stats
     dump      - Display all available ACL stats
     clracl    - Clear ACL stats
```

ACL statistics are described in the following table.

Table 68 ACL Statistics Menu Options

Command Syntax and Usage
acl *<ACL number>* Displays the Access Control List Statistics for a specific ACL. For details, see page 145.
dump Displays all ACL statistics.
clracl Clears all ACL statistics.

/stats/acl/acl [*<ACL number>*]
ACL Statistics

This option displays statistics for the selected ACL if an ACL number is specified, or for all ACLs if the option is omitted.

```
Hits for ACL 1, port 1:              26057515
Hits for ACL 2, port 1:              26057497
```

/stats/snmp [clear]
SNMP Statistics

Note – You can reset the SNMP counter to zero by using `clear` command, as follows:
>> Statistics# **`snmp clear`**

```
SNMP statistics:
snmpInPkts:              150097   snmpInBadVersions:              0
snmpInBadC'tyNames:           0   snmpInBadC'tyUses:              0
snmpInASNParseErrs:           0   snmpEnableAuthTraps:            0
snmpOutPkts:             150097   snmpInBadTypes:                 0
snmpInTooBigs:                0   snmpInNoSuchNames:              0
snmpInBadValues:              0   snmpInReadOnlys:                0
snmpInGenErrs:                0   snmpInTotalReqVars:        798464
snmpInTotalSetVars:        2731   snmpInGetRequests:          17593
snmpInGetNexts:          131389   snmpInSetRequests:            615
snmpInGetResponses:           0   snmpInTraps:                    0
snmpOutTooBigs:               0   snmpOutNoSuchNames:             1
snmpOutBadValues:             0   snmpOutReadOnlys:               0
snmpOutGenErrs:               1   snmpOutGetRequests:             0
snmpOutGetNexts:              0   snmpOutSetRequests:             0
snmpOutGetResponses:     150093   snmpOutTraps:                   4
snmpSilentDrops:              0   snmpProxyDrops:                 0
```

Table 69 SNMP Statistics

Statistics	Description
snmpInPkts	The total number of Messages delivered to the SNMP entity from the transport service.
snmpInBadVersions	The total number of SNMP Messages, which were delivered to the SNMP protocol entity and were for an unsupported SNMP version.
snmpInBadC'tyNames	The total number of SNMP Messages delivered to the SNMP entity which used an SNMP community name not known to the said entity (the switch).
snmpInBadC'tyUses	The total number of SNMP Messages delivered to the SNMP protocol entity which represented an SNMP operation which was not allowed by the SNMP community named in the Message.

Table 69 SNMP Statistics

Statistics	Description
snmpInASNParseErrs	The total number of ASN.1 or BER errors encountered by the SNMP protocol entity when decoding SNMP Messages received. **Note:** OSI's method of specifying abstract objects is called ASN.1 (Abstract Syntax Notation One, defined in X.208), and one set of rules for representing such objects as strings of ones and zeros is called the BER (Basic Encoding Rules, defined in X.209). ASN.1 is a flexible notation that allows one to define a variety of data types, from simple types such as integers and bit strings to structured types such as sets and sequences. BER describes how to represent or encode values of each ASN.1 type as a string of eight-bit octets.
snmpEnableAuth Traps	An object to enable or disable the authentication traps generated by this entity (the switch).
snmpOutPkts	The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service.
snmpInBadTypes	The total number of SNMP Messages which failed ASN parsing.
snmpInTooBigs	The total number of SNMP Protocol Data Units (PDUs) which were delivered to the SNMP protocol entity and for which the value of the error-status field is *too big*.
snmpInNoSuchNames	The total number of SNMP Protocol Data Units (PDUs) which were delivered to the SNMP protocol entity and for which the value of the error-status field is `noSuchName`.
snmpInBadValues	The total number of SNMP Protocol Data Units (PDUs) which were delivered to the SNMP protocol entity and for which the value of the error-status field is `badValue`.
snmpInReadOnlys	The total number of valid SNMP Protocol Data Units (PDUs), which were delivered to the SNMP protocol entity and for which the value of the error-status field is `read-Only'. It should be noted that it is a protocol error to generate an SNMP PDU, which contains the value `read-Only' in the error-status field. As such, this object is provided as a means of detecting incorrect implementations of the SNMP.
snmpInGenErrs	The total number of SNMP Protocol Data Units (PDUs), which were delivered to the SNMP protocol entity and for which the value of the error-status field is `genErr`.

Table 69 SNMP Statistics

Statistics	Description
snmpInTotalReqVars	The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as a result of receiving valid SNMP Get-Request and Get-Next Protocol Data Units (PDUs).
snmpInTotalSetVars	The total number of MIB objects, which have been altered successfully by the SNMP protocol entity as a result of receiving valid SNMP Set-Request Protocol Data Units (PDUs).
snmpInGetRequests	The total number of SNMP Get-Request Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInGetNexts	The total number of SNMP Get-Next Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInSetRequests	The total number of SNMP Set-Request Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInGetResponses	The total number of SNMP Get-Response Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInTraps	The total number of SNMP Trap Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpOutTooBigs	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is *too big*.
snmpOutNoSuchNames	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status is `noSuchName`.
snmpOutBadValues	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is `badValue`.
snmpOutReadOnlys	Not in use.
snmpOutGenErrs	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is `genErr`.
snmpOutGetRequests	The total number of SNMP Get-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.

Table 69 SNMP Statistics

Statistics	Description
snmpOutGetNexts	The total number of SNMP Get-Next Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutSetRequests	The total number of SNMP Set-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutGet Responses	The total number of SNMP Get-Response Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutTraps	The total number of SNMP Trap Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpSilentDrops	The total number of `GetRequest`-PDUs, `GetNextRequest`-PDUs, `GetBulkRequest`-PDUs, `SetRequest`-PDUs, and `InformRequest`-PDUs delivered to the SNMPv2 entity which were silently dropped because the size of a reply containing an alternate Response-PDU with an empty variable bindings field was greater than either a local constraint or the maximum message size associated with the originator of the request.
snmpProxyDrops	The total number of `GetRequest`-PDUs, `GetNextRequest`-PDUs, `GetBulkRequest`-PDUs, `SetRequest`-PDUs, and `InformRequest`-PDUs delivered to the SNMP entity which were silently dropped because the transmission of the message to a proxy target failed in a manner such that no Response-PDU could be returned.

/stats/ntp
NTP Statistics

BLADE OS uses NTP (Network Timing Protocol) version 3 to synchronize the switch's internal clock with an atomic time calibrated NTP server. With NTP enabled, the switch can accurately update its internal clock to be consistent with other devices on the network and generates accurate syslogs.

```
NTP statistics:
        Primary Server:
                Requests Sent:              17
                Responses Received:         17
                Updates:                    1
        Secondary Server:
                Requests Sent:              0
                Responses Received:         0
                Updates:                    0

        Last update based on response from primary server.
        Last update time: 18:04:16 Tue Jul 13, 2009
        Current system time: 18:55:49 Tue Jul 13, 2009
```

Table 70 NTP Statistics

Field	Description
Primary Server	■ **Requests Sent:** The total number of NTP requests the switch sent to the primary NTP server to synchronize time. ■ **Responses Received:** The total number of NTP responses received from the primary NTP server. ■ **Updates:** The total number of times the switch updated its time based on the NTP responses received from the primary NTP server.
Secondary Server	■ **Requests Sent:** The total number of NTP requests the switch sent to the secondary NTP server to synchronize time. ■ **Responses Received:** The total number of NTP responses received from the secondary NTP server. ■ **Updates:** The total number of times the switch updated its time based on the NTP responses received from the secondary NTP server.

Table 70 NTP Statistics

Field	Description
Last update based on response from primary server	Last update of time on the switch based on either primary or secondary NTP response received.
Last update time	The time stamp showing the time when the switch was last updated.
Current system time	The switch system time when the following command was issued: `/stats/ntp`

Note – Use the following command to delete all NTP statistics: `/stats/ntp clear`

/stats/dump
Statistics Dump

Use the dump command to dump all switch statistics available from the Statistics menu (40K or more, depending on your configuration). This data can be used to tune or debug switch performance.

If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.

CHAPTER 6
The Configuration Menu

This chapter discusses how to use the Command Line Interface (CLI) for making, viewing, and saving switch configuration changes. Many of the commands, although not new, display more or different information than in the previous version. Important differences are called out in the text.

/cfg
Configuration Menu

```
[Configuration Menu]
     sys       - System-wide Parameter Menu
     port      - Port Menu
     qos       - QOS Menu
     acl       - Access Control List Menu
     pmirr     - Port Mirroring Menu
     l2        - Layer 2 Menu
     l3        - Layer 3 Menu
     setup     - Step by step configuration set up
     dump      - Dump current configuration to script file
     ptcfg     - Backup current configuration to FTP/TFTP server
     gtcfg     - Restore current configuration from FTP/TFTP server
     cur       - Display current configuration
```

Each configuration option is briefly described in Table 71, with pointers to detailed menu commands.

Table 71 Configuration Menu Options

Command Syntax and Usage
sys Displays the System Configuration menu. To view menu options, see page 157.
port *<port alias or number>* Displays the Port Configuration menu. To view menu options, see page 197.
qos Displays the Quality of Service Configuration menu. To view menu options, see page 204.
acl Displays the ACL Configuration menu. To view menu options, see page 207.
pmirr Displays the Mirroring Configuration menu. To view menu options, see page 218.
l2 Displays the Layer 2 Configuration menu. To view menu options, see page 220.
l3 Displays the Layer 3 Configuration menu. To view menu options, see page 252.
setup Step-by-step configuration set-up of the switch. For details, see page 306.
dump Dumps current configuration to a script file. For details, see page 306.
ptcfg *<FTP/TFTP server host name or IP address> <filename on host>* Backs up current configuration to TFTP server. For details, see page 307.
gtcfg *<host name or IP address of TFTP server> <filename on host>* Restores current configuration from TFTP server. For details, see page 307.
cur Displays current configuration parameters.

Viewing, Applying, and Saving Changes

As you use the configuration menus to set switch parameters, the changes you make do not take effect immediately. All changes are considered "pending" until you explicitly apply them. Also, any changes are lost the next time the switch boots unless the changes are explicitly saved.

Note – Some operations can override the settings in the Configuration menu. Therefore, settings you view in the Configuration menu (for example, port status) might differ from run-time information that you view in the Information menu or on the management module. The Information menu displays current run-time information of switch parameters.

While configuration changes are in the pending state, you can do the following:

- View the pending changes
- Apply the pending changes
- Save the changes to flash memory

Viewing Pending Changes

You can view all pending configuration changes by entering **`diff`** at the menu prompt.

Note – The `diff` command is a global command. Therefore, you can enter **`diff`** at any prompt in the CLI.

Applying Pending Changes

To make your configuration changes active, you must apply them. To apply configuration changes, enter **`apply`** at any prompt in the CLI.

```
# apply
```

Note – The `apply` command is a global command. Therefore, you can enter **`apply`** at any prompt in the administrative interface.

Saving the Configuration

In addition to applying the configuration changes, you can save them to flash memory on the RackSwitch G8124 (G8124).

Note – If you do not save the changes, they will be lost the next time the system is rebooted.

To save the new configuration, enter the following command at any CLI prompt:

```
# save
```

When you save configuration changes, the changes are saved to the *active* configuration block. The configuration being replaced by the save is first copied to the *backup* configuration block. If you do not want the previous configuration block copied to the backup configuration block, enter the following instead:

```
# save n
```

You can decide which configuration you want to run the next time you reset the switch. Your options include:

- The active configuration block
- The backup configuration block
- Factory default configuration

You can view all pending configuration changes that have been applied but not saved to flash memory using the `diff flash` command. It is a global command that can be executed from any menu.

For instructions on selecting the configuration to run at the next system reset, see "Selecting a Configuration Block" on page 317.

/cfg/sys

System Configuration Menu

```
[System Menu]
     errdis    - ErrDisable Menu
     syslog    - Syslog Menu
     sshd      - SSH Server Menu
     radius    - RADIUS Authentication Menu
     tacacs+   - TACACS+ Authentication Menu
     ldap      - LDAP Authentication Menu
     ntp       - NTP Server Menu
     ssnmp     - System SNMP Menu
     access    - System Access Menu
     dst       - Custom DST Menu
     sflow     - sFlow Menu
     date      - Set system date
     time      - Set system time
     timezone  - Set system timezone (daylight savings)
     dlight    - Set system daylight savings
     idle      - Set timeout for idle CLI sessions
     notice    - Set login notice
     bannr     - Set login banner
     hprompt   - Enable/disable display hostname (sysName) in CLI prompt
     bootp     - Enable/disable use of BOOTP
     dhcp      - Enable/disable use of DHCP on interface 1
     reminder  - Enable/disable Reminders
     rstctrl   - Enable/disable System reset on panic
     cur       - Display current system-wide parameters
```

This menu provides configuration of switch management parameters such as user and administrator privilege mode passwords, Web-based management settings, and management access lists.

Table 72 System Configuration Menu Options

Command Syntax and Usage
errdis Displays the Error Disable Recovery menu. To view menu options, see page 161.
syslog Displays the Syslog menu. To view menu options, see page 162.
sshd Displays the SSH Server menu. To view menu options, see page 164.

Table 72 System Configuration Menu Options

Command Syntax and Usage
radius Displays the RADIUS Authentication menu. To view menu options, see page 166.
tacacs+ Displays the TACACS+ Authentication menu. To view menu options, see page 168.
ldap Displays the LDAP Authentication menu. To view menu options, see page 171.
ntp Displays the Network Time Protocol (NTP) Server menu. To view menu options, see page 173.
ssnmp Displays the System SNMP menu. To view menu options, see page 174.
access Displays the System Access menu. To view menu options, see page 187.
dst Displays the Custom Daylight Savings Time menu. To view menu options, see page 194.
sflow Displays the sFlow menu. To view menu options, see page 195.
date Prompts the user for the system date. The date retains its value when the switch is reset.
time Configures the system time using a 24-hour clock format. The time retains its value when the switch is reset.
timezone Configures the time zone where the switch resides. You are prompted to select your location (continent, country, region) by the timezone wizard. Once a region is selected, the switch updates the time to reflect local changes to Daylight Savings Time, etc.

Table 72 System Configuration Menu Options

Command Syntax and Usage
dlight enable|disable Disables or enables daylight savings time in the system clock. When enabled, the switch will add an extra hour to the system clock so that it is consistent with the local clock. The default value is **disabled**.
idle *<idle timeout in minutes>* Sets the idle timeout for CLI sessions, from 1 to 60 minutes. The default is 10 minutes.
notice *<maximum 1024 character multi-line login notice>* *<'.' to end>* Displays login notice immediately before the "Enter password:" prompt. This notice can contain up to 1024 characters and new lines.
bannr *<string, maximum 80 characters>* Configures a login banner of up to 80 characters. When a user or administrator logs into the switch, the login banner is displayed. It is also displayed as part of the output from the `/info/sys` command.
hprompt disable|enable Enables or disables displaying of the host name (system administrator's name) in the Command Line Interface (CLI).
bootp e|d Enables or disables the use of BOOTP. If you enable BOOTP, the switch will query its BOOTP server for all of the switch IP parameters. The default setting is `enabled`.
dhcp [mgta|mgtb] [enable|disable] Enables or disables Dynamic Host Control Protocol for setting the IP address on the selected management interface. When enabled, the IP address obtained from the DHCP server overrides the static IP address. The default setting is `enabled`.
reminder disable|enable Enables or disables reminder messages in the CLI. The default value is `enabled`.

Table 72 System Configuration Menu Options

Command Syntax and Usage
rstctrl disable|enable Enables or disables the reset control flag. When enabled, the switch continues to function after a crash of the main processor, using the last known Layer 2/3 information. The default value is `enabled`.
cur Displays the current system parameters.

/cfg/sys/errdis
System Error Disable and Recovery Configuration

```
[System ErrDisable Menu]
     timeout  - Set ErrDisable timeout (sec)
     ena      - Enable ErrDisable recovery
     dis      - Disable ErrDisable recovery
     cur      - Display current ErrDisable configuration
```

The Error Disable and Recovery feature allows the switch to automatically disable a port if an error condition is detected on the port. The port remains in the error-disabled state until it is re-enabled manually, or re-enabled automatically by the switch after a timeout period has elapsed. The error-disabled state of a port does not persist across a system reboot.

Table 73 Error Disable Configuration Options

Command Syntax and Usage
timeout *<30 - 86400>* Configures the error-recovery timeout, in seconds. After the timer expires, the switch attempts to re-enable the port. The default value is 300. **Note**: When you change the timeout value, all current error-recovery timers are reset.
ena Globally enables automatic error-recovery for error-disabled ports. The default setting is `disabled`. **Note**: Each port must have error-recovery enabled to participate in automatic error recovery (**/cfg/port** *x*/**errdis/ena**).
dis Globally disables error-recovery for error-disabled ports.
cur Displays the current system Error Disable configuration.

/cfg/sys/syslog
System Host Log Configuration

```
[Syslog Menu]
     host      - Set IP address of first syslog host
     host2     - Set IP address of second syslog host
     sever     - Set the severity of first syslog host
     sever2    - Set the severity of second syslog host
     facil     - Set facility of first syslog host
     facil2    - Set facility of second syslog host
     console   - Enable/disable console output of syslog messages
     log       - Enable/disable syslogging of features
     cur       - Display current syslog settings
```

Table 74 System Host Log Options

Command Syntax and Usage
host *<new syslog host IP address>* Sets the IP address of the first syslog host.
host2 *<new syslog host IP address>* Sets the IP address of the second syslog host.
sever *<syslog host local severity (0–7)>* This option sets the severity level of the first syslog host displayed. The default is 7, which means log all severity levels.
sever2 *<syslog host local severity (0–7)>* This option sets the severity level of the second syslog host displayed. The default is 7, which means, log all severity levels.
facil *<syslog host local facility (0-7)>* This option sets the facility level of the first syslog host displayed. The default is 0.
facil2 *<syslog host local facility (0-7)>* This option sets the facility level of the second syslog host displayed. The default is 0.
console disable|enable Enables or disables delivering syslog messages to the console. When necessary, disabling `console` ensures the switch is not affected by syslog messages. It is enabled by default.

Table 74 System Host Log Options

Command Syntax and Usage
log <*feature* | **all**> <**enable** | **disable**> Displays a list of features for which syslog messages can be generated. You can choose to enable or disable specific features (such as vlans, stg, or servers), or to enable or disable syslog on all available features.
cur Displays the current syslog settings.

/cfg/sys/sshd
SSH Server Configuration

```
[SSHD Menu]
     intrval  - Set Interval for generating the RSA server key
     scpadm   - Set SCP-only admin password
     hkeygen  - Generate the RSA host key
     skeygen  - Generate the RSA server key
     sshport  - Set SSH server port number
     ena      - Enable the SCP apply and save
     dis      - Disable the SCP apply and save
     on       - Turn SSH server ON
     off      - Turn SSH server OFF
     cur      - Display current SSH server configuration
```

This menu enables Secure Shell access from any SSH client. SSH scripts can be viewed by using the `/cfg/dump` command (see page 306).

Table 75 SSH Configuration Options

Command Syntax and Usage
intrval *<0 - 24>* Set the interval, in hours, for auto-generation of the RSA server key.
scpadm Set the administration password for SCP access.
hkeygen Generate the RSA host key.
skeygen Generate the RSA server key.
sshport *<TCP port number>* Sets the SSH server port number.
ena Enables the SCP apply and save.
dis Disables the SCP apply and save.
on Enables the SSH server.

Table 75 SSH Configuration Options

Command Syntax and Usage
off Disables the SSH server.
cur Displays the current SSH server configuration.

/cfg/sys/radius
RADIUS Server Configuration

```
[RADIUS Server Menu]
    prisrv  - Set primary RADIUS server address
    secsrv  - Set secondary RADIUS server address
    secret  - Set RADIUS secret
    secret2 - Set secondary RADIUS server secret
    port    - Set RADIUS port
    retries - Set RADIUS server retries
    timeout - Set RADIUS server timeout
    bckdoor - Enable/disable RADIUS backdoor for telnet/ssh/http/https
    secbd    - Enable/disable RADIUS secure backdoor for
               telnet/ssh/http/https
    on      - Turn RADIUS authentication ON
    off     - Turn RADIUS authentication OFF
    cur     - Display current RADIUS configuration
```

Table 76 System Configuration Options

Command Syntax and Usage
prisrv *<IP address>* Sets the primary RADIUS server address.
secsrv *<IP address>* Sets the secondary RADIUS server address.
secret *<1-32 character secret>* This is the shared secret between the switch and the RADIUS server(s).
secret2 *<1-32 character secret>* This is the secondary shared secret between the switch and the RADIUS server(s).
port *<RADIUS port>* Enter the number of the UDP port to be configured, between 1500 - 3000. The default is 1645.
retries *<RADIUS server retries (1-3)>* Sets the number of failed authentication requests before switching to a different RADIUS server. The default is 3 requests.
timeout *<RADIUS server timeout seconds (1-10)>* Sets the amount of time, in seconds, before a RADIUS server authentication attempt is considered to have failed. The default is 3 seconds.

Table 76 System Configuration Options

Command Syntax and Usage
bckdoor disable|enable Enables or disables the RADIUS backdoor for Telnet/SSH/HTTP/HTTPS. The default value is `disabled`. To obtain the RADIUS backdoor password for your switch, contact your Service and Support line.
secbd enable|disable Enables or disables the RADIUS back door using secure password for telnet/SSH/HTTP/HTTPS. This command does not apply when backdoor (`telnet`) is enabled.
on Enables the RADIUS server.
off Disables the RADIUS server.
cur Displays the current RADIUS server parameters.

/cfg/sys/tacacs+
TACACS+ Server Configuration

TACACS (Terminal Access Controller Access Control system) is an authentication protocol that allows a remote access server to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system. TACACS is an encryption protocol, and therefore less secure than TACACS+ and Remote Authentication Dial-In User Service (RADIUS) protocols. (Both TACACS and TACACS+ are described in RFC 1492.)

TACACS+ protocol is more reliable than RADIUS, as TACACS+ uses the Transmission Control Protocol (TCP) whereas RADIUS uses the User Datagram Protocol (UDP). Also, RADIUS combines authentication and authorization in a user profile, whereas TACACS+ separates the two operations.

TACACS+ offers the following advantages over RADIUS as the authentication device:

- TACACS+ is TCP-based, so it facilitates connection-oriented traffic.
- It supports full-packet encryption, as opposed to password-only in authentication requests.
- It supports de-coupled authentication, authorization, and accounting.

```
[TACACS+ Server Menu]
    prisrv   - Set IP address of primary TACACS+ server
    secsrv   - Set IP address of secondary TACACS+ server
    secret   - Set secret for primary TACACS+ server
    secret2  - Set secret for secondary TACACS+ server
    port     - Set TACACS+ port number
    retries  - Set number of TACACS+ server retries
    timeout  - Set timeout value of TACACS+ server retries
    usermap  - Set user privilege mappings
    bckdoor  - Enable/disable TACACS+ backdoor for telnet/ssh/http/hhtps
    secbd    - Enable/disable TACACS+ secure backdoor
    cmap     - Enable/disable TACACS+ new privilege level mapping
    cauth    - Enable/disable TACACS+ command authorization
    clog     - Enable/disable TACACS+ command logging
    dreq     - Enable/disable TACACS+ directed request
    on       - Enable TACACS+ authentication
    off      - Disable TACACS+ authentication
    cur      - Display current TACACS+ settings
```

Table 77 TACACS+ Server Options

Command Syntax and Usage
prisrv *<IP address>* **[-ma|-mgta|-mb|-mgtb|-d|-data]** Defines the primary TACACS+ server address and the interface port to use to send TACACS+ requests.
secsrv *<IP address>* **[-ma|-mgta|-mb|-mgtb|-d|-data]** Defines the secondary TACACS+ server address and the interface port to use to send TACACS+ requests.
secret *<1-32 character secret>* This is the shared secret between the switch and the TACACS+ server(s).
secret2 *<1-32 character secret>* This is the secondary shared secret between the switch and the TACACS+ server(s).
port *<TACACS port>* Enter the number of the TCP port to be configured, between 1 - 65000. The default is 49.
retries *<TACACS server retries, 1-3>* Sets the number of failed authentication requests before switching to a different TACACS+ server. The default is 3 requests.
timeout *<TACACS server timeout seconds, 4-15>* Sets the amount of time, in seconds, before a TACACS+ server authentication attempt is considered to have failed. The default is 5 seconds.
usermap *<0-15>* **user|oper|admin|none** Maps a TACACS+ authorization level to a switch user level. Enter a TACACS+ authorization level (0-15), followed by the corresponding switch user level.
bckdoor disable|enable Enables or disables the TACACS+ back door for Telnet, SSH/SCP, or HTTP/HTTPS. Enabling this feature allows you to bypass the TACACS+ servers. It is recommended that you use Secure Backdoor to ensure the switch is secured, because Secure Backdoor disallows access through the back door when the TACACS+ servers are responding. The default setting is `disabled`. To obtain the TACACS+ backdoor password for your switch, contact your Service and Support line.

Table 77 TACACS+ Server Options

Command Syntax and Usage
secbd enable|disable Enables or disables TACACS+ secure back door access through Telnet, SSH/SCP, or HTTP/HTTPS only when the TACACS+ servers are not responding. This feature is recommended to permit access to the switch when the TACACS+ servers become unresponsive. If no back door is enabled, the only way to gain access when TACACS+ servers are unresponsive is to use the back door via the console port. The default setting is `disabled`.
cmap enable|disable Enables or disables TACACS+ privilege-level mapping. The default value is `disabled`.
cauth disable|enable Enables or disables TACACS+ command authorization.
clog disable|enable Enables or disables TACACS+ command logging.
dreq disable|enable Enables or disables TACACS+ directed request, which uses a specified TACACS+ server for authentication, authorization, accounting. When enabled, When directed-request is enabled, each user must add a configured TACACS+ server hostname to the username (for example, `username@hostname`) during login. This command allows the following options: □ Restricted: Only the username is sent to the specified TACACS+ server. □ No-truncate: The entire login string is sent to the TACACS+ server.
on Enables the TACACS+ server. This is the default setting.
off Disables the TACACS+ server.
cur Displays current TACACS+ configuration parameters.

/cfg/sys/ldap
LDAP Server Configuration

LDAP (Lightweight Directory Access Protocol) is an authentication protocol that allows a remote access server to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system.

```
[LDAP Server Menu]
     prisrv   - Set IP address of primary LDAP server
     secsrv   - Set IP address of secondary LDAP server
     port     - Set LDAP port number
     retries  - Set number of LDAP server retries
     timeout  - Set timeout value of LDAP server retries
     domain   - Set domain name
     bckdoor  - Enable/disable LDAP backdoor for telnet/ssh/http/https
     on       - Enable LDAP authentication
     off      - Disable LDAP authentication
     cur      - Display current LDAP settings
```

Table 78 LDAP Server Options

Command Syntax and Usage
prisrv *<IP address>* Defines the primary LDAP server address.
secsrv *<IP address>* Defines the secondary LDAP server address.
port *<LDAP port>* Enter the number of the TCP port to be configured, between 1 - 65000. The default is 389.
retries *<LDAP server retries, 1-3>* Sets the number of failed authentication requests before switching to a different LDAP server. The default is 3 requests.
timeout *<LDAP server timeout seconds, 4-15>* Sets the amount of time, in seconds, before a LDAP server authentication attempt is considered to have failed. The default is 5 seconds.
domain *<domain name (1-128 characters)>* | **none** Sets the domain name for the LDAP server. Enter the full path for your organization. For example: `ou=people,dc=mydomain,dc=com`

Table 78 LDAP Server Options

Command Syntax and Usage
bckdoor disable|enable Enables or disables the LDAP back door for Telnet, SSH/SCP, or HTTP/HTTPS. The default setting is `disabled`. To obtain the LDAP backdoor password for your switch, contact your Service and Support line.
on Enables the LDAP server.
off Disables the LDAP server. This is the default setting.
cur Displays current LDAP configuration parameters.

/cfg/sys/ntp
NTP Server Configuration

```
[NTP Server Menu]
      prisrv  - Set primary NTP server hostname|IP address
      secsrv  - Set secondary NTP server hostname|IP address
      intrval - Set NTP server resync interval
      on      - Turn NTP service ON
      off     - Turn NTP service OFF
      cur     - Display current NTP configuration
```

This menu enables you to synchronize the switch clock to a Network Time Protocol (NTP) server. By default, this option is disabled.

Table 79 NTP Configuration Options

Command Syntax and Usage
prisrv {<*host name*>**|**<*IP address*>**}** Prompts for the hostname or IP addresses of the primary NTP server to which you want to synchronize the switch clock.
secsrv {<*host name*>**|**<*IP address*>**}** Prompts for the hostname or IP addresses of the secondary NTP server to which you want to synchronize the switch clock.
intrval <*5-44640*> Specifies the time interval, in minutes, to re-synchronize the switch clock with the NTP server.
on Enables the NTP synchronization service.
off Disables the NTP synchronization service.
cur Displays the current NTP service settings.

/cfg/sys/ssnmp
System SNMP Configuration

```
[System SNMP Menu]
     snmpv3   - SNMPv3 Menu
     name     - Set SNMP "sysName"
     locn     - Set SNMP "sysLocation"
     cont     - Set SNMP "sysContact"
     rcomm    - Set SNMP read community string
     wcomm    - Set SNMP write community string
     trsrc    - Set SNMP trap source interface for SNMPv1
     timeout  - Set timeout for the SNMP state machine
     auth     - Enable/disable SNMP "sysAuthenTrap"
     linkt    - Enable/disable SNMP link up/down trap
     cur      - Display current SNMP configuration
```

BLADE OS supports SNMP-based network management. In SNMP model of network management, a management station (client/manager) accesses a set of variables known as MIBs (Management Information Base) provided by the managed device (agent). If you are running an SNMP network management station on your network, you can manage the switch using the following standard SNMP MIBs:

- MIB II (RFC 1213)
- Ethernet MIB (RFC 1643)
- Bridge MIB (RFC 1493)

An SNMP agent is a software process on the managed device that listens on UDP port 161 for SNMP messages. Each SNMP message sent to the agent contains a list of management objects to retrieve or to modify.

SNMP parameters that can be modified include:

- System name
- System location
- System contact
- Use of the SNMP system authentication trap function
- Read community string
- Write community string
- Trap community strings

Table 80 System SNMP Options

Command Syntax and Usage
snmpv3 Displays SNMPv3 menu. To view menu options, see page 176.
name *<1-64 characters>* Configures the name for the system.
locn *<1-64 characters>* Configures the name of the system location.
cont *<1-64 characters>* Configures the name of the system contact.
rcomm *<1-32 characters>* Configures the SNMP read community string. The read community string controls SNMP "get" access to the switch. The default read community string is *public*.
wcomm *<1-32 characters>* Configures the SNMP write community string. The write community string controls SNMP "set" and "get" access to the switch. The default write community string is *private*.
trsrc *<interface number>* Configures the source interface for SNMP traps. The default value is interface 1. To send traps through management port A, specify interface 127.
timeout *<1-30>* Set the timeout value for the SNMP state machine, in minutes.
auth disable|enable Enables or disables the use of the system authentication trap facility. The default setting is `disabled`.
linkt *<port>* [**disable|enable**] Enables or disables the sending of SNMP link up and link down traps. The default setting is `enabled`.
cur Displays the current SNMP configuration.

/cfg/sys/ssnmp/snmpv3
SNMPv3 Configuration

SNMP version 3 (SNMPv3) is an extensible SNMP Framework that supplements the SNMPv2 Framework by supporting the following:

- a new SNMP message format
- security for messages
- access control
- remote configuration of SNMP parameters

For more details on the SNMPv3 architecture please refer to RFC2271 to RFC2276.

```
[SNMPv3 Menu]
     usm       - usmUser Table menu
     view      - vacmViewTreeFamily Table menu
     access    - vacmAccess Table menu
     group     - vacmSecurityToGroup Table menu
     comm      - community Table menu
     taddr     - targetAddr Table menu
     tparam    - targetParams Table menu
     notify    - notify Table menu
     v1v2      - Enable/disable V1/V2 access
     cur       - Display current SNMPv3 configuration
```

Table 81 SNMPv3 Configuration Options

Command Syntax and Usage
usm *<usmUser number [1-16]>* Defines a user security model (USM) entry for an authorized user. You can also configure this entry through SNMP. To view menu options, see page 178.
view *<vacmViewTreeFamily number [1-128]>* Allows you to create different MIB views. To view menu options, see page 180.
access *<vacmAccess number [1-32]>* Configures the access rights. The View-based Access Control Model defines a set of services that an application can use for checking access rights of the user. You need access control when you have to process retrieval or modification request from an SNMP entity. To view menu options, see page 181.

Table 81 SNMPv3 Configuration Options

group *<vacmSecurityToGroup number [1-16]>*	Maps the user name to the access group names and their access rights needed to access SNMP management objects. A group defines the access rights assigned to all names that belong to a particular group. To view menu options, see page 182.
comm *<snmpCommunity number [1-16]>*	The community table contains objects for mapping community strings and version-independent SNMP message parameters. To view menu options, see page 183.
taddr *<snmpTargetAddr number [1-16]>*	Allows you to configure destination information, consisting of a transport domain and a transport address. This is also termed as transport endpoint. The SNMP MIB provides a mechanism for performing source address validation on incoming requests, and for selecting community strings based on target addresses for outgoing notifications. To view menu options, see page 184.
tparam *<target params index [1-16]>*	Allows you to configure SNMP parameters, consisting of message processing model, security model, security level, and security name information. There may be multiple transport endpoints associated with a particular set of SNMP parameters, or a particular transport endpoint may be associated with several sets of SNMP parameters. To view menu options, see page 185.
notify *<notify index [1-16]>*	A notification application typically monitors a system for particular events or conditions, and generates Notification-Class messages based on these events or conditions. To view menu options, see page 186.
v1v2 disable|enable	Allows you to enable or disable the access to SNMP version 1 and version 2. The default setting is enabled.
cur	Displays the current SNMPv3 configuration.

/cfg/sys/ssnmp/snmpv3/usm
User Security Model Configuration

You can make use of a defined set of user identities using this Security Model. An SNMP engine must have the knowledge of applicable attributes of a user.

This menu helps you create a user security model entry for an authorized user. You need to provide a security name to create the USM entry.

```
[SNMPv3 usmUser 1 Menu]
     name      - Set USM user name
     auth      - Set authentication protocol
     authpw    - Set authentication password
     priv      - Set privacy protocol
     privpw    - Set privacy password
     del       - Delete usmUser entry
     cur       - Display current usmUser configuration
```

Table 82 User Security Model Configuration Options

Command Syntax and Usage
name *<1-32 characters>* Defines a string that represents the name of the user. This is the login name that you need in order to access the switch.
auth md5|**sha**|**none** Configures the authentication protocol between HMAC-MD5-96 or HMAC-SHA-96. The default algorithm is none.
authpw Allows you to create or change your password for authentication. If you selected an authentication algorithm using the above command, you need to provide a password, otherwise you will get an error message during validation.
priv des|**none** Configures the type of privacy protocol on your switch. The privacy protocol protects messages from disclosure. The options are des (CBC-DES Symmetric Encryption Protocol) or none. If you specify des as the privacy protocol, then make sure that you have selected one of the authentication protocols (MD5 or HMAC-SHA-96). If you select none as the authentication protocol, you will get an error message.
privpw Defines the privacy password.

Table 82 User Security Model Configuration Options

Command Syntax and Usage
del Deletes the selected USM user entries.
cur Displays the selected USM user entries.

/cfg/sys/ssnmp/snmpv3/view
SNMPv3 View Configuration

```
[SNMPv3 vacmViewTreeFamily 1 Menu]
    name    - Set view name
    tree    - Set MIB subtree(OID) which defines a family of view subtrees
    mask    - Set view mask
    type    - Set view type
    del     - Delete vacmViewTreeFamily entry
    cur     - Display current vacmViewTreeFamily configuration
```

Table 83 SNMPv3 View Options

Command Syntax and Usage
name *<1-32 characters>* Defines the name for a family of view subtrees.
tree *<object identifier, such as 1.3.6.1.2.1.1.1.0 (1-32 characters)>* Defines the MIB tree which, when combined with the corresponding mask, defines a family of view subtrees.
mask *<bitmask, 1-32 characters>* Configures the bit mask, which in combination with the corresponding tree, defines a family of view subtrees.
type included|excluded This command indicates whether the corresponding instances of `vacmViewTreeFamilySubtree` and `vacmViewTreeFamilyMask` define a family of view subtrees, which is included in or excluded from the MIB view.
del Deletes the `vacmViewTreeFamily` group entry.
cur Displays the current `vacmViewTreeFamily` configuration.

/cfg/sys/ssnmp/snmpv3/access <1-32>
View-Based Access Control Model Configuration

The view-based Access Control Model defines a set of services that an application can use for checking access rights of the user. Access control is needed when the user has to process SNMP retrieval or modification request from an SNMP entity.

```
[SNMPv3 vacmAccess 1 Menu]
     name      - Set group name
     model     - Set security model
     level     - Set minimum level of security
     rview     - Set read view index
     wview     - Set write view index
     nview     - Set notify view index
     del       - Delete vacmAccess entry
     cur       - Display current vacmAccess configuration
```

Table 84 View-based Access Control Model Options

Command Syntax and Usage
name *<1-32 characters>* Defines the name of the group.
model usm|snmpv1|snmpv2 Allows you to select the security model to be used.
level noAuthNoPriv|authNoPriv|authPriv Defines the minimum level of security required to gain access rights. The level `noAuthNoPriv` means that the SNMP message will be sent without authentication and without using a privacy protocol. The level `authNoPriv` means that the SNMP message will be sent with authentication but without using a privacy protocol. The `authPriv` means that the SNMP message will be sent both with authentication and using a privacy protocol.
rview *<1-32 characters>* Defines a read view name that allows you read access to a particular MIB view. If the value is empty or if there is no active MIB view having this value then no access is granted.
wview *<1-32 characters>* Defines a write view name that allows you write access to the MIB view. If the value is empty or if there is no active MIB view having this value then no access is granted.
nview *<1-32 characters>* Defines a long notify view name that allows you notify access to the MIB view.

Table 84 View-based Access Control Model Options

Command Syntax and Usage
del Deletes the View-based Access Control entry.
cur Displays the View-based Access Control configuration.

/cfg/sys/ssnmp/snmpv3/group
SNMPv3 Group Configuration

```
[SNMPv3 vacmSecurityToGroup 1 Menu]
     model     - Set security model
     uname     - Set USM user name
     gname     - Set group gname
     del       - Delete vacmSecurityToGroup entry
     cur       - Display current vacmSecurityToGroup configuration
```

Table 85 SNMPv3 Group Options

Command Syntax and Usage
model usm|**snmpv1**|**snmpv2** Defines the security model.
uname *<1-32 characters>* Sets the user name as defined in `/cfg/sys/ssnmp/snmpv3/usm/name` on page 178.
gname *<1-32 characters>* The name for the access group as defined in `/cfg/sys/ssnmp/snmpv3/access/name` on page 181.
del Deletes the `vacmSecurityToGroup` entry.
cur Displays the current `vacmSecurityToGroup` configuration.

/cfg/sys/ssnmp/snmpv3/comm
SNMPv3 Community Table Configuration

This command is used for configuring the community table entry. The configured entry is stored in the community table list in the SNMP engine. This table is used to configure community strings in the Local Configuration Datastore (LCD) of SNMP engine.

```
[SNMPv3 snmpCommunityTable 1 Menu]
     index    - Set community index
     name     - Set community string
     uname    - Set USM user name
     tag      - Set community tag
     del      - Delete communityTable entry
     cur      - Display current communityTable configuration
```

Table 86 SNMPv3 Community Table Configuration Options

Command Syntax and Usage
index *<1-32 characters>* Configures the unique index value of a row in this table.
name *<1-32 characters>* Defines the user name as defined in the `/cfg/sys/ssnmp/snmpv3/usm/name` command.
uname *<1-32 characters>* Defines a readable text string that represents the corresponding value of an SNMP community name in a security model.
tag *<1-255 characters>* Configures a tag that specifies a set of transport endpoints to which a command responder application sends an SNMP trap.
del Deletes the community table entry.
cur Displays the community table configuration.

/cfg/sys/ssnmp/snmpv3/taddr
SNMPv3 Target Address Table Configuration

This command is used to configure the target transport entry. The configured entry is stored in the target address table list in the SNMP engine. This table of transport addresses is used in the generation of SNMP messages.

```
[SNMPv3 snmpTargetAddrTable 1 Menu]
     name     - Set target address name
     addr     - Set target transport address IP
     port     - Set target transport address port
     taglist  - Set tag list
     pname    - Set targetParams name
     del      - Delete targetAddrTable entry
     cur      - Display current targetAddrTable configuration
```

Table 87 Target Address Table Options

Command Syntax and Usage
name *<1-32 characters>* Defines the locally arbitrary, but unique identifier, target address name associated with this entry.
addr *<transport IP address>* Configures a transport IPv4 address that can be used in the generation of SNMP traps.
port *<transport address port>* Configures a transport address port that can be used in the generation of SNMP traps.
taglist *<1-255 characters>* Allows you to configure a list of tags that are used to select target addresses for a particular operation.
pname *<1-32 characters>* Defines the name as defined in the `/cfg/sys/ssnmp/snmpv3/tparam/name` command on page 185.
del Deletes the Target Address Table entry.
cur Displays the current Target Address Table configuration.

/cfg/sys/ssnmp/snmpv3/tparam
SNMPv3 Target Parameters Table Configuration

You can configure the target parameters entry and store it in the target parameters table in the SNMP engine. This table contains parameters that are used to generate a message. The parameters include the message processing model (for example: SNMPv3, SNMPv2c, SNMPv1), the security model (for example: USM), the security name, and the security level (`noAuthnoPriv`, `authNoPriv`, or `authPriv`).

```
[SNMPv3 snmpTargetParamsTable 1 Menu]
     name      - Set target params name
     mpmodel   - Set message processing model
     model     - Set security model
     uname     - Set USM user name
     level     - Set minimum level of security
     del       - Delete targetParamsTable entry
     cur       - Display current targetParamsTable configuration
```

Table 88 Target Parameters Table Configuration Options

Command Syntax and Usage
name *<1-32 characters>* Defines the locally arbitrary, but unique identifier that is associated with this entry.
mpmodel snmpv1|**snmpv2c**|**snmpv3** Configures the message processing model that is used to generate SNMP messages.
model usm|**snmpv1**|**snmpv2** Allows you to select the security model to be used when generating the SNMP messages.
uname *<1-32 characters>* Defines the name that identifies the user in the USM table (page 178) on whose behalf the SNMP messages are generated using this entry.
level noAuthNoPriv|**authNoPriv**|**authPriv** Allows you to select the level of security to be used when generating the SNMP messages using this entry. The level `noAuthNoPriv` means that the SNMP message will be sent without authentication and without using a privacy protocol. The level `authNoPriv` means that the SNMP message will be sent with authentication but without using a privacy protocol. The `authPriv` means that the SNMP message will be sent both with authentication and using a privacy protocol.

Table 88 Target Parameters Table Configuration Options

Command Syntax and Usage
del Deletes the `targetParamsTable` entry.
cur Displays the current `targetParamsTable` configuration.

/cfg/sys/ssnmp/snmpv3/notify
SNMPv3 Notify Table Configuration

SNMPv3 uses Notification Originator to send out traps. A notification typically monitors a system for particular events or conditions, and generates Notification-Class messages based on these events or conditions.

```
[SNMPv3 snmpNotifyTable 1  Menu]
     name      - Set notify name
     tag       - Set notify tag
     del       - Delete notifyTable entry
     cur       - Display current notifyTable configuration
```

Table 89 Notify Table Options

Command Syntax and Usage
name *<1-32 characters>* Defines a locally arbitrary but unique identifier associated with this SNMP notify entry.
tag *<1-255 characters>* Allows you to configure a tag that contains a tag value which is used to select entries in the Target Address Table. Any entry in the `snmpTargetAddrTable`, that matches the value of this tag is selected.
del Deletes the notify table entry.
cur Displays the current notify table configuration.

/cfg/sys/access
System Access Configuration

```
[System Access Menu]
     mgmt      - Management Network Definition Menu
     user      - User Access Control Menu (passwords)
     https     - HTTPS Web Access Menu
     snmp      - Set SNMP access control
     tnport    - Set Telnet server port number
     tport     - Set the TFTP Port for the system
     wport     - Set HTTP (Web) server port number
     http      - Enable/disable HTTP (Web) access
     tnet      - Enable/disable Telnet access
     tsbbi     - Enable/disable Telnet/SSH configuration from BBI
     userbbi   - Enable/disable user configuration from BBI
     cur       - Display current system access configuration
```

Table 90 System Access Options

Command Syntax and Usage
mgmt Displays the Management Configuration menu. To view menu options, see page 189.
user Displays the User Access Control menu. To view menu options, see page 190.
https Displays the HTTPS menu. To view menu options, see page 193.
snmp disable|**read-only**|**read-write** Disables or provides read-only/write-read SNMP access.
tnport *<TCP port number>* Sets an optional telnet server port number for cases where the server listens for telnet sessions on a non-standard port.
tport *<TFTP port number (1-65535)>* Sets the TFTP port for the switch. The default is port 69.
wport *<TCP port number (1-65535)>* Sets the switch port used for serving switch Web content. The default is HTTP port 80. If Global Server Load Balancing is to be used, set this to a different port (such as 8080).

Table 90 System Access Options

Command Syntax and Usage
http disable|enable Enables or disables HTTP (Web) access to the Browser-Based Interface. It is enabled by default.
tnet enable|disable Enables or disables Telnet access. This command is enabled by default.
tsbbi enable|disable Enables or disables Telnet/SSH configuration access through the Browser-Based Interface (BBI).
userbbi enable|disable Enables or disables user configuration access through the Browser-Based Interface (BBI).
cur Displays the current system access parameters.

/cfg/sys/access/mgmt
Management Networks Configuration

```
[Management Networks Menu]
     add      - Add mgmt network definition
     rem      - Remove mgmt network definition
     cur      - Display current mgmt network definitions
     clear    - Clear current mgmt network definitions
```

This menu is used to define IP address ranges which are allowed to access the switch for management purposes.

Table 91 Management Network Options

Command Syntax and Usage
add *<mgmt network address> <mgmt network mask>* Adds a defined network through which switch access is allowed through Telnet, SNMP, RIP, or the Browser-Based Interface. A range of IP addresses is produced when used with a network mask address. Specify an IP address and mask address in dotted-decimal notation. **Note**: If you configure the management network without including the switch interfaces, the configuration causes the Firewall Load Balancing health checks to fail and creates a "Network Down" state on the network.
rem *<mgmt network address> <mgmt network mask>* Removes a defined network, which consists of a management network address and a management network mask address.
cur Displays the current configuration.
clear Removes all defined management networks.

/cfg/sys/access/user
User Access Control Configuration

```
[User Access Control Menu]
     uid      - User ID Menu
     eject    - Eject user
     usrpw    - Set user password (user)
     opw      - Set operator password (oper)
     admpw    - Set administrator password (admin)
     strongpw - Strong password menu
     cur      - Display current user status
```

Note – Passwords can be a maximum of 128 characters.

Table 92 User Access Control Options

Command Syntax and Usage
uid *<User ID (1-10)>* Displays the User ID menu. To view menu options, see page 191.
eject user|**oper**|**admin**|**<***user name***>** Ejects the specified user from the G8124.
usrpw *<1-128 characters>* Sets the user (`user`) password. This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password.
opw *<1-128 characters>* Sets the operator (`oper`) password. This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password.
admpw *<1-128 characters>* Sets the administrator (`admin`) password. This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password. Access includes "`oper`" functions.

Table 92 User Access Control Options

Command Syntax and Usage
strongpw Displays the Strong User Password menu. To view menu options, see page 192.
cur Displays the current user status.

/cfg/sys/access/user/uid <1-10>
System User ID Configuration

```
[User ID 1 Menu]
     cos       - Set class of service
     name      - Set user name
     pswd      - Set user password
     ena       - Enable user ID
     dis       - Disable user ID
     del       - Delete user ID
     cur       - Display current user configuration
```

Table 93 User ID Configuration Options

Command Syntax and Usage
cos *<user | oper | admin>* Sets the Class-of-Service to define the user's authority level. BLADE OS defines these levels as: User, Operator, and Administrator, with User being the most restricted level.
name *<1-8 characters>* Sets the user name (maximum of eight characters).
pswd *<1-128 characters>* Sets the user password.
ena Enables the user ID.
dis Disables the user ID.

Table 93 User ID Configuration Options

Command Syntax and Usage
del Deletes the user ID.
cur Displays the current user ID configuration.

/cfg/sys/access/user/strongpw
Strong Password Configuration

```
[Strong Pwd Menu]
     ena       - Enable usage of strong passwords
     dis       - Disable usage of strong passwords
     expiry    - Set password validity
     warning   - Set warning days before pswd expiry
     faillog   - Set number of failed logins for security notification
     cur       - Display current strong password configuration
```

Table 94 Strong Password Options

Command Syntax and Usage
ena Enables Strong Password requirement.
dis Disables Strong Password requirement.
expiry *<1-365>* Configures the number of days allowed before the password must be changed.
warning *<1-365>* Configures the number of days before password expiration, that a warning is issued to users.
faillog *<1-255>* Configures the number of failed login attempts allowed before a security notification is logged.
cur Displays the current Strong Password configuration.

/cfg/sys/access/https
HTTPS Access Configuration

```
[https Menu]
     access   - Enable/Disable HTTPS Web access
     port     - HTTPS WebServer port number
     generate - Generate self-signed HTTPS server certificate
     certSave - save HTTPS certificate
     cur      - Display current SSL Web Access configuration
```

Table 95 HTTPS Access Configuration Options

Command Syntax and Usage
access ena|dis Enables or disables BBI access (Web access) using HTTPS.
port *<TCP port number>* Defines the HTTPS Web server port number.
generate Allows you to generate a certificate to connect to the SSL to be used during the key exchange. A default certificate is created when HTTPS is enabled for the first time. The user can create a new certificate defining the information that they want to be used in the various fields. For example: □ Country Name (2 letter code) []: CA □ State or Province Name (full name) []: Ontario □ Locality Name (for example, city) []: Ottawa □ Organization Name (for example, company) []: Blade □ Organizational Unit Name (for example, section) []: Datacenter □ Common Name (for example, user's name) []: Mr Smith □ Email (for example, email address) []: info@bladenetwork.net You will be asked to confirm if you want to generate the certificate. It will take approximately 30 seconds to generate the certificate. Then the switch will restart SSL agent.
certSave Allows the client, or the Web browser, to accept the certificate and save the certificate to Flash to be used when the switch is rebooted.
cur Displays the current SSL Web Access configuration.

/cfg/sys/dst
Custom Daylight Savings Time Configuration

```
[Custom DST Menu]
     dststart - Set the DST start day
     dstend   - Set the DST stop day
     ena      - Enable custom DST
     dis      - Disable custom DST
     cur      - Display custom DST configuration
```

Use this menu to configure custom Daylight Savings Time. The DST will be defined by two rules, the start rule and end rule. The rules specify the date and time when the DST starts and finishes. These dates are represented as specific calendar dates or as relative offsets in a month (for example, 'the second Sunday of September').

Relative offset example:
2070901 = Second Sunday of September, at 1:00 a.m.

Calendar date example:
0070901 = September 7, at 1:00 a.m.

Table 96 Custom DST Configuration Options

Command Syntax and Usage
dststart {<*WDDMMhh*>**}** Configures the start date for custom DST, as follows: `WDMMhh` W = week (0-5, where 0 means use the calender date) D = day of the week (01-07, where 01 is Monday) MM = month (1-12) hh = hour (0-23)
dstend {<*WDDMMhh*>**}** Configures the end date for custom DST, as follows: `WDMMhh` W = week (0-5, where 0 means use the calender date) D = day of the week (01-07, where 01 is Monday) MM = month (1-12) hh = hour (0-23)
ena Enables the Custom Daylight Savings Time settings.

Table 96 Custom DST Configuration Options

Command Syntax and Usage
dis Disables the Custom Daylight Savings Time settings.
cur Displays the current Custom DST configuration.

/cfg/sys/sflow
sFlow Configuration

```
[sFlow Menu]
     ena       - Enable sFlow
     dis       - Disable sFlow
     saddress  - Set the sFlow Analyzer IP address
     sport     - Set the sFlow Analyzer port
     port      - sFlow port Menu
     cur       - Display sFlow configuration
```

sFlow is a sampling method used for monitoring high speed switched networks. Use this menu to configure the sFlow agent on the switch.

Table 97 sFlow Configuration Options

Command Syntax and Usage
ena Enables the sFlow agent.
dis Disables the sFlow agent.
saddress *<IP address>* **[-ma|-mgta|-mb|-mgtb|-d|-data]** Defines the sFlow server address and interface port.
sport *<1-65535>* Configures the UDP port for the sFlow server. The default value is 6343.

Table 97 sFlow Configuration Options

Command Syntax and Usage
port *<port alias or number>* Configures the sFlow interface port.
cur Displays the current sFlow configuration.

/cfg/sys/sflow/port *<port alias or number>*
sFlow Port Configuration

```
[sFlow Port Menu]
     polling  - Set the sFlow polling interval
     sampling - Set the sFlow sampling rate
     cur      - Display sFlow port configuration
```

Use this menu to configure the sFlow port on the switch.

Table 98 sFlow Port Configuration Options

Command Syntax and Usage
polling *<5-60>*|**0** Configures the sFlow polling interval, in seconds. The default value is 0 (disabled).
sampling *<1-16777215>*|**0** Configures the sFlow sampling rate, in packets per sample. The default value is 0 (disabled).
cur Displays the current sFlow port configuration.

/cfg/port <port alias or number>

Port Configuration Menu

```
[Port 1 Menu]
     errdis   - ErrDisable Menu
     gig      - Gig Phy Menu
     aclqos   - Acl/Qos Configuration Menu
     stp      - STP Menu - for PVRST only
     8021ppri - Set default 802.1p priority
     pvid     - Set default port VLAN id
     name     - Set port name
     bpdugrd  - Enable/disable BPDU Guard
     dscpmrk  - Enable/disable DSCP remarking for port
     learn    - Enable/Disable FDB Learning for port
     tag      - Enable/disable VLAN tagging for port
     tagpvid  - Enable/disable tagging on pvid
     floodblk - Enable/disable Port flood blocking
     macnotif - Enable/disable MAC address notification
     brate    - Set BroadCast Threshold
     mrate    - Set MultiCast Threshold
     drate    - Set Dest. Lookup Fail Threshold
     ena      - Enable port
     dis      - Disable port
     cur      - Display current port configuration
```

Use the Port Configuration menu to configure settings for interface ports.

Table 99 Port Configuration Menu

Command Syntax and Usage
errdis Displays the Error Disable and Recovery menu. To view menu options, see page 200.
gig If a port is configured to support Gigabit Ethernet, this option displays the Gigabit Ethernet Physical Link menu. To view menu options, see page 201.
aclqos Displays the ACL/QoS Configuration menu. To view menu options, see page 202.
stp Displays the Spanning Tree Port menu. To view menu options, see page 203.

Table 99 Port Configuration Menu

Command Syntax and Usage
8021ppri *<0-7>* Configures the port's 802.1p priority level.
pvid *<VLAN number>* Sets the default VLAN number which will be used to forward frames which are not VLAN tagged. The default number is 1 for non-management ports.
name *<1-64 characters>* | **none** Sets a name for the port. The assigned port name appears next to the port number on some information and statistics screens. The default setting is `none`.
bpdugrd e|d Enables or disables BPDU guard, to avoid Spanning-Tree loops on ports with Port Fast Forwarding enabled (**/cfg/l2/stp** *x*/**port** *x*/**fastfwd ena**), or ports configured as `edge` ports.
dscpmark e|d Enables or disables DSCP re-marking on a port. The default setting is `disabled`.
learn disable|enable Enables or disables FDB learning on the port.
tag disable|enable Disables or enables VLAN tagging for this port. The default setting is `disabled`.
tagpvid disable|enable Disables or enables VLAN tag persistence. When disabled, the VLAN tag is removed from packets whose VLAN tag matches the port PVID. The default setting is `disabled`.
floodblk disable|enable Enables or disables port Flood Blocking. When enabled, unicast and multicast packets with unknown destination MAC addresses are blocked from the port.
macnotif enable|disable Enables or disables MAC Address Notification. With MAC Address Notification enabled, the switch generates a syslog message when a MAC address is added or removed from the MAC address table.

Table 99 Port Configuration Menu

Command Syntax and Usage
brate <*0-262143*>**|dis** Limits the number of broadcast packets per second to the specified value. If disabled (`dis`), the port forwards all broadcast packets.
mrate <*0-262143*>**|dis** Limits the number of multicast packets per second to the specified value. If disabled (`dis`), the port forwards all multicast packets.
drate <*0-262143*>**|dis** Limits the number of unknown unicast packets per second to the specified value. If disabled (`dis`), the port forwards all unknown unicast packets.
ena Enables the port.
dis Disables the port. (To temporarily disable a port without changing its configuration attributes, refer to "Temporarily Disabling a Port" on page 199.)
cur Displays current port parameters.

Temporarily Disabling a Port

To temporarily disable a port without changing its stored configuration attributes, enter the following command at any prompt:

```
Main# /oper/port <port alias or number>/dis
```

Because this configuration sets a temporary state for the port, you do not need to use `apply` or `save`. The port state will revert to its original configuration when the G8124 is reset. See the "Operations Menu" on page 309 for other operations-level commands.

/cfg/port <port alias or number>/errdis
Port Error Disable and Recovery Configuration

```
[Port 2 ErrDisable Menu]
     ena      - Enable ErrDisable recovery
     dis      - Disable ErrDisable recovery
     cur      - Display current ErrDisable configuration
```

The Error Disable and Recovery feature allows the switch to automatically disable a port if an error condition is detected on the port. The port remains in the error-disabled state until it is re-enabled manually, or re-enabled automatically by the switch after a timeout period has elapsed. The error-disabled state of a port does not persist across a system reboot.

Table 100 Port Error Disable Configuration Options

Command Syntax and Usage
ena Enables automatic error-recovery for the port. The default setting is `enabled`. **Note**: Error-recovery must be enabled globally before port-level commands become active (**/cfg/sys/errdis/ena**).
dis Enables automatic error-recovery for the port.
cur Displays current port Error Disable parameters.

/cfg/port <port alias or number>/gig
Port Link Configuration

```
[Gigabit Link Menu]
     speed    - Set link speed
     mode     - Set full or half duplex mode
     fctl     - Set flow control
     auto     - Set autonegotiation
     cur      - Display current gig link configuration
```

Port link menu options are described in the following table.

Table 101 Port Link Configuration Options

Command Syntax and Usage
speed 10|100|1000|10000|any Sets the link speed. Some options are not valid on all ports. The choices include: □ 10 Mbps □ 100 Mbps □ 1000 Mbps □ any (auto negotiate port speed) **Note**: Data ports are fixed at 10000 Mbps.
mode full|half|any Sets the operating mode. Some options are not valid on all ports. The choices include: □ Full-duplex □ Half-duplex □ "Any," for auto negotiation (default) **Note**: Data ports are fixed at full duplex.
fctl rx|tx|both|none Sets the flow control. The choices include: □ Receive flow control □ Transmit flow control □ Both receive and transmit flow control (default) □ No flow control

Table 101 Port Link Configuration Options

Command Syntax and Usage
auto on|off Turns auto-negotiation on or off. **Note**: Data ports are fixed at 10000 Mbps, and cannot be set to auto-negotiate, unless a 1 Gb SFP transceiver is used.
cur Displays current port parameters.

/cfg/port <port alias or number>/aclqos
Port ACL Configuration

```
[Port 1 ACL Menu]
     add      - Add ACL to this port
     rem      - Remove ACL from this port
     cur      - Display current ACLs for this port
```

Table 102 Port ACL Options

Command Syntax and Usage
add acl *<1-254>* Adds the specified ACL to the port. You can add multiple ACLs to a port, but the total number of precedence levels allowed is two.
rem acl *<1-254>* Removes the specified ACL from the port.
cur Displays current ACL QoS parameters.

/cfg/port <port alias or number> /stp
Port Spanning Tree Configuration

```
[Port 1 STP Menu]
    edge    - Enable/disable edge port
    link    - Set port link type (for PVRST only)
    cur     - Display current port stp configuration
```

Table 103 Port STP Options

Command Syntax and Usage
edge e|d Enables or disables this port as an edge port. An edge port is not connected to a bridge, and can begin forwarding traffic as soon as the link is up. Configure server ports as edge ports (`enabled`).
link auto|p2p|shared Defines the type of link connected to the port, as follows: □ **auto**: Configures the port to detect the link type, and automatically match its settings. □ **p2p**: Configures the port for Point-To-Point protocol. □ **shared**: Configures the port to connect to a shared medium (usually a hub).
cur Displays current STP parameters for the port.

/cfg/qos

Quality of Service Configuration Menu

```
[QOS Menu]
     8021p     - 802.1p Menu
     dscp      - Dscp Menu
     cur       - Display current QOS configuration
```

Use the Quality of Service (QoS) menus to configure the 802.1p priority value and DiffServ Code Point (DSCP) value of incoming packets. This allows you to differentiate between various types of traffic, and provide different priority levels.

Table 104 Quality of Service Menu Options

Command Syntax and Usage
8021p Displays 802.1p configuration menu. To view menu options, see page 205.
dscp Displays DSCP configuration menu. To view menu options, see page 206.
cur Displays the current QOS parameters.

/cfg/qos/8021p
802.1p Configuration

```
[802.1p Menu]
     priq      - Set priority to COS queue mapping
     qweight   - Set weight to a COS queue
     default   - Reset 802.1p configuration to default values.
     cur       - Display current 802.1p configuration
```

This feature provides the capability to filter IP packets based on the 802.1p bits in the packet's VLAN header. The 802.1p bits specify the priority that you should give to the packets while forwarding them. The packets with a higher (non-zero) priority bits are given forwarding preference over packets with numerically lower priority bits value.

Table 105 802.1p Options

Command Syntax and Usage
priq *<priority (0-7)> <COSq number>* Maps the 802.1p priority to the Class of Service queue (COSq) priority. Enter the 802.1p priority value (0-7), followed by the COSq that handles the matching traffic. The valid range of the COSq number is set using the `numcos` command.
qweight *<COSq number> <weight (0-15)>* Configures the weight of the selected COSq. Enter the COSq number, followed by the scheduling weight (0-15). The valid range of the COSq number is set using the `numcos` command.
default Resets 802.1p parameters to their default values.
cur Displays the current 802.1p parameters.

/cfg/qos/dscp
DSCP Configuration

```
[dscp Menu]
     dscp      - Remark DSCP value to a new DSCP value
     prio      - Remark DSCP value to a 802.1p priority
     on        - Globally turn DSCP remarking ON
     off       - Globally turn DSCP remarking OFF
     cur       - Display current DSCP remarking configuration
```

Use this menu map the DiffServ Code Point (DSCP) value of incoming packets to a new value, or to an 802.1p priority value.

Table 106 DSCP Options

Command Syntax and Usage
dscp *<DSCP (0-63)> <new DSCP (0-63)>* Maps the initial DiffServ Code Point (DSCP) value to a new value. Enter the DSCP value (0-63) of incoming packets, followed by the new value.
prio *<DSCP (0-63)> <priority (0-7)>* Maps the DiffServ Code point value to an 802.1p priority value. Enter the DSCP value, followed by the corresponding 802.1p value.
on Turns on DSCP re-marking globally.
off Turns off DSCP re-marking globally.
cur Displays the current DSCP parameters.

/cfg/acl

Access Control List Configuration Menu

```
[ACL Menu]
     acl       - Access Control List Item Config Menu
     outdscp   - Set the update DSCP for out profile
     cur       - Display current ACL configuration
```

Use this menu to create Access Control Lists (ACLs). ACLs define matching criteria used for IP filtering and Quality of Service functions.

Table 107 ACL Configuration Options

Command Syntax and Usage
acl *<1-254>* Displays Access Control List configuration menu. To view menu options, see page 208.
outdscp *<1-63>* Configures the global DSCP re-marking value for out-of-profile packets. Sets the DiffServ Code Point (DSCP) of Out-of-Profile packets to the selected value.
cur Displays the current ACL parameters.

/cfg/acl/acl <ACL number>
ACL Configuration

```
[ACL 1 Menu]
     mirror   - Mirror Options Menu
     ethernet - Ethernet Header Options Menu
     ipv4     - IP Header Options Menu
     tcpudp   - TCP/UDP Header Options Menu
     meter    - ACL Metering Configuration Menu
     re-mark  - ACL Re-mark Configuration Menu
     action   - Set filter action
     stats    - Enable/disable statistics for this acl
     reset    - Reset filtering parameters
     cur      - Display current filter configuration
```

These menus allow you to define filtering criteria for each Access Control List (ACL).

Table 108 ACL Options

Command Syntax and Usage
mirror Displays the ACL Port Mirror menu. To view menu options, see page 209.
ethernet Displays the ACL Ethernet Header menu. To view menu options, see page 210.
ipv4 Displays the ACL IP Header menu. To view menu options, see page 211.
tcpudp Displays the ACL TCP/UDP Header menu. To view menu options, see page 213.
meter Displays the ACL Metering menu. To view menu options, see page 214.
re-mark Displays the ACL Re-mark menu. To view menu options, see page 215.
action permit|deny Configures a filter action for packets that match the ACL definitions. You can choose to permit (pass) or deny (drop) packets.

Table 108 ACL Options

Command Syntax and Usage
stats e|d Enables or disables the statistics collection for the Access Control List.
reset Resets the ACL parameters to their default values.
cur Displays the current ACL parameters.

/cfg/acl/acl *<ACL number>*/mirror
ACL Mirroring Configuration

```
[Mirror Options Menu]
     dest      - Set mirror destination
     port      - Set port as mirror target
     del       - Clear mirror settings
     cur       - Display current mirror configuration
```

This menu allows you to define port mirroring for an ACL. Packets that match the ACL are mirrored to the destination interface.

Table 109 ACL Port Mirroring Options

Command Syntax and Usage
dest port|none Configures the interface type of the destination.
port *<port alias or number>* Configures the destination to which packets that match this ACL are mirrored.
del Removes this ACL from port mirroring.
cur Displays the current port mirroring parameters for the ACL.

/cfg/acl/acl <ACL number>/ethernet
Ethernet Filtering Configuration

```
      smac      - Set to filter on source MAC
      dmac      - Set to filter on destination MAC
      vlan      - Set to filter on VLAN ID
      etype     - Set to filter on ethernet type
      pri       - Set to filter on priority
      reset     - Reset all fields
      cur       - Display current parameters
```

This menu allows you to define Ethernet matching criteria for an ACL.

Table 110 Ethernet Filtering Options

Command Syntax and Usage
smac *<MAC address (such as 00:60:cf:40:56:00)> <mask (FF:FF:FF:FF:FF:FF)>* Defines the source MAC address for this ACL.
dmac *<MAC address (such as 00:60:cf:40:56:00)> <mask (FF:FF:FF:FF:FF:FF)>* Defines the destination MAC address for this ACL.
vlan *<VLAN number> <VLAN mask (0xfff)>* Defines a VLAN number and mask for this ACL.
etype ARP | **IP** | **IPv6** | **MPLS** | **RARP** | **any** | *<other (0xXXXX)>* Defines the Ethernet type for this ACL.
pri *<0-7>* Defines the Ethernet priority value for the ACL.
reset Resets Ethernet parameters for the ACL to their default values.
cur Displays the current Ethernet parameters for the ACL.

/cfg/acl/acl <ACL number>/ipv4
IP version 4 Filtering Configuration

```
[Filtering IPv4 Menu]
     sip       - Set to filter on source IP address
     dip       - Set to filter on destination IP address
     proto     - Set to filter on prototype
     tos       - Set to filter on TOS
     reset     - Reset all fields
     cur       - Display current parameters
```

This menu allows you to define IPv4 matching criteria for an ACL.

Table 111 IP version 4 Filtering Options

Command Syntax and Usage
sip *<IP address> <mask (such as 255.255.255.0)>* Defines a source IP address for the ACL. If defined, traffic with this source IP address will match this ACL. Specify an IP address in dotted decimal notation.
dip *<IP address> <mask (such as 255.255.255.0)>* Defines a destination IP address for the ACL. If defined, traffic with this destination IP address will match this ACL.
proto *<0-255>* Defines an IP protocol for the ACL. If defined, traffic from the specified protocol matches this filter. Specify the protocol number. Listed below are some of the well-known protocols. Number Name 1 icmp 2 igmp 6 tcp 17 udp 89 ospf 112 vrrp
tos *<0-255>* Defines a Type of Service (ToS) value for the ACL. For more information on ToS, refer to RFC 1340 and 1349.

Table 111 IP version 4 Filtering Options

Command Syntax and Usage
reset Resets the IPv4 parameters for the ACL to their default values.
cur Displays the current IPV4 parameters.

/cfg/acl/acl <ACL number>/tcpudp
TCP/UDP Filtering Configuration

```
[Filtering TCP/UDP Menu]
     sport    - Set to filter on TCP/UDP source port
     dport    - Set to filter on TCP/UDP destination port
     flags    - Set to filter TCP/UDP flags
     reset    - Reset all fields
     cur      - Display current parameters
```

This menu allows you to define TCP/UDP matching criteria for an ACL.

Table 112 TCP/UDP Filtering Options

Command Syntax and Usage
sport *<source port (1-65535)> <mask (0xFFFF)>* Defines a source port for the ACL. If defined, traffic with the specified TCP or UDP source port will match this ACL. Specify the port number. Listed below are some of the well-known ports: **Number Name** 20 ftp-data 21 ftp 22 ssh 23 telnet 25 smtp 37 time 42 name 43 whois 53 domain 69 tftp 70 gopher 79 finger 80 http
dport *<destination port (1-65535)> <mask (0xFFFF)>* Defines a destination port for the ACL. If defined, traffic with the specified TCP or UDP destination port will match this ACL. Specify the port number, just as with `sport` above.
flags *<value (0x0-0x3f)>* Defines a TCP/UDP flag for the ACL.

Table 112 TCP/UDP Filtering Options

Command Syntax and Usage
reset Resets the TCP/UDP parameters for the ACL to their default values.
cur Displays the current TCP/UDP Filtering parameters.

/cfg/acl/acl <ACL number>/meter
ACL Metering Configuration

```
[Metering Menu]
     cir       - Set committed rate in KiloBits/s
     mbsize    - Set maximum burst size in KiloBits
     enable    - Enable/disable port metering
     dpass     - Set to Drop or Pass out of profile traffic
     reset     - Reset meter parameters
     cur       - Display current settings
```

This menu defines the metering profile for the selected ACL.

Table 113 ACL Metering Options

Command Syntax and Usage
cir *<100-10000>* Configures the committed rate, in Kilobits per second. The committed rate must be a multiple of 100.
mbsize *<32-4096>* Configures the maximum burst size, in Kilobits. Enter one of the following values for `mbsize`: 32, 64, 128, 256, 512, 1024, 2048, 4096
enable e|d Enables or disables metering on the ACL.
dpass drop|pass Configures the ACL Meter to either drop or pass out-of-profile traffic.

Table 113 ACL Metering Options

Command Syntax and Usage
reset Reset ACL Metering parameters to their default values.
cur Displays current ACL Metering parameters.

/cfg/acl/acl <ACL number>/re-mark
Re-Mark Configuration

```
[Re-mark Menu]
     inprof   - In Profile Menu
     outprof  - Out Profile Menu
     up1p     - Set Update User Priority Menu
     reset    - Reset re-mark settings
     cur      - Display current settings
```

You can choose to re-mark IP header data for the selected ACL. You can configure different re-mark values, based on whether packets fall within the ACL Metering profile, or out of the ACL Metering profile.

Table 114 ACL Re-mark Options

Command Syntax and Usage
inprof Displays the re-mark In-Profile menu. To view menu options, see page 216.
outprof Displays the re-mark Out-of-Profile menu. To view menu options, see page 216.
up1p Displays the re-mark Update User Priority menu. To view menu options, see page 217.
reset Reset ACL re-mark parameters to their default values.
cur Displays current re-mark parameters.

/cfg/acl/acl <ACL number>/re-mark/inprof
Re-Marking In-Profile Configuration

```
[Re-marking - In Profile Menu]
     updscp    - Set the update DSCP
     reset     - Reset update DSCP settings
     cur       - Display current settings
```

Table 115 ACL Re-Mark In-Profile Options

Command Syntax and Usage
updscp *<0-63>* Sets the DiffServ Code Point (DSCP) of In-Profile packets to the selected value.
reset Resets the update DSCP parameters to their default values.
cur Displays current Re-Mark In-Profile parameters.

/cfg/acl/acl <ACL number>/re-mark/outprof
Re-Marking Out-of-Profile Configuration

```
[Re-marking - Out Of Profile Menu]
     dscp      - Enable/disable DSCP remarking
     reset     - reset update DSCP setting
     cur       - Display current settings
```

Table 116 ACL Re-Mark Out-of-Profile Options (/cfg/acl/acl x/re-mark/outprof)

Command Syntax and Usage
dscp e|d Enables or disables DSCP re-marking on out-of-profile packets for the ACL.
reset Resets the update DSCP parameters for Out-of-Profile packets to their default values.
cur Displays current Re-Mark Out-of-Profile parameters.

/cfg/acl/acl <ACL number>/re-mark/up1p
Update User Priority Configuration

```
[Update User Priority Menu]
     value    - Set the update user priority
     reset    - Reset in profile up1p settings
     cur      - Display current settings
```

Table 117 ACL Re-Mark Update User Priority Options

Command Syntax and Usage
value <*0-7*> Defines 802.1p value. The value is the priority bits information in the packet structure.
reset Resets UP1P settings to their default values.
cur Displays current Re-Mark In-Profile User Priority parameters.

/cfg/pmirr
Port Mirroring Configuration Menu

```
[Port Mirroring Menu]
      monport - Monitoring Port based PM Menu
      mirror  - Enable/Disable Mirroring
      cur     - Display All Mirrored and Monitoring Ports
```

Port mirroring is disabled by default. For more information about port mirroring on the G8124, see "Appendix A: Troubleshooting" in the *BLADE OS Application Guide*.

The Port Mirroring menu is used to configure, enable, and disable the monitor port. When enabled, network packets being sent and/or received on a target port are duplicated and sent to a monitor port. By attaching a network analyzer to the monitor port, you can collect detailed information about your network performance and usage.

Table 118 Port Mirroring Menu Options

Command Syntax and Usage
monport *<port alias or number>* Displays port-mirroring menu. To view menu options, see page 219.
mirror disable|enable Enables or disables port mirroring
cur Displays current settings of the mirrored and monitoring ports.

/cfg/pmirr/monport <port alias or number>
Port-Mirroring Configuration

```
[Port 1 Menu]
     add      - Add "Mirrored" port
     rem      - Rem "Mirrored" port
     delete   - Delete this "Monitor" port
     cur      - Display current Port-based Port Mirroring configuration
```

Table 119 Port Mirroring Monitor Port Options

Command Syntax and Usage

add *<mirrored port (port to mirror from)> <direction (in, out, or both)>*

Adds the port to be mirrored. This command also allows you to enter the direction of the traffic. It is necessary to specify the direction because:

If the source port of the frame matches the mirrored port and the mirrored direction is ingress or both (ingress and egress), the frame is sent to the monitoring port.

If the destination port of the frame matches the mirrored port and the mirrored direction is egress or both, the frame is sent to the monitoring port.

rem *<mirrored port (port to mirror from)>*

Removes the mirrored port.

delete

Deletes this monitor port.

cur

Displays the current settings of the monitoring port.

/cfg/l2

Layer 2 Configuration Menu

```
[Layer 2 Menu]
     mrst      - Multiple Spanning Tree/Rapid Spanning Tree Menu
     nostp     - Disable Spanning Tree
     stp       - Spanning Tree Menu
     fdb       - FDB Menu
     trunk     - Trunk Group Menu
     thash     - Trunk Hash Menu
     lacp      - Link Aggregation Control Protocol Menu
     failovr   - Failover Menu
     hotlink   - Hot Links Menu
     vlan      - VLAN Menu
     pvstcomp  - Enable/disable PVST+ compatibility mode
     upfast    - Enable/disable Uplink Fast
     update    - UplinkFast station update rate
     cur       - Display current layer 2 parameters
```

Table 120 Layer 2 Configuration Menu Options

Command Syntax and Usage
mrst Displays the Rapid Spanning Tree/Multiple Spanning Tree Protocol Configuration menu. To view menu options, see page 222.
nostp enable|disable When enabled, globally turns Spanning Tree `off`. All ports are placed into forwarding state. Any BPDU's received are flooded. BPDU Guard is not affected by this command.
stp *<group number (1-128)>* Displays the Spanning Tree Configuration menu. To view menu options, see page 228.
fdb Displays the Forwarding Database menu. To view menu options, see page 233.
trunk *<trunk number (1-12)>* Displays the Trunk Group Configuration menu. To view menu options, see page 235.
thash Displays the IP Trunk Hash menu. To view menu options, see page 236.

Table 120 Layer 2 Configuration Menu Options

Command Syntax and Usage
lacp Displays the Link Aggregation Control Protocol menu. To view menu options, see page 238.
failovr Displays the Failover Configuration menu. To view menu options, see page 240.
hotlink Displays the Hot Links Configuration menu. To view menu options, see page 245.
vlan *<VLAN number (1-4094)>* Displays the VLAN Configuration menu. To view menu options, see page 249.
pvstcomp enable|disable Enables or disables VLAN tagging of Spanning Tree BPDUs. The default setting is **enabled**.
upfast enable|disable Enables or disables Fast Uplink Convergence, which provides rapid Spanning Tree convergence to an upstream switch during failover. **Note**: When enabled, this feature increases bridge priorities to 65535 for all STGs and path cost by 3000 for all external STP ports.
update *<10-200>* Configures the station update rate. The default value is 40.
cur Displays current Layer 2 parameters.

/cfg/l2/mrst
RSTP/MSTP Configuration

```
[Multiple Spanning Tree Menu]
   cist     - Common and Internal Spanning Tree menu
   name     - Set MST region name
   rev      - Set revision level of this MST region
   maxhop   - Set Maximum Hop Count for MST (4 - 60)
   mode     - Spanning Tree Mode
   on       - Globally turn Multiple Spanning Tree (MSTP/RSTP/PVRST) ON
   off      - Globally turn Multiple Spanning Tree (MSTP/RSTP/PVRST) OFF
   cur      - Display current MST parameters
```

BLADE OS supports the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP), IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), and Per VLAN Rapid Spanning Tree Protocol (PVRST). MSTP allows you to map many VLANs to a small number of Spanning Tree Groups (STGs), each with its own topology.

Up to 32 Spanning Tree Groups can be configured in **mstp** mode. MRST is turned off by default.

Note – When Multiple Spanning Tree is turned on, VLAN 4095 is moved from Spanning Tree Group 128 to the Common Internal Spanning Tree (CIST). When Multiple Spanning Tree is turned off, VLAN 4095 is moved back to Spanning Tree Group 128.

Table 121 MSTP/RSTP/PVRST Configuration Options

Command Syntax and Usage
cist Displays the Common Internal Spanning Tree (CIST) menu. To view menu options, see page 224.
name *<1-32 characters>* Configures a name for the MSTP region. All devices within a MSTP region must have the same region name.
rev *<0-65535>* Configures a version number for the MSTP region. The version is used as a numerical identifier for the region. All devices within a MSTP region must have the same version number.
maxhop *<4-60>* Configures the maximum number of bridge hops a packet may traverse before it is dropped. The default is 20.

Table 121 MSTP/RSTP/PVRST Configuration Options

Command Syntax and Usage
mode rstp|mstp|pvrst Selects the Spanning Tree mode, as follows: Per VLAN Rapid Spanning Tree Plus (**pvrst**), Rapid Spanning Tree (**rstp**), Multiple Spanning Tree (**mstp**). The default mode is RSTP.
on Globally turns RSTP/MSTP/PVRST ON. **Note**: When RSTP is turned on, the configuration parameters for STG 1 apply to RSTP.
off Globally turns RSTP/MSTP/PVRST OFF.
cur Displays the current RSTP/MSTP/PVRST configuration.

/cfg/l2/mrst/cist
Common Internal Spanning Tree Configuration

```
[Common Internal Spanning Tree Menu]
  brg     - CIST Bridge parameter menu
  port    - CIST Port parameter menu
  add     - Add VLAN(s) to CIST
  default - Default Common Internal Spanning Tree and Member parameters
  cur     - Display current CIST parameters
```

Table 122 describes the commands used to configure Common Internal Spanning Tree (CIST) parameters. The CIST provides compatibility with different MSTP regions and with devices running different Spanning Tree instances. It is equivalent to Spanning Tree Group 0.

Table 122 CIST Configuration Options

Command Syntax and Usage
brg Displays the CIST Bridge menu. To view menu options, see page 225.
port *<port alias or number>* Displays the CIST Port menu. To view menu options, see page 226.
add *<VLAN numbers>* Adds selected VLANs to the CIST.
default Resets all CIST parameters to their default values.
cur Displays the current CIST configuration.

/cfg/l2/mrst/cist/brg
CIST Bridge Configuration

```
[CIST Bridge Menu]
      prior   - Set CIST bridge Priority (0-65535)
      mxage   - Set CIST bridge Max Age (6-40 secs)
      fwd     - Set CIST bridge Forward Delay (4-30 secs)
      cur     - Display current CIST bridge parameters
```

CIST bridge parameters are used only when the switch is in MSTP mode. CIST parameters do not affect operation of STP/PVST+.

Table 123 CIST Bridge Configuration Options

Command Syntax and Usage
prior *<0-65535>* Configures the CIST bridge priority. The bridge priority parameter controls which bridge on the network is the MSTP root bridge. To make this switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority. The range is 0 to 65535, in steps of 4096 (0, 4096, 8192...). The default value is 61440.
mxage *<6-40 seconds>* Configures the CIST bridge maximum age. The maximum age parameter specifies the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the MSTP network. The range is 6 to 40 seconds, and the default is 20 seconds.
fwd *<4-30 seconds>* Configures the CIST bridge forward delay parameter. The forward delay parameter specifies the amount of time that a bridge port has to wait before it changes from the listening state to the learning state and from the learning state to the forwarding state. The range is 4 to 30 seconds, and the default is 15 seconds.
cur Displays the current CIST bridge configuration.

/cfg/l2/mrst/cist/port <port alias or number>
CIST Port Configuration

```
[CIST Port 1 Menu]
   prior   - Set port Priority (0-240)
   cost    - Set port Path Cost (1-200000000, 0 for auto)
   hello   - Set CIST port Hello Time (1-10 secs)
   link    - Set MSTP link type (auto, p2p, or shared; default: auto)
             (for MSTP only)
   pvst-pro - Enable/disable PVST Protection (for MSTP only)
   on      - Turn port's Spanning Tree ON
   off     - Turn port's Spanning Tree OFF
   cur     - Display current port Spanning Tree parameters
```

CIST port parameters are used to modify MRST operation on an individual port basis. CIST parameters do not affect operation of STP/PVST+, RSTP, or PVRST. For each port, RSTP/MSTP is turned on by default.

Table 124 CIST Port Configuration Options

Command Syntax and Usage
prior *<0-240>* Configures the CIST port priority. The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment. The range is 0 to 240, in steps of 16 (0, 16, 32...), and the default is 128.
cost *<0-200000000>* Configures the CIST port path cost. The port path cost is used to help determine the designated port for a segment. Port path cost is based on the port speed, and is calculated as follows: □ 1Gbps = 20000 □ 10Gbps = 2000 The default value of 0 (zero) indicates that the default path cost will be computed for an auto negotiated link speed.
hello *<1-10 seconds>* Configures the CIST port Hello time.The Hello time specifies how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge Hello value. The range is 1 to 10 seconds, and the default is 2 seconds.

Table 124 CIST Port Configuration Options

Command Syntax and Usage
link [**auto**|**p2p**|**shared**] Defines the type of link connected to the port, as follows: □ auto: Configures the port to detect the link type, and automatically match its settings. □ p2p: Configures the port for Point-To-Point protocol. □ shared: Configures the port to connect to a shared medium (usually a hub). The default link type is auto.
edge enable|disable Enables or disables this port as an edge port. An edge port is not connected to a bridge, and can begin forwarding traffic as soon as the link is up. Configure server ports as edge ports (enabled). The default setting is disabled. **Note**: After you configure the port as an edge port, you must disable the port (**/oper/port** *x***/dis**) and then re-enable the port (**/oper/port** *x***/ena**) for the change to take effect.
pvst-pro e|d Configures PVST Protection on the selected port. If the port receives any PVST+/PVRST+ BPDUs, it error disabled. PVST Protection works only in MSTP mode. The default setting is enabled.
on Enables MRST on the port.
off Disables MRST on the port.
cur Displays the current CIST port configuration.

/cfg/l2/stp <STP group index>
Spanning Tree Configuration

```
[Spanning Tree Group 1 Menu]
      brg     - Bridge parameter menu
      port    - Port parameter menu
      add     - Add VLAN(s) to Spanning Tree Group
      remove  - Remove VLAN(s) from Spanning Tree Group
      clear   - Remove all VLANs from Spanning Tree Group
      on      - Globally turn Spanning Tree ON
      off     - Globally turn Spanning Tree OFF
      default - Default Spanning Tree and Member parameters
      cur     - Display current bridge parameters
```

BLADE OS supports the IEEE 802.1D Spanning Tree Protocol (STP). STP is used to prevent loops in the network topology. Up to 128 Spanning Tree Groups can be configured on the switch (STG 128 is reserved for management).

Note – When VRRP is used for active/active redundancy, STG must be enabled.

Table 125 Spanning Tree Configuration Options

Command Syntax and Usage
brg Displays the Bridge Spanning Tree menu. To view menu options, see page 230.
port *<port alias or number>* Displays the Spanning Tree Port menu. To view menu options, see page 231.
add *<VLAN number>* Associates a VLAN with a Spanning Tree and requires an external VLAN ID as a parameter.
remove *<VLAN number>* Breaks the association between a VLAN and a Spanning Tree and requires an external VLAN ID as a parameter.
clear Removes all VLANs from a Spanning Tree.
on Globally enables Spanning Tree Protocol. STG is turned on by default.

Table 125 Spanning Tree Configuration Options

Command Syntax and Usage
off Globally disables Spanning Tree Protocol.
default Restores a Spanning Tree instance to its default configuration.
cur Displays current Spanning Tree Protocol parameters.

/cfg/l2/stp <STP group number>/brg
Spanning Tree Bridge Configuration

```
[Bridge Spanning Tree Menu]
      prior   - Set bridge Priority [0-65535]
      hello   - Set bridge Hello Time [1-10 secs]
      mxage   - Set bridge Max Age (6-40 secs)
      fwd     - Set bridge Forward Delay (4-30 secs)
      cur     - Display current bridge parameters
```

Spanning Tree bridge parameters affect the global STG operation of the switch. STG bridge parameters include:

- Bridge priority
- Bridge hello time
- Bridge maximum age
- Forwarding delay

Table 126 Spanning Tree Bridge Options

Command Syntax and Usage
prior *<new bridge priority (0-65535)>* Configures the bridge priority. The bridge priority parameter controls which bridge on the network is the STG root bridge. To make this switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority. The default value is 32768.
hello *<new bridge hello time (1-10 secs)>* Configures the bridge hello time.The hello time specifies how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value. The range is 1 to 10 seconds, and the default is 2 seconds. This command does not apply to MSTP (see CIST on page 224).
mxage *<new bridge max age (6-40 secs)>* Configures the bridge maximum age. The maximum age parameter specifies the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it re configures the STG network. The range is 6 to 40 seconds, and the default is 20 seconds. This command does not apply to MSTP (see CIST on page 224).

Table 126 Spanning Tree Bridge Options

Command Syntax and Usage
fwd *<new bridge Forward Delay (4-30 secs)>* Configures the bridge forward delay parameter. The forward delay parameter specifies the amount of time that a bridge port has to wait before it changes from the listening state to the learning state and from the learning state to the forwarding state. The range is 4 to 30 seconds, and the default is 15 seconds. This command does not apply to MSTP (see CIST on page 224).
cur Displays the current bridge STG parameters.

When configuring STG bridge parameters, the following formulas must be used:

- 2*(*fwd*-1) ≥ *mxage*
- 2*(*hello*+1) ≤ *mxage*

/cfg/l2/stp *<STP Group Index>*/port *<port alias or number>* Spanning Tree Port Configuration

```
[Spanning Tree Port 1 Menu]
  prior    - Set port Priority (0-255)
  cost     - Set port Path Cost (1-65535 (802.1d) /
             1-200000000 (MSTP/RSTP) /0 for auto)
  link     - Set port link type (auto, p2p, or shared; default: auto)
             (for RSTP only)
  fastfwd  - Enable/disable Port Fast Forwarding mode
  on       - Turn port's Spanning Tree ON
  off      - Turn port's Spanning Tree OFF
  cur      - Display current port Spanning Tree parameters
```

By default, Spanning Tree is turned `off` for management ports, and turned `on` for data ports. STG port parameters include:

- Port priority
- Port path cost

The `port` option of STG is turned on by default.

Table 127 Spanning Tree Port Options

Command Syntax and Usage
`prior` *<new port Priority (0-255)>* Configures the port priority. The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment. The default value is 128. **RSTP/MSTP**: The range is 0 to 240, in steps of 16 (0, 16, 32...) and the default is 128.
`cost` *<1-65535, 0 for default)>* Configures the port path cost. The port path cost is used to help determine the designated port for a segment. Port path cost is based on the port speed, and is calculated as follows: □ 1Gbps = 4 □ 10Gbps = 2 The default value of 0 (zero) indicates that the default path cost will be computed for an auto negotiated link speed.
`link` [**`auto`**|**`p2p`**|**`shared`**] Defines the type of link connected to the port, as follows: □ `auto`: Configures the port to detect the link type, and automatically match its settings. □ `p2p`: Configures the port for Point-To-Point protocol. □ `shared`: Configures the port to connect to a shared medium (usually a hub). The default link type is `auto`.
`fastfwd enable|disable` Disables or enables Port Fast Forwarding, which permits a port that participates in Spanning Tree to bypass the Listening and Learning states and enter directly into the Forwarding state. While in the Forwarding state, the port listens to the BPDUs to learn if there is a loop and, if dictated by normal STG behavior (following priorities, etc.), the port transitions into the Blocking state. This feature permits the switch to interoperate well within Rapid Spanning Tree networks. The default setting is `disabled`.
`on` Enables STG on the port.

Table 127 Spanning Tree Port Options

Command Syntax and Usage
off Disables STG on the port.
cur Displays the current STG port parameters.

/cfg/l2/fdb
Forwarding Database Configuration

```
[FDB Menu]
     static   - Static FDB Menu
     aging    - Configure FDB aging value
     cur      - Display current FDB configuration
```

Use the following commands to configure the Forwarding Database (FDB) for the G8124.

Table 128 FDB Configuration Options

Command Syntax and Usage
static Displays the static FDB menu. To view menu options, see page 234.
aging *<0-65535>* Configures the aging value for FDB entries, in seconds. The default value is 300.
cur Displays the current FDB parameters.

/cfg/l2/fdb/static
Static FDB Configuration

```
[Static FDB Menu]
     add      - Add a permanent FDB entry
     del      - Delete a static FDB entry
     clear    - Clear static FDB entries
     cur      - Display current static FDB configuration
```

Use the following commands to configure static entries in the Forwarding Database (FBD).

Table 129 Static FDB Configuration Options

Command Syntax and Usage
add *<MAC address> <VLAN number> <port number>* Adds a permanent FDB entry. Enter the MAC address using the following format: `xx:xx:xx:xx:xx:xx` For example, `08:00:20:12:34:56` You can also enter the MAC address as follows: `xxxxxxxxxxxx` For example, `080020123456`
del *<MAC address> <VLAN number>* Deletes a permanent FDB entry.
clear *<MAC address>***|all {mac|vlan|port}** Clears static FDB entries.
cur Display current static FDB configuration.

/cfg/l2/trunk <trunk group number>
Trunk Configuration

```
[Trunk group 1 Menu]
      add     - Add port to trunk group
      rem     - Remove port from trunk group
      ena     - Enable trunk group
      dis     - Disable trunk group
      del     - Delete trunk group
      cur     - Display current Trunk Group configuration
```

Trunk groups can provide super-bandwidth connections between G8124s or other trunk capable devices. A *trunk* is a group of ports that act together, combining their bandwidth to create a single, larger port. Up to 12 static trunk groups can be configured on the G8124, with the following restrictions:

- Any physical switch port can belong to no more than one trunk group.
- Up to 12 ports can belong to the same trunk group.
- Configure all ports in a trunk group with the same properties (speed, duplex, flow control, STG, VLAN, and so on).
- Trunking from non-BLADE devices must comply with Cisco® EtherChannel® technology.

By default, each trunk group is empty and disabled.

Table 130 Trunk Configuration Options

Command Syntax and Usage
add *<port alias or number>* Adds a physical port to the current trunk group.
rem *<port alias or number>* Removes a physical port from the current trunk group.
ena Enables the current trunk group.
dis Disables the current trunk group.
del Removes the current trunk group configuration.
cur Displays current trunk group parameters.

/cfg/l2/thash
IP Trunk Hash Configuration

```
[IP Trunk Hash Menu]
     set      - IP Trunk Hash Settings Menu
     cur      - Display current IP trunk hash configuration
```

Use the following commands to configure IP trunk hash settings for the G8124. The trunk hash settings affect both static trunks and LACP trunks.

Table 131 IP Trunk Hash Options

Command Syntax and Usage
set Displays the Trunk Hash Settings menu. To view menu options, see page 237.
cur Display current trunk hash configuration.

/cfg/l2/thash/set
IP Trunk Hash

```
[set IP Trunk Hash Settings Menu]
     smac      - Enable/disable smac hash
     dmac      - Enable/disable dmac hash
     sip       - Enable/disable sip hash
     dip       - Enable/disable dip hash
     cur       - Display current trunk hash setting
```

Trunk hash parameters are set globally for the G8124. You can enable one or two parameters, to configure any of the following valid combinations:

- SMAC (source MAC only)
- DMAC (destination MAC only)
- SIP (source IP only)
- DIP (destination IP only)
- SIP + DIP (source IP and destination IP)
- SMAC + DMAC (source MAC and destination MAC)

Use the following commands to configure IP trunk hash parameters for the G8124.

Table 132 IP Trunk Hash Options

Command Syntax and Usage
smac enable|disable Enable or disable trunk hashing on the source MAC.
dmac enable|disable Enable or disable trunk hashing on the destination MAC.
sip enable|disable Enable or disable trunk hashing on the source IP.
dip enable|disable Enable or disable trunk hashing on the destination IP.
cur Display current layer 2 trunk hash setting.

/cfg/l2/lacp
LACP Configuration

```
[LACP Menu]
     port      - LACP Port Menu
     sysprio   - Set LACP system priority
     timeout   - Set LACP system timeout scale for timing out partner
                 info
     delete    - Delete an LACP trunk
     default   - Restore default LACP system configuration
     cur       - Display current LACP configuration
```

Use the following commands to configure Link Aggregation Control Protocol (LACP) for the G8124.

Table 133 LACP Configuration Options

Command Syntax and Usage
port *<port alias or number>* Displays the LACP Port menu. To view menu options, see page 239.
sysprio *<1-65535>* Defines the priority value (1 through 65535) for the G8124. Lower numbers provide higher priority. The default value is 32768.
timeout short|long Defines the timeout period before invalidating LACP data from a remote partner. Choose **short** (3 seconds) or **long** (90 seconds). The default value is **long**. **Note**: It is recommended that you use a timeout value of **long**, to reduce LACPDU processing. If your G8124's CPU utilization rate remains at 100% for periods of 90 seconds or more, consider using static trunks instead of LACP.
delete *<1-65535>* Deletes a selected LACP trunk, based on its *admin key.*
default sysprio|timeout Restores the selected parameters to their default values.
cur Display current LACP configuration.

/cfg/l2/lacp/port <port alias or number>
LACP Port Configuration

```
[LACP Port 1 Menu]
     mode     - Set LACP mode
     prio     - Set LACP port priority
     adminkey - Set LACP port admin key
     default  - Restore default LACP port configuration
     cur      - Display current LACP port configuration
```

Use the following commands to configure Link Aggregation Control Protocol (LACP) for the selected port.

Table 134 LACP Port Options

Command Syntax and Usage
mode off|active|passive Set the LACP mode for this port, as follows: □ `off`: Turn LACP off for this port. You can use this port to manually configure a static trunk. The default value is `off`. □ `active`: Turn LACP on and set this port to active. Active ports initiate LACPDUs. □ `passive`: Turn LACP on and set this port to passive. Passive ports do not initiate LACPDUs, but respond to LACPDUs from active ports.
prio *<1-65535>* Sets the priority value for the selected port. Lower numbers provide higher priority. The default value is 32768.
adminkey *<1-65535>* Set the admin key for this port. Only ports with the same *admin key* and *oper key* (operational state generated internally) can form a LACP trunk group.
default adminkey|mode|prio Restores the selected parameters to their default values.
cur Displays the current LACP configuration for this port.

/cfg/l2/failovr
Layer 2 Failover Configuration

```
[Failover Menu]
     trigger  - Trigger Menu
     on       - Globally turn Failover ON
     off      - Globally turn Failover OFF
     cur      - Display current Failover configuration
```

Use this menu to configure Layer 2 Failover. For more information about Layer 2 Failover, see "High Availability" in the *BLADE OS Application Guide*.

Table 135 Layer 2 Failover Configuration Options

Command Syntax and Usage
trigger *<1-8>* Displays the Failover Trigger menu. To view menu options, see page 241.
on Globally turns Layer 2 Failover `on`.
off Globally turns Layer 2 Failover `off`.
cur Displays current Layer 2 Failover parameters.

/cfg/l2/failovr/trigger <1-8>
Failover Trigger Configuration

```
[Trigger 1 Menu]
     mmon      - Manual Monitor Menu
     limit     - Limit of Trigger
     ena       - Enable Trigger
     dis       - Disable Trigger
     del       - Delete Trigger
     cur       - Display current Trigger configuration
```

Table 136 Failover Trigger Options

Command Syntax and Usage
mmon Displays the Manual Monitor menu for the selected trigger. To view menu options, see page 242.
limit *<0-1024>* Configures the minimum number of operational links allowed within each trigger before the trigger initiates a failover event. If you enter a value of zero (0), the switch triggers a failover event only when no links in the trigger are operational.
ena Enables the selected trigger.
dis Disables the selected trigger.
del Deletes the selected trigger.
cur Displays the current failover trigger settings.

/cfg/l2/failovr/trigger/mmon
Manual Monitor Configuration

```
[Manual Monitor Menu]
     monitor  - Monitor Menu
     control  - Control Menu
     cur      - Display current Manual Monitor configuration
```

Use this menu to configure Failover Manual Monitor. These menus allow you to manually define both the monitor and control ports that participate in failover teaming.

Table 6-1 Failover Manual Monitor Options

Command Syntax and Usage
monitor Displays the Manual Monitor - Monitor menu for the selected trigger.
control Displays the Manual Monitor - Control menu for the selected trigger.
cur Displays the current Manual Monitor settings.

/cfg/l2/failovr/trigger/mmon/monitor

Manual Monitor Port Configuration

```
[Monitor Menu]
     addport  - Add port to Monitor
     remport  - Remove port from Monitor
     addtrnk  - Add trunk to Monitor
     remtrnk  - Remove trunk from Monitor
     addkey   - Add LACP port adminkey to Monitor
     remkey   - Remove LACP port adminkey from Monitor
     cur      - Display current Monitor configuration
```

Use this menu to define the port link(s) to monitor. The Manual Monitor - Monitor configuration accepts only external uplink ports.

Table 137 Failover Manual Monitor - Monitor Options

Command Syntax and Usage
addport *<port alias or number>* Adds the selected port to the Manual Monitor - Monitor.
remport *<port alias or number>* Removes the selected port from the Manual Monitor - Monitor.
addtrnk *<trunk number>* Adds a trunk group to the Manual Monitor - Monitor.
remtrnk *<trunk number>* Removes a trunk group from the Manual Monitor - Monitor.
addkey *<1-65535>* Adds a LACP admin key to the Manual Monitor - Monitor. LACP trunks formed with this admin key will be included in the Manual Monitor - Monitor.
remkey *<1-65535>* Removes a LACP admin key from the Manual Monitor - Monitor.
cur Displays the current Manual Monitor - Monitor configuration.

/cfg/l2/failovr/trigger/mmon/control
Manual Monitor Control Configuration

```
[Control Menu]
     addport  - Add port to Control
     remport  - Remove port from Control
     addtrnk  - Add trunk to Control
     remtrnk  - Remove trunk from Control
     addkey   - Add LACP port adminkey to Control
     remkey   - Remove LACP port adminkey from Control
     cur      - Display current Control configuration
```

Use this menu to define the port link(s) to control.

The Manual Monitor–Control configuration accepts internal and external ports, but not management ports.

Table 138 Failover Manual Monitor - Control Options

Command Syntax and Usage
addport *<port alias or number>* Adds the selected port to the Manual Monitor - Control.
remport *<port alias or number>* Removes the selected port from the Manual Monitor - Control.
addtrnk *<trunk number>* Adds a trunk group to the Manual Monitor - Control.
remtrnk *<trunk number>* Removes a trunk group from the Manual Monitor - Control.
addkey *<1-65535>* Adds a LACP admin key to the Manual Monitor - Control. LACP trunks formed with this admin key will be included in the Manual Monitor - Control.
remkey *<1-65535>* Removes a LACP admin key from the Manual Monitor - Control.
cur Displays the current Manual Monitor - Control configuration.

/cfg/l2/hotlink
Hot Links Configuration

```
[Hot Links Menu]
     trigger  - Trigger Menu
     bpdu     - Enable/disable BPDU flood
     sndfdb   - Enable/disable FDB update
     on       - Globally turn Hot Links ON
     off      - Globally turn Hot Links OFF
     cur      - Display current Hot Links configuration
```

Table 139 describes the Hot Links menu options.

Table 139 Hot Links Configuration Options

Command Syntax and Usage
trigger *<1-25>* Displays the Hot Links Trigger menu. To view menu options, see page 246.
bpdu enable|disable Enables or disables the ability to flood BPDUs on the active Hot Links interface when the interface belongs to a Spanning Tree group that is globally turned `off`. The default setting is `disabled`.
sndfdb enable|disable Enables or disables FDB Update, which allows the switch to send FDB and MAC update packets over the active interface. The default setting is `disabled`.
on Globally turns Hot Links `on`. The default value is `off`.
off Globally turns Hot Links `off`.
cur Displays current Hot Links configuration.

/cfg/l2/hotlink/trigger <1-25>
Hot Links Trigger Configuration

```
[Trigger 2 Menu]
     master   - Master Menu
     backup   - Backup Menu
     fdelay   - Set Forward Delay (secs)
     name     - Set Trigger Name
     preempt  - Enable/disable Preemption
     ena      - Enable Trigger
     dis      - Disable Trigger
     del      - Delete Trigger
     cur      - Display current Trigger configuration
```

Table 140 Hot Links Trigger Options

Command Syntax and Usage
master Displays the Master interface menu for the selected trigger. To view menu options, see page 247.
backup Displays the Backup interface menu for the selected trigger. To view menu options, see page 248.
fdelay *<0-3600>* Configures the Forward Delay interval, in seconds. The default value is `1`.
name *<1-32 characters>* Configures a name for the trigger.
preempt e|d Enables or disables pre-emption, which allows the Master interface to transition to the Active state whenever it becomes available. The default setting is `enabled`.
ena Enables the Hot Links trigger.
dis Disables the Hot Links trigger.

Table 140 Hot Links Trigger Options

Command Syntax and Usage
del Deletes the Hot Links trigger.
cur Displays the current Hot Links Trigger configuration.

/cfg/l2/hotlink/trigger <1-25>/master
Hot Links Trigger Master Configuration

```
[Master Menu]
     port     - Set port in Master
     trunk    - Set trunk in Master
     adminkey - Set adminkey in Master
     cur      - Display current Master configuration
```

Table 141 Hot Links Trigger Master Options

Command Syntax and Usage
port *<port name or alias>* Adds the selected port to the Master interface. Enter 0 (zero) to clear the port.
trunk *<trunk number>* Adds the selected trunk group to the Master interface. Enter 0 (zero) to clear the trunk group.
adminkey *<0-65535>* Adds a LACP admin key to the Master interface. LACP trunks formed with this admin key will be included in the Master interface. Enter 0 (zero) to clear the admin key.
cur Displays the current Hot Links Master interface configuration.

/cfg/l2/hotlink/trigger <1-25>/backup
Hot Links Trigger Backup Configuration

```
[Backup Menu]
     port     - Set port in Backup
     trunk    - Set trunk in Backup
     adminkey - Set adminkey in Backup
     cur      - Display current Backup configuration
```

Table 142 Hot Links Trigger Backup Options

Command Syntax and Usage
port *<port name or alias>* Adds the selected port to the Backup interface. Enter 0 (zero) to clear the port.
trunk *<trunk number>* Adds the selected trunk to the Backup interface. Enter 0 (zero) to clear the trunk group.
adminkey *<0-65535>* Adds a LACP admin key to the Backup interface. LACP trunks formed with this admin key will be included in the Backup interface. Enter 0 (zero) to clear the admin key.
cur Displays the current Hot Links Backup interface settings.

/cfg/l2/vlan <VLAN number>
VLAN Configuration

```
[VLAN 1 Menu]
     privlan  - Private-VLAN Menu
     name     - Set VLAN name
     stg      - Assign VLAN to a Spanning Tree Group
     add      - Add port to VLAN
     rem      - Remove port from VLAN
     def      - Define VLAN as list of ports
     ena      - Enable VLAN
     dis      - Disable VLAN
     del      - Delete VLAN
     cur      - Display current VLAN configuration
```

The commands in this menu configure VLAN attributes, change the status of each VLAN, change the port membership of each VLAN, and delete VLANs. For more information on configuring VLANs, see "Setup Part 3: VLANs" on page 26.

By default, VLAN 1 is the only VLAN configured on the switch. All ports are members of VLAN 1 by default. Up to 1024 VLANs can be configured on the G8124.

VLANs can be assigned any number between 1 and 4094. VLAN 4095 is reserved for switch management.

Table 143 VLAN Configuration Options

Command Syntax and Usage
privlan Displays the Private VLAN menu. To view menu options, see page 251.
name Assigns a name to the VLAN or changes the existing name. The default VLAN name is the first one.
stg *<Spanning Tree Group index>* Assigns a VLAN to a Spanning Tree Group.
add *<port alias or number>* Adds port(s) to the VLAN membership.
rem *<port alias or number>* Removes port(s) from this VLAN.

Table 143 VLAN Configuration Options

Command Syntax and Usage
def *<list of port numbers>* Defines which ports are members of this VLAN. Every port must be a member of at least one VLAN. By default, all ports are members of VLAN 1.
ena Enables this VLAN.
dis Disables this VLAN without removing it from the configuration.
del Deletes this VLAN.
cur Displays the current VLAN configuration.

Note – All ports must belong to at least one VLAN. Any port which is removed from a VLAN and which is not a member of any other VLAN is automatically added to default VLAN 1. You cannot remove a port from VLAN 1 if the port has no membership in any other VLAN. Also, you cannot add a port to more than one VLAN unless the port has VLAN tagging turned on (see the `tag` command on page 197).

/cfg/l2/vlan/privlan
Private VLAN Configuration

```
[privlan Menu]
     type      - Set Private-VLAN type
     map       - Associate secondary VLAN with a primary VLAN
     ena       - Enable Private-VLAN
     dis       - Disable Private-VLAN
     cur       - Display current Private-VLAN configuration
```

Use this menu to configure a Private VLAN.

Table 144 Private VLAN Configuration Options

Command Syntax and Usage
type primary|isolated|community Defines the VLAN type, as follows: □ `primary`: A Private VLAN must have only one primary VLAN. The primary VLAN carries unidirectional traffic to ports on the isolated VLAN or to community VLAN. □ `isolated`: The isolated VLAN carries unidirectional traffic from host ports. A Private VLAN may have only one isolated VLAN. □ `community`: Community VLANs carry upstream traffic from host ports. A Private VLAN may have multiple community VLANs.
map *<2-4094>* Configures Private VLAN mapping between a secondary VLAN (`isolated` or `community`) and a primary VLAN. Enter the primary VLAN ID.
ena Enables the Private VLAN.
dis Disables the Private VLAN.
cur Displays current parameters for the selected Private VLAN.

/cfg/l3

Layer 3 Configuration Menu

```
[Layer 3 Menu]
     if        - Interface Menu
     gw        - Default Gateway Menu
     route     - Static Route Menu
     arp       - ARP Menu
     frwd      - Forwarding Menu
     nwf       - Network Filters Menu
     rmap      - Route Map Menu
     rip       - Routing Information Protocol Menu
     ospf      - Open Shortest Path First (OSPF) Menu
     igmp      - IGMP Menu
     dns       - Domain Name System Menu
     bootp     - Bootstrap Protocol Relay Menu
     vrrp      - Virtual Router Redundancy Protocol Menu
     rtrid     - Set router ID
     cur       - Display current IP configuration
```

Table 145 Layer 3 Configuration Menu

Command Syntax and Usage
if *<interface number (1-128>* Displays the IP Interface menu. To view menu options, see page 254.
gw *<default gateway number (1-4>* Displays the IP Default Gateway menu. To view menu options, see page 255.
route Displays the IP Static Route menu. To view menu options, see page 257.
arp Displays the Address Resolution Protocol menu. To view menu options, see page 259.
frwd Displays the IP Forwarding menu. To view menu options, see page 261.
nwf *<network filter number (1-256)>* Displays the Network Filter Configuration menu. To view menu options see page 262.
rmap *<route map number (1-32)>* Displays the Route Map menu. To view menu options see page 263.

Table 145 Layer 3 Configuration Menu

Command Syntax and Usage
rip Displays the Routing Interface Protocol menu. To view menu options, see page 267.
ospf Displays the OSPF menu. To view menu options, see page 271.
igmp Displays the IGMP menu. To view menu options, see page 283.
dns Displays the IP Domain Name System menu. To view menu options, see page 293.
bootp Displays the Bootstrap Protocol menu. To view menu options, see page 294.
vrrp Displays the Virtual Router Redundancy Configuration menu. To view menu options, see page 295.
rtrid *<IP address (such as, 192.4.17.101)>* Sets the router ID.
cur Displays the current IP configuration.

/cfg/l3/if <interface number>
IP Interface Configuration

```
[IP Interface 1 Menu]
     addr     - Set IP address
     mask     - Set subnet mask
     vlan     - Set VLAN number
     relay    - Enable/disable BOOTP relay
     ena      - Enable IP interface
     dis      - Disable IP interface
     del      - Delete IP interface
     cur      - Display current interface configuration
```

The G8124 can be configured with up to 128 IP interfaces. Each IP interface represents the G8124 on an IP subnet on your network. The Interface option is disabled by default.

Interface 127 and interface 128 are reserved for switch management.

Table 146 IP Interface Configuration Options

Command Syntax and Usage
addr *<IPv4 address (such as 192.4.17.101)>* Configures the IPv4 address of the switch interface, using dotted decimal notation.
mask *<subnet mask (such as 255.255.255.0)>* Configures the subnet address mask for the interface, using dotted decimal notation.
vlan *<VLAN number>* Configures the VLAN number for this interface. Each interface can belong to only one VLAN. Each VLAN can contain multiple IPv4 interfaces.
relay disable|enable Enables or disables the BOOTP relay on this interface. It is enabled by default.
ena Enables this IP interface.
dis Disables this IP interface.

Table 146 IP Interface Configuration Options

Command Syntax and Usage
del Removes this IP interface.
cur Displays the current interface settings.

/cfg/l3/gw <gateway number>
Default Gateway Configuration

```
[Default gateway 1 Menu]
      addr    - Set IP address
      intr    - Set interval between ping attempts
      retry   - Set number of failed attempts to declare gateway DOWN
      arp     - Enable/disable ARP only health checks
      ena     - Enable default gateway
      dis     - Disable default gateway
      del     - Delete default gateway
      cur     - Display current default gateway configuration
```

The switch can be configured with up to four IPv4 gateways. Gateway 4 is reserved for switch management.

This option is disabled by default.

Table 147 Default Gateway Configuration Options

Command Syntax and Usage
addr *<default gateway address (such as, 192.4.17.44)>* Configures the IP address of the default IP gateway using dotted decimal notation.
intr *<0-60 seconds>* The switch pings the default gateway to verify that it's up. The `intr` option sets the time between health checks. The range is from 0 to 60 seconds. The default is 2 seconds.
retry *<number of attempts (1-120)>* Sets the number of failed health check attempts required before declaring this default gateway inoperative. The range is from 1 to 120 attempts. The default is 8 attempts.

Table 147 Default Gateway Configuration Options

Command Syntax and Usage
arp disable|enable Enables or disables Address Resolution Protocol (ARP) health checks. The default value is **disabled**. The **arp** option does not apply to management gateways.
ena Enables the gateway for use.
dis Disables the gateway.
del Deletes the gateway from the configuration.
cur Displays the current gateway settings.

/cfg/l3/route
IPv4 Static Route Configuration

```
[IP Static Route Menu]
     add      - Add static route
     rem      - Remove static route
     clear    - Clear static routes
     interval - Change ECMP route health check ping interval
     retries  - Change the number of retries for ECMP health check
     ecmphash - Choose ECMP hash mechanism
     cur      - Display current static route configuration
```

Up to 128 IPv4 static routes can be configured.

Table 148 IP Static Route Configuration Options

Command Syntax and Usage
add *<destination> <mask> <gateway>* [*<interface number>*] Adds a static route. You will be prompted to enter a destination IP address, destination subnet mask, and gateway address. Enter all addresses using dotted decimal notation.
rem *<destination> <mask>* [*<interface number>*] Removes a static route. The destination address of the route to remove must be specified using dotted decimal notation.
clear {*<destination IP address>***|***<gateway IP address>***|all} [***<value>***]** Clears the selected IPv4 static routes.
interval *<1-60>* Configures the ECMP health-check ping interval, in seconds. The default value is 1 second.
retries *<1-60>* Configures the number of ECMP health-check retries. The default value is 3.

Table 148 IP Static Route Configuration Options

Command Syntax and Usage
ecmphash [sip][dip][protocol][tcpl4][udpl4][sport][dport] Configures ECMP hashing parameters. You may choose one or more of the following parameters: □ `sip`: Source IP address □ `dip`: Destination IP address □ `protocol`: Layer 3 protocol □ `tcpl4`: Layer 4 TCP traffic □ `udpl4`: Layer 4 UDP traffic □ `sport`: Source port □ `dport`: Destination port
cur Displays the current IPv4 static routes.

/cfg/l3/arp
ARP Configuration

Address Resolution Protocol (ARP) is the TCP/IP protocol that resides within the Internet layer. ARP resolves a physical address from an IP address. ARP queries machines on the local network for their physical addresses. ARP also maintains IP to physical address pairs in its cache memory. In any IP communication, the ARP cache is consulted to see if the IP address of the computer or the router is present in the ARP cache. Then the corresponding physical address is used to send a packet.

```
[ARP Menu]
     static   - Static ARP Menu
     rearp    - Set re-ARP period in minutes
     cur      - Display current ARP configuration
```

Table 149 ARP Configuration Options

Command Syntax and Usage
static Displays Static ARP menu. To view options, see page 260.
rearp *<2-120 minutes>* Defines re-ARP period in minutes. You can set this duration between two and 120 minutes.
cur Displays the current ARP configurations.

/cfg/l3/arp/static
ARP Static Configuration

Static ARP entries are permanent in the ARP cache and do not age out like the ARP entries that are learned dynamically. Static ARP entries enable the switch to reach the hosts without sending an ARP broadcast request to the network. Static ARPs are also useful to communicate with devices that do not respond to ARP requests. Static ARPs can also be configured on some gateways as a protection against malicious ARP Cache corruption and possible DOS attacks.

```
[Static ARP Menu]
     add      - Add a permanent ARP entry
     del      - Delete an ARP entry
     clear    - Clear static ARP entries
     cur      - Display current static ARP configuration
```

Table 150 ARP Static Configuration Options

Command Syntax and Usage
add *<IP address> <MAC address> <VLAN number> <port number>* Adds a permanent ARP entry.
del *<IP address (such as, 192.4.17.101)>* Deletes a permanent ARP entry.
clear [*<interface number>* | *<VLAN number>* | *<port number>* | **all]** *<ARP entry number>* Clears static ARP entries.
cur Displays current static ARP configuration.

/cfg/l3/frwd
IP Forwarding Configuration

```
[IP Forwarding Menu]
     dirbr    - Enable or disable forwarding directed broadcasts
     noicmprd - Enable/disable No ICMP Redirects
     on       - Globally turn IP Forwarding ON
     off      - Globally turn IP Forwarding OFF
     cur      - Display current IP Forwarding configuration
```

Table 151 IP Forwarding Configuration Options

Command Syntax and Usage
dirbr disable|enable Enables or disables forwarding directed broadcasts. The default setting is `disabled`.
noicmprd disable|enable Enables or disables ICMP re-directs. The default setting is `disabled`.
on Enables IP forwarding (routing) on the G8124. Forwarding is turned on by default.
off Disables IP forwarding (routing) on the G8124.
cur Displays the current IP forwarding settings.

/cfg/l3/nwf <1-256>
Network Filter Configuration

```
[IP Network Filter 1 Menu]
      addr    - IP Address
      mask    - IP network filter mask
      enable  - Enable Network Filter
      disable - Disable Network Filter
      delete  - Delete Network Filter
      cur     - Display current Network Filter configuration
```

Table 152 IP Network Filter Options

Command Syntax and Usage
addr *<IP address, such as 192.4.17.44>* Sets the IP address that will be accepted by the peer when the filter is enabled. If used with the `mask` option, a range of IP addresses is accepted. The default address is `0.0.0.0`
mask *<IP network filter mask>* Sets the network filter mask that is used with `addr`. The default value is `0.0.0.0`
enable Enables the Network Filter configuration.
disable Disables the Network Filter configuration.
delete Deletes the Network Filter configuration.
cur Displays the current the Network Filter configuration.

/cfg/l3/rmap <route map number>
Routing Map Configuration

Note – The *map number* (1-32) represents the routing map you wish to configure.

```
[IP Route Map 1 Menu]
      alist   - Access List number
      aspath  - AS Filter Menu
      ap      - Set as-path prepend of the matched route
      lp      - Set local-preference of the matched route
      metric  - Set metric of the matched route
      type    - Set OSPF metric-type of the matched route
      prec    - Set the precedence of this route map
      weight  - Set weight of the matched route
      enable  - Enable route map
      disable - Disable route map
      delete  - Delete route map
      cur     - Display current route map configuration
```

Routing maps control and modify routing information.

Table 153 Routing Map Configuration Options

Command Syntax and Usage
alist *<number 1-8>* Displays the Access List menu. For more information, see page 265.
aspath *<number 1-8>* Displays the Autonomous System (AS) Filter menu. For more information, see page 266.
ap *<AS number>* [*<AS number>*] [*<AS number>*] | **none** Sets the AS path preference of the matched route. You can configure up to three path preferences.
lp *<(0-4294967294)>* | **none** Sets the local preference of the matched route, which affects both inbound and outbound directions. The path with the higher preference is preferred.
metric *<(1-4294967294)>* | **none** Sets the metric of the matched route.

Table 153 Routing Map Configuration Options

Command Syntax and Usage
type <*value (1 | 2)*>	**none** Assigns the type of OSPF metric. The default is type 1. □ Type 1—External routes are calculated using both internal and external metrics. □ Type 2—External routes are calculated using only the external metrics. Type 1 routes have more cost than Type 2. □ none—Removes the OSPF metric.
prec <*value (1-255)*> Sets the precedence of the route map. The smaller the value, the higher the precedence. Default value is 10.
weight <*value (0-65534)*>	**none** Sets the weight of the route map.
enable Enables the route map.
disable Disables the route map.
delete Deletes the route map.
cur Displays the current route configuration.

/cfg/l3/rmap <route map number>/alist <access list number>
IP Access List Configuration

Note – The *route map number (*1-32) and the *access list number* (1-8) represent the IP access list you wish to configure.

```
[IP Access List 1 Menu]
      nwf     - Network Filter number
      metric  - Metric
      action  - Set Network Filter action
      enable  - Enable Access List
      disable - Disable Access List
      delete  - Delete Access List
      cur     - Display current Access List configuration
```

Table 154 IP Access List Options

Command Syntax and Usage
nwf *<network filter number (1-256)>* Sets the network filter number. See "/cfg/l3/nwf <1-256>" on page 262 for details.
metric *<(1-4294967294)>*|**none** Sets the metric value in the AS-External (ASE) LSA.
action permit|**deny** Permits or denies action for the access list.
enable Enables the access list.
disable Disables the access list.
delete Deletes the access list.
cur Displays the current Access List configuration.

/cfg/l3/rmap <route map number> /aspath <autonomous system path> Autonomous System Filter Path

Note – The *rmap number (*1-32) and the *path number* (1-8) represent the AS path you wish to configure.

```
[AS Filter 1 Menu]
      as      - AS number
      action  - Set AS Filter action
      enable  - Enable AS Filter
      disable - Disable AS Filter
      delete  - Delete AS Filter
      cur     - Display current AS Filter configuration
```

Table 155 AS Filter Options

Command Syntax and Usage
as *<AS number (1-65535)>* Sets the Autonomous System filter's path number.
action *<permit | deny (p | d)>* Permits or denies Autonomous System filter action.
enable Enables the Autonomous System filter.
disable Disables the Autonomous System filter.
delete Deletes the Autonomous System filter.
cur Displays the current Autonomous System filter configuration.

/cfg/l3/rip
Routing Information Protocol Configuration

```
[Routing Information Protocol Menu]
     if       - RIP Interface Menu
     update   - Set update period in seconds
     redist   - RIP Route Redistribute Menu
     on       - Globally turn RIP ON
     off      - Globally turn RIP OFF
     current  - Display current RIP configuration
```

The RIP menu is used for configuring Routing Information Protocol (RIP) parameters. This option is turned off by default.

Table 156 RIP Configuration Options

Command Syntax and Usage
if *<interface number>* Displays the RIP Interface menu. For more information, see page 268.
update *<1-120>* Configures the time interval for sending for RIP table updates, in seconds. The default value is 30 seconds.
redist fixed|static|ospf|eospf Displays the RIP Route Redistribution menu. For more information, see page 270.
on Globally turns RIP **on**.
off Globally turns RIP **off**.
cur Displays the current RIP configuration.

/cfg/l3/rip/if *<interface number>*
Routing Information Protocol Interface Configuration

```
[RIP Interface 1 Menu]
     version  - Set RIP version
     supply   - Enable/disable supplying route updates
     listen   - Enable/disable listening to route updates
     poison   - Enable/disable poisoned reverse
     split    - Enable/disable split horizon
     trigg    - Enable/disable triggered updates
     mcast    - Enable/disable multicast updates
     default  - Set default route action
     metric   - Set metric
     auth     - Set authentication type
     key      - Set authentication key
     enable   - Enable interface
     disable  - Disable interface
     current  - Display current RIP interface configuration
```

The RIP interface menu is used for configuring Routing Information Protocol parameters for the selected interface.

Note – Do not configure RIP version 1 parameters if your routing equipment uses RIP version 2.

Table 157 RIP Interface Options

Command Syntax and Usage
version 1|2|both Configures the RIP version used by this interface. The default value is version 2.
supply disable|enable When enabled, the switch supplies routes to other routers. The default value is enabled.
listen disable|enable When enabled, the switch learns routes from other routers. The default value is enabled.
poison disable|enable When enabled, the switch uses split horizon with poisoned reverse. When disabled, the switch uses only split horizon. The default value is disabled.
split disable|enable Enables or disables split horizon. The default value is enabled.

Table 157 RIP Interface Options

Command Syntax and Usage
trigg disable|enable Enables or disables Triggered Updates. Triggered Updates are used to speed convergence. When enabled, Triggered Updates force a router to send update messages immediately, even if it is not yet time for the update message. The default value is `enabled`.
mcast disable|enable Enables or disables multicast updates of the routing table (using address 224.0.0.9). The default value is `enabled`.
default none|listen|supply|both When enabled, the switch accepts RIP default routes from other routers, but gives them lower priority than configured default gateways. When disabled, the switch rejects RIP default routes. The default value is `none`.
metric *<1-15>* Configures the route metric, which indicates the relative distance to the destination. The default value is `1`.
auth none|password Configures the authentication type. The default is `none`.
key Configures the authentication key password.
enable Enables this RIP interface.
disable Disables this RIP interface.
current Displays the current RIP configuration.

/cfg/l3/rip/redist fixed|static|ospf|eospf
RIP Route Redistribution Configuration

```
[RIP Redistribute Fixed Menu]
     add      - Add rmap into route redistribution list
     rem      - Remove rmap from route redistribution list
     export   - Export all routes of this protocol
     cur      - Display current route-maps added
```

The following table describes the RIP Route Redistribute menu options.

Table 158 RIP Redistribution Options

Command Syntax and Usage
add *<1-32>* *<1-32>***|all** Adds selected routing maps to the RIP route redistribution list. To add specific route maps, enter routing map numbers, separated by a comma (**,**). To add all 32 route maps, type **all**. The routes of the redistribution protocol matched by the route maps in the route redistribution list will be redistributed.
rem *<1-32>* *<1-32>***|all** Removes the route map from the RIP route redistribution list. To remove specific route maps, enter routing map numbers, separated by a comma (**,**). To remove all 32 route maps, type **all**.
export *<1-15>***|none** Exports the routes of this protocol in which the metric and metric type are specified. To remove a previous configuration and stop exporting the routes of the protocol, enter **none**.
cur Displays the current RIP route redistribute configuration.

/cfg/l3/ospf
Open Shortest Path First Configuration

```
[Open Shortest Path First Menu]
      aindex  - OSPF Area (index) menu
      range   - OSPF Summary Range menu
      if      - OSPF Interface menu
      virt    - OSPF Virtual Links menu
      md5key  - OSPF MD5 Key Menu
      host    - OSPF Host Entry menu
      redist  - OSPF Route Redistribute menu
      lsdb    - Set the LSDB limit
      default - Originate default route information
      on      - Globally turn OSPF ON
      off     - Globally turn OSPF OFF
      cur     - Display current OSPF configuration
```

Table 159 OSPF Configuration Options

Command Syntax and Usage
aindex *<area index (0-2)>* Displays the area index menu. This area index does not represent the actual OSPF area number. See page 273 to view menu options.
range *<1-16>* Displays summary routes menu for up to 16 IP addresses. See page 275 to view menu options.
if *<interface number>* Displays the OSPF interface configuration menu. See page 276 to view menu options.
virt *<virtual link (1-3)>* Displays the Virtual Links menu used to configure OSPF for a Virtual Link. See page 278 to view menu options.
md5key *<key ID (1-255)>* Assigns a string to MD5 authentication key.
host *<1-128>* Displays the menu for configuring OSPF for the host routes. Up to 128 host routes can be configured. Host routes are used for advertising network device IP addresses to external networks to perform server load balancing within OSPF. It also makes Area Border Route (ABR) load sharing and ABR failover possible. See page 280 to view menu options.

Table 159 OSPF Configuration Options

Command Syntax and Usage
redist fixed|static|rip Displays the OSPF Route Distribution menu. See page 281 to view menu options.
lsdb *<LSDB limit (0-12288, 0 for no limit)>* Sets the link state database limit.
default *<metric (1-16777214)>* *<metric-type 1|2>* **|none** Sets one default route among multiple choices in an area. Use `none` for no default.
on Enables OSPF on the G8124.
off Disables OSPF on the G8124.
cur Displays the current OSPF configuration settings.

/cfg/l3/ospf/aindex <area index>
Area Index Configuration

```
[OSPF Area (index) 1 Menu]
      areaid  - Set area ID
      type    - Set area type
      metric  - Set stub area metric
      auth    - Set authentication type
      spf     - Set time interval between two SPF calculations
      enable  - Enable area
      disable - Disable area
      delete  - Delete area
      cur     - Display current OSPF area configuration
```

Table 160 Area Index Configuration Options

Command Syntax and Usage
areaid *<IP address (such as, 192.4.17.101)>* Defines the IP address of the OSPF area number.
type transit|stub|nssa Defines the type of area. For example, when a virtual link has to be established with the backbone, the area type must be defined as transit. **Transit area:** allows area summary information to be exchanged between routing devices. Any area that is not a stub area or NSSA is considered to be transit area. **Stub area:** is an area where external routing information is not distributed. Typically, a stub area is connected to only one other area. **NSSA:** Not-So-Stubby Area (NSSA) is similar to stub area with additional capabilities. For example, routes originating from within the NSSA can be propagated to adjacent transit and backbone areas. External routes from outside the Autonomous System (AS) can be advertised within the NSSA but are not distributed into other areas.
metric *<metric value (1-65535)>* Configures a stub area to send a numeric metric value. All routes received via that stub area carry the configured metric to potentially influencing routing decisions. Metric value assigns the priority for choosing the switch for default route. Metric type determines the method for influencing routing decisions for external routes.

Table 160 Area Index Configuration Options

Command Syntax and Usage
auth none|password|md5 □ none: No authentication required. □ password: Authenticates simple passwords so that only trusted routing devices can participate. □ md5: This parameter is used when MD5 cryptographic authentication is required.
spf *<interval (1-255)>* Sets time interval between two successive SPF (shortest path first) calculations of the shortest path tree using the Dijkstra's algorithm.
enable Enables the OSPF area.
disable Disables the OSPF area.
delete Deletes the OSPF area.
cur Displays the current OSPF configuration.

/cfg/l3/ospf/range <range number>
OSPF Summary Range Configuration

```
[OSPF Summary Range 1 Menu]
      addr    - Set IP address
      mask    - Set IP mask
      aindex  - Set area index
      hide    - Enable/disable hide range
      enable  - Enable range
      disable - Disable range
      delete  - Delete range
      cur     - Display current OSPF summary range configuration
```

Table 161 OSPF Summary Range Configuration Options

Command Syntax and Usage
addr *<IP Address (such as, 192.4.17.101)>* Configures the base IP address for the range.
mask *<IP mask (such as, 255.255.255.0)>* Configures the IP address mask for the range.
aindex *<area index (0-2)>* Configures the area index used by the G8124.
hide disable|enable Hides the OSPF summary range.
enable Enables the OSPF summary range.
disable Disables the OSPF summary range.
delete Deletes the OSPF summary range.
current Displays the current OSPF summary range.

/cfg/l3/ospf/if <interface number>
OSPF Interface Configuration

```
[OSPF Interface 1 Menu]
      aindex  - Set area index
      prio    - Set interface router priority
      cost    - Set interface cost
      hello   - Set hello interval in seconds or milliseconds
      dead    - Set dead interval in seconds or milliseconds
      trans   - Set transit delay in seconds
      retra   - Set retransmit interval in seconds
      key     - Set authentication key
      mdkey   - Set MD5 key ID
      passive - Enable/disable passive interface
      ptop    - Enable/disable point-to-point interface
      enable  - Enable interface
      disable - Disable interface
      delete  - Delete interface
      cur     - Display current OSPF interface configuration
```

Table 162 OSPF Interface Configuration Options

Command Syntax and Usage
aindex *<area index (0-2)>* Configures the OSPF area index.
prio *<priority value (0-255)>* Configures the priority value for the G8124's OSPF interfaces. (A priority value of 255 is the highest and 1 is the lowest. A priority value of 0 specifies that the interface cannot be used as Designated Router (DR) or Backup Designated Router (BDR).)
cost *<1-65535>* Configures cost set for the selected path—preferred or backup. Usually the cost is inversely proportional to the bandwidth of the interface. Low cost indicates high bandwidth.
hello *<1-65535>* Configures the interval, in seconds, between the `hello` packets for the interfaces.
dead *<1-65535>* Configures the health parameters of a `hello` packet, in seconds, before declaring a silent router to be down.

Table 162 OSPF Interface Configuration Options

Command Syntax and Usage
trans *<1-3600>* Configures the transit delay in seconds.
retra *<1-3600>* Configures the retransmit interval in seconds.
key *<key>* | **none** Sets the authentication key to clear the password.
mdkey *<key ID (1-255)>* | **none** Assigns an MD5 key to the interface.
passive enable|disable Sets the interface as passive. On a passive interface, you can disable OSPF protocol exchanges, but the router advertises the interface in its LSAs so that IP connectivity to the attached network segment will be established.
ptop enable|disable Sets the interface as point-to-point.
enable Enables OSPF interface.
disable Disables OSPF interface.
delete Deletes OSPF interface.
cur Displays the current settings for OSPF interface.

/cfg/l3/ospf/virt <link number>
OSPF Virtual Link Configuration

```
[OSPF Virtual Link 1 Menu]
      aindex  - Set area index
      hello   - Set hello interval in seconds or milliseconds
      dead    - Set dead interval in seconds or milliseconds
      trans   - Set transit delay in seconds
      retra   - Set retransmit interval in seconds
      nbr     - Set router ID of virtual neighbor
      key     - Set authentication key
      mdkey   - Set MD5 key ID
      enable  - Enable interface
      disable - Disable interface
      delete  - Delete interface
      cur     - Display current OSPF interface configuration
```

Table 163 OSPF Virtual Link Configuration Options

Command Syntax and Usage
aindex *<area index (0-2)>* Configures the OSPF area index.
hello *<1-65535)>* **hello** *<50-65535ms)>* Configures the authentication parameters of a hello packet, in seconds or milliseconds.
dead *<1-65535>* **dead** *<1000-65535ms>* Configures the health parameters of a hello packet, in seconds or milliseconds. The default value is 60 seconds.
trans *<1-3600>* Configures the delay in transit, in seconds. Default is one second.
retra *<1-3600>* Configures the retransmit interval, in seconds. Default is five seconds.
nbr *<NBR router ID (IP address)>* Configures the router ID of the virtual neighbor. Default is 0.0.0.0.
key *<password>* Configures the password (up to eight characters) for each virtual link. Default is `none`.

Table 163 OSPF Virtual Link Configuration Options

Command Syntax and Usage
mdkey *<key ID (1-255)>* | **none** Sets MD5 key ID for each virtual link. Default is `none`.
enable Enables OSPF virtual link.
disable Disables OSPF virtual link.
delete Deletes OSPF virtual link.
cur Displays the current OSPF virtual link settings.

/cfg/l3/ospf/host <host number>
OSPF Host Entry Configuration

```
[OSPF Host Entry 1 Menu]
      addr    - Set host entry IP address
      aindex  - Set area index
      cost    - Set cost of this host entry
      enable  - Enable host entry
      disable - Disable host entry
      delete  - Delete host entry
      cur     - Display current OSPF host entry configuration
```

Table 164 OSPF Host Entry Configuration Options

Command Syntax and Usage
addr *<IP address (such as, 192.4.17.101)>* Configures the base IP address for the host entry.
aindex *<area index (0-2)>* Configures the area index of the host.
cost *<1-65535>* Configures the cost value of the host.
enable Enables OSPF host entry.
disable Disables OSPF host entry.
delete Deletes OSPF host entry.
cur Displays the current OSPF host entries.

/cfg/l3/ospf/redist fixed|static|rip
OSPF Route Redistribution Configuration

```
[OSPF Redistribute Fixed Menu]
      add     - Add rmap into route redistribution list
      rem     - Remove rmap from route redistribution list
      export  - Export all routes of this protocol
      cur     - Display current route-maps added
```

Table 165 OSPF Route Redistribution Options

Command Syntax and Usage
add *(<route map (1-32)> <route map [1-32]>)...* | **all** Adds selected routing maps to the rmap list.To add all the 32 route maps, enter `all`. To add specific route maps, enter routing map numbers one per line, NULL at the end. This option adds a route map to the route redistribution list. The routes of the redistribution protocol matched by the route maps in the route redistribution list will be redistributed.
rem *(<route map (1-32)> <route map (1-32)>) ...* | **all** Removes the route map from the route redistribution list. Removes routing maps from the `rmap` list. To remove all 32 route maps, enter `all`. To remove specific route maps, enter routing map numbers one per line, NULL at end.
export *<metric (1-16777214)> <metric type [1|2]>* | **none** Exports the routes of this protocol as external OSPF AS-external LSAs in which the metric and metric type are specified. To remove a previous configuration and stop exporting the routes of the protocol, enter `none`.
cur Displays the current route map settings.

/cfg/l3/ospf/md5key <key ID>
OSPF MD5 Key Configuration

```
[OSPF MD5 Key 1 Menu]
      key     - Set authentication key
      delete  - Delete key
      cur     - Display current MD5 key configuration
```

Table 166 OSPF MD5 Key Configuration Options

Command Syntax and Usage
key *<1-16 characters>* Sets the authentication key for this OSPF packet.
delete Deletes the authentication key for this OSPF packet.
cur Displays the current MD5 key configuration.

/cfg/l3/igmp
IGMP Configuration

```
[IGMP Menu]
     snoop    - IGMP Snoop Menu
     mrouter  - Static Multicast Router Menu
     igmpflt  - IGMP Filtering Menu
     querier  - IGMP Querier Menu
     on       - Globally turn IGMP ON
     off      - Globally turn IGMP OFF
     cur      - Display current IGMP configuration
```

Table 167 describes the commands used to configure basic IGMP parameters.

Table 167 IGMP Configuration Options

Command Syntax and Usage
snoop Displays the IGMP Snooping menu. To view menu options, see page 284.
mrouter Displays the Static Multicast Router menu. To view menu options, see page 287.
igmpflt Displays the IGMP Filtering menu. To view menu options, see page 288.
querier *<VLAN number>* Displays the IGMP Querier menu. To view menu options, see page 291.
on Globally turns IGMP on.
off Globally turns IGMP off.
cur Displays the current IGMP configuration parameters.

/cfg/l3/igmp/snoop
IGMP Snooping Configuration

```
[IGMP Snoop Menu]
     igmpv3   - IGMP Version3 Snoop Menu
     timeout  - Set report timeout
     mrto     - Set multicast router timeout
     qintrval - Set IGMP query interval
     robust   - Set expected packet loss on subnet
     flood    - Flood unregistered IPMC
     aggr     - Aggregate IGMP report
     srcip    - Set source ip to use when proxying GSQ
     add      - Add VLAN(s) to IGMP Snooping
     rem      - Remove VLAN(s) from IGMP Snooping
     clear    - Remove all VLAN(s) from IGMP Snooping
     fastlv   - Enable/disable Fastleave processing in VLAN
     def      - Set IGMP Snooping settings to factory default
     cur      - Display current IGMP Snooping configuration
```

IGMP Snooping allows the switch to forward multicast traffic only to those ports that request it. IGMP snooping prevents multicast traffic from being flooded to all ports. The switch learns which server hosts are interested in receiving multicast traffic, and forwards it only to ports connected to those servers.

Table 168 describes the commands used to configure IGMP Snooping.

Table 168 IGMP Snoop Options

Command Syntax and Usage
igmpv3 Displays the IGMP version 3 menu. To view menu options, see page 286.
timeout *<1-255>* Configures the timeout value for IGMP Membership Reports (host). Once the timeout value is reached, the switch removes the host from its IGMP table, if the conditions are met. The range is from 1 to 255 seconds. The default is 10 seconds.
mrto *<1-600 seconds>* Configures the timeout value for IGMP Membership Queries (mrouter). Once the timeout value is reached, the switch removes the multicast router from its IGMP table, if the proper conditions are met. The range is from 1 to 600 seconds. The default is 255 seconds.
qinterval *<1-600>* Configures the interval for IGMP Query Reports. The default value is 125 seconds.

Table 168 IGMP Snoop Options

Command Syntax and Usage
robust *<2-10>* Configures the IGMP Robustness variable, which allows you to tune the switch for expected packet loss on the subnet. If the subnet is expected to be lossy (high rate of packet loss), increase the value. The default value is 2.
flood enable|disable Configures the switch to flood unregistered IP multicast traffic to all ports. The default setting is `enabled`. **Note:** If none of the IGMP hosts reside on the VLAN of the streaming server for a IPMC group, you must disable IGMP flooding to ensure that multicast data is forwarded across the VLANs for that IPMC group.
aggr enable|disable Enables or disables IGMP Membership Report aggregation.
srcip *<IP address (such as, 192.4.17.101)>* Configures the source IP address used as a proxy for IGMP Group Specific Queries.
add *<VLAN number>* Adds the selected VLAN(s) to IGMP Snooping.
rem *<VLAN number>* Removes the selected VLAN(s) from IGMP Snooping.
clear Removes all VLANs from IGMP Snooping.
fastlv *<VLAN number>* **disable|enable** Enables or disables Fastleave processing. Fastleave allows the switch to immediately remove a port from the IGMP port list, if the host sends a Leave message, and the proper conditions are met. This command is disabled by default.
def Resets IGMP Snooping parameters to their default values.
cur Displays the current IGMP Snooping parameters.

/cfg/l3/igmp/snoop/igmpv3
IGMP Version 3 Configuration

```
[IGMP V3 Snoop Menu]
     sources  - Set the number of sources to snoop in group record
     v1v2     - Enable/disable snooping IGMPv1/v2 reports
     exclude  - Enable/disable snooping EXCLUDE mode reports
     ena      - Enable IGMPv3 Snooping
     dis      - Disable IGMPv3 Snooping
     cur      - Display current IGMP Snooping V3 configuration
```

Table 169 describes the commands used to configure IGMP version 3.

Table 169 IGMP V3 Options

Command Syntax and Usage
sources *<1-64>* Configures the maximum number of IGMP multicast sources to snoop from within the group record. Use this command to limit the number of IGMP sources to provide more refined control.
v1v2 enable|disable Enables or disables snooping on IGMP version 1 and version 2 reports. When disabled, the switch drops IGMPv1 and IGMPv2 reports. The default value is `enabled`.
exclude enable|disable Enables or disables snooping on IGMPv3 Exclude Reports. When disabled, the switch ignores Exclude Reports. The default value is `enabled`.
ena Enables IGMP version 3. The default value is **disabled**.
dis Disables IGMP version 3.
cur Displays the current IGMP version 3 configuration.

/cfg/l3/igmp/mrouter
IGMP Static Multicast Router Configuration

```
[Static Multicast Router Menu]
      add     - Add port as Multicast Router Port
      rem     - Remove port as Multicast Router Port
      clear   - Remove all Static Multicast Router Ports
      cur     - Display current Multicast Router configuration
```

Table 170 describes the commands used to configure a static multicast router.

Note – When static Mrouters are used, the switch continues learning dynamic Mrouters via IGMP snooping. However, dynamic Mrouters may not replace static Mrouters. If a dynamic Mrouter has the same port and VLAN combination as a static Mrouter, the dynamic Mrouter is not learned.

Table 170 IGMP Static Multicast Router Options

Command Syntax and Usage
add *<port alias or number> <VLAN number> <IGMP version number>* Selects a port/VLAN combination on which the static multicast router is connected, and configures the IGMP version (1, 2, or 3) of the multicast router.
remove *<port alias or number> <VLAN number> <IGMP version number>* Removes a static multicast router from the selected port/VLAN combination.
clear Clears all static multicast routers from the switch.
cur Displays the current IGMP Static Multicast Router parameters.

/cfg/l3/igmp/igmpflt
IGMP Filtering Configuration

```
[IGMP Filter Menu]
      filter  - IGMP Filter Definition Menu
      port    - IGMP Filtering Port Menu
      ena     - Enable IGMP Filtering
      dis     - Disable IGMP Filtering
      cur     - Display current IGMP Filtering configuration
```

Table 171 describes the commands used to configure an IGMP filter.

Table 171 IGMP Filtering Options

Command Syntax and Usage
filter *<filter number (1-16)>* Displays the IGMP Filter Definition menu. To view menu options, see page 289.
port *<port alias or number>* Displays the IGMP Filtering Port menu. To view menu options, see page 290.
ena Enables IGMP filtering globally.
dis Disables IGMP filtering globally.
cur Displays the current IGMP Filtering parameters.

/cfg/l3/igmp/igmpflt/filter <filter number>
IGMP Filter Definition

```
[IGMP Filter 1 Definition Menu]
      range   - Set IP Multicast address range
      action  - Set filter action
      ena     - Enable filter
      dis     - Disable filter
      del     - Delete filter
      cur     - Display current IGMP filter configuration
```

Table 172 describes the commands used to define an IGMP filter.

Table 172 IGMP Filter Definition Options

Command Syntax and Usage
range *<IP multicast address (such as 224.0.0.10)>* *<IP multicast address>* Configures the range of IP multicast addresses for this filter.
action allow|deny Allows or denies multicast traffic for the IP multicast addresses specified.
ena Enables this IGMP filter.
dis Disables this IGMP filter.
del Deletes this filter's parameter definitions.
cur Displays the current IGMP filter.

/cfg/l3/igmp/igmpflt/port <port number>
IGMP Filtering Port Configuration

```
[IGMP Port 1 Menu]
      filt    - Enable/disable IGMP filtering on port
      add     - Add IGMP filter to port
      rem     - Remove IGMP filter from port
      cur     - Display current IGMP filtering Port configuration
```

Table 173 describes the commands used to configure a port for IGMP filtering.

Table 173 IGMP Filter Port Options

Command Syntax and Usage
filt enable|disable Enables or disables IGMP filtering on this port.
add *<filter number (1-16)>* Adds an IGMP filter to this port.
rem *<filter number (1-16)>* Removes an IGMP filter from this port.
cur Displays the current IGMP filter parameters for this port.

/cfg/l3/igmp/querier <VLAN number>
IGMP Querier Configuration

```
[IGMP Querier VLAN 1 Menu]
     type     - Set IGMP querier type
     time     - Set Queriers max response time
     interval - Set IGMP querier interval
     robust   - Set Queriers robustness
     srcip    - Set source IP to be used for IGMP
     count    - Set startup count for IGMP
     sinter   - Set startup query interval for IGMP
     version  - Sets the operating version of the IGMP snooping switch
     on       - Globally turn IGMP Querier ON
     off      - Globally turn IGMP Querier OFF
     default  - Set IGMP Querier settings to factory default
     cur      - Display current IGMP Querier configuration
```

Table 171 describes the commands used to configure IGMP Querier.

Table 174 IGMP Querier Options

Command Syntax and Usage
type [ipv4|mac] Sets the IGMP Querier election criteria as IPv4 address or Mac address. The default setting is IPv4.
time *<1-256>* Configures the maximum time, in tenths of a second, allowed before responding to a Membership Query message. The default value is 100. By varying the Query Response Intrerval, an administrator may tune the burstiness of IGMP messages on the subnet; larger values make the traffic less bursty, as host responses are spread out over a larger interval.
interval *<1-608>* Configures the interval between IGMP Query broadcasts.
robust *<2-10>* Configures the IGMP Robustness variable, which is the number of times that the switch sends each IGMP message. The default value is 2.
srcip *<IP address>* Configures the IGMP snooping source IP address for the selected VLAN.

Table 174 IGMP Querier Options

Command Syntax and Usage
count *<1-10>* Configures the Startup Query Count, which is the number of IGMP Queries sent out at startup. Each Query is separated by the Startup Query Interval.
sinter *<1-608>* Configures the Startup Query Interval, which is the interval between General Queries sent out at startup.
version [v1|v2|v3] Configures the IGMP version.
on Globally turns IGMP Querier on.
off Globally turns IGMP Querier off.
default Resets IGMP Querier parameters to default values.
cur Displays the current IGMP Querier parameters.

/cfg/l3/dns
Domain Name System Configuration

```
[Domain Name System Menu]
     prima    - Set IP address of primary DNS server
     secon    - Set IP address of secondary DNS server
     dname    - Set default domain name
     cur      - Display current DNS configuration
```

The Domain Name System (DNS) menu is used for defining the primary and secondary DNS servers on your local network, and for setting the default domain name served by the switch services. DNS parameters must be configured prior to using hostname parameters with the `ping`, `traceroute`, and `tftp` commands.

Table 175 Domain Name Service Options

Command Syntax and Usage
prima *<IPv4 address (such as 192.4.17.101)>* You are prompted to set the IP address for your primary DNS server. To set an IPv4 address, use dotted decimal notation.
secon *<IPv4 address (such as 192.4.17.101)>* You are prompted to set the IP address for your secondary DNS server. To set an IPv4 address, use dotted decimal notation. If the primary DNS server fails, the configured secondary will be used instead. Enter the IP address using dotted decimal notation.
dname *<dotted DNS notation>* | **none** Sets the default domain name used by the switch. For example: `mycompany.com`
cur Displays the current Domain Name System settings.

/cfg/l3/bootp
Bootstrap Protocol Relay Configuration

```
[Bootstrap Protocol Relay Menu]
      addr    - Set IP address of BOOTP server
      addr2   - Set IP address of second BOOTP server
      on      - Globally turn BOOTP relay ON
      off     - Globally turn BOOTP relay OFF
      cur     - Display current BOOTP relay configuration
```

The Bootstrap Protocol (BOOTP) Relay menu is used to allow hosts to obtain their configurations from a Dynamic Host Configuration Protocol (DHCP) server. The BOOTP configuration enables the switch to forward a client request for an IP address to two DHCP/BOOTP servers with IP addresses that have been configured on the G8124.

BOOTP relay is turned off by default.

Table 176 Bootstrap Protocol Relay Configuration Options

Command Syntax and Usage
addr *<IPv4 address (such as 192.4.17.101)>* Sets the IP address of the BOOTP server. To set an IPv4 address, use dotted decimal notation.
addr2 *<IPv4 address (such as 192.4.17.101)>* Sets the IP address of the second BOOTP server. To set an IPv4 address, use dotted decimal notation.
on Globally turns on BOOTP relay.
off Globally turns off BOOTP relay.
cur Displays the current BOOTP relay configuration.

/cfg/l3/vrrp
VRRP Configuration

```
[Virtual Router Redundancy Protocol Menu]
      vr      - VRRP Virtual Router menu
      group   - VRRP Virtual Router Group menu
      if      - VRRP Interface menu
      track   - VRRP Priority Tracking menu
      on      - Globally turn VRRP ON
      off     - Globally turn VRRP OFF
      cur     - Display current VRRP configuration
```

Virtual Router Redundancy Protocol (VRRP) support on the G8124 provides redundancy between routers in a LAN. This is accomplished by configuring the same virtual router IP address and ID number on each participating VRRP-capable routing device. One of the virtual routers is then elected as the master, based on a number of priority criteria, and assumes control of the shared virtual router IP address. If the master fails, one of the backup virtual routers will assume routing authority and take control of the virtual router IP address.

By default, VRRP is disabled. BLADE OS has extended VRRP to include virtual servers as well, allowing for full active/active redundancy between switches. For more information on VRRP, see the "High Availability" chapter in the *Application Guide*.

Table 177 VRRP Configuration Options

Command Syntax and Usage
vr *<virtual router number (1-16)>* Displays the VRRP Virtual Router menu. This menu is used for configuring virtual routers on this switch. To view menu options, see page 296.
group Displays the VRRP Virtual Router Group menu, used to combine all virtual routers together as one logical entity. Group options must be configured when using two or more switches in a hot-standby failover configuration where only one switch is active at any given time. To view menu options, see page 301.
if *<interface number>* Displays the VRRP Virtual Router Interface menu. To view menu options, see page 304.
track Displays the VRRP Tracking menu. This menu is used for weighting the criteria used when modifying priority levels in the master router election process. To view menu options, see page 305.

Table 177 VRRP Configuration Options

Command Syntax and Usage
on Globally enables VRRP on this switch.
off Globally disables VRRP on this switch.
cur Displays the current VRRP parameters.

/cfg/l3/vrrp/vr *<router number>*
Virtual Router Configuration

```
[VRRP Virtual Router 1 Menu]
      track    - Priority Tracking Menu
      vrid     - Set virtual router ID
      addr     - Set IP address
      if       - Set interface number
      prio     - Set renter priority
      adver    - Set advertisement interval
      predelay - Set preempt-delay interval
      preem    - Enable or disable preemption
      fadver   - Enable/disable fast advertisement
      ena      - Enable virtual router
      dis      - Disable virtual router
      del      - Delete virtual router
      cur      - Display current VRRP virtual router configuration
```

This menu is used for configuring virtual routers for this switch. A virtual router is defined by its virtual router ID and an IP address. On each VRRP-capable routing device participating in redundancy for this virtual router, a virtual router will be configured to share the same virtual router ID and IP address.

Virtual routers are disabled by default.

Table 178 VRRP Virtual Router Options

Command Syntax and Usage
track Displays the VRRP Priority Tracking menu for this virtual router. Tracking is an BLADE OS proprietary extension to VRRP, used for modifying the standard priority system used for electing the master router. To view menu options, see page 299.
vrid *<virtual router ID (1-255)>* Defines the virtual router ID. This is used in conjunction with `addr` (below) to define a virtual router on this switch. To create a pool of VRRP-enabled routing devices which can provide redundancy to each other, each participating VRRP device must be configured with the same virtual router: one that shares the same `vrid` and `addr` combination. The `vrid` for standard virtual routers (where the virtual router IP address is not the same as any virtual server) can be any integer between 1 and 255. The default value is 1. All `vrid` values must be unique within the VLAN to which the virtual router's IP interface belongs.
addr *<IP address (such as, 192.4.17.101)>* Defines the IP address for this virtual router using dotted decimal notation. This is used in conjunction with the `vrid` (above) to configure the same virtual router on each participating VRRP device. The default address is 0.0.0.0.
if *<interface number>* Selects a switch IP interface. If the IP interface has the same IP address as the `addr` option above, this switch is considered the "owner" of the defined virtual router. An owner has a special priority of 255 (highest) and will always assume the role of master router, even if it must pre-empt another virtual router which has assumed master routing authority. This pre-emption occurs even if the `preem` option below is disabled. The default interface is 1.

Table 178 VRRP Virtual Router Options

Command Syntax and Usage
prio *<1-254>* Defines the election priority bias for this virtual server. This can be any integer between 1 and 254. The default value is 100. During the master router election process, the routing device with the highest virtual router priority number wins. If there is a tie, the device with the highest IP interface address wins. If this virtual router's IP address (`addr`) is the same as the one used by the IP interface, the priority for this virtual router will automatically be set to 255 (highest). When priority tracking is used (`/cfg/l3/vrrp/track` or `/cfg/l3/vrrp/vr #/track`), this base priority value can be modified according to a number of performance and operational criteria.
adver *<1-255>* Defines the time interval between VRRP master advertisements. This can be any integer between 1 and 255 seconds. The default value is 1.
predelay *<0-255>* Configures the preempt delay interval. This timer is configured on the VRRP Owner and prevents the switch from transitioning back to Master state until the preempt delay interval has expired. Ensure that the interval is long enough for OSPF or other routing protocols to converge.
preem disable|enable Enables or disables master preemption. When enabled, if this virtual router is in backup mode but has a higher priority than the current master, this virtual router will preempt the lower priority master and assume control. Note that even when `preem` is disabled, this virtual router will always preempt any other master if this switch is the owner (the IP interface address and virtual router `addr` are the same). By default, this option is enabled.
fadver e|d Enables or disables Fast Advertisements. When enabled, the VRRP master advertisements interval is calculated in units of centi-seconds, instead of seconds. For example, if **adver** is set to 1 and **fadver** is enabled, master advertisements are sent every .01 second. When you disable fast advertisement, the advertisement interval is set to the default value of 1 second. To support Fast Advertisements, set the interval between 20-100 centi-seconds.
ena Enables this virtual router.

Table 178 VRRP Virtual Router Options

Command Syntax and Usage
dis Disables this virtual router.
del Deletes this virtual router from the switch configuration.
cur Displays the current configuration information for this virtual router.

/cfg/l3/vrrp/vr *<router number>*/track
Virtual Router Priority Tracking Configuration

```
[VRRP Virtual Router 1 Priority Tracking Menu]
      vrs     - Enable/disable tracking master virtual routers
      ifs     - Enable/disable tracking other interfaces
      ports   - Enable/disable tracking VLAN switch ports
      cur     - Display current VRRP virtual router configuration
```

This menu is used for modifying the priority system used when electing the master router from a pool of virtual routers. Various tracking criteria can be used to bias the election results. Each time one of the tracking criteria is met, the priority level for the virtual router is increased by an amount defined through the VRRP Tracking menu (see page 305).

Criteria are tracked dynamically, continuously updating virtual router priority levels when enabled. If the virtual router pre-emption option (see `preem` in Table 178 on page 297) is enabled, this virtual router can assume master routing authority when its priority level rises above that of the current master.

Some tracking criteria (`vrs`, `ifs`, and `ports` below) apply to standard virtual routers, otherwise called "virtual interface routers." A virtual *server* router is defined as any virtual router whose IP address (`addr`) is the same as any configured virtual server IP address.

Table 179 Virtual Router Priority Tracking Options

Command Syntax and Usage
vrs disable|enable When enabled, the priority for this virtual router will be increased for each virtual router in master mode on this switch. This is useful for making sure that traffic for any particular client/server pairing are handled by the same switch, increasing routing and load balancing efficiency. This command is disabled by default.
ifs disable|enable When enabled, the priority for this virtual router will be increased for each other IP interface active on this switch. An IP interface is considered active when there is at least one active port on the same VLAN. This helps elect the virtual routers with the most available routes as the master. This command is disabled by default.
ports disable|enable When enabled, the priority for this virtual router will be increased for each active port on the same VLAN. A port is considered "active" if it has a link and is forwarding traffic. This helps elect the virtual routers with the most available ports as the master. This command is disabled by default.
cur Displays the current configuration for priority tracking for this virtual router.

/cfg/l3/vrrp/group
Virtual Router Group Configuration

```
[VRRP Virtual Router Group Menu]
      track   - Priority Tracking Menu
      vrid    - Set virtual router ID
      if      - Set interface number
      prio    - Set renter priority
      adver   - Set advertisement interval
      preem   - Enable or disable preemption
      fadver  - Enable/disable fast advertisement
      ena     - Enable virtual router
      dis     - Disable virtual router
      del     - Delete virtual router
      cur     - Display current VRRP virtual router configuration
```

The Virtual Router Group menu is used for associating all virtual routers into a single logical virtual router, which forces all virtual routers on the G8124 to either be master or backup as a group. A virtual router is defined by its virtual router ID and an IP address. On each VRRP-capable routing device participating in redundancy for this virtual router, a virtual router will be configured to share the same virtual router ID and IP address.

Note – This option is required to be configured only when using at least two G8124s in a hot-standby failover configuration, where only one switch is active at any time.

Table 180 Virtual Router Group Options

Command Syntax and Usage
track Displays the VRRP Priority Tracking menu for the virtual router group. Tracking is an BLADE OS proprietary extension to VRRP, used for modifying the standard priority system used for electing the master router. To view menu options, see page 303.
vrid *<virtual router ID (1-255)>* Defines the virtual router ID. The `vrid` for standard virtual routers (where the virtual router IP address is not the same as any virtual server) can be any integer between 1 and 255. All `vrid` values must be unique within the VLAN to which the virtual router's IP interface (see `if` below) belongs. The default virtual router ID is 1.
if *<interface number>* Selects a switch IP interface. The default switch IP interface number is 1.

Table 180 Virtual Router Group Options

Command Syntax and Usage
prio *<1-254>* Defines the election priority bias for this virtual router group. This can be any integer between 1 and 254. The default value is 100. During the master router election process, the routing device with the highest virtual router priority number wins. If there is a tie, the device with the highest IP interface address wins. If this virtual router's IP address (`addr`) is the same as the one used by the IP interface, the priority for this virtual router will automatically be set to 255 (highest). When priority tracking is used (`/cfg/l3/vrrp/track` or `/cfg/l3/vrrp/vr #/track`), this base priority value can be modified according to a number of performance and operational criteria.
adver *<1-255>* Defines the time interval between VRRP master advertisements. This can be any integer between 1 and 255 seconds. The default is 1.
preem disable|enable Enables or disables master preemption. When enabled, if the virtual router group is in backup mode but has a higher priority than the current master, this virtual router will preempt the lower priority master and assume control. Note that even when `preem` is disabled, this virtual router will always preempt any other master if this switch is the owner (the IP interface address and virtual router `addr` are the same). By default, this option is `enabled`.
fadver Enables or disables Fast Advertisements. When enabled, the VRRP master advertisements interval is calculated in units of centi-seconds, instead of seconds. For example, if **adver** is set to 1 and **fadver** is enabled, master advertisements are sent every .01 second. When you disable fast advertisement, the advertisement interval is set to the default value of 1 second. To support Fast Advertisements, set the interval between 20-100 centi-seconds.
ena Enables the virtual router group.
dis Disables the virtual router group.

Table 180 Virtual Router Group Options

Command Syntax and Usage
del Deletes the virtual router group from the switch configuration.
cur Displays the current configuration information for the virtual router group.

/cfg/l3/vrrp/group/track
Virtual Router Group Priority Tracking Configuration

```
[Virtual Router Group Priority Tracking Menu]
      ifs     - Enable/disable tracking other interfaces
      ports   - Enable/disable tracking VLAN switch ports
      cur     - Display current VRRP Group Tracking configuration
```

Note – If *Virtual Router Group Tracking* is enabled, then the tracking option will be available only under *group* option. The tracking setting for the other individual virtual routers will be ignored.

Table 181 Virtual Router Group Priority Tracking Options

Command Syntax and Usage
ifs disable|enable When enabled, the priority for this virtual router will be increased for each other IP interface active on this switch. An IP interface is considered active when there is at least one active port on the same VLAN. This helps elect the virtual routers with the most available routes as the master. This command is disabled by default.
ports disable|enable When enabled, the priority for this virtual router will be increased for each active port on the same VLAN. A port is considered “active” if it has a link and is forwarding traffic. This helps elect the virtual routers with the most available ports as the master. This command is disabled by default.
cur Displays the current configuration for priority tracking for this virtual router.

/cfg/l3/vrrp/if <interface number>
VRRP Interface Configuration

Note – The *interface-number* represents the IP interface on which authentication parameters must be configured.

```
[VRRP Interface 1 Menu]
      auth    - Set authentication types
      passw   - Set plain-text password
      del     - Delete interface
      cur     - Display current VRRP interface configuration
```

This menu is used for configuring VRRP authentication parameters for the IP interfaces used with the virtual routers.

Table 182 VRRP Interface Options

Command Syntax and Usage
auth none|password Defines the type of authentication that will be used: `none` (no authentication), or `password` (password authentication).
passw <*password*> Defines a plain text password up to eight characters long. This password will be added to each VRRP packet transmitted by this interface when password authentication is chosen (see **auth** above).
del Clears the authentication configuration parameters for this IP interface. The IP interface itself is not deleted.
cur Displays the current configuration for this IP interface's authentication parameters.

/cfg/l3/vrrp/track
VRRP Tracking Configuration

```
[VRRP Tracking Menu]
      vrs     - Set priority increment for virtual router tracking
      ifs     - Set priority increment for IP interface tracking
      ports   - Set priority increment for VLAN switch port tracking
      cur     - Display current VRRP Priority Tracking configuration
```

This menu is used for setting weights for the various criteria used to modify priority levels during the master router election process. Each time one of the tracking criteria is met (see "VRRP Virtual Router Priority Tracking" on page 299), the priority level for the virtual router is increased by an amount defined through this menu.

Table 183 VRRP Tracking Options

Command Syntax and Usage
vrs *<0-254>* Defines the priority increment value (0 through 254) for virtual routers in master mode detected on this switch. The default value is 2.
ifs *<0-254>* Defines the priority increment value (0 through 254) for active IP interfaces detected on this switch. The default value is 2.
ports *<0-254>* Defines the priority increment value (0 through 254) for active ports on the virtual router's VLAN. The default value is 2.
cur Displays the current configuration of priority tracking increment values.

Note – These priority tracking options only define increment values. These options do not affect the VRRP master router election process until options under the VRRP Virtual Router Priority Tracking menu (see page 299) are enabled.

/cfg/setup
Setup

The setup program steps you through configuring the system date and time, BOOTP, IP, Spanning Tree, port speed/mode, VLAN parameters, and IP interfaces.

To start the setup program, at the `Configuration#` prompt, enter:

```
Configuration# setup
```

For a complete description of how to use `setup`, see "First-Time Configuration" on page 21.

/cfg/dump
Dump

The dump program writes the current switch configuration to the terminal screen. To start the dump program, at the `Configuration#` prompt, enter:

```
Configuration# dump
```

The configuration is displayed with parameters that have been changed from the default values. The screen display can be captured, edited, and placed in a script file, which can be used to configure other switches through a Telnet connection. When using Telnet to configure a new switch, paste the configuration commands from the script file at the command line prompt of the switch. The active configuration can also be saved or loaded via TFTP, as described on page 307.

/cfg/ptcfg <FTP/TFTP server> <filename>
Saving the Active Switch Configuration

When the ptcfg command is used, the switch's active configuration commands (as displayed using /cfg/dump) will be uploaded to the specified script configuration file on the FTP/TFTP server. To start the switch configuration upload, at the Configuration# prompt, enter:

```
Configuration# ptcfg <FTP or TFTP server> <filename>
```

Where *server* is the FTP/TFTP server IPv4 address or hostname, and *filename* is the name of the target script configuration file. The output file is formatted with line-breaks but no carriage returns—the file cannot be viewed with editors that require carriage returns (such as Microsoft Notepad).

Note – If the FTP/TFTP server is running SunOS or the Solaris operating system, the specified ptcfg file must exist prior to executing the ptcfg command and must be writable (set with proper permission, and not locked by any application). The contents of the specified file will be replaced with the current configuration data.

/cfg/gtcfg <FTP/TFTP server> <filename>
Restoring the Active Switch Configuration

When the gtcfg command is used, the active configuration will be replaced with the commands found in the specified configuration file. The file can contain a full switch configuration or a partial switch configuration. The configuration loaded using gtcfg is not activated until the apply command is used. If the apply command is found in the configuration script file loaded using this command, the apply action will be performed automatically.

To start the switch configuration download, at the Configuration# prompt, enter:

```
Configuration# gtcfg <FTP or TFTP server> <filename>
```

Where *server* is the FTP/TFTP server IPv4 address or hostname, and *filename* is the name of the target script configuration file.

CHAPTER 7

The Operations Menu

The Operations menu is generally used for commands that affect switch performance immediately, but do not alter permanent switch configurations. For example, you can use the Operations menu to immediately disable a port (without the need to apply or save the change), with the understanding that when the switch is reset, the port returns to its normally configured operation.

/oper
Operations Menu

```
[Operations Menu]
     port     - Operational Port Menu
     vrrp     - Operational Virtual Router Redundancy Menu
     sys      - Operational System Menu
     passwd   - Change current user password
     clrlog   - Clear syslog messages
     tnetsshc - Close all telnet/SSH connections
     cfgtrk   - Track last config change made
     ntpreq   - Send NTP request
```

The commands of the Operations menu enable you to alter switch operational characteristics without affecting switch configuration.

Table 184 Operations Menu Options

Command Syntax and Usage
port *<port alias or number>* Displays the Operational Port menu. To view menu options, see page 311.
vrrp Displays the Operational Virtual Router Redundancy menu. To view menu options, see page 312.
sys Displays the Operational System menu. To view menu options, see page 312.
passwd *<1-128 characters>* Allows the user to change the password. You need to enter the current password in use for validation.
clrlog Clears all Syslog messages.
tnetsshc Closes all open Telnet and SSH connections.
cfgtrk Displays a list of configuration changes made since the last `apply` command. Each time the `apply` command is sent, the configuration-tracking log is cleared.
ntpreq Allows the user to send requests to the NTP server.

/oper/port <port alias or number>

Operations-Level Port Options

```
[Operations Port 1 Menu]
     ena       - Enable port
     dis       - Disable port
     lena      - Enable FDB Learning
     ldis      - Disable FDB Learning
     cur       - Current port state
```

Operations-level port options are used for temporarily disabling or enabling a port, and for re-setting the port.

Table 185 Operations-Level Port Options

Command Syntax and Usage
ena Temporarily enables the port. The port will be returned to its configured operation mode when the switch is reset.
dis Temporarily disables the port. The port will be returned to its configured operation mode when the switch is reset.
lena Temporarily enables FDB learning on the port.
ldis Temporarily disables FDB learning on the port.
cur Displays the current settings for the port.

/oper/vrrp
Operations-Level VRRP Options

```
[VRRP Operations Menu]
        back    - Set virtual router to backup
```

Table 186 Operations-Level VRRP Options

Command Syntax and Usage

back {<*virtual router number (1-128)*>**|group}**

Forces the specified master virtual router on this switch into backup mode. This is generally used for passing master control back to a preferred switch once the preferred switch has been returned to service after a failure. When this command is executed, the current master gives up control and initiates a new election by temporarily advertising its own priority level as 0 (lowest). After the new election, the virtual router forced into backup mode by this command will resume master control in the following cases:

- This switch owns the virtual router (the IP addresses of the virtual router and its IP interface are the same)
- This switch's virtual router has a higher priority and preemption is enabled.
- There are no other virtual routers available to take master control.

/oper/sys
System Operations

```
[Operational System Menu]
     i2c       - System I2C
```

I2C device commands are to be used only by Technical Support personnel.

CHAPTER 8

The Boot Options Menu

To use the Boot Options menu, you must be logged in to the switch as the administrator. The Boot Options menu provides options for:

- Selecting a switch software image to be used when the switch is next reset
- Selecting a configuration block to be used when the switch is next reset
- Downloading or uploading a new software image to the switch via FTP/TFTP

In addition to the Boot Options menu, you can use a Web browser or SNMP to work with switch image and configuration files. To use SNMP, refer to "Switch Images and Configuration Files" on page 379.

/boot
Boot Options

```
[Boot Options Menu]
        image - Select software image to use on next boot
        conf  - Select config block to use on next boot
        mode  - Select CLI mode to use on next boot
        prompt- Prompt for selectable boot mode
        gtimg - Download new software image via TFTP
        ptimg - Upload selected software image via TFTP
        reset - Reset switch [WARNING: Restarts Spanning Tree]
        cur   - Display current boot options
```

Each of these options is discussed in greater detail in the following sections.

Updating the Switch Software Image

The switch software image is the executable code running on the RackSwitch G8124. A version of the image ships with the switch, and comes pre-installed on the device. As new versions of the image are released, you can upgrade the software running on your switch.

On the support site, click on software updates. On the switch, use the `/boot/cur` command to determine the current software version.

The typical upgrade process for the software image consists of the following steps:

- Place the new image onto a FTP or TFTP server on your network, or on a local computer.
- Transfer the new image to your switch.
- Select the new software image to be loaded into switch memory the next time the switch is reset.

Loading New Software to Your Switch

The switch can store up to two different software images, called `image1` and `image2`, as well as boot software, called `boot`. When you load new software, you must specify where it should be placed: either into `image1`, `image2`, or `boot`.

For example, if your active image is currently loaded into `image1`, you would probably load the new image software into `image2`. This lets you test the new software and reload the original active image (stored in `image1`), if needed.

To load a new software image to your switch, you need the following:

- The image or boot software loaded on a FTP/TFTP server on your network
- The hostname or IPv4 address of the FTP/TFTP server
- The name of the new software image or boot file

Note – The DNS parameters must be configured if specifying hostnames. See "Domain Name System Configuration" on page 293.

When the above requirements are met, use the following procedure to download the new software to your switch.

1. At the `Boot Options#` prompt, enter:

```
Boot Options# gtimg
```

2. Enter the name of the switch software to be replaced:

```
Enter name of switch software image to be replaced
 ["image1"/"image2"/"boot"]: <image>
```

3. Enter the hostname or IPv4 address of the FTP or TFTP server.

```
Enter hostname or IP address of FTP/TFTP server: <name or IP address>
```

4. Enter the name of the new software file on the server.

```
Enter name of file on FTP/TFTP server: <filename>
```

The exact form of the name will vary by server. However, the file location is normally relative to the FTP or TFTP directory (usually `/tftpboot`).

5. Enter your username for the server, if applicable.

```
Enter username for FTP server or hit return for TFTP server: <username>
or <Enter>
```

6. The system prompts you to confirm your request.

You should next select a software image to run, as described below.

Selecting a Software Image to Run

You can select which software image (`image1` or `image2`) you want to run in switch memory for the next reboot.

1. At the `Boot Options#` prompt, enter:

```
Boot Options# image
```

2. Enter the name of the image you want the switch to use upon the next boot.

The system informs you of which image is currently set to be loaded at the next reset, and prompts you to enter a new choice:

```
Currently set to use switch software "image1" on next reset.
Specify new image to use on next reset ["image1"/"image2"]:
```

Uploading a Software Image from Your Switch

You can upload a software image from the switch to a FTP or TFTP server.

1. At the `Boot Options#` prompt, enter:

```
Boot Options# ptimg
```

2. The system prompts you for information. Enter the desired image:

```
Enter name of switch software image to be uploaded
["image1"|"image2"|"boot"]: <image>
```

3. Enter the name or the IPv4 address of the FTP or TFTP server:

```
Enter hostname or IP address of FTP/TFTP server: <name or IP address>
```

4. Enter the name of the file into which the image will be uploaded on the FTP or TFTP server:

```
Enter name of file on FTP/TFTP server: <filename>
```

5. The system then requests confirmation of what you have entered. To have the file uploaded, enter **y**.

```
image2 currently contains Software Version 5.0
 that was downloaded at 0:23:39 Thu Jan  4, 2009.
Upload will transfer image2 (2788535 bytes) to file "image1"
 on FTP/TFTP server 192.1.1.1.
Confirm upload operation (y/n) ? y
```

Selecting a Configuration Block

When you make configuration changes to the G8124, you must save the changes so that they are retained beyond the next time the switch is reset. When you perform the `save` command, your new configuration changes are placed in the *active* configuration block. The previous configuration is copied into the *backup* configuration block.

There is also a *factory* configuration block. This holds the default configuration set by the factory when your G8124 was manufactured. Under certain circumstances, it may be desirable to reset the switch configuration to the default. This can be useful when a custom-configured G8124 is moved to a network environment where it will be re-configured for a different purpose.

Use the following procedure to set which configuration block you want the switch to load the next time it is reset:

1. At the `Boot Options#` prompt, enter:

```
Boot Options# conf
```

2. Enter the name of the configuration block you want the switch to use:

   The system informs you of which configuration block is currently set to be loaded at the next reset, and prompts you to enter a new choice:

```
Currently set to use active configuration block on next reset.
Specify new block to use ["active"/"backup"/"factory"]:
```

Resetting the Switch

You can reset the switch to make your software image file and configuration block changes occur.

Note – Resetting the switch causes the Spanning Tree Group to restart. This process can be lengthy, depending on the topology of your network.

To reset the switch, at the `Boot Options#` prompt, enter:

```
>> Boot Options# reset
```

You are prompted to confirm your request.

Accessing the ISCLI

The default command-line interface for the G8124 is the BLADE OS CLI. To access the ISCLI, enter the following command and reset the G8124:

```
Main# boot/mode iscli
```

To access the BLADE OS CLI, enter the following command from the ISCLI and reload the G8124:

```
Switch (config)# boot cli-mode bladeos-cli
```

Users can select the CLI mode upon login, if the `/boot/prompt` command is enabled. Only an administrator can view and enable `/boot/prompt`. When `/boot/prompt` is enabled, the first user to log in can select the CLI mode. Subsequent users must use the selected CLI mode, until all users have logged out.

CHAPTER 9

The Maintenance Menu

The Maintenance menu is used to manage dump information and forward database information. It also includes a debugging menu to help with troubleshooting.

/maint
Maintenance Menu

Note – To use the Maintenance menu, you must be logged in to the switch as the administrator.

```
[Maintenance Menu]
     sys       - System Maintenance Menu
     fdb       - Forwarding Database Manipulation Menu
     debug     - Debugging Menu
     arp       - ARP Cache Manipulation Menu
     route     - IP Route Manipulation Menu
     igmp      - IGMP Multicast Group Menu
     uudmp     - Uuencode FLASH dump
     ptdmp     - Upload FLASH dump via FTP/TFTP
     cldmp     - Clear FLASH dump
     tsdmp     - Tech support dump
     pttsdmp   - Upload tech support dump via FTP/TFTP
```

Dump information contains internal switch state data that is written to flash memory on the RackSwitch G8124 after any one of the following occurs:

- The watchdog timer forces a switch reset. The purpose of the watchdog timer is to reboot the switch if the switch software freezes.
- The switch detects a hardware or software problem that requires a reboot.

Table 187 Maintenance Menu Options (/maint)

Command Syntax and Usage
sys Displays the System Maintenance menu. To view menu options, see page 321.
fdb Displays the Forwarding Database Manipulation menu. To view menu options, see page 322.
debug Displays the Debugging menu. To view menu options, see page 323.
arp Displays the ARP Cache Manipulation menu. To view menu options, see page 324.
route Displays the IP Route Manipulation menu. To view menu options, see page 325.
igmp Displays the IGMP Maintenance menu. To view menu options, see page 326.
uudmp Displays dump information in uuencoded format. For details, see page 329.
ptdmp *<host name> <file name>* Saves the system dump information via TFTP. For details, see page 329.
cldmp Clears dump information from flash memory. For details, see page 330.
tsdmp Dumps all G8124 information, statistics, and configuration.You can log the tsdump output into a file.
pttsdmp Redirects the technical support dump (tsdmp) to an external TFTP server.

/maint/sys
System Maintenance

This menu is reserved for use by Technical Support personnel. The options are used to perform system debugging.

```
[System Maintenance Menu]
      flags    - Set NVRAM flag word
      tmask    - Set MP trace mask word
```

Table 188 System Maintenance Options

Command Syntax and Usage
flags *<new NVRAM flags word as 0xXXXXXXXX>* This command sets the flags that are used for debugging purposes by Technical Support personnel.
tmask *<new trace mask word as 0xXXXXXXXX>* [**p**] This command sets the trace mask that is used for debugging purposes by Technical Support personnel.

/maint/fdb
Forwarding Database Maintenance

```
[FDB Manipulation Menu]
     find     - Show a single FDB entry by MAC address
     port     - Show FDB entries for a single port
     vlan     - Show FDB entries for a single VLAN
     dump     - Show all FDB entries
     del      - Delete an FDB entry
     clear    - Clear entire FDB
```

The Forwarding Database Manipulation menu can be used to view information and to delete a MAC address from the forwarding database or clear the entire forwarding database. This is helpful in identifying problems associated with MAC address learning and packet forwarding decisions.

Table 189 FDB Manipulation Options

Command Syntax and Usage
find *<MAC address>* [*<VLAN number>*] Displays a single database entry by its MAC address. You are prompted to enter the MAC address of the device. Enter the MAC address using one of the following formats: □ `xx:xx:xx:xx:xx:xx` (such as `08:00:20:12:34:56`) □ `xxxxxxxxxxxx` (such as `080020123456`)
port *<port alias or number>* Displays all FDB entries for a particular port.
vlan *<VLAN number>* Displays all FDB entries on a single VLAN.
dump Displays all entries in the Forwarding Database. For details, see page 64.
del *<MAC address>* [*<VLAN number>*] Removes a single FDB entry.
clear Clears the entire Forwarding Database from switch memory.

/maint/debug
Debugging

```
[Miscellaneous Debug Menu]
     tbuf     - Show MP trace buffer
     snap     - Show MP snap (or post-mortem) trace buffer
     clrcfg   - Clear all flash configs
```

The Miscellaneous Debug menu displays trace buffer information about events that can be helpful in understanding switch operation. You can view the following information using the debug menu:

- Events traced by the Management Processor (MP)
- Events traced to a buffer area when a reset occurs

If the switch resets for any reason, the MP trace buffer is saved into the snap trace buffer area. The output from these commands can be interpreted by Technical Support personnel.

Table 190 Miscellaneous Debug Options

Command Syntax and Usage
tbuf Displays the Management Processor trace buffer. Header information similar to the following is shown: `MP trace buffer at 13:28:15 Fri May 30, 2008; mask: 0x2ffdf748` The buffer information is displayed after the header.
snap Displays the Management Processor snap (or post-mortem) trace buffer. This buffer contains information traced at the time that a reset occurred.
clrcfg Deletes all flash configuration blocks.

/maint/arp
ARP Cache Maintenance

```
[Address Resolution Protocol Menu]
     find      - Show a single ARP entry by IP address
     port      - Show ARP entries on a single port
     vlan      - Show ARP entries on a single VLAN
     addr      - Show ARP entries for switch's interfaces
     dump      - Show all ARP entries
     clear     - Clear ARP cache
```

Table 191 ARP Maintenance Options

Command Syntax and Usage

find *<IP address (such as, 192.4.17.101)>*

Shows a single ARP entry by IP address.

port *<port alias or number>*

Shows ARP entries on a single port.

vlan *<VLAN number>*

Shows ARP entries on a single VLAN.

addr

Shows the list of IP addresses which the switch will respond to for ARP requests.

dump

Shows all ARP entries.

clear

Clears the entire ARP list from switch memory.

Note – To display all ARP entries currently held in the switch, or a portion according to one of the options listed on the menu above (`find`, `port`, `vlan`, `dump`), you can also refer to "ARP Information" on page 85.

/maint/route

IP Route Manipulation

```
[IP Routing Menu]
        find  - Show a single route by destination IP address
        gw    - Show routes to a single gateway
        type  - Show routes of a single type
        tag   - Show routes of a single tag
        if    - Show routes on a single interface
        dump  - Show all routes
        clear - Clear route table
```

Table 192 IP Route Manipulation Options

Command Syntax and Usage
find *<IP address (such as, 192.4.17.101)>* Shows a single route by destination IP address.
gw *<default gateway address (such as, 192.4.17.44)>* Shows routes to a default gateway.
type indirect|direct|local|broadcast|martian|multicast Shows routes of a single type. For a description of IP routing types, see Table 27 on page 83
tag fixed|static|addr|rip|ospf|broadcast|martian|multicast Shows routes of a single tag. For a description of IP routing tags, see Table 28 on page 84
if *<interface number>* Shows routes on a single interface.
dump Shows all routes.
clear Clears the route table from switch memory.

Note – To display all routes, you can also refer to "IP Routing Information" on page 82.

/maint/igmp
IGMP Maintenance

```
[IGMP Multicast Group Menu]
     snoop    - IGMP Snooping Menu
     mrouter  - IGMP Multicast Router Port Menu
     clear    - Clear group and mrouter tables
```

Table 193 describes the IGMP Maintenance commands.

Table 193 IGMP Maintenance Options

Command Syntax and Usage
group Displays the IGMP Snooping maintenance menu. To view menu options, see page 327.
mrouter Displays the Multicast Router Port menu. To view menu options, see page 326.
clear Clears the IGMP group table and Mrouter tables.

/maint/igmp/snoop
IGMP Group Maintenance

```
[IGMP Multicast Group Menu]
     find     - Show a single group by IP group address
     vlan     - Show groups on a single vlan
     port     - Show groups on a single port
     trunk    - Show groups on a single trunk
     detail   - Show detail of a single group by IP address
     dump     - Show all groups
     clear    - Clear group tables
```

Table 193 describes the IGMP Snooping maintenance commands.

Table 194 IGMP Snooping Maintenance Options

Command Syntax and Usage
find *<IP address>* Displays a single IGMP multicast group by its IP address.
vlan *<VLAN number>* Displays all IGMP multicast groups on a single VLAN.
port *<port number or alias>* Displays all IGMP multicast groups on a single port.
trunk *<trunk number>* Displays all IGMP multicast groups on a single trunk group.
detail *<IP address>* Displays detailed information about a single IGMP multicast group.
dump Displays information for all multicast groups.
clear Clears the IGMP group tables.

/maint/igmp/mrouter
IGMP Multicast Routers Maintenance

```
[IGMP Multicast Routers Menu]
     vlan     - Show all multicast router ports on a single vlan
     dump     - Show all multicast router ports
     clear    - Clear multicast router port table
```

Table 195 describes the IGMP multicast router (Mrouter) maintenance commands.

Table 195 IGMP Mrouter Maintenance Options

Command Syntax and Usage
vlan *<VLAN number>* Shows all IGMP multicast router ports on a single VLAN.
dump Shows all multicast router ports.
clear Clears the IGMP Multicast Router port table.

/maint/uudmp
Uuencode Flash Dump

Using this command, dump information is presented in uuencoded format. This format makes it easy to capture the dump information as a file or a string of characters.

If you want to capture dump information to a file, set your communication software on your workstation to capture session data prior to issuing the `uudmp` command. This will ensure that you do not lose any information. Once entered, the `uudmp` command will cause approximately 23,300 lines of data to be displayed on your screen and copied into the file.

Using the `uudmp` command, dump information can be read multiple times. The command does not cause the information to be updated or cleared from flash memory.

Note – Dump information is not cleared automatically. In order for any subsequent dump information to be written to flash memory, you must manually clear the dump region. For more information on clearing the dump region, see page 330.

To access dump information, at the `Maintenance#` prompt, enter:

```
Maintenance# uudmp
```

The dump information is displayed on your screen and, if you have configured your communication software to do so, captured to a file. If the dump region is empty, the following appears:

```
No FLASH dump available.
```

/maint/ptdmp *<FTP/TFTP server> <filename>*
FTP/TFTP System Dump Put

Use this command to `put` (save) the system dump to a FTP/TFTP server.

Note – If the FTP/TFTP server is running SunOS or the Solaris operating system, the specified `ptdmp` file must exist *prior* to executing the `ptdmp` command, and must be writable (set with proper permission, and not locked by any application). The contents of the specified file will be replaced with the current dump data.

To save dump information via FTP/TFTP, at the `Maintenance#` prompt, enter:

```
Maintenance# ptdmp <FTP/TFTP server> <filename>
```

Where *server* is the FTP/TFTP server IPv4 address or hostname, and *filename* is the target dump file.

/maint/cldmp

Clearing Dump Information

To clear dump information from flash memory, at the `Maintenance#` prompt, enter:

```
Maintenance# cldmp
```

The switch clears the dump region of flash memory and displays the following message:

```
FLASH dump region cleared.
```

If the flash dump region is already clear, the switch displays the following message:

```
FLASH dump region is already clear.
```

Unscheduled System Dumps

If there is an unscheduled system dump to flash memory, the following message is displayed when you log on to the switch:

```
Note: A system dump exists in FLASH. The dump was saved
      at 13:43:22 Wednesday January 30, 2009. Use /maint/uudmp to
      extract the dump for analysis and /maint/cldmp to
      clear the FLASH region. The region must be cleared
      before another dump can be saved.
```

APPENDIX A
BLADE OS Syslog Messages

The following syntax is used when outputting syslog messages:

<*Time stamp*><*Log Label*>BLADEOS<*Thread ID*>**:**<*Message*>

The following parameters are used:

- <*Timestamp*>

  The time of the message event is displayed in month day hour:minute:second format. For example: `Aug 19 14:20:30`

- <*Log Label*>

  The following types of log messages are recorded: `LOG_EMERG`, `LOG_ALERT`, `LOG_CRIT`, `LOG_ERR`, `LOG_WARNING`, `LOG_NOTICE`, `LOG_INFO`, and `LOG_DEBUG`

- <*Thread ID*>

  This is the software thread that reports the log message, such as: `stg`, `ip`, `console`, `telnet`, `vrrp`, `system`, `web server`, `ssh`

- <*Message*>: The log message

Following is a list of potential syslog messages. To keep this list as short as possible, only the <*Thread ID*> and <*Message*> are shown. The messages are sorted by <*Log Label*>.

Where the <*Thread ID*> is listed as `mgmt`, one of the following may be shown: `console`, `telnet`, `web server`, or `ssh`.

LOG_CRIT

Thread	Message
SSH	can't allocate memory in load_MP_INT()
SSH	currently not enough resource for loading RSA {private | public key}
SYSTEM	System memory is at <*n*> percent

Log_WARNING

Thread	Message
	There is an IP address (<*IP address*>) conflict on the network.
CFG	Authentication should be disabled to run RIPv2 in RIPv1 compatibility mode on interface <*interface*>.
CFG	Multicast should be disabled to run RIPv2 in RIPv1 compatibility mode on interface <*interface*>.
HOTLINKS	"Error" is set to "Standby | Active"
HOTLINKS	"Learning" is set to "Standby | Active"
HOTLINKS	"None" is set to "Standby | Active"
HOTLINKS	"Side Max" is set to "Standby | Active"
HOTLINKS	has no "{Side Max | None | Learning | Error}" interface
IP	IGMP: Switch {became | is no longer} a Querier for Vlan <*VLAN*>
IP	IGMP: Switch is [not] elected as Querier for Vlan <*VLAN*>
IP	IGMP: Switch Querier election process started for Vlan <*VLAN*>
IP	IGMP: Switch Querier election type changed for Vlan <*VLAN*>
IP	IGMP: Querier {disabled | enabled} on Vlan <*VLAN*>
IP	IGMP: Warning Querier Source-IP is not configured on Vlan <*VLAN*> Queries with Source-IP Zero may be ignored in Querier election process.
IP	IGMP: Warning Snooping is not enabled on Vlan <*VLAN*>, Querier configured only to send queries.
NTP	cannot contact NTP server <*IP address*> - {Mgmt | Ext-mgt} port unavailable
NTP	cannot contact [primary | secondary] NTP server <*IP address*>

Thread	Message
SYSTEM	I2C device <*ID*> <*description*> set to access state <*state*> [from CLI]
SYSTEM	Interface <interface> failed to renew DHCP Lease. Use factory default while requesting for a new DHCP offer.
TEAMING	error, action is undefined
TEAMING	is down, but teardown is blocked
TEAMING	is down, control ports are auto disabled
TEAMING	is up, control ports are auto controlled

LOG_ALERT

Thread	Message
	Possible buffer overrun attack detected! ■ Connect Retry Expire ■ Holdtime Expire ■ Invalid ■ Keepalive Expire ■ Receive KEEPALIVE ■ Receive NOTIFICATION ■ Receive OPEN ■ Receive UPDATE ■ Start ■ Stop ■ Transport Conn Closed ■ Transport Conn Failed ■ Transport Conn Open ■ Transport Fatal Error
HOTLINKS	LACP trunk <*trunk ID*> and <*trunk ID*> formed with admin key <*key*>
IP	cannot contact default gateway <*IP address*>
IP	cannot contact {MGTA | MGTB} port default gateway <*IP address*>
IP	Dynamic Routing table is full
IP	Route table full
MGMT	Maximum number of login failures (<*threshold*>) has been exceeded.
OSPF	Interface IP <*IP address*>, Interface State {Down | Loopback | Waiting | P To P | DR | BackupDR | DR Other}: Interface down detached
OSPF	LS Database full: likely incorrect/missing routes or failed neighbors

Thread	Message
OSPF	Neighbor Router ID <*router ID*>, Neighbor State {Down | Attempt | Init | 2 Way | ExStart | Exchange | Loading | Full | Loopback | W aiting | P To P | DR | BackupDR | DR Other}
OSPF	OSPF Route table full: likely incorrect/missing routes
STP	CIST new root bridge
STP	CIST topology change detected
STP	Fast Forward port <*port*> active, putting port into forwarding state
STP	New preferred Fast Uplink port <*port*> active for STG <*STG*>, restarting timer
STP	own BPDU received from port <*port*>
STP	Port <*port*>, putting port into blocking state
STP	Preferred STG <*STG*> Fast Uplink port has gone down. Putting secondary Fast Uplink port <*port*> into forwarding
STP	Setting STG <*STG*> Fast Uplink primary port <*port*> forwarding and backup port <*port*> blocking
STP	STG <*STG*> preferred Fast Uplink port <*port*> active. Waiting <*seconds*> seconds before switching from port <*port*>
STP	STG <*STG*>, new root bridge
STP	STG <*STG*>, topology change detected
STP	STG <*STG*> root port <*port*> has gone down. Putting backup Fast Uplink port <*port*> into forwarding
SYSTEM	<*SFP type*> inserted at port <*port*> is UNAPPROVED ! Device is DISABLED.
SYSTEM	LACP trunk <*trunk ID*> and <*trunk ID*> formed with admin key <key>
SYSTEM	link down on management port <*port*>
VRRP	received errored advertisement from <*IP address*>
VRRP	received incorrect addresses from <*IP address*>
VRRP	received incorrect advertisement interval <interval> from <*IP address*>
VRRP	received incorrect VRRP adver type from <*IP address*>
VRRP	received incorrect VRRP authentication type from <*IP address*>
VRRP	received incorrect VRRP password from <*IP address*>

Thread	Message
VRRP	VRRP : received incorrect IP addresses list from <*IP address*>
VRRP	VRRP : received incorrect IP addresses list from <*IP address*>. Received <*number*> virtual routers instead of <*IP address*>

LOG_ERR

Thread	Message
CFG	Configuration file is EMPTY
CFG	Configuration is too large
CFG	Default VLAN cannot be a private-VLAN.
CFG	Error writing active config to FLASH! Another save is in progress
CFG	Error writing active config to FLASH! Configuration is too large
CFG	Error writing active config to FLASH! Unknown error
CFG	TFTP Copy attempting to redirect a previously redirected output
LLDP	Port <*port*>: Cannot add new entry. MSAP database is full!
MGMT	Apply is issued by another user. Try later
MGMT	cannot contact {primary | secondary} DNS server <*IP address*> - {Mgmt | Ext-mgt} port unavailable
MGMT	Critical Error failed to add Interface <*interface*>
MGMT	Diff is issued by another user. Try later
MGMT	Dump is issued by another user. Try later
MGMT	Error: Apply not done
MGMT	Error: Save not done.
MGMT	Firmware download failed (insufficient memory
MGMT	Revert Apply is issued by another user. Try later
MGMT	Revert is issued by another user. Try later.
MGMT	Save is issued by another user. Try later
NTP	unable to listen to NTP port

Thread	Message
PORT_MIRR	ERROR: Management port <*port*> cannot be a mirrored port
PORT_MIRR	ERROR: Only 4 monitoring port sessions can be supported
STP	Cannot set "{Hello Time | Max Age | Forward Delay | Aging}" (Switch is in MSTP mode)
SYSTEM	Error: BOOTP Offer was found incompatible with the other IP interfaces
SYSTEM	Error: DHCP Offer was found invalid by ip configuration checking; please see system log for details.
SYSTEM	I2C device <*ID*> <*description*> set to access state <*state*> [from CLI]
SYSTEM	Insert another transceiver or change configuration and manually enable port <*port*>
SYSTEM	Not enough memory!
SYSTEM	Port <*port*> disabled. Link params(speed/mode) mismatch with <*trunk name*> <*trunk ID*>
SYSTEM	Port <*port*> disabled. Same LACP admin_key with port "PORT_INT_<*port*> rent link params(speed/mode)"

LOG_NOTICE

Thread	Message
	ARP table is full.
	Current config successfully tftp'd <*filename*> from <*hostname*>
	Current config successfully tftp'd to <*hostname*>: <*filename*>
	Number of COSqs has been changed since boot. Save and reset the switch to activate the new configuration.
	Port <*port*> mode is changed to full duplex for 1000 Mbps operation.
	Warning: DHCP will be disabled
8021X	RADIUS server <*IP address*> auth response has a VLAN id (<*VLAN*>) of a non-existent or disabled VLAN, and cannot be assigned to port <*port*>
CONSOLE	RADIUS: authentication timeout. Retrying...
CONSOLE	RADIUS: failed to contact primary | secondary server

Thread	Message
CONSOLE	RADIUS: No configured RADIUS server
CONSOLE	RADIUS: trying alternate server...
HOTLINKS	"Error" is set to "Standby | Active"
HOTLINKS	"Learning" is set to "Standby | Active"
HOTLINKS	"None" is set to "Standby | Active"
HOTLINKS	"Side Max" is set to "Standby | Active"
HOTLINKS	has no "{Side Max | None | Learning | Error}" interface
IP	default gateway <*IP address*> {disabled | enabled | operational}
IP	Either Route or Arp table is full. Please check GEA L3 statistics (/stat/l3/gea) to verify.
IP	{MGTA | MGTB} port default gateway <*IP address*> operational
IP	New Multicast router learned on <*IP address*>, Vlan <*VLAN*>, Version V<*version*>
IP	On Vlan <*VLAN*> IGMP version updated to <*version*>
IP	Warning: DHCP will be disabled
IP	Warning: Enabling dhcp will delete IP interface <*interface*> and IP gateway <gateway>'s configurations.
IP	Warning: gateway (<*gateway*>) will be deleted
LACP	LACP is {up | down} on port <*port*>
MGMT	<*username*> automatically logged out from BBI because changing of authentication type
MGMT	<*username*>(<*user type*>) {logout | ejected | idle timeout | connection closed} from {BBI | Console | Telnet/SSH}
MGMT	<*username*>(<*user type*>) login {on Console | from host <*IP address*> | from BBI}
MGMT	ACL <*old number*> from old configuration file moved to ACL <*new number*> in new configuration file
MGMT	Authentication failed for backdoor.
MGMT	Authentication failed for backdoor. Password incorrect!

Thread	Message
MGMT	Authentication failed for backdoor. Telnet disabled!
MGMT	boot config block changed
MGMT	boot image changed
MGMT	boot mode changed
MGMT	enable password changed
MGMT	Error in setting the new config
MGMT	Failed login attempt via {BBI | TELNET} from host <*IP address*>.
MGMT	Failed login attempt via the CONSOLE
MGMT	FLASH Dump cleared from BBI
MGMT	Mgt Gateway <*IP address*> not in the same subnet as the Mgt IP <*IP address*>/<netmask>
MGMT	New config set
MGMT	new configuration saved from ISCLI
MGMT	New Management IP Address <*IP address*> configured
MGMT	packet-buffer statistics cleared
MGMT	PANIC command from CLI
MGMT	PASSWORD FIX-UP MODE IN USE
MGMT	Password for {oper | operator} changed by {SNMP user | <*username*>}, notifying admin to save.
MGMT	Radius authentication has been enabled. Please try again with a Radius user and password.
MGMT	RADIUS server timeouts
MGMT	RADIUS: authentication timeout. Retrying...
MGMT	RADIUS: failed to contact primary|secondary server
MGMT	RADIUS: No configured RADIUS server
MGMT	RADIUS: trying alternate server...
MGMT	scp<*username*>(<*user type*>) {logout | ejected | idle timeout | connection closed} from {Console | Telnet/SSH}

Thread	Message
MGMT	scp<*username*>(<*user type*>) login {on Console | from host <*IP address*>}
MGMT	second syslog host changed to {this host | <*IP address*>}
MGMT	selectable [boot] mode changed
MGMT	STP BPDU statistics cleared
MGMT	switch reset from CLI
MGMT	syslog host changed to {this host | <*IP address*>}
MGMT	System clock set to <time>.
MGMT	System date set to <date>.
MGMT	Tacacs authentication has been enabled. Please try again with a Tacacs user and password.
MGMT	Terminating BBI connection from host <*IP address*>
MGMT	User <*username*> deleted by {SNMP user | <*username*>}.
MGMT	User <*username*> is {deleted | disabled} and will be ejected by {SNMP user | <*username*>}
MGMT	User oper | operator is disabled and will be ejected by {SNMP user | <*username*>}.
MGMT	Wrong config file type
NTP	System clock updated
OSPF	Neighbor Router ID <*router ID*>, Neighbor State {Down | Loopback | Waiting | P To P | DR | BackupDR | DR Other | Attempt | Init | 2 Way | ExStart | Exchange | Loading | Full}
SERVER	link {down | up} on port <*port*>
SERVER	MAC address <*MAC address*> for Vlan <*VLAN*> on {<*trunk*> | Port <*port*>} was {added to | removed from} network
SSH	(remote disconnect msg)
SSH	<*username*>(<*user type*>) {logout | ejected | idle timeout | connection closed} from {Console | Telnet/SSH}
SSH	<*username*>(<*user type*>) login {on Console | from host <*IP address*>}
SSH	Error in setting the new config

Thread	Message
SSH	Failed login attempt via SSH
SSH	New config set
SSH	scp<*username*>(<*user type*>) {logout | ejected | idle timeout | connection closed} from {Console | Telnet/SSH}
SSH	scp<*username*>(<*user type*>) login {on Console | from host <*IP address*>}
SSH	Wrong config file type
SYSTEM	BOOTP Offer (continue): Domain name: <*domain*>
SYSTEM	BOOTP Offer (continue): Host name: <*host*>
SYSTEM	BOOTP Offer (continue): Primary DNS: <*IP address*>, Secondary DNS: <*IP address*>
SYSTEM	Change fiber GIG port <*port*> mode to full duplex
SYSTEM	Change fiber GIG port <*port*> speed to 1000
SYSTEM	Changed ARP entry for IP <*IP address*> to: MAC <MAC address>, Port <*port*>, VLAN <*VLAN*>
SYSTEM	Could not add L2 multicast entry! L2 table is full.
SYSTEM	ECMP route gateway <*IP address*> is {down | up}
SYSTEM	Enable auto negotiation for copper GIG port: <*port*>
SYSTEM	Fan Fault Detected
SYSTEM	I2C device <ID> <description> set to access state <state> [from CLI]
SYSTEM	Ingress PVST+ BPDU's spotted from port <*port*>
SYSTEM	link {down | up} on management port <*port*>
SYSTEM	link {down | up} on port <*port*>
SYSTEM	**** MAX TEMPERATURE (<*temperature*>) ABOVE FAIL THRESH ****
SYSTEM	**** MAX TEMPERATURE (<*temperature*>) ABOVE WARN THRESH ****
SYSTEM	Port <*port*> disabled
SYSTEM	Port <*port*> disabled by BPDU Guard
SYSTEM	Port <*port*> disabled by OAM (unidirectional | TX-RX Loop)
SYSTEM	Port <*port*> disabled by PVST Protection

Thread	Message
SYSTEM	Port <*port*> disabled due to reason code <*reason code*>
SYSTEM	Power Fault {Cleared | Detected}
SYSTEM	rebooted (<*reason*>)[, administrator logged in] Reason: ■ Boot watchdog reset ■ console PANIC command ■ console RESET KEY ■ hard reset by SNMP ■ hard reset by WEB-UI ■ hard reset from console ■ hard reset from Telnet ■ low memory ■ MM Cycled Power Domain ■ power cycle ■ Reset Button was pushed ■ reset by SNMP ■ reset by WEB-UI ■ reset from console ■ reset from EM ■ reset from Telnet/SSH ■ scheduled reboot ■ SMS-64 found an over-voltage ■ SMS-64 found an under-voltage ■ software ASSERT ■ software PANIC ■ software VERIFY ■ Telnet PANIC command ■ unknown reason ■ watchdog timer
SYSTEM	Received BOOTP Offer: IP: <*IP address*>, Mask: <netmask>, Broadcast <*IP address*>, GW: <*IP address*>
SYSTEM	Received DHCP Offer: IP: <*IP address*>, Mask: <*netmask*> Broadcast <*IP address*>, GW: <*IP address*>
SYSTEM	Static route gateway <*IP address*> is {down | up}
SYSTEM	Watchdog threshold changed from <old value> to <new value> seconds
SYSTEM	Watchdog timer has been {enabled | disabled}
TEAMING	error, action is undefined
TEAMING	is down, but teardown is blocked
TEAMING	is down, control ports are auto disabled
TEAMING	is up, control ports are auto controlled
UPGRADE	UFD couldn't be converted to Failover
UPGRADE	UpLinkFast is not supported in MSTP/RST/PVRST mode

Thread	Message
VLAN	Default VLAN can not be deleted
VRRP	virtual router <*IP address*> is now BACKUP|MASTER
VRRP	Virtual Router Group is disabled due to no enabled virtual routers.
WEB	<*username*> ejected from BBI
WEB	<*username*> ejected from BBI because username password was changed
WEB	RSA host key is being saved to Flash ROM, please don't reboot the box immediately.

LOG_INFO

Thread	Message
	System log cleared by user <*username*>.
	System log cleared via SNMP.
DIFFTRAK	/* Config changes at <time> by <*username*> */ <*config diff*> /* Done */
HOTLINKS	"Error" is set to "{Active | Standby}"
HOTLINKS	"Learning" is set to "{Active | Standby}"
HOTLINKS	"None" is set to "{Active | Standby}"
HOTLINKS	"Side Max" is set to "{Active | Standby}"
HOTLINKS	has no "{Side Max | None | Learning | Error}" interface
MGMT	/* Config changes at <time> by <*username*> */ <*config diff*> /* Done */
MGMT	<*username*> ejected from BBI
MGMT	<*username*>(<*user type*>) {logout | ejected | idle timeout | connection closed} from {Console | Telnet/SSH}
MGMT	<*username*>(<*user type*>) login {on Console | from host <*IP address*>}
MGMT	boot kernel download completed. Now writing to flash.
MGMT	boot kernel downloaded from host <*hostname*>, file'<*filename*>', software version <*version*>
MGMT	boot kernel downloaded {from host <*hostname*> | via browser}, filename too long to be displayed, software version <*version*>

Thread	Message
MGMT	boot kernel Firmware upload failed.
MGMT	boot kernel Firmware uploaded.
MGMT	Can't downgrade to image with only single flash support
MGMT	Could not revert unsaved changes
MGMT	Download already currently in progress. Try again later via
MGMT	Error in setting the new config
MGMT	Failed to allocate buffer for diff track.
MGMT	Firmware download failed to {invalid image | image1 | image2 | boot kernel | undefined | SP boot kernel}
MGMT	Firmware downloaded to {invalid image | image1 | image2 | boot kernel | undefined | SP boot kernel}.
MGMT	Flash dump failed
MGMT	Flash dump successfully tftp'd to <*hostname*>:<*filename*>
MGMT	FLASH ERROR - invalid address used
MGMT	Flash Read Error. Failed to read flash into holding structure. Quitting
MGMT	Flash Write Error
MGMT	Flash Write Error. Failed to allocate buffer. Quitting
MGMT	Flash Write Error. Trying again
MGMT	{image1 | image2} download completed. Now writing to flash.
MGMT	{image1 | image2} downloaded from host <*hostname*>, file'<*filename*>', software version <*version*>
MGMT	{image1 | image2} downloaded {from host <*hostname*> | via browser}, filename too long to be displayed, software version <*version*>
MGMT	{image1 | image2} Firmware upload failed.
MGMT	{image1 | image2} Firmware uploaded.
MGMT	Incorrect image being loaded
MGMT	Invalid diff track address. Continuing with apply()
MGMT	Invalid image being loaded for this switch type

Thread	Message
MGMT	invalid image download completed. Now writing to flash.
MGMT	invalid image downloaded from host <*hostname*>, file '<*filename*>', software version <*version*>
MGMT	invalid image downloaded {from host <*hostname*> | via browser}, filename too long to be displayed, software version <*version*>
MGMT	invalid image Firmware upload failed.
MGMT	invalid image Firmware uploaded.
MGMT	New config set
MGMT	new configuration applied [from BBI | EM | SCP | SNMP|Stacking Master]
MGMT	new configuration saved from {BBI | ISCLI | SNMP}
MGMT	scp<*username*>(<*user type*>) {logout | ejected | idle timeout | connection closed} from {Console | Telnet/SSH}
MGMT	scp<*username*>(<*user type*>) login {on Console | from host <*IP address*>}
MGMT	SP boot kernel download completed. Now writing to flash.
MGMT	SP boot kernel downloaded from host <*hostname*>, file '<*filename*>', software version <*version*>
MGMT	SP boot kernel downloaded {from host <*hostname*> | via browser}, filename too long to be displayed, software version <*version*>
MGMT	SP boot kernel Firmware upload failed.
MGMT	SP boot kernel Firmware uploaded.
MGMT	Starting Firmware download for {invalid image | image1 | image2 | boot kernel | undefined | SP boot kernel}.
MGMT	Static FDB entry on disabled VLAN
MGMT	Tech support dump failed
MGMT	Tech support dump successfully tftp'd to <*hostname*>:<*filename*>
MGMT	Two Phase Apply Failed in Creating Backup Config Block.
MGMT	undefined download completed. Now writing to flash.
MGMT	undefined downloaded from host <*hostname*>, file '<*filename*>', software version <*version*>

Thread	Message
MGMT	undefined downloaded {from host <*hostname*> | via browser}, filename too long to be displayed, software version <*version*>
MGMT	undefined Firmware upload failed.
MGMT	undefined Firmware uploaded.
MGMT	unsaved changes reverted [from BBI | from SNMP]
MGMT	Unsupported GBIC {accepted | refused}
MGMT	user (SNMP user | <*username*>) ejected from BBI
MGMT	Watchdog has been {enabled | disabled}
MGMT	Watchdog timeout interval is now <*seconds*> seconds)
MGMT	Wrong config file type
SSH	<*username*>(<*user type*>) {logout | ejected | idle timeout | connection closed} from {Console | Telnet/SSH}
SSH	<*username*>(<*user type*>) login {on Console | from host <*IP address*>}
SSH	Error in setting the new config
SSH	New config set
SSH	scp<*username*>(<*user type*>) {logout | ejected | idle timeout | connection closed} from {Console | Telnet/SSH}
SSH	scp<*username*>(<*user type*>) login {on Console | from host <*IP address*>}
SSH	server key autogen {starts | completes}
SSH	Wrong config file type
SYSTEM	booted version <*version*> from Flash image <*image*>, {active | backup | factory} config block
SYSTEM	FDB Learning DISABLED|ENABLED for port <*port*>
SYSTEM	Insert another transceiver or change configuration and manually enable port <*port*>

Index

Symbols

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W