Part No. 315545-C Rev 00
May 2004

4655 Great American Parkway
Santa Clara, CA 95054

Managing Platform Operations

Passport 8000 Series Software Release 3.7

315545-C REV 00

Copyright © 2004 Nortel Networks

Trademarks

Nortel Networks, the Nortel Networks logo, the Globemark, Unified Networks, and PASSPORT are trademarks of Nortel Networks.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

UNIX is a trademark of X/Open Company Limited.

The asterisk after a name denotes a trademarked item.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Nortel Networks Inc. software license agreement

This Software License Agreement (“License Agreement”) is between you, the end-user (“Customer”) and Nortel Networks Corporation and its subsidiaries and affiliates (“Nortel Networks”). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

“Software” is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

1. Licensed Use of Software. Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment (“CFE”), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer’s Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.

2. Warranty. Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided “AS IS” without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABLITITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

3. Limitation of Remedies. IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER’S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The forgoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. General

a. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States

Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

b. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.

c. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.

d. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.

e. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.

f. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

Contents

Chapter 5

Chapter 6

Chapter 7
Configuring chassis operations 155

Chapter 8
Configuring NTP using the CLI. 171

Chapter 9
Configuring NTP using Device Manager 181

Figures

Tables

Preface

Nortel Networks* Passport* 8000 Series switch is a flexible and multifunctional switch that supports a diverse range of network architectures and protocols. This guide provides procedures for configuring, monitoring, and managing the Passport 8000 Series switch.

Before you begin

This guide is intended for network designers and administrators with the following background:

- Working knowledge of the UNIX operating system
- Basic knowledge of networks, Ethernet bridging, and IP routing
- Familiarity with networking concepts and terminology
- Familiarity with the network topologies (for example, Domain Manager)
- Experience with windowing systems or graphical user interfaces (GUIs)

Text conventions

This guide uses the following text conventions:

angle brackets (< >)

Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command.

Example: If the command syntax is `ping <ip_address>`, you enter `ping 192.32.10.12`

`bold Courier text`

Indicates command names and options and text that you need to enter.

Example: Use the **`dinfo`** command.

Example: Enter **`show ip`** {**`alerts`**|**`routes`**}.

braces ({})

Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command.

Example: If the command syntax is `show ip {alerts|routes}`, you must enter either `show ip alerts` or `show ip routes`, but not both.

brackets ([ ])

Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command.

Example: If the command syntax is `show ip interfaces [-alerts]`, you can enter either `show ip interfaces` or `show ip interfaces -alerts`.

ellipsis points (. . .)

Indicate that you repeat the last element of the command as needed.

Example: If the command syntax is `ethernet/2/1 [<parameter> <value>] . . .` , you enter `ethernet/2/1` and as many parameter-value pairs as needed.

italic text	Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is `show at <valid_route>`, *`valid_route`* is one variable and you substitute one value for it.
`plain Courier text`	Indicates command syntax and system output, for example, prompts and system messages. Example: `Set Trap Monitor Filters`
separator (>)	Shows menu paths. Example: Protocols > IP identifies the IP command on the Protocols menu.
vertical line (|)	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is `show ip {alerts|routes}`, you enter either `show ip alerts` or `show ip routes`, but not both.

Acronyms

This guide uses the following acronyms:

ARP	Address Resolution Protocol
BootP	Bootstrap Protocol
DVMRP	Distance Vector Multicast Routing protocol
IP	Internet Protocol
IPX RIP	Internetwork packet exchange Routing Information Protocol
ITU-T	International Telecommunication Union-Telecommunication Standardization Sector (formerly CCITT)
MAC	Media Access Control

MAU	Media Access Unit
MDI-X	Medium Dependent Interface Crossover
MLT	MultiLink Trunking
NBMA	Non-broadcast Multi-access
OSPF	Open Shortest Path First
PGM	Pragmatic group Multicasting
PIM	Protocol Independent Multicasting
POS	Packet over sonet
PPP	Point-to-Point Protocol
RIP	Routing Information Protocol
RWA	Read, Write, All
SAP	Service Access Protocol
SMDS	Switched Multimegabit Data Service
SNMP	Simple Network Management Protocol
SSH	Secure Shell
STG	Spanning Tree Group
STP	Shielded Twisted Pair
TPE	Twisted Pair Ethernet
UDP	User Datagram Protocol
VRRP	Virtual Redundancy Router Protocol

Hard-copy technical manuals

You can print selected technical manuals and release notes free, directly from the Internet. Go to the www.nortelnetworks.com/documentation URL. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe* Acrobat Reader* to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe Systems at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader.

How to get help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact Nortel Networks Technical Support. To obtain contact information online, go to the www.nortelnetworks.com/cgi-bin/comments/comments.cgi URL, then click on Technical Support.

From the Technical Support page, you can open a Customer Service Request online or find the telephone number for the nearest Technical Solutions Center. If you are not connected to the Internet, you can call 1-800-4NORTEL (1-800-466-7835) to learn the telephone number for the nearest Technical Solutions Center.

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the http://www.nortelnetworks.com/help/contact/erc/index.html URL.

Chapter 1
System Platform Overview

This chapter provides overview information about a variety of system platform operations and diagnostic tools. Specifically, it includes information about the following topics:

Operating modes

A Passport 8000 Series switch can run in the following operating modes:

- Automatic save-to-standby mode — Sets a flag that copies the configuration files from the primary CPU to the backup CPU.
- M mode (128K records mode) — Supports 128K hardware records.
- Enhanced operational mode — Increases the maximum number of VLANs.
- CPU high-availability mode — High availability (HA), or "hot standby," refers to a multiprocessing system that can quickly recover from a failure.

For instructions on configuring these modes, see Chapter 7, “Configuring chassis operations.”

Module types

The Passport 8000 Series switch modules fall into the following types:

- Legacy modules are older modules that manufacturing has discontinued, but are still supported.
  - Legacy modules do **not** support egress port mirroring.
  - Legacy modules support 32K records **only** and cannot operate in M mode.
  - Legacy modules cannot operate in enhanced operational mode.
- E-modules have an “E” suffix and replace the modules that have the same number without the E.
  - E-modules support egress port mirroring.
  - E-modules support 32K records **only** and cannot operate in M mode.
- M-modules did not replace E-modules. They are both available and have different part numbers. The only exception is the 8683POSE module, which was replaced with the 8683POSM.
  - M-modules have an “M” suffix. Two exceptions to this rule are the 10 Gigabit Ethernet modules (8661XLR and 8661XLW).
  - M-modules support 128K records and operate in M mode.

Table 1 lists all the supported Passport 8000 Series modules.

Table 1 Passport 8000 Series modules

Legacy	**E-modules**	**M-modules**
8608GB	8608GBE (DS1404038)	8608GBM (DS1404059)
8608GT	8608GTE (DS1404044)	8608GTM (DS1404061)
8608SX	8608SXE (DS1404036)	Not supported
8616SX	8616SXE (DS1404011)	Not supported
8624FX	8624FXE (DS1404037)	Not supported
8632TX	8632TXE (DS1404024)	8632TXM (DS1404055)
8648TX	8648TXE (DS1404035)	8648TXM (DS1404056)

Table 1 Passport 8000 Series modules

Legacy	E-modules	M-modules
8672ATM	8672ATME (DS1304008)	8672ATMM (DS1304009)
8683POS	8683POSE	8683POSM (DS1404060)
	8616GTE (DS1404034)	Not supported
		8661XLR (DS1404053)
		8661XLW (DS1404052)
		8661 SSL Acceleration Module (DS1404070
		Web Switching Module (WSM) (DS1404045)

Microsoft* Network Load Balancing Support

Passport 8000 Series switch software allows you to choose whether ARP entries for multicast MAC addresses are associated with the VLAN or the port on which it was learned.

This enhancement is useful if multiple endstations/servers are sharing a multicast MAC address as is the case with certain Microsoft network load balancing applications, wherein the traffic is flooded to the VLAN to ensure that every endstation using this virtual multicast MAC address is receiving a copy of the stream.

This feature is disabled by default.

To enable or disable NLBS support, enter the CLI command:

```
config ip arp multicast-mac-flooding <enable|disable>
```

Note: This option is not dynamic. That is, if the setting of this feature is changed, it will not dynamically reprogram all previously learned ARP entries from multicast MAC addresses.

Port mirroring

Passport 8000 Series switches have a port mirroring feature that helps you to monitor and analyze network traffic. The port mirroring feature supports both *ingress* (incoming traffic) and *egress* (outgoing traffic) port mirroring. When this feature is enabled, the *mirrored* (source) port's ingress or egress packets are forwarded normally and a copy of the packets is sent out of the mirrored port to the *mirroring* (destination) port. Although you can configure Passport 8000 Series switches to monitor both ingress and egress traffic, some restrictions apply:

- Passport 8100 switches
  - Ingress port mirroring is always supported
  - Egress port mirroring is supported only in half-duplex mode of operation
- Passport 8600 switches
  - Ingress port mirroring is always supported
  - Egress port mirroring is currently supported only on Passport 8600 E-modules

You can configure up to 100 entries in the port mirroring table for mirroring, and you can have up to 25 entries active at any given time.

Egress port mirroring can be enabled separately, allowing you to monitor packets as they leave specified ports. In addition, you can monitor traffic for MAC addresses, where traffic with a given MAC source address (SA) or MAC destination address (DA) is copied to the specified mirroring port.

To avoid seeing unintended traffic, you should remove mirroring (destination) ports from all virtual local area networks (VLANs) and Spanning Tree Groups (STGs).

You can observe and analyze packet traffic at the mirroring port using a network analyzer — a copy of the packet can be captured and analyzed. Unlike other methods that are used to analyze packet traffic, the packet traffic is uninterrupted and packets flow normally through the mirrored port.

Configuration considerations

Note: Nortel Networks recommends that you disable port mirroring when not in use to reduce the load on the switch.

In release 3.2 and prior, you could configure only 25 mirrored ports to 1 mirroring port. With release 3.2.0.1 and up:

Passport 8100 switch

- You can configure 25 mirrored ports to 1 mirroring port
- Ethernet MDAs can also be a part of these 25 ports
- Ingress and Egress mirroring is supported
- Half duplex ONLY for Egress mirroring

Passport 8600 switch

In release 3.2.2 and later:

- The number of port mirroring entries can now be configured between 1 and 383, and ALL entries can be active simultaneously
- The number of mirroring ports plus the number of mirrored ports cannot exceed 384.
- Hardware limitations:
  - — Ports supported by the same OCTAPID (group of 8 10/100 ports or 1 Gig port) can only be mirrored to the same destination.
  - — One port cannot be mirrored to multiple destinations.
  - — A maximum of 64 destination ports can be configured at one time without violating hardware imitations.

Note: Egress mirroring is supported only on E-modules.

Note: If a port mirroring rule is disregarded, the following error message displays: `error: invalid diag-logure operation`.

For more information about the port mirroring feature, see "Port mirroring" on page 26.

Packet Capture Tool (PCAP)

PCAP is an onboard data packet capture tool capturing packets ingressing and egressing on selected I/O ports. This feature allows customer support personnel to capture, save, and download one or more traffic flows through the Passport 8600 switch and analyze the captured traffic offline. All captured packets are stored on the secondary CPU in the PCAP engine. The primary CPU maintains its protocol handling and will not be affected by any PCAP capture activity. For more information about PCAP, refer to *Using the Packet Capture (PCAP) Tool*.

Syslog

On any UNIX*-based management platform, you can use the syslog messaging feature of the Passport 8000 Series 8000 Series switch to manage event messages. The Passport 8000 Series syslog software communicates with a server software component named *syslogd* on your management workstation. The UNIX daemon syslogd is a software component that receives and locally logs, displays, prints, and/or forwards messages that originate from sources internal and external to the workstation. For example, syslogd on a UNIX workstation concurrently handles messages received from applications running on the workstation, as well as messages received from a Passport 8000 Series switch running in a network accessible to the workstation.

➡ **Note:** Syslog and Trap Log may not capture all log session messages for the Web Switching Module.

CLI command logging

The CLI command logging feature provides the functionality of encrypting and logging the CLI, ftp and tftp commands. This provides a secured logging mechanism within the switch. The commands which are executed in the switch after booting up is stored in an encrypted format in a PCMCIA file accessible only to the RWA user.

When you execute a command from a session, the command is encrypted and stored in clilog.txt file in the PCMCIA. The following attributes of the command are captured while logging:

- Sequence Number: Identifies a specific command.
- CPU Slot Number: Indicates the CPU slot from which the command is logged.
- Date & Time: The Switch time at which the command is executed.
- Context: The type of the session used to connect to the switch. This includes Console, Modem, Telnet, SSH, Rlogin, ftp, tftp. If it is a remote session, the remote IP address is identified.
- User name: This is the username used to login to the switch.
- The command: The commands typed on the session as such. Anything typed on the session will be logged as soon as the return key (enter key) is pressed.

The commands logged can be decrypted and viewed by using the show commands provided by the feature. The commands can be decrypted and stored in the secondary storage devices or remote server by using the save command of the feature. All the above commands are accessible only to the RWA user. If the clilog.txt file in PCMCIA exceeds the maximum file size settings, then the file is automatically wrapped from the top.

Network Time Protocol (NTP)

The Network Time Protocol (NTP) synchronizes the internal clocks of various network devices across large, diverse networks to universal standard time. NTP runs over UDP, which in turn runs over IP. The NTP protocol specification is documented in RFC 1305.

Every network device relies on an internal system clock to maintain accurate time. On local devices, the internal system clock is usually set by eye or by wristwatch to within a minute or two of the actual time and is rarely reset at regular intervals. Many local clocks are battery-backed devices that use room temperature clock oscillators that can drift as much as several seconds each day. NTP solves this problem by automatically adjusting the time of the devices so that they are synchronized within a millisecond (ms) on LANs and up to a few tens of milliseconds on WANs relative to Coordinated Universal Time (UTC).

The current implementation of NTP supports only unicast client mode. In this mode, the NTP client, which is tailored to the limitations of the Real Time Clock (RTC) on the CPU board (Dallas Semiconductors DS1307 series), sends NTP time requests to other remote time servers in an asynchronous fashion. The NTP client collects four samples of time from each remote time server. A clock selection algorithm determines the best server among the selected samples based on stratum, delay, dispersion and the last updated time of the remote server. The RTC is adjusted to the selected sample from the chosen server.

NTP terms

A *peer* can be any device that runs NTP software. However, this implementation of NTP refers to peers as remote time servers that provide time information to other time servers on the network and to the local *NTP client*. An NTP client refers to the local network device — in this case, a Passport 8000 Series switch — that accepts time information from other remote time servers.

NTP system implementation model

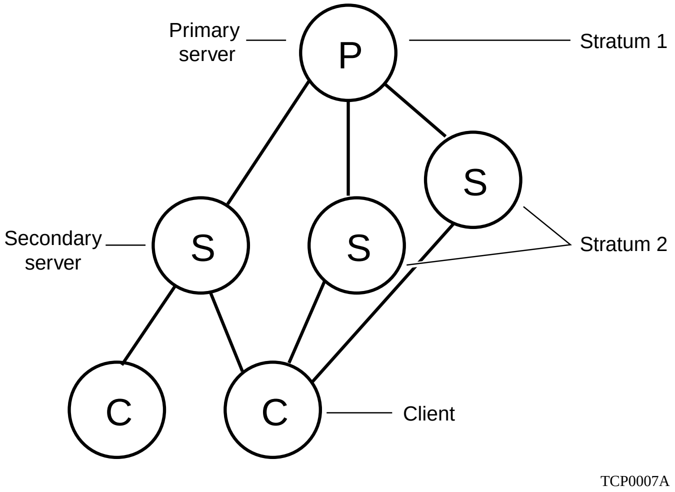
NTP is based on a hierarchical model that consists of a local NTP client that runs on the Passport 8000 Series switch and on remote time servers. The NTP client requests and receives time information from one or more remote time servers. The local NTP client reviews the time information from all available time servers and synchronizes its internal clock to the time server whose time is most accurate. The NTP client does not forward time information to other devices running NTP.

There are two types of time servers in the NTP model: primary time servers and secondary time servers. A *primary time server* is directly synchronized to a primary reference source, usually a wire or radio clock that is synchronized to a radio station providing a standard time service. The primary time server is the authoritative time source in the hierarchy, meaning that it is the one true time source to which the other NTP devices in the subnet synchronize their internal clocks.

A *secondary time server* uses a primary time server or one or more secondary time servers to synchronize its time, forming a synchronization subnet (Figure 1). A *synchronization subnet* is a self-organizing, hierarchical master-slave configuration with the primary servers at the root and secondary servers of decreasing accuracy at successive levels.

Figure 1 shows NTP time servers forming a synchronization subnet.

Figure 1 NTP time servers forming a synchronization subnet



In the NTP model, the synchronization subnet automatically reconfigures in a hierarchical primary-secondary (master-slave) configuration to produce accurate and reliable time, even if one or more primary time servers or the path between them fails. This feature applies in a case in which all the primary servers on a partitioned subnet fail, but one or more backup primary servers continue to operate. If all of the primary time servers in the subnet fail, the remaining secondary servers synchronize among themselves.

How NTP distributes time within a subnet

NTP distributes time through a hierarchy of primary and secondary servers, with each server adopting a stratum (see Figure 1 on page 31). A *stratum* defines how many NTP *hops* away a particular secondary time server is from an authoritative time source (primary time server) in the synchronization subnet. A “stratum 1” time server is located at the top of the hierarchy and is directly attached to an external time source, typically a wire or radio clock; a “stratum 2” time server receives its time via NTP from a “stratum 1” time server; a “stratum 3” time server receives its time via NTP from a “stratum 2” time server, and so forth.

Each NTP client in the synchronization subnet chooses as its time source the server with the lowest stratum number with which it is configured to communicate via NTP. This strategy effectively builds a self-organizing tree of NTP speakers. The number of strata is limited to 15 to avoid long synchronization loops.

NTP tries not to synchronize to a remote time server whose time might not be accurate. It avoids doing this in two ways. First, NTP never synchronizes to a remote time server that is not itself synchronized. Second, NTP compares the times reported by several remote time servers.

Synchronizing with the best available time server

Unlike other time synchronization protocols, NTP does not attempt to synchronize the remote time servers’ internal clocks to each other. Rather, NTP synchronizes the servers’ clocks to universal standard time, using the “best” available time source and transmission paths to that time source.

NTP uses the following criteria to determine the time server whose time is best:

- The time server with the lowest stratum
- The time server closest in proximity to the primary time server (reduces network delays)
- The time server offering the highest claimed precision

NTP prefers to have access to several (at least three) servers at the lower stratum level, since it can apply an agreement algorithm to detect a problem on any part of the time source.

NTP modes of operation

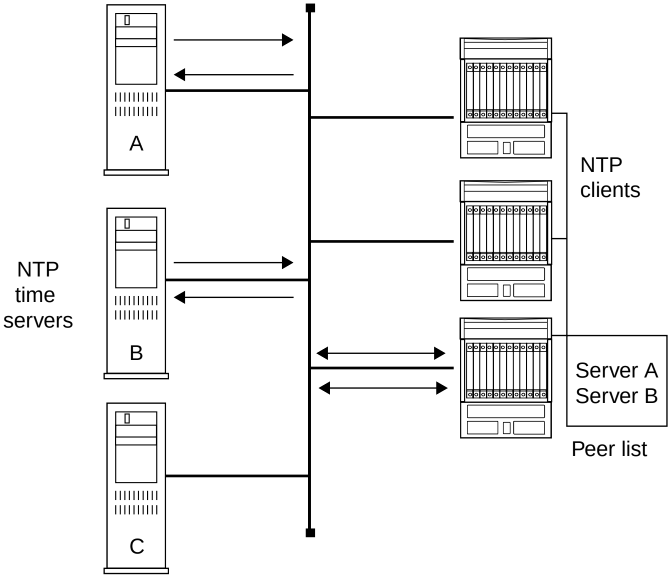
NTP uses unicast client mode to enable time servers and NTP clients to communicate in the synchronization subnet. The Passport 8000 Series switch supports only unicast client mode.

When you configure a set of remote time servers (peers), NTP creates a list that includes each time server’s IP address. The NTP client uses this list to determine which remote time servers to query for time information.

When the NTP client queries the remote time servers, they respond with various timestamps, along with information about their clocks, such as stratum, precision, and time reference (Figure 2). The NTP client reviews the list of responses from all available servers and chooses one as the “best” available time source from which to synchronize its internal clock.

Figure 2 shows how NTP time servers operate in unicast mode.

Figure 2 NTP time servers operating in unicast client mode



TCP0006A

NTP authentication

You can authenticate time synchronization to ensure that the local time server obtains its time services only from known sources. NTP authentication adds a level of security to your NTP configuration. By default, network time synchronization is not authenticated.

When you select authentication, the Passport 8000 Series switch uses the Message Digest 5 (MD5) algorithm to produce a *message digest* of the key. The message digest is created using the key and the message, but the key itself is not sent. The MD5 algorithm verifies the integrity of the communication, authenticates the origin, and checks for timeliness.

To authenticate the message, the client authentication key must match that of the time server. Therefore, the authentication key must be securely distributed in advance (the client administrator must get the key from the server administrator and configure it on the client).

While a server may know many keys (identified by many key IDs) it is possible to declare only a subset of these as trusted. This feature allows the time server to share keys with a client that requires authenticated time and that trusts the server, but that is not trusted by the time server.

BootP/DHCP relay

The Dynamic Host Configuration Protocol (DHCP) is an extension of the Bootstrap Protocol (BootP) and provides host configuration information to the workstations on a dynamic basis. To lower administrative overhead, network managers prefer to configure a small number of DHCP servers in a central location. It is necessary for routers to support the BootP/DHCP relay function so that hosts can access configuration information from servers several router hops away. IP subnet-based VLANs do not support DHCP relay functions because the DHCP request does not specify to which subnet the inquiry should be related.

Differences between DHCP and BootP

The following differences between DHCP and BootP are specified in RFC 2131 and include functions that BootP does not address:

- DHCP defines mechanisms through which clients can be assigned a network address for a finite lease (allowing for reuse of IP addresses).
- DHCP provides the mechanism for clients to acquire all of the IP configuration parameters needed to operate.

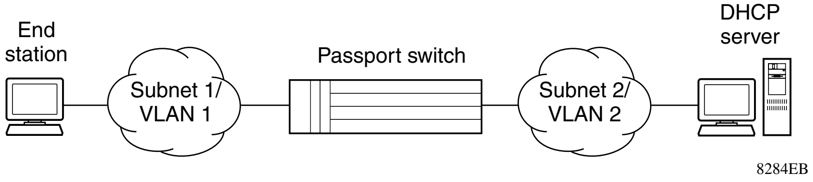
DHCP uses the BootP message format defined in RFC 951. A packet is classified as DHCP if the first four octets in the options field are 99, 130, 83, 99, and the fifth octet is 53. The first four octets are referred to as the “Magic Cookie,” while the fifth is the DHCP message type code. The remainder of the options field consists of a list of tagged parameters that are called “options” (RFC 2131).

Summary of DHCP relay operation

BootP/DHCP clients (workstations) generally use UDP/IP broadcasts to determine their IP addresses and configuration information. If such a host is on a network or a subnet segment (or VLAN) that does not include a DHCP server, the UDP broadcasts are by default not forwarded to the server located on a different network segment or VLAN. The Passport 8000 Series can be configured to overcome this issue by forwarding the broadcasts to the server through virtual router interfaces. The router interfaces can be configured to forward DHCP broadcasts to other locally connected network segments or directly to the server’s IP address. DHCP must be enabled on a per-routable-interface basis.

Figure 3 shows an end station connected to subnet 1, corresponding to VLAN 1. The Passport 8000 Series connects two subnets by means of the virtual routing function. When the end station generates a DHCP request as a limited UDP broadcast to the IP address of all 1s (that is, 255.255.255.255) with the DHCP relay function configured, the Passport 8000 Series forwards DHCP requests to subnet 2 or to the host address of the DHCP server, depending on the configuration.

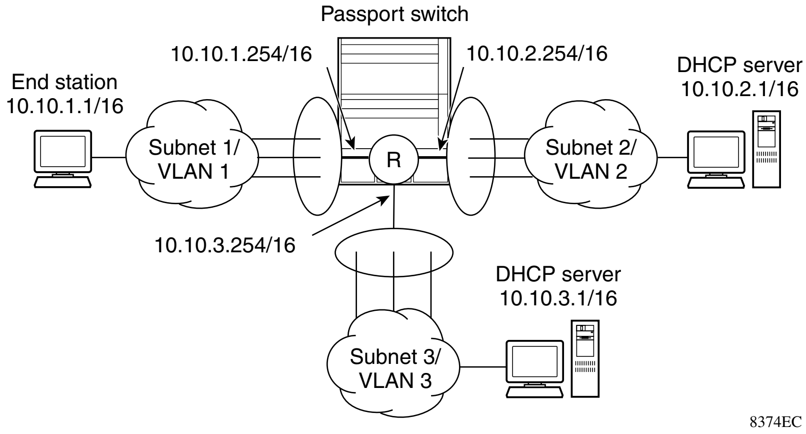
Figure 3 DHCP operation



Forwarding DHCP packets

In the example shown in Figure 4, the *agent address* is 10.10.1.2. To configure the Passport 8000 Series to forward DHCP packets from the end station to the server, use 10.10.2.1 as the *server address*.

Figure 4 Forwarding DHCP packets



All BootP broadcast packets, including DHCP packets that appear on the VLAN 1 router interface (10.10.1.2), will be forwarded to the DHCP server. In this case, the DHCP packets will be forwarded as unicast to the DHCP server's IP address.

To forward BootP/DHCP packets as broadcast packets to VLAN 2, specify the IP address of the switch VLAN 2 router interface (10.10.2.2) as the server address.

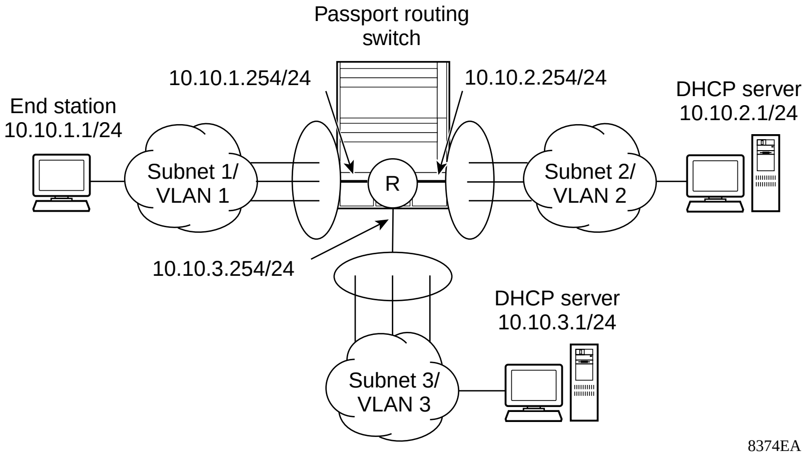
Multiple BootP/DHCP servers

Most enterprise networks use multiple BootP/DHCP servers for fault tolerance. The Passport 8000 Series allows you to configure the switch to forward BootP/DHCP requests to multiple servers. You can configure up to 10 servers to receive copies of the forwarded BootP/DHCP messages.

If a DHCP client is connected to a routable interface, to configure DHCP requests to be sent to 10 different routable interfaces or 10 different server IP addresses, enable DHCP on the client (agent address) and then enable DHCP from the client to each of the interfaces or IP addresses (server addresses).

In the example shown in Figure 5, two DHCP servers are located on two different subnets. To configure the Passport 8000 Series to forward the copies of the BootP/DHCP packets from the end station to both servers, specify the switch (10.10.1.254) as the agent address. Then enable DHCP to each of the DHCP servers by entering 10.10.2.1 and 10.10.3.1 as the server addresses.

Figure 5 Configuring multiple BootP/DHCP servers



UDP broadcast forwarding

Some network applications such as the NetBIOS name service rely on a User Datagram Protocol (UDP) broadcast to request a service or locate a server for an application. If a host is on a network, subnet segment, or VLAN that does not include a server for the service, UDP broadcasts are by default not forwarded to the server located on a different network segment or VLAN. Resolve this problem by forwarding the broadcasts to the server through physical or virtual router interfaces.

UDP broadcast forwarding is a general mechanism for selectively forwarding limited UDP broadcasts received on an IP interface out to other router IP interfaces as a rebroadcast or to a configured IP address.

- If the address is that of a server, the packet is sent as a unicast packet to this address.
- If the address is that of an interface on the router, the frame is rebroadcast.

To follow the basic steps for setting up UDP broadcast forwarding:

1. Enter protocols into a table.
2. Create policies (protocol/server pairs).
3. Assemble these policies into lists or profiles.
4. Apply the list to the appropriate interfaces.

When a UDP broadcast is received on a router interface, it must meet the following criteria if it is to be considered for forwarding:

- Be a MAC-level broadcast
- Be an IP limited broadcast
- Be for the specified UDP protocol
- Have a TTL value of at least 2

For each ingress interface and protocol, the policy specifies how the UDP broadcast is retransmitted: to a unicast host address or to a broadcast address.

Hardware record optimization

The Passport 8600 switch creates hardware records for routing protocol destination multicast addresses that allows dropping these frames at the hardware level in the case they are received when the corresponding protocol is not enabled. This results in creating these records for RIP, OSPF, VRRP, DVMRP and PIM on all VLANs. In the case of a scaled environment, a new feature has been introduced that allows you to optimize record utilization by not programming these records, especially that they are used only when routing is not enabled on the interface. When this feature is enabled (boot flag set to true), these records are not created and the switch can achieve higher record scaling as well as a faster boot time.

Note: This feature is not supported in high availability (HA) mode.

To enable this feature:

1. Execute the following CLI command:

   `config bootconfig flags control-record-optimization` `[true/ false]`. (The default value is false.)

2. Save the configuration: `save bootconfig`.
3. Reboot the switch.

Layer 2/Layer 3 redundancy clarification

When using L2/L3 redundancy, the bootconfig file is saved onto both the master and the standby CPUs and the standby CPU is reset automatically. You must manually reset the master CPU.

L3 redundancy limitations and considerations

This section describes the limitations and considerations of the L3 redundancy feature:

- HA-CPU is not compatible with PCAP.
- L3 redundancy does not currently support the following protocols:
  - DVMRP/PIM/PGM
  - IPX RIP/SAP
  - WSM
  - POS
  - Route policies
  - IP filters

The following CLI commands were added:

show ip dhcp-relay command

The **`show ip dhcp-relay show-all`** command displays all relevant IP dhcp-relay information.

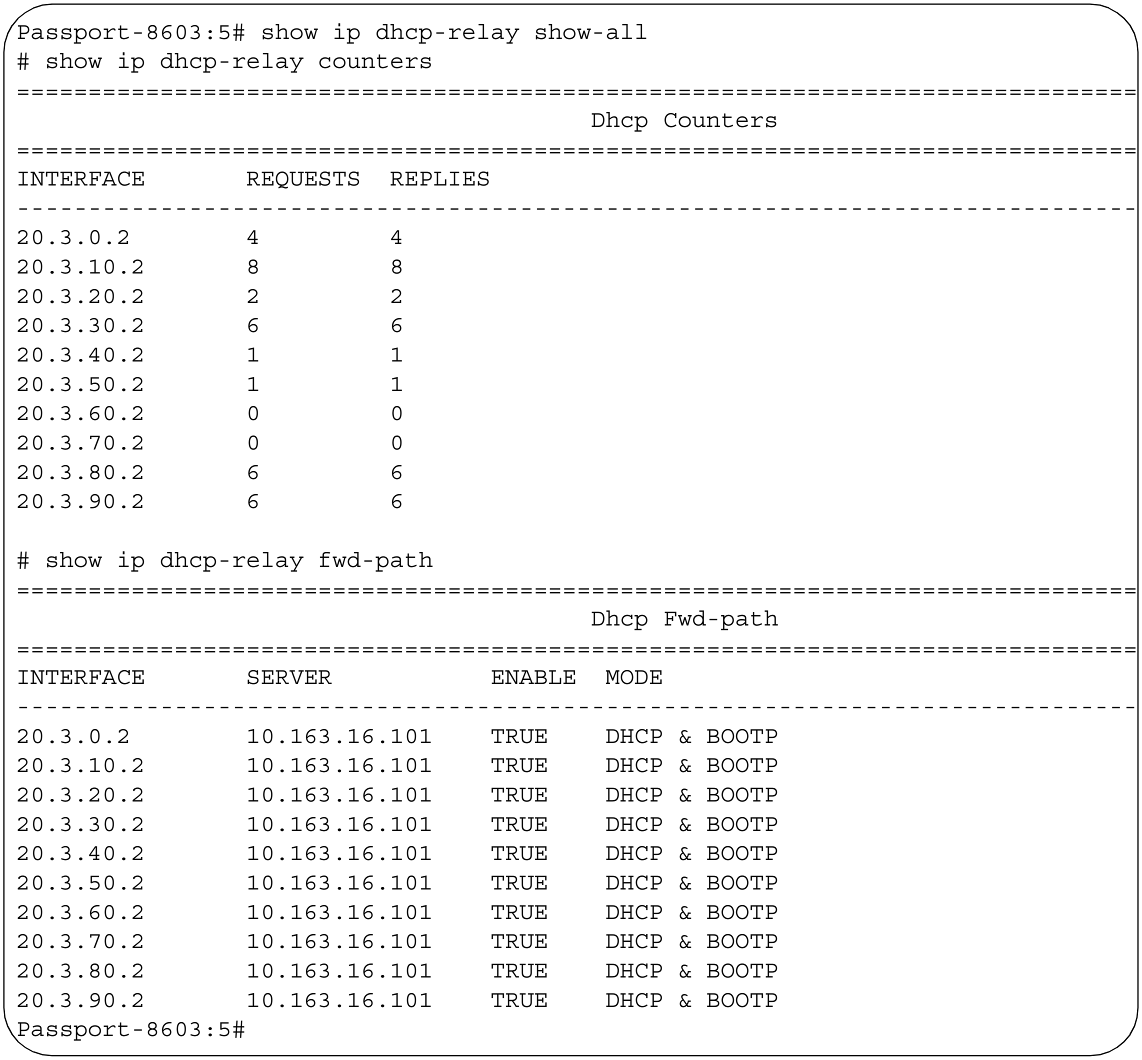
The command uses the syntax:

```
show ip dhcp-relay show-all [file <value>]
```

where `<value>` is the filename to which the output will be redirected.

Figure 6 shows sample output for the **`show ip dhcp-relay show-all`** command.

Figure 6 show ip dhcp-relay show-all command output



```
Passport-8603:5# show ip dhcp-relay show-all
# show ip dhcp-relay counters
==============================================================================
                                        Dhcp Counters
==============================================================================
INTERFACE       REQUESTS  REPLIES
------------------------------------------------------------------------------
20.3.0.2        4         4
20.3.10.2       8         8
20.3.20.2       2         2
20.3.30.2       6         6
20.3.40.2       1         1
20.3.50.2       1         1
20.3.60.2       0         0
20.3.70.2       0         0
20.3.80.2       6         6
20.3.90.2       6         6

# show ip dhcp-relay fwd-path
==============================================================================
                                        Dhcp Fwd-path
==============================================================================
INTERFACE       SERVER           ENABLE  MODE
------------------------------------------------------------------------------
20.3.0.2        10.163.16.101    TRUE    DHCP & BOOTP
20.3.10.2       10.163.16.101    TRUE    DHCP & BOOTP
20.3.20.2       10.163.16.101    TRUE    DHCP & BOOTP
20.3.30.2       10.163.16.101    TRUE    DHCP & BOOTP
20.3.40.2       10.163.16.101    TRUE    DHCP & BOOTP
20.3.50.2       10.163.16.101    TRUE    DHCP & BOOTP
20.3.60.2       10.163.16.101    TRUE    DHCP & BOOTP
20.3.70.2       10.163.16.101    TRUE    DHCP & BOOTP
20.3.80.2       10.163.16.101    TRUE    DHCP & BOOTP
20.3.90.2       10.163.16.101    TRUE    DHCP & BOOTP
Passport-8603:5#
```

show ip udpfwd command

The **`show ip udpfwd show-all`** command displays all relevant IP UDP forwarding information.

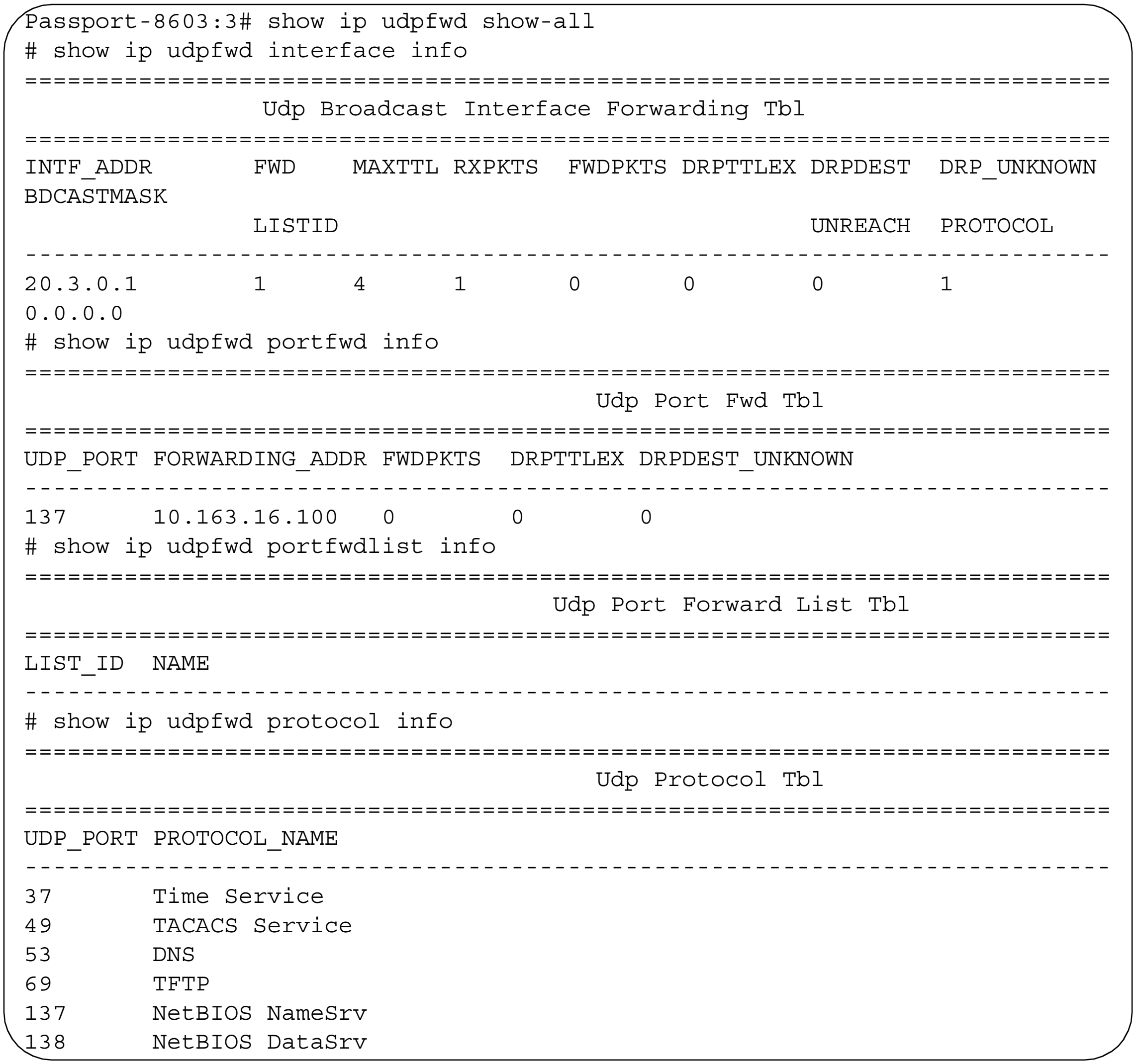
The command uses the syntax:

show ip udpfwd show-all [file *<value>*]

where *<value>* is the filename to which the output will be redirected.

Figure 7 shows sample output for the **show ip udpfwd show-all** command.

Figure 7 show ip udpfwd show-all command output



```
Passport-8603:3# show ip udpfwd show-all
# show ip udpfwd interface info
============================================================================
                 Udp Broadcast Interface Forwarding Tbl
============================================================================
INTF_ADDR       FWD    MAXTTL RXPKTS  FWDPKTS DRPTTLEX DRPDEST  DRP_UNKNOWN
BDCASTMASK
                LISTID                                 UNREACH  PROTOCOL
----------------------------------------------------------------------------
20.3.0.1        1      4      1       0       0        0        1
0.0.0.0
# show ip udpfwd portfwd info
============================================================================
                                        Udp Port Fwd Tbl
============================================================================
UDP_PORT FORWARDING_ADDR FWDPKTS  DRPTTLEX DRPDEST_UNKNOWN
----------------------------------------------------------------------------
137      10.163.16.100   0        0        0
# show ip udpfwd portfwdlist info
============================================================================
                                     Udp Port Forward List Tbl
============================================================================
LIST_ID  NAME
----------------------------------------------------------------------------
# show ip udpfwd protocol info
============================================================================
                                        Udp Protocol Tbl
============================================================================
UDP_PORT PROTOCOL_NAME
----------------------------------------------------------------------------
37       Time Service
49       TACACS Service
53       DNS
69       TFTP
137      NetBIOS NameSrv
138      NetBIOS DataSrv
```

show ipx command

The **`show ipx show-all`** command displays all relevant IPX information.

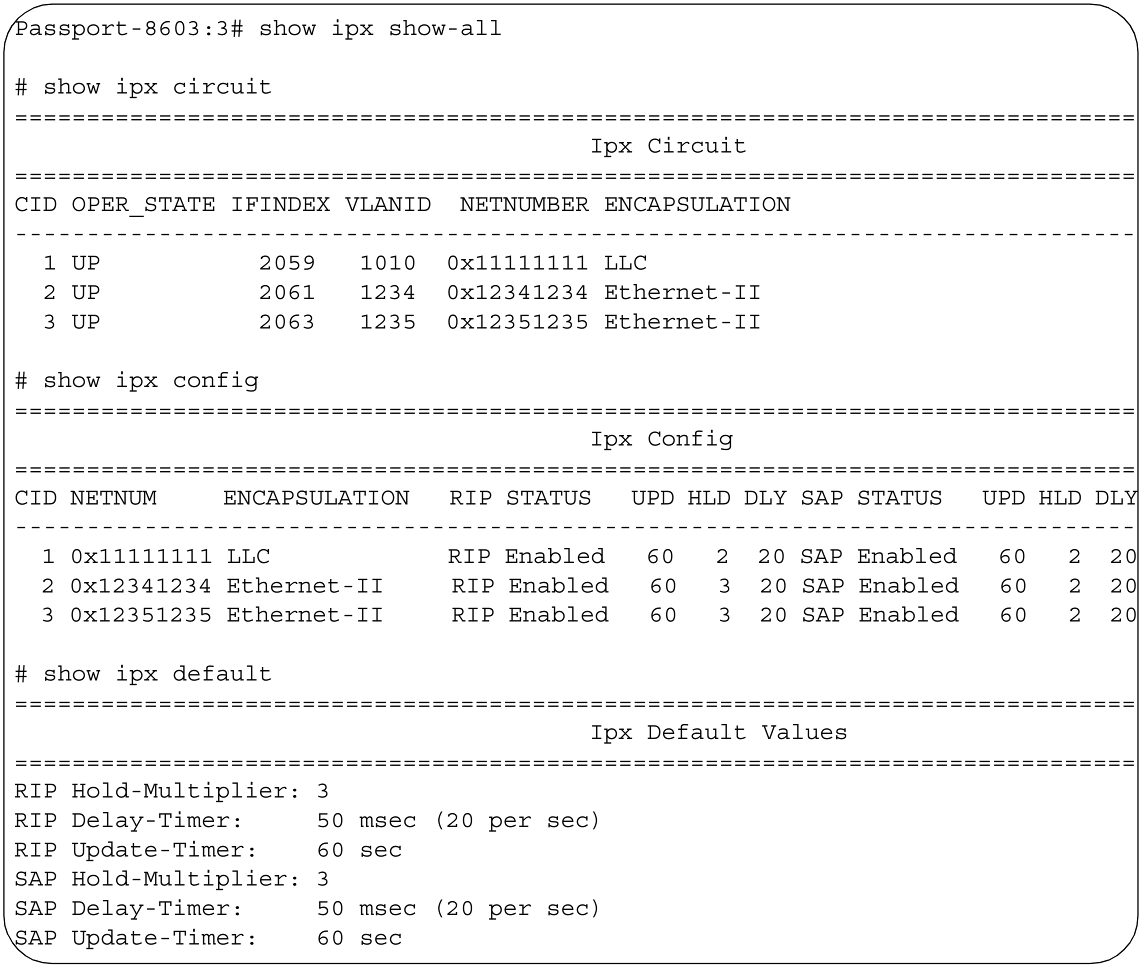
The command uses the syntax:

```
show ipx show-all [file <value>]
```

where *`<value>`* is the filename to which the output will be redirected.

Figure 8 shows sample output for the **`show ipx show-all`** command.

Figure 8 show ipx show-all command output



```
Passport-8603:3# show ipx show-all

# show ipx circuit
===============================================================================
                                        Ipx Circuit
===============================================================================
CID OPER_STATE IFINDEX VLANID  NETNUMBER ENCAPSULATION
-------------------------------------------------------------------------------
  1 UP           2059   1010  0x11111111 LLC
  2 UP           2061   1234  0x12341234 Ethernet-II
  3 UP           2063   1235  0x12351235 Ethernet-II

# show ipx config
===============================================================================
                                        Ipx Config
===============================================================================
CID NETNUM    ENCAPSULATION   RIP STATUS   UPD HLD DLY SAP STATUS   UPD HLD DLY
-------------------------------------------------------------------------------
  1 0x11111111 LLC            RIP Enabled   60   2  20 SAP Enabled   60   2  20
  2 0x12341234 Ethernet-II    RIP Enabled   60   3  20 SAP Enabled   60   2  20
  3 0x12351235 Ethernet-II    RIP Enabled   60   3  20 SAP Enabled   60   2  20

# show ipx default
===============================================================================
                                        Ipx Default Values
===============================================================================
RIP Hold-Multiplier: 3
RIP Delay-Timer:     50 msec (20 per sec)
RIP Update-Timer:    60 sec
SAP Hold-Multiplier: 3
SAP Delay-Timer:     50 msec (20 per sec)
SAP Update-Timer:    60 sec
```

show ports error command

The **`show ports error show-all`** command displays all relevant port error information.

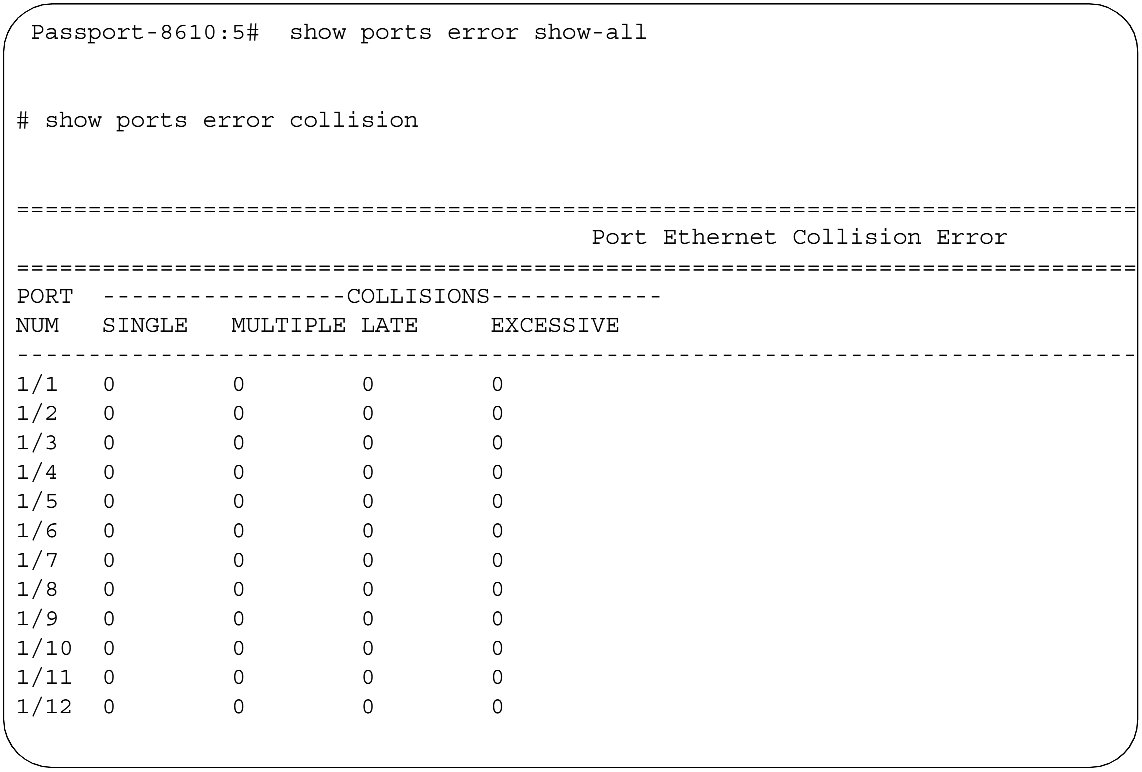
The command uses the syntax:

`show ports error show-all` `[file` *`<value>`*`]`

where *`<value>`* is the filename to which the output will be redirected.

Figure 9 shows sample output for the **show ports error show-all** command.

Figure 9 show ports error show-all command output



```
 Passport-8610:5#  show ports error show-all


# show ports error collision


==============================================================================
                                        Port Ethernet Collision Error
==============================================================================
PORT  -----------------COLLISIONS------------
NUM   SINGLE   MULTIPLE LATE     EXCESSIVE
------------------------------------------------------------------------------
1/1   0        0        0        0
1/2   0        0        0        0
1/3   0        0        0        0
1/4   0        0        0        0
1/5   0        0        0        0
1/6   0        0        0        0
1/7   0        0        0        0
1/8   0        0        0        0
1/9   0        0        0        0
1/10  0        0        0        0
1/11  0        0        0        0
1/12  0        0        0        0
```

show ports stats command

The **show ports stats show-all** command displays all relevant port statistical information.

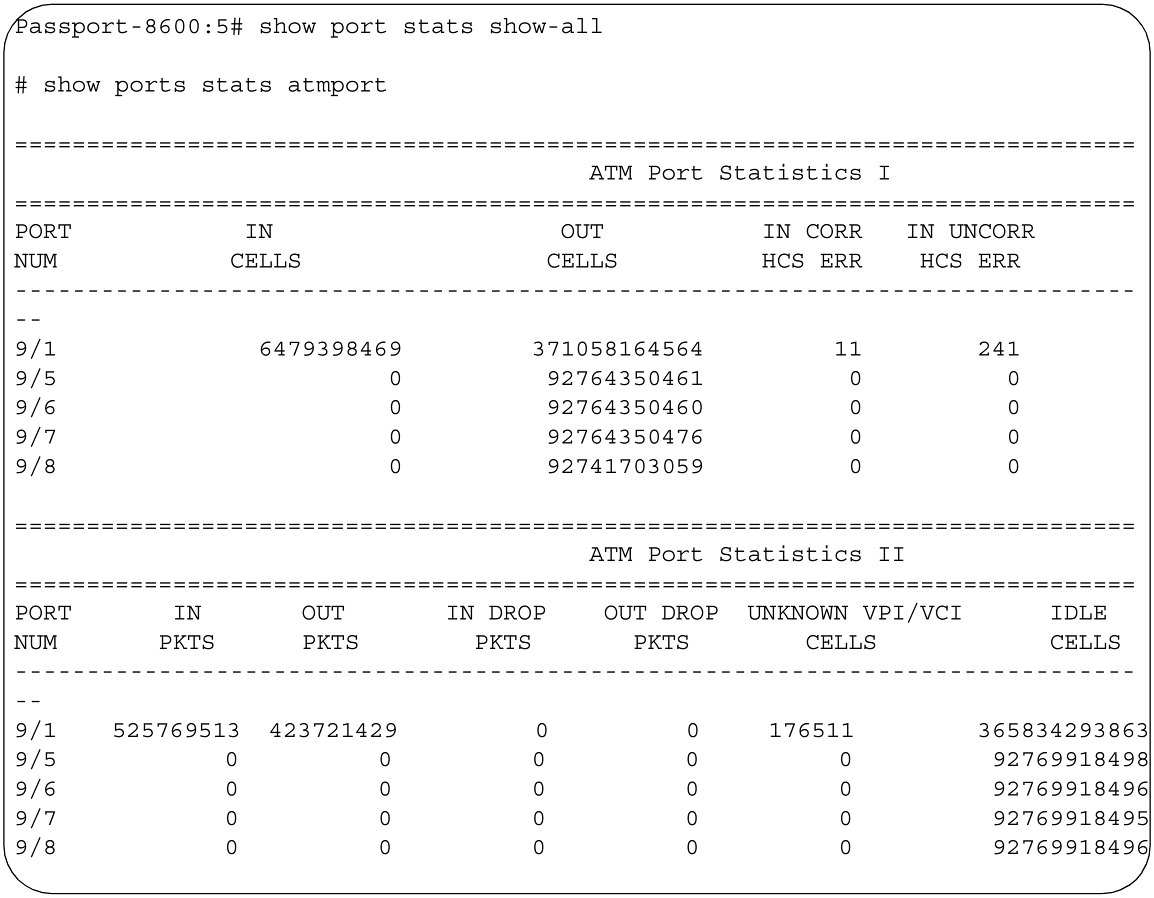
The command uses the syntax:

show ports stats show-all [file *<value>*]

where *<value>* is the filename to which the output will be redirected.

Figure 10 shows sample output for the **show ports stats show-all** command.

Figure 10 show ports stats show-all command output



```
Passport-8600:5# show port stats show-all

# show ports stats atmport

==============================================================================
                                        ATM Port Statistics I
==============================================================================
PORT            IN                    OUT           IN CORR   IN UNCORR
NUM            CELLS                 CELLS          HCS ERR    HCS ERR
------------------------------------------------------------------------------
--
9/1              6479398469         371058164564         11        241
9/5                       0          92764350461          0          0
9/6                       0          92764350460          0          0
9/7                       0          92764350476          0          0
9/8                       0          92741703059          0          0

==============================================================================
                                        ATM Port Statistics II
==============================================================================
PORT       IN       OUT       IN DROP    OUT DROP  UNKNOWN VPI/VCI      IDLE
NUM       PKTS      PKTS        PKTS       PKTS        CELLS            CELLS
------------------------------------------------------------------------------
--
9/1    525769513  423721429         0          0     176511         365834293863
9/5            0          0         0          0          0          92769918498
9/6            0          0         0          0          0          92769918496
9/7            0          0         0          0          0          92769918495
9/8            0          0         0          0          0          92769918496
```

Chapter 2
Booting and accessing the switch

This chapter describes the four-stage boot sequence, instructions for accessing the Boot Monitor and Run-Time CLI, and instructions for navigating the CLI. This section includes the following topics:

Booting the switch

Passport 8000 Series switches go through a four-stage boot sequence before they become fully operational. When you turn on power to the switch, the 8690/8691SF or 8190SM module starts its built-in boot loader. In a Passport 8000 Series switch with redundant switch fabric or switch management modules, the module in slot 5 provides the active CPU functions when the switch powers up or resets. (Options in the Boot Monitor CLI allow you to specify which module is the active CPU.) The switch fabric subsystems of both modules are active and share the switching functions for the switch.

The boot sequence consists of the following four file loads:

- Stage 1: Boot monitor image load
- Stage 2: Boot configuration load
- Stage 3: Run-time image load
- Stage 4: Switch configuration load

The following sections describe what happens at each stage in the boot process.

Stage 1: Loading the boot monitor image

At power-up or reset, the CPU subsystem on the 8691SF module loads the boot monitor image.

When the boot monitor image is loaded, the CPU and basic system devices such as the console port, modem port, PCMCIA card slot, and management port are initialized. (At this stage, the I/O ports are not available; they are not initialized until later in the boot process.)

Stage 2: Loading the boot configuration

After the boot monitor image loads, the boot configuration is loaded from a file called /pcmcia/pcmboot.cfg from the PCMCIA if PCMCIA card is present. If PCMCIA card is not present or file /pcmcia/pcmboot.cfg is not present, then the boot configuration is loaded from a file called /flash/boot.cfg on the onboard flash memory (Nortel Networks recommends having a copy of the boot.cfg file in the /flash directory). If the /flash/boot.cfg file is not present, and if there is a PCMCIA card present, the 8000 Series switch will search for the file /pcmcia/boot.cfg.

Note: If the boot configuration file loaded is corrupted, then the switch may start a loop process.

If none of the boot configuration files are present (/pcmcia/pcmboot.cfg or /flash/boot.cfg or /pcmcia/boot.cfg), the 8000 Series switch will boot using the default boot-configuration settings.

Note: If using a PCMCIA card manufactured by Sandisk, the 8000 Series switch may not be able to access the /pcmcia/pcmboot.cfg or /pcmcia/boot.cfg file during boot-up. This limitation has only been observed during boot-up. No limitation has been observed when accessing the Sandisk(*) device after boot-up.

If the Autoboot flag is set to disabled or if the boot process is interrupted at the console, the boot process stops. At this stage, you have access to the Boot Monitor CLI at the console. In the Boot Monitor CLI, you can set the boot configuration and perform upgrades to the boot monitor image and run-time image (loaded in stage 3). Any changes made and saved at the Boot Monitor CLI change the boot configuration.

After you save changes, you can reinitiate the boot process from the Boot Monitor CLI using the boot command.

Stage 3: Loading the run-time image

The run-time image loads after the boot configuration. This software image initializes the I/O modules and provides full routing switch functionality. The run-time image can be loaded from the flash memory, from a PCMCIA card, or from a TFTP server using the management port.

The default load order is defined in the boot configuration file (/pcmcia/boot.cfg or /flash/boot.cfg). You can redefine the source and order from which to load the run-time image if you interrupt the Autoboot process. You can also specify the order using the CLI or Device Manager.

Stage 4: Loading the switch configuration file

The final step before the boot process is complete is to load the switch configuration file (/flash/config.cfg). The switch configuration consists of any higher-level functionality, including:

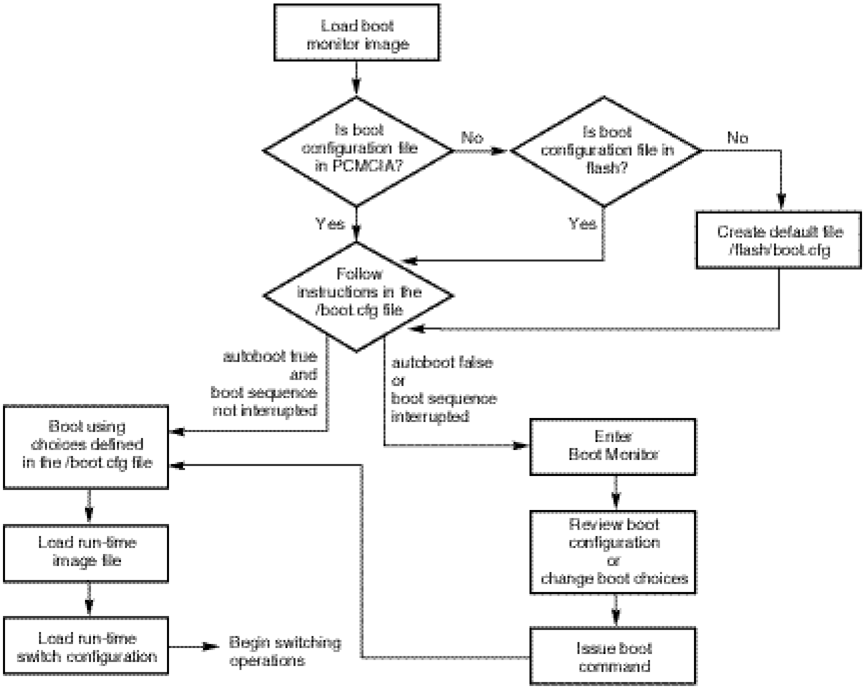
- Chassis configuration
- Port configuration
- Spanning tree group configuration
- VLAN configuration
- Routing configuration
- IP address assignments
- RMON configuration

The default switch configuration includes:

- All ports in a single spanning tree group, STG number 1 (The default Spanning Tree Group is 802.1D compliant, and its BPDUs are never tagged.)
- A single, port-based default VLAN with a VLAN identification number of 1, bound to the default spanning tree group
- Spanning Tree FastStart disabled on all ports
- No interfaces assigned IP addresses
- Traffic priority for all ports set to normal priority
- All ports as nontagged ports
- Default communication protocol settings for the Console port (see *Getting Started* for information about these protocol settings.)

Figure 11 shows a summary of the boot sequence.

Figure 11 Switch boot sequence

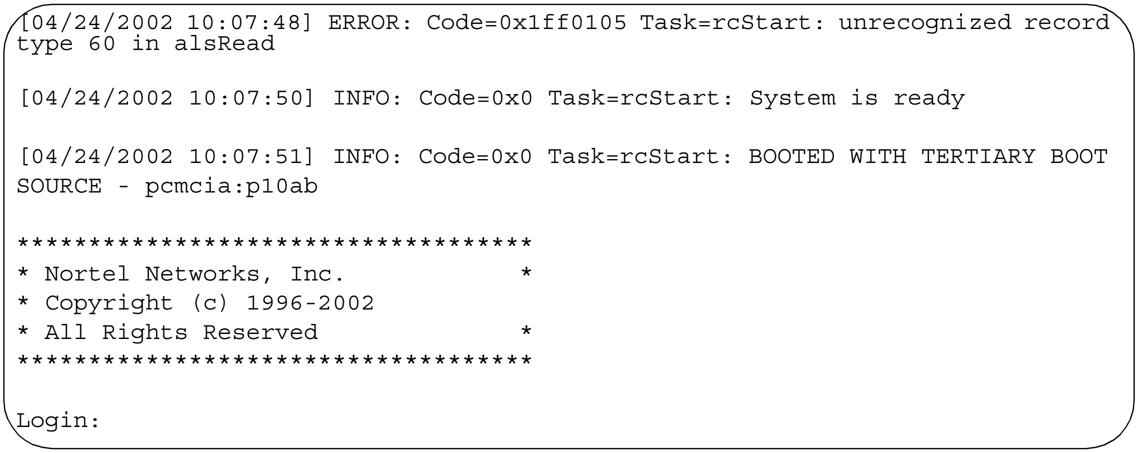

Load boot monitor image
Is boot configuration file in PCMCIA?
No
Is boot configuration file in flash?
No
Create default file /flash/boot.cfg
Yes
Yes
Follow instructions in the /boot.cfg file
autoboot true and boot sequence not interrupted
autoboot false or boot sequence interrupted
Boot using choices defined in the /boot.cfg file
Enter Boot Monitor
Load run-time image file
Review boot configuration or change boot choices
Load run-time switch configuration
Begin switching operations
Issue boot command

Verifying the boot image source after the boot process

After a switch boot, the system notes the boot source and logs a message in the system log file that informs you about the selected boot source. For more information about the different boot sources, see Chapter 3.

Figure 12 displays the boot source messages observed on the console port:

Figure 12 Console port boot source messages



```
[04/24/2002 10:07:48] ERROR: Code=0x1ff0105 Task=rcStart: unrecognized record
type 60 in alsRead

[04/24/2002 10:07:50] INFO: Code=0x0 Task=rcStart: System is ready

[04/24/2002 10:07:51] INFO: Code=0x0 Task=rcStart: BOOTED WITH TERTIARY BOOT
SOURCE - pcmcia:p10ab

*************************************
* Nortel Networks, Inc.             *
* Copyright (c) 1996-2002
* All Rights Reserved               *
*************************************

Login:
```

Accessing the Boot Monitor CLI

The Boot Monitor CLI allows you to configure and manage the boot process. To access the Boot Monitor CLI, do one of the following tasks:

- Reboot and interrupt the boot sequence by pressing the Enter key when the following prompt is displayed:

  ```
  Press Enter to stop autoboot.
  ```

- From the Run-Time CLI, enter the following commands, and then reboot:

```
8610-# config bootconfig flags autoboot false
8610-# save bootconfig
8610-# boot -y
```

Note: You must be using a terminal connected directly to the Console port on the switch. If you reboot the switch from a remote terminal, the connection is terminated.

When you enter the Boot Monitor CLI, the following prompt is displayed:

```
monitor#
```

Accessing the Run-Time CLI

When the Passport 8000 Series switch is up and running, the Run-time CLI commands enable you to perform most of the configuration and management functions necessary to manage the switch. These functions include:

- Resetting or rebooting the Passport 8000 Series switch.
- Adding, deleting, and displaying address resolution protocol (ARP) table entries.
- Pinging another network device.
- Displaying and setting configuration parameters for the entire switch and for individual ports.
- Configuring and displaying Spanning Tree Group (STG) parameters and enable or disable Spanning Tree Protocol on an STG.
- Configuring and displaying MultiLink Trunking (MLT) parameters.
- Testing the switching fabric and perform internal and external loopback tests on individual ports.
- Creating and managing port-based VLANs or policy-based VLANs.

To access the Run-Time CLI, wait until the boot process is complete.

To access the Run-Time CLI you need a connection from a PC or Terminal to the switch. The connection can be direct to the switch through the Console or Modem port or can be either through telnet, rlogin or SSH sessions.

- Telnet Access

  To login to the switch using telnet, type the following command from any PC/Terminal:

  ```
  telnet <ip addr>
  ```

  where
  <*ip address*> is the IP address of the switch to which you want to connect to.

- Rlogin Access

  To remotely login to the switch, type the following command from any PC/Terminal:

  ```
  rlogin <ip addr>
  ```

  where
  <*ip address*> is the IP address of the switch to which you want to connect to.

- SSH Access

  To access the switch using the SSH, see the *Configuring and Managing Security* guide for more information.

Note: Before trying to access the switch by any of the above sessions, make sure you had enabled the corresponding daemon flags in the **config boot flags**. See "Setting system flags" on page 79 for more information.

At the login prompt, enter your user name and password.

Configuring CLI user names

The CLI user names can be configured using the **config cli password** command.

To configure CLI user names, enter the following command:

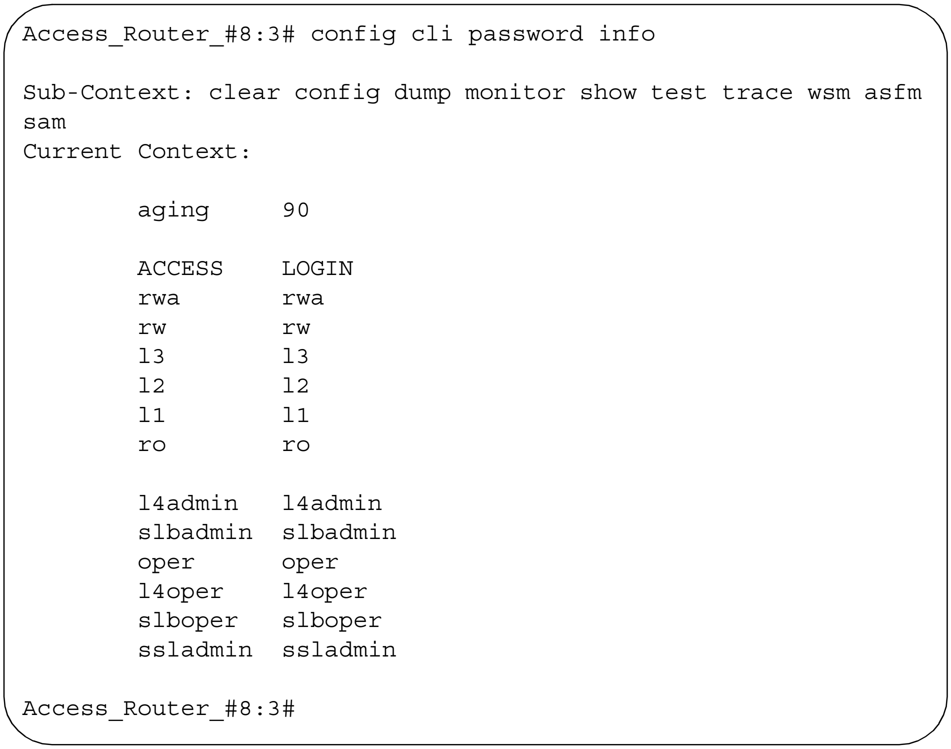
```
config cli password
```

This command includes the following options:

`config cli password` followed by:	
`ro <username> [<password>]`	Sets the read only login and/or password for the user.
`l1 <username> [<password>]`	Sets the layer 1 login and/or password for the user.
`l2 <username> [<password>]`	Sets the layer 2 login and/or password for the user.
`l3 <username> [<password>]`	Sets the layer 3 login and/or password for the user.
`rw <username> [<password>]`	Sets the Read-write login and/or password for the user.
`rwa <username> [<password>]`	Sets the Read-write-all login and/or password for the user.

Figure 13 shows sample output for the **`config cli password info`** command.

Figure 13 config cli password info command output



```
Access_Router_#8:3# config cli password info

Sub-Context: clear config dump monitor show test trace wsm asfm
sam
Current Context:

        aging     90

        ACCESS    LOGIN
        rwa       rwa
        rw        rw
        l3        l3
        l2        l2
        l1        l1
        ro        ro

        l4admin   l4admin
        slbadmin  slbadmin
        oper      oper
        l4oper    l4oper
        slboper   slboper
        ssladmin  ssladmin

Access_Router_#8:3#
```

To set the password aging time, enter the following command:

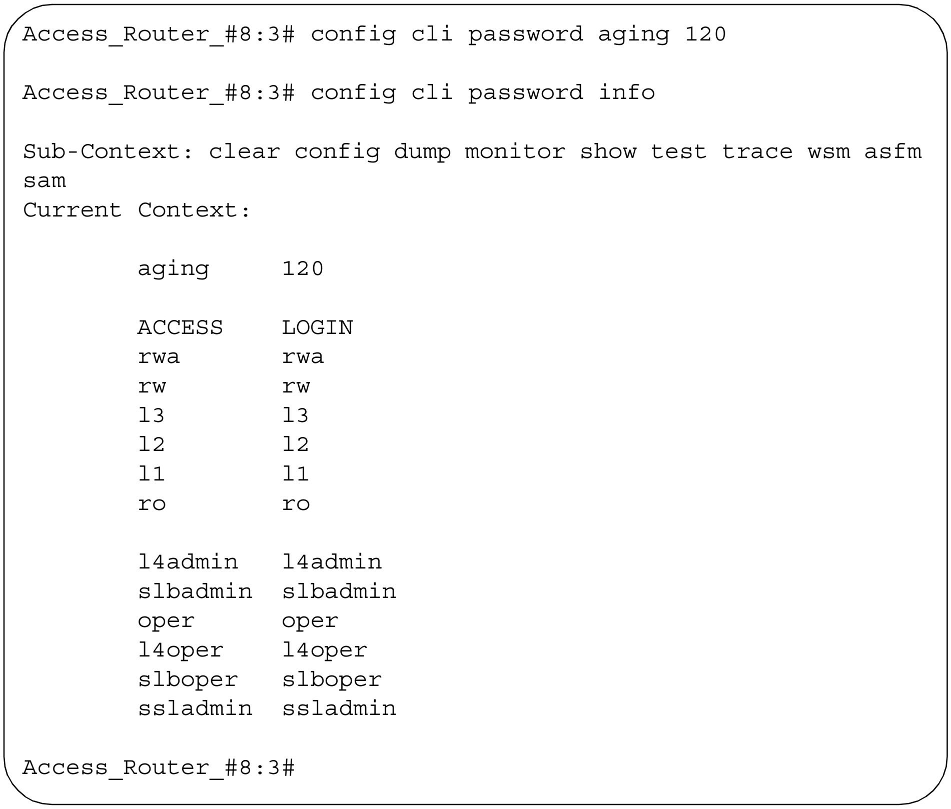
`config cli password aging` *`<days>`*

where
<*days*> is the age-out time for passwords/community strings {1..365}.

Note: The 'aging' field is used only if hsecure flag is enabled. See "Setting system flags" on page 79 for more information.

Figure 14 shows sample output for the **`config cli password aging`** command.

Figure 14 config cli password aging command output

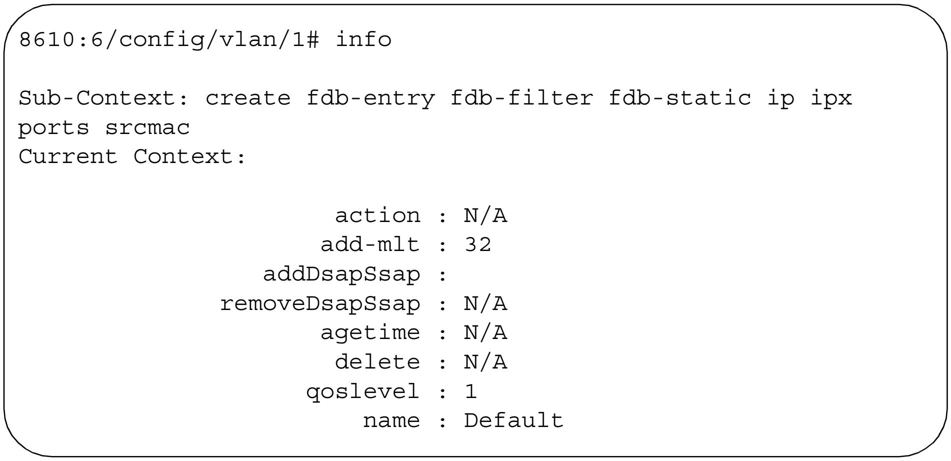


```
Access_Router_#8:3# config cli password aging 120

Access_Router_#8:3# config cli password info

Sub-Context: clear config dump monitor show test trace wsm asfm
sam
Current Context:

        aging     120

        ACCESS    LOGIN
        rwa       rwa
        rw        rw
        l3        l3
        l2        l2
        l1        l1
        ro        ro

        l4admin   l4admin
        slbadmin  slbadmin
        oper      oper
        l4oper    l4oper
        slboper   slboper
        ssladmin  ssladmin

Access_Router_#8:3#
```

Navigating the CLI

Each CLI is organized into a tree data structure. When you type a command, you see the command’s context (the current level or branch) and subcontext. Context indicates commands at that level, and subcontext indicates one or more command layers available. Figure 15 shows the screen output, including context and subcontext, for the **`config vlan 1 info`** command.

Figure 15 Context and subcontext in the CLI



```
8610:6/config/vlan/1# info

Sub-Context: create fdb-entry fdb-filter fdb-static ip ipx
ports srcmac
Current Context:

                       action : N/A
                      add-mlt : 32
                  addDsapSsap :
               removeDsapSsap : N/A
                      agetime : N/A
                       delete : N/A
                     qoslevel : 1
                         name : Default
```

When you are in a given branch of the tree, you need to type only the subcommand for that level. For example, to view the configuration information of VLAN 1 from the top or prompt level, type **`config vlan 1 info`**. When you are already in the “config vlan” branch (as in Figure 15), you need to only type **`info`**. In addition, when you are at a certain level, you will remain at that level until you type **`box`** or **`top`**. (These two commands return the CLI context to the system-level prompt.) This feature enables you to create, delete, or change all relevant parameters for a port without reentering information.

Figure 16 and Figure 17 show sample command hierarchies for the Run-Time and Boot Monitor CLI, respectively. These samples do not include all commands.

Figure 16 Run-Time CLI—partial command hierarchy

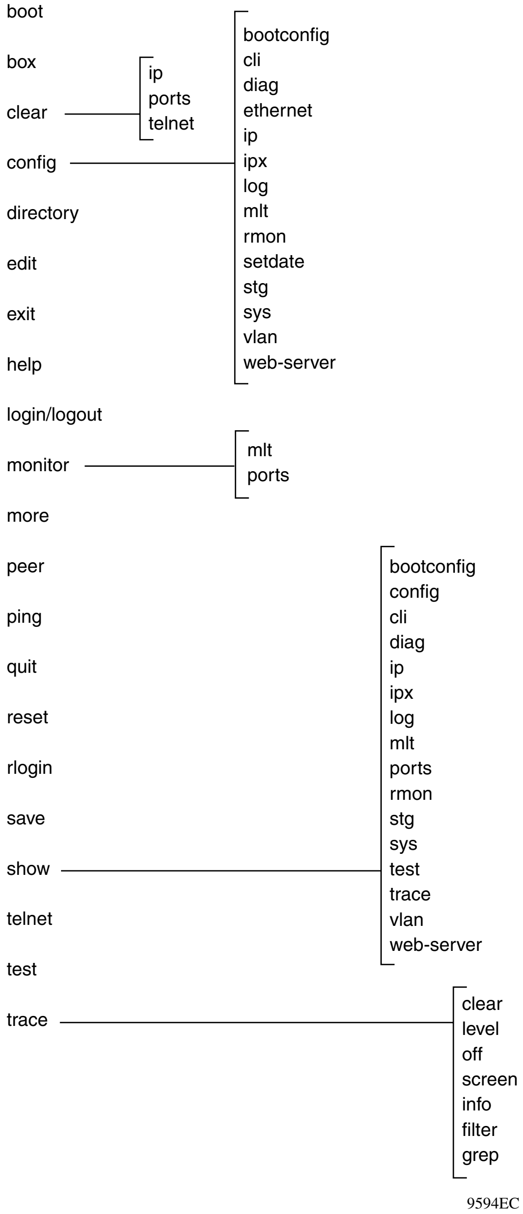
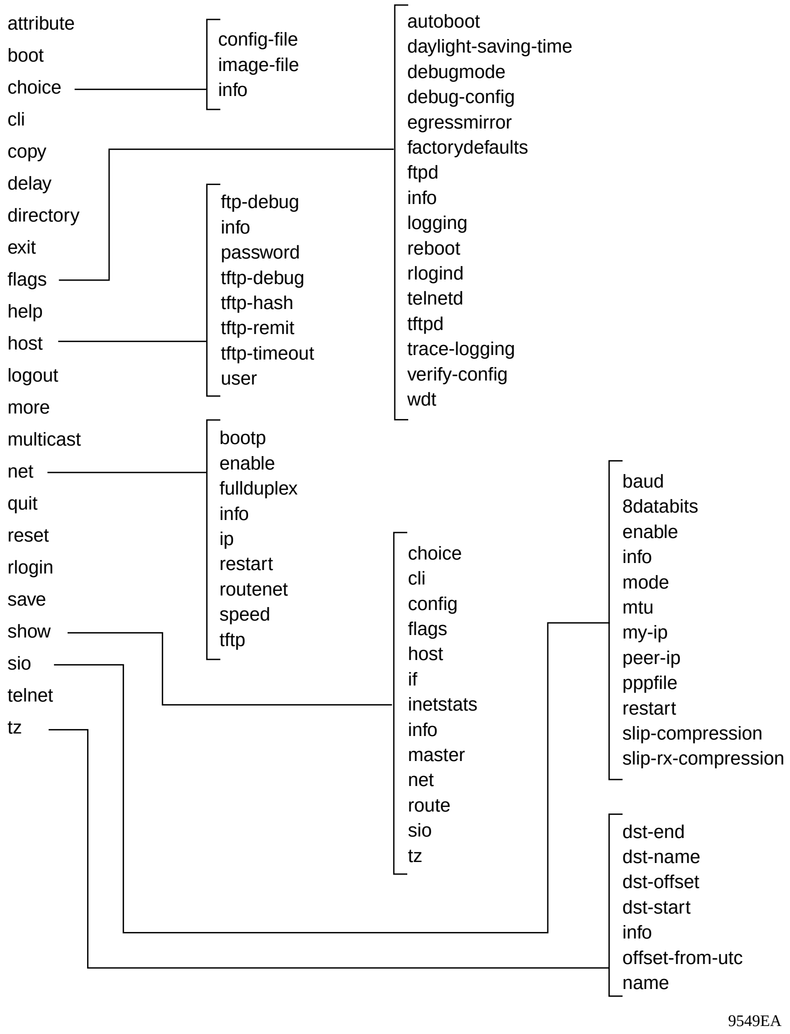


Figure 17 Boot Monitor CLI—partial command hierarchy



Command syntax

Commands are generally in the form *<top-level command> <command option> <argument>*. For example, to enable access to the switch through the Web management interface, you use the following command:

```
config web-server enable
```

where:

config is the top-level command.
web-server is one of the possible options for the **config** command.
enable is the argument.

The system prompt on the screen indicates the level or branch of the command structure at which you are operating. When the system prompt is 8600#, you are at the top level. If you type only the top-level command and press Enter, you move into that branch of the command tree and the system prompt changes to indicate the new context. For example, if you type **config** and press Enter, the system prompt changes to 8600/config#. When you are in a given branch of the tree, you need to type only the subcommand for that level. For example, to set the system contact from the top level, type **config sys set contact** <*contact*>. When you are already in the “config sys” branch, you need only type **set contact** <*contact*>.

In addition, after you have entered information to put you at a certain level, you remain at that level until you type back or reenter the original command. For example, when you use a command that begins with config ethernet <*ports*>, after you enter a port number, you do not have to reenter this information unless you go back up a level. This feature enables you to create, delete, or change all relevant parameters for this port without reentering information.

To avoid having to type complete commands, you can enter a shortened version of the command, such as **dis** for disable or **en** for enable, or type part of a command and then press the Tab key to complete the command. If the letters you typed are unique to a command, the command is completed automatically. If not, a bell sounds to indicate that more information is necessary.

Navigation commands

The following navigation commands are available in the Boot Monitor and Run-Time CLIs:

- **back**—takes you back up one level.
- **box**—goes to the top or the box level.
- **cwc**—changes the current working context.

- **`pwc`**—displays the current working context.
- **`pwd`**—prints the current working directory in the file system.
- **`top`**—goes to the box or top level (same as the **`box`** command).
- **`..`**—goes back up one level (same as the **`back`** command).

Throughout the CLI, you can use the following keystrokes:

- The up arrow key or Control-P: to view and scroll through the previous history commands.
- The down arrow key or Control-N: to view and scroll through the next history commands.
- Control-U: to delete a line; clears the line and allows you to enter a new command.
- Control-C: to abort a line entry; aborts the command entry and puts you at a new prompt. Note that this command does not abort the current command level that is running, only the new entry.
- Control-D: logs you off the system.
- Control-S/Control-Q: software flow control XON/XOFF.
- The Tab key or Control-I: command completion; completes the command when you have entered part of a word (`sh` for show).
- The Backspace key or Control-H: backspace.

For a complete list of the keystrokes available in the CLI, see Appendix C.

Parameter values in the CLI are indicated by angle brackets < >. Parameters can be optional or required. Required parameters must be in the specified order, followed by optional parameters. Optional parameters are displayed in brackets [ ].

When you enter multiple CLI commands, you can terminate a command within a single line of input by using the semicolon (;) as the separator. A semicolon is treated like a carriage return by the CLI.

Specifying ports

Each port identifier in the CLI has two components: a slot number and a port number. The slot number identifies the chassis slot containing the switch module that the port is on. The port number identifies the position of the port on the switch module. Port numbers begin with port 1 on top at the far left of the module. For more details about the port numbering in the modules, see Appendix A.

In a Passport 8000 Series switch, chassis slots are numbered from the top slot down, beginning with 1 for the top slot.

To specify a single port, type the slot number, a forward slash, and then the port number. For example, to specify port 20 on the switch management module in slot 3 of the switch, express the port number as follows:

```
3/20
```

To specify a list of port numbers, separate individual port numbers with commas. There is no space between the port numbers and the commas. Some examples of port lists are:

```
3/4,3/10,3/30,7/2,8/16
```

```
2/7,1/3,4/4
```

To specify a range of ports, type the low port number in the range, a dash, and then the high port number in the range. There is no space between the port numbers and the dashes. Some examples of port ranges are:

```
3/1-3/6
```

```
2/2-2/9
```

```
2/5-3/5
```

When you specify ports, you can specify any combination of port lists and port ranges. For example, the following port arguments are valid:

```
2/7,3/1-3/6
```

```
3/2-3/5,1/1-1/7,7/1
```

```
7/6,2/5,3/1-3/7,2/1
```

Specifying IP addresses and subnet masks

All IP addresses in the CLI are specified in dotted-decimal notation as follows:

```
<xxx>.<xxx>.<xxx>.<xxx>
```

An IP address with a subnet mask can be specified in two forms:

```
<xxx>.<xxx>.<xxx>.<xxx>/<yyy>.<yyy>.<yyy>.<yyy>
```

or

```
<xxx>.<xxx>.<xxx>.<xxx>/<n>
```

where:

`<xxx>.<xxx>.<xxx>.<xxx>` is the IP address in dotted-decimal notation.

`<yyy>.<yyy>.<yyy>.<yyy>` is the subnet mask in dotted-decimal notation.

`<n>` is the number of subnet mask bits.

The following examples both refer to the same IP address and subnet mask pair:

```
10.10.10.1/255.255.255.0
```

```
10.10.10.1/24
```

Chapter 3
Managing the boot process

This chapter describes how to configure and manage the boot process using the Boot Monitor CLI. You access the Boot Monitor CLI by either interrupting the boot process or from the Run-Time CLI. See "Accessing the Boot Monitor CLI" on page 51 for instructions.

This section includes the following topics:

- "Roadmap of Boot Monitor CLI commands," next
- "Configuring the Boot Monitor CLI" on page 70
- "Configuring the Boot Monitor CLI from the Run-Time CLI" on page 72
- "Saving the boot configuration to a file" on page 92

Roadmap of Boot Monitor CLI commands

The following roadmap lists the commands and their parameters that you use to configure the Boot Monitor CLI. Use this list as a quick reference or click on any entry for more information:

Command	Parameter
`config cli`	`info`
	`more <true|false>`
	`prompt <value>`
	`rlogin-sessions <value>`
	`screenlines <value>`
	`telnet-sessions <value>`
	`timeout <seconds>`
`config bootconfig`	`info`
	`delay <seconds>`
	`master <cpu-slot>`
	`multicast <value>`
	`logfile minsize maxsize maxoccupyPercentage`
`config bootconfig cli`	`info`
	`more <true|false>`
	`prompt <value>`
	`rlogin-sessions <value>`
	`screenlines <value>`
	`telnet-sessions <value>`
	`timeout <seconds>`
`config bootconfig choice <boot-choice>`	`info`
	`config-file <filename>`
	`image-file <filename>`
`config bootconfig delay <seconds>`	

Command	Parameter
config bootconfig flags	info
	8100-mode <true|false>
	autoboot <true|false>
	daylight-saving- time <true|false>
	debugmode <true|false>
	debug-config <true|false>
	egress-mirror <true|false>
	factorydefaults <true|false>
	ftpd <true|false>
	logging <true|false>
	reboot <true|false>
	rlogind <true|false>
	savetostandby <true|false>
	block-snmp <true|false>
	sshd <true|false>
	telnetd <true|false>
	tftpd <true|false>
	trace-logging <true|false>
	verify-config <true|false>
	wdt <true|false>
config bootconfig host	info
	ftp-debug <true|false>
	password <value>
	tftp-debug <true|false>
	tftp-hash <true|false>
	tftp-rexmit <seconds>
	tftp-timeout <seconds>
	user <value>
config bootconfig master <cpu-slot>	
show bootconfig master	

Command	Parameter
config bootconfig net <cpu-net-port>	info
	autonegotiate <true|false>
	bootp <true|false>
	enable <true|false>
	fullduplex <true|false>
	ip <addr/mask> [cpu-slot <value>]
	restart
	route <net|add|del> <netaddr> <gateway>
	speed <10|100>
	tftp <ipaddr>
show bootconfig	info
	choice
	cli
	config [verbose]
	flags
	host
	master
	net
	show-all [file <value>]
	sio
	tz
	wlan
config bootconfig sio <cpu-sio-port>	info
	baud <rate>
	8databits <true|false>
	enable <true|false>
	mode <ascii|slip|ppp>
	mtu <bytes>

Command	Parameter
	my-ip <ipaddr>
	peer-ip <ipaddr>
	pppfile <file>
	restart
	slip-compression <true|false>
	slip-rx-compression <true|false>
config bootconfig tz	info
	dst-end <Mm.n.d/hhmm| MMddhhmm>
	dst-name <dstname>
	dst-offset <minutes>
	dst-start <Mm.n.d/hhmm| MMddhhmm>
	offset-from-utc <minutes>
	name <tz>
config bootconfig show	info
	choice
	cli
	config [verbose]
	flags
	host
	master
	net
	show-all [file <value>]
	sio
	tz
	wlan

➡ **Note:** You can initiate a Boot Monitor CLI session only through a direct serial-port connection to the switch. After the Boot Monitor CLI is active, you can access it through a Telnet or rlogin session. (The flags for Telnet and rlogin must be set to allow remote access.) Within the Boot Monitor CLI, you can change the boot configuration, including boot choices and boot flags.

Configuring the Boot Monitor CLI

If you accessed the Boot Monitor CLI by interrupting the boot process (see page 51 for instructions), you can configure and manage the Boot Monitor CLI using the following command:

```
config cli
```

➡ **Note:** For the changes made to the Boot Monitor CLI to take effect, you must use the **`save`** command to save the changed configuration file and then reboot the switch. See "Saving the boot configuration to a file" on page 92 for more information.

This command includes the following options:

`config cli` followed by	
`info`	Displays information about the current settings of CLI display options.
`more <true|false>`	Enables scrolling of display output. The default is true. • `true` sets output display scrolling to one page at a time. • `false` sets the output display to continuous scrolling.
`prompt <value>`	Sets the root-level prompt. The default is monitor. • *`value`* is a string (1 to 1024 characters).
`rlogin-sessions <value>`	Sets the allowable number of allowed inbound rlogin/rsh sessions. The default is 8. • *`value`* is the number of sessions (0 to 8).

`config cli` followed by	
`screenlines <value>`	Sets the number of lines displayed on the terminal screen. The default is 23. • *`value`* is the number of lines (8 to 64).
`telnet-sessions <value>`	Sets the allowable number of inbound Telnet sessions. The default is 8. • *`value`* is the number of sessions (0 to 8).
`timeout <seconds>`	Sets the idle timeout period before automatic logout for CLI sessions; the default is 0. • *`seconds`* is the timeout period in seconds (30 to 65536).

Figure 18 shows sample output from the **`cli info`** command.

Figure 18 cli info command output

```
monitor# cli info
cli more true
cli prompt "monitor"
cli rlogin-sessions 8
cli screenlines 23
cli telnet-sessions 8
cli timeout 0
monitor#
```

The Boot Monitor **`config cli`** command contains several sub-commands, which are similar to the Run-Time **`config cli`** commands described in Chapter 4, “Managing the Run-Time process.”

Configuring the Boot Monitor CLI from the Run-Time CLI

When you are in the Run-Time CLI, you can make changes to the Boot Monitor CLI using the following command:

```
config bootconfig
```

➡ **Note:** You can also execute the commands in this section from the `monitor` prompt. This prompt appears if you accessed the Boot Monitor CLI by interrupting the boot process.

➡ **Note:** If you make changes to the Boot Monitor CLI using the **`config bootconfig`** command, you must use the **`save bootconfig`** command to save the changed configuration file. For the changes to take effect, you must then reboot the switch. See "Saving the boot configuration to a file" on page 92 for more information.

The **`config bootconfig`** command includes the following options:

`config bootconfig` followed by:	
`info`	Displays the configured values for `delay`, `master`, and `multicast`.
`delay <`*`seconds`*`>`	Sets the number of seconds a standby CPU should wait (delay) before trying to become the master CPU. This command applies only during a cold start and does not apply to a failover start. The default is 2 seconds delay.
`master <`*`cpu-slot`*`>`	Indicates which CPU should become master when the switch is turned on. The master CPU performs a loopback test to test the switch fabric. The default master is set for slot 5. • *`cpu-slot`* specifies the module position, either slot 5 or slot 6.

config bootconfig followed by:	
multicast *<value>*	Sets the system multicast scaling parameter. Valid values are 0 to 2147483647.
logfile minsize maxsize maxoccupyPercentage	Sets the parameters for the log file. • minsize specifies the minimum size of the log file. The valid values are 64 to 500 KB. • maxsize specifies the maximum size of the log file. The valid values are 500 to 16384 KB. • maxoccupyPercentage is the percentage of free PCMCIA that can be used for a log file. The valid values are 10 to 90.

The **config bootconfig** command contains several sub-commands. The following topics describe some of the tasks that you can perform using this command:

- "Modifying Boot Monitor CLI operation," next
- "Modifying the boot sequence" on page 75
- "Changing the boot source order" on page 77
- "Setting the standby-to-master delay" on page 78
- "Setting system flags" on page 79
- "Configuring the remote host login" on page 82
- "Specifying the master CPU" on page 83
- "Configuring CPU network port devices" on page 83
- "Displaying the Boot Monitor configuration" on page 85
- "Configuring the CPU serial port devices" on page 87
- "Setting the time zone" on page 88
- "Displaying the Boot Monitor configuration" on page 91

Modifying Boot Monitor CLI operation

To change the operation of the Boot Monitor CLI, use the following command:

```
config bootconfig cli
```

The **`config bootconfig cli`** command includes the following options:

`config bootconfig cli` followed by:	
`info`	Displays the current settings for the Boot Monitor CLI (Figure 19).
`more <`*`true`*`|`*`false`*`>`	Sets scrolling for the output display. The default is true. • `true` sets output display scrolling to one page at a time. • `false` sets the output display to continuous scrolling.
`prompt <`*`value`*`>`	Changes the Boot Monitor prompt to the defined string. • *`value`* is a string from 1 to 32 characters.
`rlogin-sessions <`*`value`*`>`	Sets the allowable number of inbound remote Boot Monitor CLI login sessions; the default is 8. • *`value`* is the number of sessions (0 to 8).
`screenlines <`*`value`*`>`	Sets the number of lines in the output display; the default is 23. • *`value`* is the number of lines (8 to 64).
`telnet-sessions <`*`value`*`>`	Sets the allowable number of inbound Telnet sessions; the default is 8. • *`value`* is the number of sessions (0 to 8).
`timeout <`*`seconds`*`>`	Sets the idle timeout period before automatic logout for CLI sessions; the default is 0. • *`seconds`* is the timeout period in seconds (0 to 65536).

Figure 19 shows output from the **`config bootconfig cli info`** command.

Figure 19 config bootconfig cli info command output

```
config bootconfig cli info
config bootconfig cli info
cli more true
cli prompt "monitor"
cli rlogin-sessions 8
cli screenlines 23
cli telnet-sessions 8
cli timeout 0
```

Modifying the boot sequence

The default boot sequence directs the switch to look for its image and configuration files first on the PCMCIA card, then in the onboard flash memory, and then from a server on the network. That is, the PCMCIA card is the *primary* source for the files, the onboard flash memory is the *secondary* source, and the network server is the *tertiary* source. These source and file name definitions are in the boot configuration file.

➡ **Note:** If a Passport 8000 Series switch loads its secondary software image file because it cannot find its primary software image, during this process, it also loads the secondary configuration file.

You can change the boot sequence in the following ways:

- Change the primary, secondary, and tertiary designations for file sources. For example, you can specify the network as the primary file source and update the configuration file or image file using a single copy of the file on the server. In the CLI, use the **`config bootconfig choice`** command. For instructions on using this command, see "Changing the boot source order" on page 77. In Device Manager, select the switch fabric module on the device view, and choose Edit > Card > Boot Config.

➡ **Note:** Each choice of a file source (primary, secondary, or tertiary) specifies an image file and a matching configuration file. When you specify a source, you specify the associated pair of files.

- Change the file names from the default values. You can store several versions of the image or configuration file and specify a particular one by file name when you reboot the switch. In the CLI, use the **`config bootconfig choice`** command. In Device Manager, select the switch fabric module on the device view, and choose Edit > Card > Boot Config.
- Boot the switch without loading a configuration file, so that the switch uses its factory default configuration settings. Bypassing the switch configuration does not affect any saved switch configuration; the configuration is simply not loaded.

Whether the switch configuration is loaded or not is controlled by the boot configuration. You can bypass loading of the switch configuration in the following ways:

- Use the Boot Monitor CLI and the following **`flags`** command:

  `flags factorydefault true`

- Use the Run-Time CLI and issue this command:

  `config bootconfig flags factorydefault true`

- In Device Manager, select the switch fabric module on the device view. Then choose Edit > Card > Boot Config and set the EnableFactoryDefaults parameter to true.

When the configuration is bypassed, the switch boots with the default switch configuration settings and the boot flag settings that were loaded as the boot configuration file in stage 2.

Figure 20 describes the boot source text added to the system log file:

Figure 20 Boot source text added to the system log file

```
157: [04/24/2002 10:07:50] INFO: Code=0x0 Task=rcStart: System
is ready

158: [04/24/2002 10:07:51] INFO: Code=0x0 Task=rcStart: BOOTED
WITH TERTIARY BOOT SOURCE - pcmcia:p10ab

159: [04/24/2002 10:07:51] WARNING: Code=0x0 Task=rcStart:
CANNOT ACCESS SECONDARY BOOT SOURCE

160: [04/24/2002 10:07:51] WARNING: Code=0x0 Task=rcStart:
PRIMARY BOOT SOURCE IS NON-EXECUTABLE

161: [04/24/2002 10:07:52] INFO: Code=0x0 Task=tTrapd: Link
Up(1/1)
```

Changing the boot source order

To display or change the order in which the boot sources (flash and PCMCIA card) are accessed, use the following command:

`config bootconfig choice` *`<boot-choice>`*

where:
`boot-choice` is the order in which the specified boot devices are accessed when you reboot the switch. The options for *`boot-choice`* are `primary, secondary, or tertiary`. The default order is to access the PCMCIA card first, and then the onboard flash.

This command includes the following options:

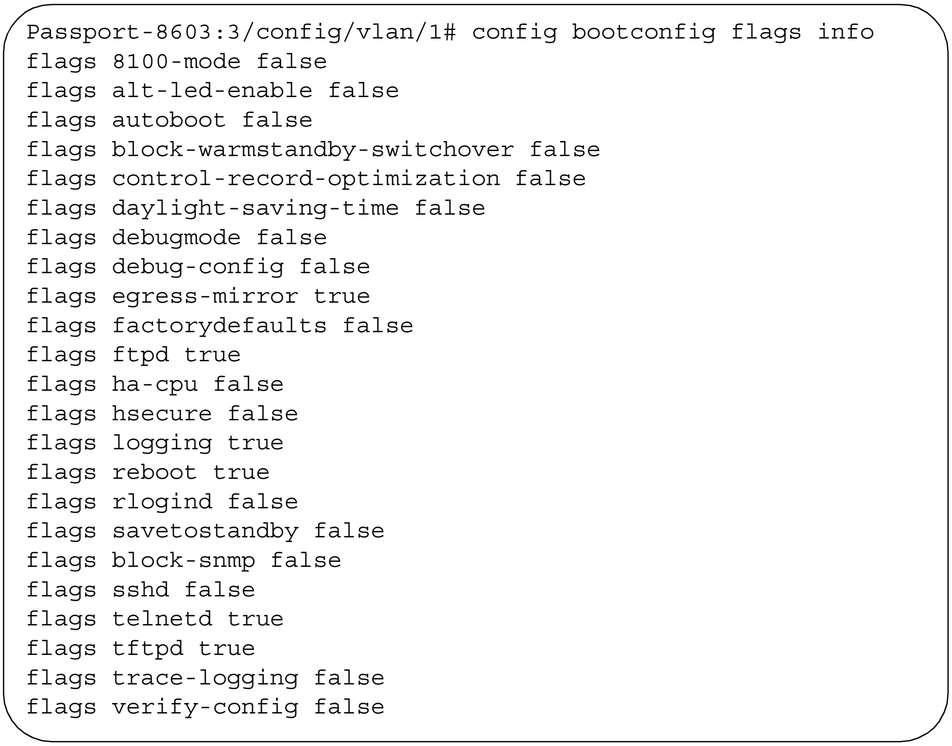
`config bootconfig choice` *`<boot-choice>`* followed by:	
`info`	Displays the current boot choices and associated files (Figure 21).
`config-file <`*`filename`*`>`	Identifies the boot configuration file. • *`filename`* is the device and file name, up to 256 characters including the path.
`image-file <`*`filename`*`>`	Identifies the image file. • *`filename`* is the device and file name, up to 256 characters including the path.

For example, to specify the configuration file in flash memory as the primary boot source, use the following command:

```
config bootconfig choice primary config-file /flash/
config.cfg
```

Figure 21 shows the output from the **`config bootconfig choice primary info`** command.

Figure 21 choice primary info command output



```
Passport-8603:3/config/vlan/1# config bootconfig flags info
flags 8100-mode false
flags alt-led-enable false
flags autoboot false
flags block-warmstandby-switchover false
flags control-record-optimization false
flags daylight-saving-time false
flags debugmode false
flags debug-config false
flags egress-mirror true
flags factorydefaults false
flags ftpd true
flags ha-cpu false
flags hsecure false
flags logging true
flags reboot true
flags rlogind false
flags savetostandby false
flags block-snmp false
flags sshd false
flags telnetd true
flags tftpd true
flags trace-logging false
flags verify-config false
```

In this example, the switch is set to use the onboard flash as the primary source for the configuration file and a TFTP server as the primary source for the image file.

Setting the standby-to-master delay

To set the number of seconds a standby CPU should wait (delay) before trying to become the master CPU (refer to the **`config bootconfig master`** command on page 83), use the following command:

`config bootconfig delay` *`<seconds>`*

This command applies only during a cold start and does not apply to a failover start. The default is 2 seconds delay.

Setting system flags

To enable or disable flags for configuration settings, use the following command:

```
config bootconfig flags
```

Note: When you change the configuration parameters using the **`config bootconfig flags`** command, you must save the changes to the configuration file and reboot the switch before the changes take effect. See “Saving the boot configuration to a file” on page 92 for more information.

This command includes the following options:

`config bootconfig flags` followed by:	
`info`	Displays information about the current flag settings.
`8100-mode <true|false>`	Enables the 8000 Series switch to act as a switch only. In a switch with Passport 8100 modules, this flag defaults to true. For Passport 8600 modules, the default is false.
`autoboot <true|false>`	Controls whether the switch automatically runs the run-time image after being reset or stops at the monitor prompt. Setting autoboot to false is useful for some debugging tasks. The default is true.
`daylight-saving-time <true|false>`	Enables or disables daylight saving time for the switch. The default is false.
`debugmode <true|false>`	Controls whether the switch stops in debug mode following a fatal error. Debug mode provides information equivalent to the **`trace`** commands. • `true` means the switch is not rebooted following a fatal error. • `false` means the switch is automatically rebooted following a fatal error. The default is false.
`debug-config <true|false>`	Enables or disables run-time debugging of the configuration file. The default is false.
`egress-mirror <true|false>`	Enables the ability to mirror egress traffic. The default is true.

config bootconfig flags followed by:	
factorydefaults *<true|false>*	Specifies whether or not the switch boots with the factory defaults. The default is true.
ftpd *<true|false>*	Enables or disables FTP server on the switch. The default is false. To enable FTP, make sure the **config bootconfig flags tftpd** command is set to false.
ha-cpu *<true|false>*	Enables or disables High Availability (HA) mode. HA mode enables switches with two CPUs to recover quickly from a failure of one of the CPUs. See Chapter 8 for more information about HA mode.
hsecure *<true|false>*	Enables or disables hsecure mode in the switch.
logging *<true|false>*	Enables or disables system logging to a PCMCIA file. The default is true.
reboot *<true|false>*	Enables or disables automatic reboot on a fatal error. The default is true. This command is equivalent to the **debugmode** command.
rlogind *<true|false>*	Enables or disables the rlogin/rsh server. The default is false.
savetostandby *<true|false>*	Enables or disables the ability to save the configuration or boot configuration file automatically to the standby CPU. The default is false.
block-snmp *<true|false>*	Enables or disables SNMP access. The default is false.
sshd *<true|false>*	Enables or disables the SSH daemon. The default is false.
telnetd *<true|false>*	Enables or disables the Telnet server. The default is false.
tftpd *<true|false>*	Enables or disables TFTP. The default is false.
trace-logging *<true|false>*	Enables or disables the creation of trace logs. The default is false.
verify-config *<true|false>*	Enables syntax checking of the configuration file and does not execute the file if an error is found. The factory default configuration file is loaded if a syntax error is found. The default is true.
wdt *<true|false>*	Enables or disables the hardware watchdog timer, which monitors a hardware circuit. The watchdog timer reboots the switch based on software errors. The default for this command is true.

Figure 22 shows output from the **config bootconfig flags info** command.

Figure 22 config bootconfig flags info command output

```
8610# config bootconfig flags info
flags 8100-mode false
flags autoboot true
flags daylight-saving-time false
flags debugmode false
flags debug-config false
flags egress-mirror true
flags factorydefaults true
flags ftpd false
flags ha-cpu false
flags logging true
flags reboot true
flags rlogind false
flags savetostandby false
flags block-snmp false
flags sshd false
flags telnetd false
flags tftpd false
flags trace-logging false
flags verify-config true
flags wdt true
```

Troubleshooting switch's failure to read configuration file

The switch may fail to read and load a saved configuration file when it boots. This situation occurs if the `factorydefaults` boot configuration flag is set to true.

To make sure the switch boots using a saved configuration file, set the `factorydefaults` flag to false, using one of the following commands:

- From the Run-Time CLI, the command is:

  config bootconfig flags factorydefaults false

- From the Boot Monitor CLI, the command is:

  flags factorydefaults false

Configuring the remote host login

To define conditions for remote host login, use the following command:

`config bootconfig host`

This command includes the following options:

`config bootconfig host` followed by:	
`info`	Displays the current remote host login settings (Figure 23).
`ftp-debug` *`<true|false>`*	Enables or disables debug mode on FTP. If you enable debug mode, debug messages are displayed on the management console screen. The default is false.
`password` *`<value>`*	Sets the password to enable FTP transfers. • *`value`* is the password, up to 16 characters long. When this password is set, only FTP is used for remote host login. **Note:** This password must match the password set for the FTP server, or the FTP operation fails.
`tftp-debug` *`<true|false>`*	Enables or disables debug mode on TFTP/TFTPD. If you enable debug mode, debug messages are displayed on the management console screen. The default is false.
`tftp-hash` *`<true|false>`*	Enables or disables the TFTP hash bucket display. The default is false.
`tftp-rexmit` ***`<seconds>`***	Sets the TFTP retransmission timeout. The default value is 2 seconds. • *`seconds`* is the number of seconds (1 to 2147483647).
`tftp-timeout` *`<seconds>`*	Sets the TFTP timeout. The default value is 10 seconds. • *`seconds`* is the number of seconds (1 to 120).
`user` *`<value>`*	Sets the remote user login. • *`value`* is the user login name, up to 16 characters long.

Figure 23 shows output for the **`host info`** command.

Figure 23 host info command output

```
monitor# host info
host password ""
host tftp-hash false
host tftp-rexmit 2
host tftp-timeout 6
host user "target"
host ftp-debug false
host tftp-debug false
```

Specifying the master CPU

The master CPU performs a loopback test to test the switch fabric. To indicate which CPU should become master when the switch is turned on, use the following command:

`config bootconfig master` *`<cpu-slot>`*

where *`cpu-slot`* can be 5 or 6. The default master is set for slot 5.

To display the current setting for the master CPU, use the following command:

`show bootconfig master`

Configuring CPU network port devices

The three network ports are the management port (mgmt), the CPU port (cpu2cpu), and the PCMCIA card (pccard), if it is acting as a network port. To configure the CPU network port devices, use the following command:

`config bootconfig net` *`<cpu-net-port>`*

where:
`cpu-net-port` is `mgmt`, `cpu2cpu`, or `pccard`.

Note: Use the **`net mgmt ip <`*`addr/mask`*`>`** command to assign an IP address to the switch.

This command includes the following options:

config bootconfig net *<cpu-net-port>* followed by:	
info	Displays information about the current configuration of the specified port (Figure 24).
autonegotiate *<true|false>*	Enables or disables autonegotiation for the port. The default is false.
bootp *<true|false>*	Enables or disables the Bootstrap Protocol (BootP) for the port. The default is true.
enable *<true|false>*	Enables or disables the specified port. The default is true.
fullduplex *<true|false>*	Enables or disables full-duplex mode on the specified port. The default is true.
ip *<addr/mask>* [cpu-slot *<value>*]	Assigns an IP address/mask for the management port, CPU, or PCMCIA card. **Optional parameter**: • cpu-slot *value* allows you to specify the slot number to which the IP address applies. The valid options are 3 to 6. If you do not specify a slot, the IP address is assigned to the port in the currently active CPU. **Note:** In an 8003 chassis, the only available CPU slot is 3.
restart	Restarts the port.
route <net|add|del> *<netaddr> <gateway>*	Sets a route for the port. • net|add|del adds a route (add or net) or deletes a route (del). • *netaddr* is the IP address of the network to be reached. • *gateway* is the gateway IP address.
speed *<10|100>*	Sets the connection speed for ports to 10 Mb/s or 100 Mb/s. The default is 10.
tftp *<ipaddr>*	Specifies a TFTP server for the port. • *ipaddr* is the IP address of the TFTP server.

Figure 24 shows output for the **net mgmt info** command, that is, the settings for the management port.

Figure 24 net mgmt info command output

```
8610:5/config/bootconfig/net/mgmt# info
net mgmt autonegotiate false
net mgmt bootp true
net mgmt enable true
net mgmt fullduplex false
net mgmt speed 10
net mgmt tftp 198.202.188.174
net mgmt ip 192.168.150.212/255.255.255.0 cpu-slot 3
net mgmt route add 198.202.168.174 192.168.150.1
net mgmt route add 198.202.189.0 192.168.150.1
net mgmt route add 198.202.188.174 192.168.150.1
net mgmt route add 206.236.134.0 192.168.150.1
current status: link: true speed: 10 duplex: half
8610:5/config/bootconfig/net/mgmt#
```

Displaying the Boot Monitor configuration

To display the current Boot Monitor configuration, using the following command:

`show bootconfig`

This command includes the following options:

`show bootconfig` followed by:	
`info`	Displays the current settings for the boot monitor.
`choice`	Displays the current boot configuration choices.
`cli`	Displays the current cli configuration.
`config [verbose]`	Displays the current boot configuration. • `verbose` includes all possible information. If you omit `verbose`, only the values that have been changed from their default settings are displayed.
`flags`	Displays the current flag settings.
`host`	Displays the current host configuration.
`master`	Displays the current CPU slot set as master and the settings for the **`delay`** and **`multicast`** commands.
`net`	Displays the current configuration of the CPU network ports.

`show bootconfig` followed by:	
`show-all [file <value>]`	Displays all relevant information about boot configuration on the switch. • *`value`* is the filename to which the output will be redirected.
`sio`	Displays the current configuration of the CPU serial ports.
`tz`	Displays the current configuration of the switch time zone.
`wlan`	Displays wireless LAN information.

Figure 25 shows output from the **`show bootconfig choice`** command.

Figure 25 show bootconfig choice command output

```
8610:5# show bootconfig choice
choice primary backup-config-file ""
choice primary config-file "/flash/config.cfg"
choice primary image-file "/pcmcia/p80a3500b032.img"
choice secondary backup-config-file ""
choice secondary config-file "/flash/config.cfg"
choice secondary image-file "/flash/p80a3000.img"
choice tertiary backup-config-file ""
choice tertiary config-file "/flash/config.cfg"
choice tertiary image-file "0.0.0.0:"
```

Warning: Do not edit the boot.cfg file manually, because the switch reads this file during the boot process. Errors generated while editing the file could render the switch inoperable.

Figure 26 shows output from the **`show bootconfig info`** command.

Figure 26 show bootconfig info command

```
8610:5# show bootconfig info
CPU Slot 3:     PPC 740 Map B
Version:        3.7.0.0/065
Memory Size:    0x04000000
```

Configuring the CPU serial port devices

To configure the CPU serial port devices, use the following command:

config bootconfig sio *<cpu-sio-port>*

where *cpu-sio-port* can be console, modem, or pccard.

This command includes the following options:

config bootconfig sio *<cpu-sio-port>* followed by:	
info	Displays information about the specified port (Figure 27).
baud *<rate>*	Sets the baud rate for the port. The default is 9600.
8databits *<true|false>*	Specifies either 8 (true) or 7 (false) data bits per byte for software to interpret. The default is false.
enable *<true|false>*	Enables or disables the port. The default is true.
mode *<ascii|slip|ppp>*	Sets the communication mode for the serial port. The default is ascii. If you are configuring the Modem port, you can set the port to use the same SLIP or PPP communication mode as the modem. For instructions to connect a modem to the Modem port, refer to *Getting Started*.
mtu *<bytes>*	Sets the size of the maximum transmission unit for a point-to-point link (0 to 2048). The default is 0.
my-ip *<ipaddr>*	Sets the near-end IP address on the point-to-point link. The default is 0.0.0.0.
peer-ip *<ipaddr>*	Sets the peer IP address on the point-to-point link. The default is 0.0.0.0.
pppfile *<file>*	Identifies which file to use for PPP initialization parameters.
restart	Shuts down and reinitializes the port.
slip-compression *<true|false>*	Enables or disables TCP/IP header compression. The default is false.
slip-rx-compression *<true|false>*	Enables or disables TCP/IP header compression on the receive packet. The default is false.

In PPP mode, you can configure additional parameters. Those configuration options are listed in *Configuring PPP and SLIP for Remote Access*.

Warning: Nortel Networks does not recommend setting the Console port mode to SLIP or PPP, because the log, trace, and error messages may be displayed on this port and will interfere with the SLIP or PPP operation.

Figure 27 shows output from the **`sio console info`** command.

Figure 27 sio console info command output

```
monitor# sio console info
sio console baud 9600
sio console 8databits false
sio console enable true
sio console mode ascii
sio console mtu 0
sio console my-ip 0.0.0.0
sio console peer-ip 0.0.0.0
sio console pppfile ""
sio console slip-compression false
sio console slip-rx-compression false
current status: active: true mode: ascii baud: 9600 options: 7
bit data 1 stop no parity cts dsr ri
```

Setting the time zone

To set the switch’s relation to time zones, use the following command:

```
config bootconfig tz
```

This command includes the following options:

config bootconfig tz followed by:	
info	Displays time zone information (Figure 28).
dst-end *<Mm.n.d/hhmm| MMddhhmm>*	Sets the ending date of daylight saving time. You can specify the time in one of the two ways: • Specify an hour on the nth occurrence of a weekday in a month. For example, M10.5.0/0200 means the 5th occurrence of Sunday in the 10th month (October) at 2:00 a.m. • Specify a month, day, hour, and minute. For example, 10310200 means October 31 at 2:00 a.m.
dst-name *<dstname>*	Sets an abbreviated name for the local daylight saving time zone. • *dstname* is the name (for example, “pdt” is Pacific Daylight Time).
dst-offset *<minutes>*	Sets the daylight saving adjustment in minutes. The default is 60.
dst-start *<Mm.n.d/hhmm| MMddhhmm>*	Sets the starting date of daylight saving time. The format is the same as for setting the ending date.
offset-from-utc *<minutes>*	Sets the time zone offset, in minutes to subtract from Universal Coordinated Time (UTC), where positive numbers mean west of Greenwich and negative numbers mean east of Greenwich.
name *<tz>*	Sets an abbreviated name for the local time zone name. • *tz* is the name (for example “pst” is Pacific Standard Time).

Figure 28 shows output from the **tz info** command.

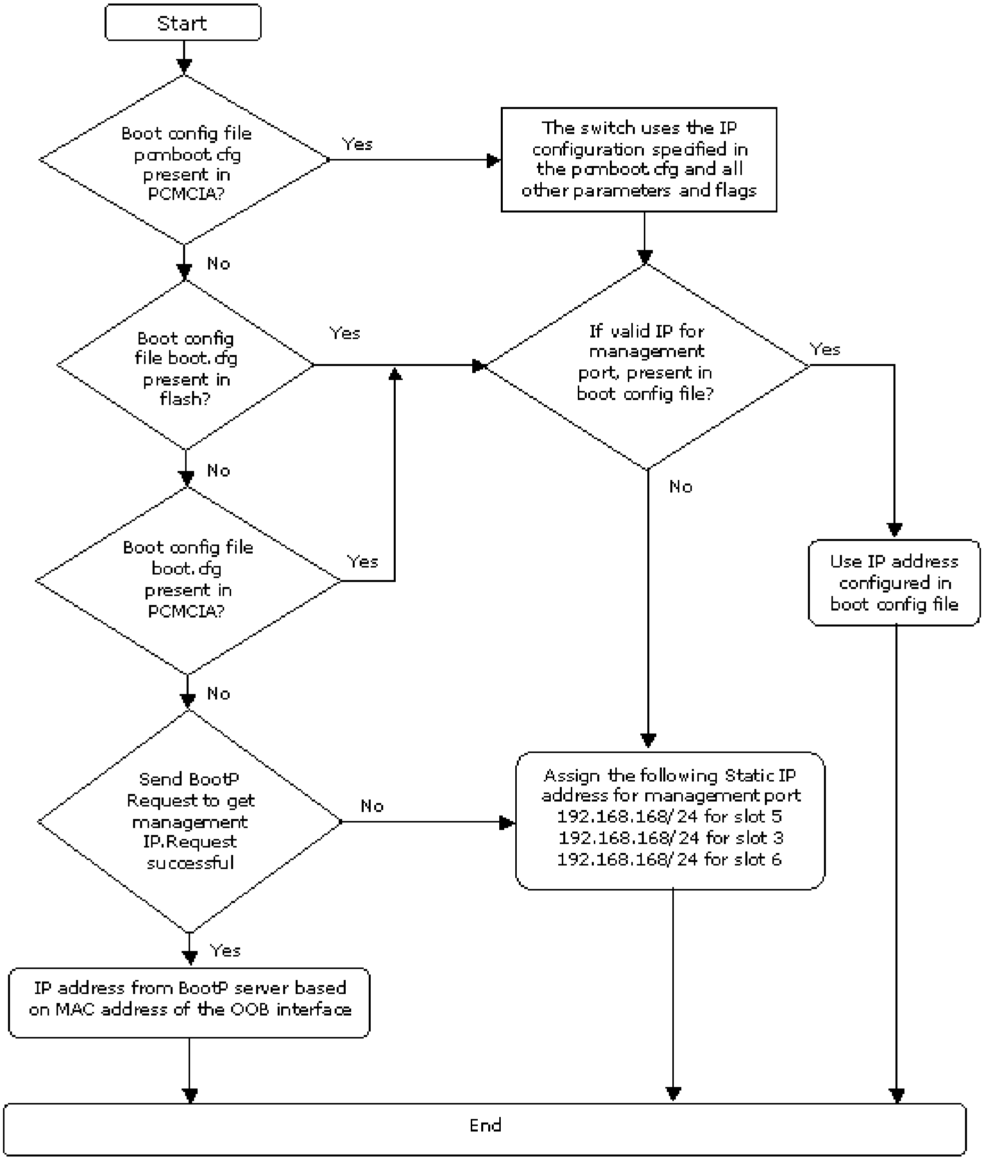
Figure 28 tz info command output

```
8610# tz info
tz dst-end M10.5.0/0200
tz dst-name "UTC"
tz dst-offset 60
tz dst-start M4.1.0/0200
tz offset-from-utc 0
tz name "UTC"
TIMEZONE=UTC:UTC:0:::0
Passport-8603:3/config/bootconfig/tz#
```

Static IP entry for the OOB network management interface

The default IP for the Out of Band (OOB) network management port is assigned as shown in Figure 29:

Figure 29 Flowchart for the default IP for the OOB network management port


Start
Boot config file pcmboot.cfg present in PCMCIA?
Yes
The switch uses the IP configuration specified in the pcmboot.cfg and all other parameters and flags
No
Boot config file boot.cfg present in flash?
Yes
If valid IP for management port, present in boot config file?
Yes
No
No
Boot config file boot.cfg present in PCMCIA?
Yes
Use IP address configured in boot config file
No
Send BootP Request to get management IP.Request successful
No
Assign the following Static IP address for management port 192.168.168/24 for slot 5 192.168.168/24 for slot 3 192.168.168/24 for slot 6
Yes
IP address from BootP server based on MAC address of the OOB interface
End

The switch first checks for the file pcmboot.cfg, in PCMCIA. If not found, it checks for file boot.cfg in flash.

➡ **Note:** Users using boot.cfg file from PCMCIA must rename the file to pcmboot.cfg (As boot.cfg file is no more checked in PCMCIA. It is checked ONLY in flash)

Displaying the Boot Monitor configuration

To display the current configuration of the Boot Monitor and the Boot Monitor CLI, use the following command:

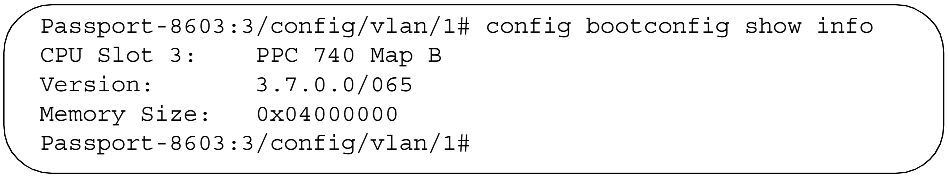
```
config bootconfig show
```

This command includes the following options:

config bootconfig show followed by:	
`info`	Displays the current boot monitor settings (Figure 30).
`choice`	Displays the boot configuration choices.
`cli`	Displays the CLI configuration.
`config [verbose]`	Displays the current boot configuration. `verbose` displays all possible information.
`flags`	Displays the flags settings.
`host`	Displays the host configuration.
`master`	Displays the current CPU slot set as master.
`net`	Displays the current configuration of the CPU network ports.
`show-all [file <value>]`	Displays all relevant information about boot configuration on the switch. *`value`* is the filename to which the output will be redirected.
`sio`	Displays the current configuration of CPU serial ports.
`tz`	Displays the switch's time zone setting.
wlan	Displays wireless LAN information.

Figure 30 shows output for the **`config bootconfig show info`** command:

Figure 30 config bootconfig show info command output



```
Passport-8603:3/config/vlan/1# config bootconfig show info
CPU Slot 3:    PPC 740 Map B
Version:       3.7.0.0/065
Memory Size:   0x04000000
Passport-8603:3/config/vlan/1#
```

Saving the boot configuration to a file

To save the boot configuration to a file, or to save a log or trace file, enter the following command:

```
save <savetype> [file <value>] [verbose] [standby <value>]
[backup <value>]
```

where:

- `savetype` specifies what to save. Possible values for this parameter are `config`, `bootconfig`, `log`, and `trace`.
- `file <value>` is a file name in one of the following formats:
  - `[a.b.c.d]:<file>`
  - `/pcmcia/<file>`
  - `/flash/<file>`
- `verbose` saves default and current configuration. If you omit this parameter, only parameters you have changed are saved.
- `standby <value>` saves the specified file name to the standby CPU.
- `backup <value>` saves the specified file name and identifies the file as a backup file.

➡ **Note:** If a PCMCIA card is removed before a write operation (e.g., upload), is complete, the file that is being written to, may have a corrupted EOF marker. Before removing the PCMCIA card, execute the CLI command **`stop-pcmcia`**.

Also, some PCMCIA cards do not contain a file attribute table (FAT). Therefore, you may need to use the **`dos-chkdsk /pcmcia`** CLI command to check the card. If you receive error messages, use the **`dos-chkdsk /pcmcia/ repair`** command or the **`dos-format`** command.

For example, to save a boot configuration file as a backup file, you might use the following command:

```
save bootconfig file boot.cfg backup2
```

➡ **Note:** The boot configuration file must be named boot.cfg for the system to boot using it.

➡ **Note:** To save a file to the standby CPU, you must enable TFTP on the standby CPU. To enable TFTP, enter **`flags tftpd true`** in the Boot Monitor CLI or **`config bootconfig flags tftpd true`** in the Run-Time CLI.

Chapter 4
Managing the Run-Time process

This chapter describes how to configure and manage the runtime process using the Run-Time CLI. To access the Run-Time CLI, wait until the boot process is complete. At the login prompt, enter your user name and password.

This section includes the following topics:

Roadmap of Run-Time CLI commands

The following roadmap lists some of the commands and their parameters that you use to configure and manage the Run-Time CLI. Use this list as a quick reference or click on any entry for more information:

Command	Parameter
`config cli`	`info`
	`banner add <string>`
	`banner defaultbanner <true|false>`
	`banner delete`
	`banner info`
	`defaultlogin <true|false>`
	`defaultpassword <true|false>`
	`loginprompt <string>`
	`monitor duration <integer>`
	`monitor info`
	`monitor interval <integer>`
	`more <true|false>`
	`motd add <string>`
	`motd displaymotd <true|false>`
	`motd delete`
	`motd info`
	`passwordprompt <string>`
	`prompt <prompt>`
	`rlogin-sessions <nsessions>`
	`screenlines <nlines>`
	`telnet-sessions <nsessions>`
	`timeout <seconds>`
`show cli info`	

Command	Parameter
show cli who	
show cli password	
show cli show-all [file <value>]	
show config [verbose] [module <value>]	
show tech	
show sys info [card] [asic] [mda]	
config sys set action	info
	cpuswitchover
	resetconsole
	resetcounters
	resetmodem
config sys set snmp	force-iphdr-sender <true|false>
	force-trap-sender <true|false>
	info
	sender-ip <target_address> <source_address>
config sys set clock-sync-time <minutes>	
config sys set mgmt-virtual-ip <ipaddr/mask>	
config sys set	info
	clock-sync-time <minutes>
	contact <contact>
	ecn-compatibility <enable|disable>
	global-filter <enable|disable>
	location <location>
	mroute-stream-limit <enable|disable>

Command	Parameter
	mgmt-virtual-ip <ipaddr/mask>
	msg-control <enable|disable>
	mtu <bytes>
	name <prompt>
	portlock <on|off>
	sendAuthenticationTrap <true|false>
	smlt-on-single-cp <enable|disable> [timer <value>]
	topology <on|off>
	udpsrc-by-vip <enable|disable>
	vlan-bysrcmac <enable|disable>
show sys	dns
	eapol
	info [card] [asic] [mda]
	mcast-mlt-distribution
	mcast-software-forwarding
	msg-control
	perf
	record-reservation
	sw
	topology
config sys link-flap-detect	info
	auto-port-down <enable|disable>
	frequency <frequency>
	interval <interval>
	send-trap <enable|disable>
config slot <slots> state <enable|disable>	
config slot <slots> info	

Configuring the Run-Time CLI

You can configure and manage the Run-Time CLI using the following command:

```
config cli
```

This command includes the following options:

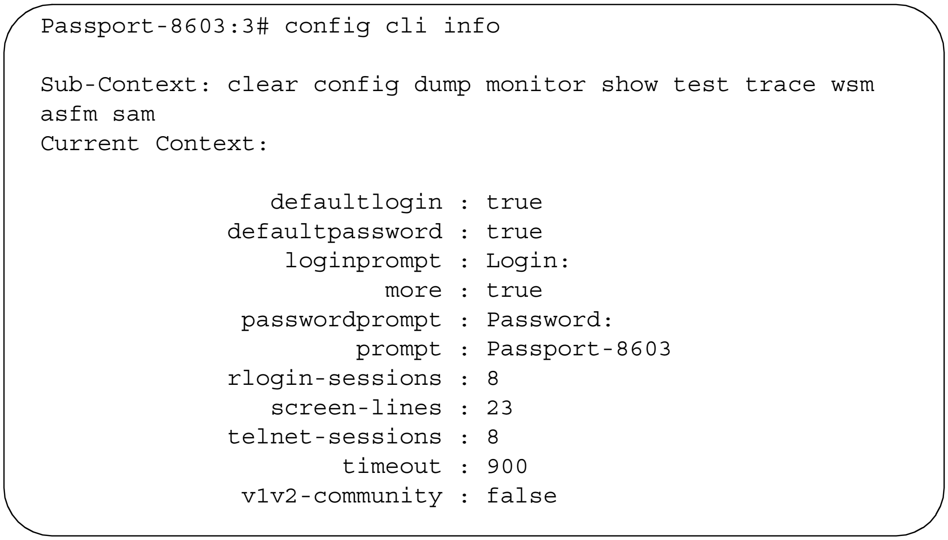
config cli followed by:	
`info`	Displays the current CLI parameter settings (Figure 31).
`banner add <string>`	Adds lines of text to the CLI login banner. • *string* is an ASCII string from 1 to 1024 characters.
`banner defaultbanner <true|false>`	Enables or disables using the default CLI login banner.
`banner delete`	Deletes an existing customized login banner.
`banner info`	Displays the text that was added to the login banner using the **banner add** command.
`defaultlogin <true|false>`	Enables or disables using the default login string. • `false` disables the default login banner and displays the new banner.
`defaultpassword <true|false>`	Enables or disables using the default password string.
`loginprompt <string>`	Changes the CLI login prompt. • *string* is an ASCII string from 1 to 1024 characters.
`monitor duration <integer>`	Changes the monitoring time duration (refresh rate) for the **monitor** commands. • *integer* is the time duration in seconds (1 to 1800). The default is 300.
`monitor info`	Displays the current setting for the monitor duration and interval used by the **monitor** commands.

config cli followed by:	
monitor interval <*integer*>	Changes the monitoring time interval between screen updates set by the **monitor** commands. *integer* is the time duration in seconds (1 to 600). The default is 5.
more <*true*|*false*>	Sets scrolling for the output display. The default is true. • true sets output display scrolling to one page at a time. • false sets the output display to continuous scrolling.
motd add <*string*>	Creates a “message of the day” that can be displayed with the login banner. • *string* is an ASCII string from 1 to 1024 characters.
motd displaymotd <*true*|*false*>	Displays (true) or does not display (false) the message of the day.
motd delete	Deletes the message of the day.
motd info	Displays information about the message of the day.
passwordprompt <*string*>	Changes the CLI password prompt. • *string* is an ASCII string from 1 to 1024 characters.
prompt <*prompt*>	Sets the root level prompt and sysName to a defined string. • *prompt* is a string from 1 to 32 characters.
rlogin-sessions <*nsessions*>	Sets the allowable number of inbound remote CLI login sessions; the default is 8. • *nsessions* is the number of sessions (0 to 8).
screenlines <*nlines*>	Sets the number of lines in the output display; the default is 23. • *nlines* is the number of lines (8 to 64).

config cli followed by:	
telnet-sessions <*nsessions*>	Sets the allowable number of inbound Telnet sessions; the default is 8. • *nsessions* is the number of sessions (0 to 8).
timeout <*seconds*>	Sets the idle timeout period before automatic logout for CLI sessions; the default is 0. • *seconds* is the timeout period in seconds (0 to 65536).

Figure 31 shows output from the **config cli info** command.

Figure 31 config cli info command output



```
Passport-8603:3# config cli info

Sub-Context: clear config dump monitor show test trace wsm
asfm sam
Current Context:

               defaultlogin : true
            defaultpassword : true
                loginprompt : Login:
                       more : true
             passwordprompt : Password:
                     prompt : Passport-8603
            rlogin-sessions : 8
               screen-lines : 23
            telnet-sessions : 8
                    timeout : 900
             v1v2-community : false
```

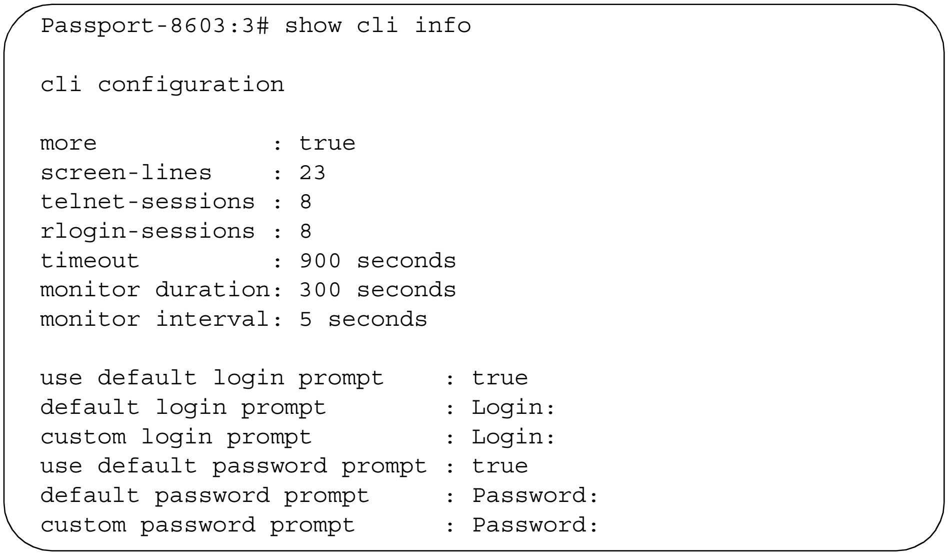
Displaying CLI configuration information

To display information about the CLI configuration, use the following command:

show cli info

Figure 32 shows sample output from the **show cli info** command.

Figure 32 show cli info command output



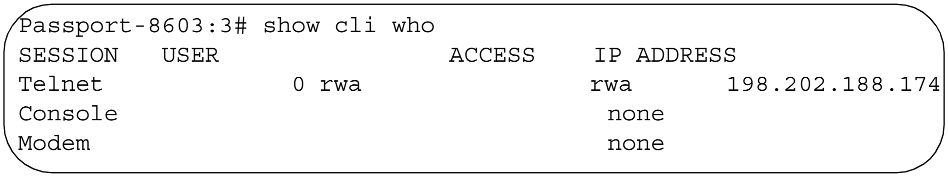
```
Passport-8603:3# show cli info

cli configuration

more             : true
screen-lines     : 23
telnet-sessions : 8
rlogin-sessions : 8
timeout          : 900 seconds
monitor duration: 300 seconds
monitor interval: 5 seconds

use default login prompt    : true
default login prompt        : Login:
custom login prompt         : Login:
use default password prompt : true
default password prompt     : Password:
custom password prompt      : Password:
```

To displays a list of users who are logged in to the switch, use the following command:

show cli who

Figure 33 shows output from the **show cli who** command.

Figure 33 show cli who command output



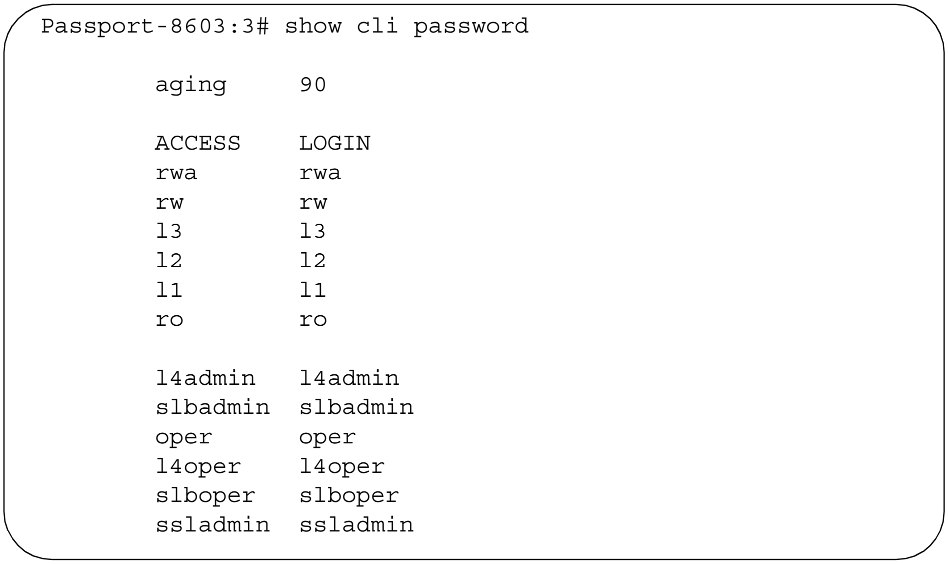
```
Passport-8603:3# show cli who
SESSION   USER                ACCESS    IP ADDRESS
Telnet            0 rwa                rwa       198.202.188.174
Console                                 none
Modem                                   none
```

To display the CLI access, login, and password combinations, use the following command:

show cli password

Figure 34 shows output from the **show cli password** command.

Figure 34 show cli password command output



```
Passport-8603:3# show cli password

        aging     90

        ACCESS    LOGIN
        rwa       rwa
        rw        rw
        l3        l3
        l2        l2
        l1        l1
        ro        ro

        l4admin   l4admin
        slbadmin  slbadmin
        oper      oper
        l4oper    l4oper
        slboper   slboper
        ssladmin  ssladmin
```

For definitions of the different access levels of the switch and instructions on changing the login or password for these levels, see *Configuring and Managing Security*.

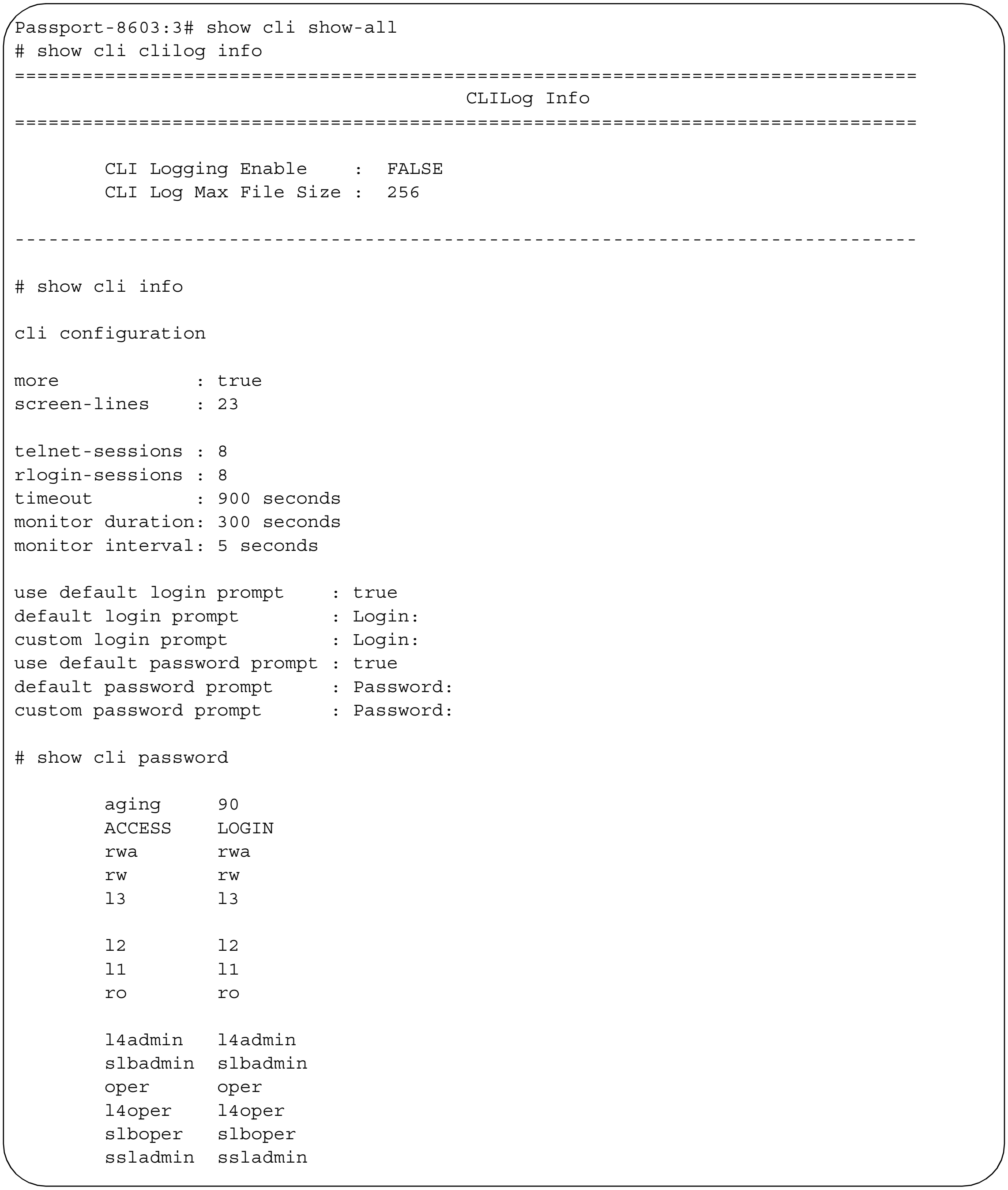
To display all relevant CLI information, use the following command:

`show cli show-all` `[file <value>]`

where *`<value>`* is the filename to which the output will be redirected.

See Figure 35 on page 104 for sample output.

Figure 35 show cli show-all command output



```
Passport-8603:3# show cli show-all
# show cli clilog info
================================================================================
                                        CLILog Info
================================================================================

        CLI Logging Enable    :  FALSE
        CLI Log Max File Size :  256

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

# show cli info

cli configuration

more            : true
screen-lines    : 23

telnet-sessions : 8
rlogin-sessions : 8
timeout         : 900 seconds
monitor duration: 300 seconds
monitor interval: 5 seconds

use default login prompt    : true
default login prompt        : Login:
custom login prompt         : Login:
use default password prompt : true
default password prompt     : Password:
custom password prompt      : Password:

# show cli password

        aging     90
        ACCESS    LOGIN
        rwa       rwa
        rw        rw
        l3        l3

        l2        l2
        l1        l1
        ro        ro

        l4admin   l4admin
        slbadmin  slbadmin
        oper      oper
        l4oper    l4oper
        slboper   slboper
        ssladmin  ssladmin
```

Displaying the current switch configuration

To display the current switch configuration, use the following command:

```
show config [verbose] [module <value>]
```

where:

- `verbose` specifies a complete list of all configuration information about the switch.
- `module <value>` specifies the command group for which you are requesting configuration settings. The *value* option can be `cli`, `sys`, `web`, `rmon`, `vlan`, `port`, `qos`, `traffic-filter`, `mlt`, `stg`, `ip`, `ipx`, `diag`, `dvmrp`, `radius`, `atm`, `ntp`, `or svlan`.

If you make a change to the switch, it is displayed under that configuration heading. A complete display is too long to include here; Figure 36 shows representative information.

Figure 36 show config command (partial output)

```
Passport-8603:3# show config
Preparing to Display Configuration...
#
# TUE JAN 27 15:13:41 2004 UTC
# box type             : Passport-8003
# software version     : REL3.7.0.0_B065
# monitor version      : 3.7.0.0/065
#
# Asic Info :
# SlotNum|Name   |CardType   |MdaType |Parts Description
#
# Slot  1 8648TXE  0x20210130 0x00000000   IOM: PLRO=3  BFM:
OP=3 TMUX=2 RARU=4 CPLD=4
# Slot  2 ALTEON WSM 0x71320104 0x00000000  BFM: OP=3 TMUX=2
RARU=4 CPLD=5
# Slot  3 8690SF   0x200e0100 0x00000000  CPU: CPLD=14 SFM:
OP=2 TMUX=2 SWIP=2 FAD=1 CF=11
#
#!flags m-mode false
#!flags enhanced-operational-mode false
#!flags vlan-optimization-mode false
#!flags global-filter-ordering false
#!record-reservation filter 4096
#!record-reservation ipmc 500
#!record-reservation local 2000
#!record-reservation mac 2000
#!record-reservation static-route 200
#!record-reservation vrrp 500
#!end
config

# LICENSE CONFIGURATION
mac-flap-time-limit 500
#
# CLI CONFIGURATION
# SYSTEM CONFIGURATION
```

When you add `verbose` to the **`show config`** command, the output contains current switch configuration including software (versions), performance, VLANs (such as numbers, port members), ports (such as type, status), routes, OSPF (such as area, interface, neighbors), memory, interface, and log and trace files. With this command (Figure 37), you can see current configuration and default values. Without `verbose`, not all of the default values are displayed.

Figure 37 show config verbose command (partial output)

```
Passport-8603:3# show config verbose
Preparing to Display Configuration...
#
# TUE JAN 27 15:18:57 2004 UTC
# box type             : Passport-8003
# software version     : REL3.7.0.0_B062
# monitor version      : 3.7.0.0/062
#
# Asic Info :
# SlotNum|Name  |CardType   |MdaType |Parts Description
#
# Slot  1 8648TXE  0x20210130 0x00000000   IOM: PLRO=3  BFM: OP=3 TMUX=2
RARU=4 CPLD=4
# Slot  2 ALTEON WSM 0x71320104 0x00000000  BFM: OP=3 TMUX=2 RARU=4
CPLD=5
# Slot  3 8690SF   0x200e0100 0x00000000  CPU: CPLD=14 SFM: OP=2 TMUX=2
SWIP=2 FAD=1 CF=11
#
#!flags m-mode false
#!flags enhanced-operational-mode false
#!flags vlan-optimization-mode false
#!flags global-filter-ordering false
#!record-reservation filter 4096
config

# LICENSE CONFIGURATION
mac-flap-time-limit 500
#
# CLI CONFIGURATION

cli monitor duration 300
cli monitor interval 5
cli more true
cli prompt "Passport-8603"
cli rlogin-sessions 8
cli screenlines 23
cli telnet-sessions 8
cli timeout 900
cli defaultlogin true
cli v1v2-community false
cli defaultpassword true
cli banner defaultbanner true
cli motd displaymotd false
#!record-reservation ipmc 500
#!record-reservation local 2000
#!record-reservation mac 2000
#!record-reservation static-route 200
#!record-reservation vrrp 500
#!end
```

Displaying system status

To display technical information about system status and information about the hardware, software, and operation of the switch, use the following command:

```
show tech
```

The information available from the **`show tech`** command includes general information about the system (such as location), hardware (chassis, power supplies, fans, and modules), system errors, boot configuration, software versions, memory, port information (locking status, configurations, names, interface status), VLANs and STGs (numbers, port members), OSPF (area, interface, neighbors), and log and trace files. This command displays more information than the similar **`show sys info`** command, which is described in the following section.

Figure 38 shows representative output from the **`show tech`** command.

Figure 38 show tech command (partial output)

```
Passport-8603:3/config/vlan/1# show tech

Sys Info:
---------------

General Info :
        SysDescr     : Passport-8603 (3.7.0.0)
        SysName      : Passport-8603
        SysUpTime    : 0 day(s), 00:20:12
        SysContact   : support@nortelnetworks.com
       SysLocation  : 4401 Great America Parkway, Santa Clara,
CA 95054

Chassis Info :
        Chassis     : 8003
        Serial#     : SSNMTO29WG
        HwRev       : 01
        NumSlots    : 3
        NumPorts    : 52
        GlobalFilter: enable
        VlanBySrcMac: disable
        Ecn-Compatib: enable
        BaseMacAddr : 00:04:38:7e:84:00

        MacAddrCapacity : 1024
        Temperature : 36 C
        MgmtMacAddr : 00:04:38:7e:87:f4
        System MTU  : 1950
        clock_sync_time : 60

Power Supply Info :
        Ps#1 Status       : empty
        Ps#2 Status       : up
        Ps#2 Type         : ac
        Ps#2 Description  : 8003 500W 110/220V AC Power Supply
        Ps#2 Serial Number: ARTSAT001440
        Ps#2 Version      : A
        Ps#2 Part Number  : 211036-A

Fan Info :
        Fan#1: up, air temp: 32 C
```

Displaying hardware information

To display system status and technical information about the switch hardware components. (Compare this command with the **`show tech`** command on page 108.) The command displays several pages of information, including general information about the system (such as location), chassis (type, serial number, and base MAC address), temperature, power supplies, fans, cards, system errors, port locks, topology status, and message control information.

The command syntax is:

```
show sys info [card] [asic] [mda]
```

where:

`card` displays information about all the installed modules.

`asic` displays information about the ASIC installed on each module.

`mda` displays information about installed MDAs.

Figure 39 shows partial output from the **`show sys info`** command.

Figure 39 show sys info command (partial output)

```
Passport-8603:3/config/vlan/1# show sys info

General Info :
        SysDescr     : Passport-8603 (3.7.0.0)
        SysName      : Passport-8603
        SysUpTime    : 0 day(s), 00:23:06
        SysContact   : support@nortelnetworks.com
        SysLocation  : 4401 Great America Parkway, Santa Clara, CA 95054

Chassis Info :
        Chassis     : 8003
        Serial#     : SSNMTO29WG
        HwRev       : 01
        NumSlots    : 3
        NumPorts    : 52
        GlobalFilter: enable
        VlanBySrcMac: disable
        Ecn-Compatib: enable
        BaseMacAddr : 00:04:38:7e:84:00
        MacAddrCapacity : 1024
        Temperature : 36 C
        MgmtMacAddr : 00:04:38:7e:87:f4

Power Supply Info :
        Ps#1 Status       : empty
        Ps#2 Status       : up
        Ps#2 Type         : ac
        Ps#2 Description  : 8003 500W 110/220V AC Power Supply
        Ps#2 Serial Number: ARTSAT001440
        Ps#2 Version      : A
        Ps#2 Part Number  : 211036-A

Fan Info :
        Fan#1: up, air temp: 31 C

Card Info :
        Slot#        FrontType  FrontHw    Oper   Admin  BackType   BackHw
                                Version  Status  Status             Version
            1    48x100BaseTX-E        A      up      up      BFM6

Card Info :
        Slot#        FrontType  FrontHw    Oper   Admin  BackType   BackHw
                                Version  Status  Status             Version
            1    48x100BaseTX-E        A      up      up      BFM6
            2        ALTEON_WSM        3      up      up      BFM4        2
            3               CPU        A      up      up       SFM        A

System Error Info :
        Send Authentication Trap  : false
        Error Code                : 0
        Error Severity            : 0

Port Lock Info :
        Status       : off
        LockedPorts  :

Topology Status Info :
        Status       : on

Message Control Info :
        Status       : disable
```

Resetting system functions

The Run-Time CLI allows you to reset all statistics counters, the modem port, the console port, and the operation of the switchover function.

To reset these system functions, use the following command:

config sys set action

This command includes the following options:

config sys set action followed by:	
info	Displays the current settings for system actions.
cpuswitchover	Resets the switch to change over to the backup CPU**.**
resetconsole	Reinitializes the hardware UART drivers. Use this command only if the console or modem connection is hung.
resetcounters	Resets all the statistics counters in the switch to zero.
resetmodem	Resets the modem port.

Configuration example

This configuration example uses the above commands to reset the switch to change over to the backup CPU and to reset the statistics counters to zero. The example also uses the **`config sys set action info`** command to display information about the system functions.

```
Passport-8610:5# config sys set action cpuswitchover
Passport-8610:5# config sys set action resetcounters
Are you sure you want to reset system counters (y/n)? y
Passport-8610:5# config sys set action info

Sub-Context: clear config dump monitor show test trace wsm
Current Context:

rcCliSettingSysSetAction: before set
               cpuswitchover : (N/A)
                resetconsole : (N/A)
               resetcounters : (N/A)
                  resetmodem : (N/A)

rcCliSettingSysSetAction: after set
Passport-8610:5#
```

Note: N/A displayed in a command output indicates that the information is Not Available or Not Applicable.

Configuring SNMP setting

To configure SNMP settings, use the following command:

`config sys set snmp`

This command includes the following options:

`config sys set snmp` followed by:	
`force-iphdr-sender` *`<true|false>`*	If set to true, the configured source address is sent in the IP header of the notification message as the source address.
`force-trap-sender` *`<true|false>`*	If set to true, the configured source address is sent in the notification message as the sender network.
`info`	Displays the current SNMP settings.

`sender-ip` *`<target_address>`*
`<source_address>`
	Configures a source IP address which is set in the notification sent to the target. The source IP address should be a circuitless IP address.

Configuration example

This configuration example uses the above commands to set the SNMP community and set an SNMP trap receiver. The example also uses the **`config sys set snmp info`** command to display information about the SNMP setup.

```
Passport-8603:3# config sys set snmp info
Sub-Context: clear config dump monitor show test trace wsm asfm sam
Current Context:

                 trap-sender :

           force-trap-sender : FALSE
          force-iphdr-sender : FALSE
```

Synchronizing clocks

The 8000 Series switch automatically synchronizes the real-time clocks (hardware) on the master and standby CPUs, and synchronizes the real-time and system (software) clocks.

Synchronizing the real-time clocks

When you configure the real-time clock on the master CPU, the standby CPU real-time clock is immediately updated, and both clocks are set to the same time. A log message is then added in the log file stating that clock synchronization is complete. Note the following conditions regarding CPU clock synchronization:

- When the switch is operating normally with a redundant CPU, clock synchronization is done at 24 hour intervals. When the switch is operating normally with no redundant CPU, if a standby CPU card is inserted, the real-time clocks on the master CPU and the standby CPU are immediately synchronized. A log message is added in the log file, stating that clock synchronization is complete. If the synchronization process continues successfully, no more log messages are generated and clock synchronization continues at 24 hour intervals.

  At boot time, after the switch is initialized, the clocks on the master CPU and the standby CPU are immediately synchronized and clock synchronization continues at 24 hour intervals. In the event the standby CPU is removed, the CPU clock synchronization process is stopped. Also, if the clock synchronization process fails, a log message is generated in the log file. Once the real-time clock synchronization begins to fail, a log message is generated for each failed attempt.
- If the Inter CPU Communication (ICC) channel is in use by another process at the time of clock synchronization, the synchronization process is not performed, but attempted again after the scheduled 24 hour interval. A log message is added in the log file stating that synchronization was not successful.

Synchronizing the real-time and system clocks

Synchronizing the real-time and system clocks occurs at regular intervals that you define. To configure the synchronization time, use the following command:

```
config sys set clock-sync-time <minutes>
```

where:
`minutes` is the number of minutes between synchronizations. The range is 15 to 3600 minutes; the default is 60 minutes.

Log messages are generated when the drift between the real-time clock and the system clock is more than 5 seconds.

Creating a virtual management port

To create a virtual management port in addition to the physical management ports on the switch management modules, use the following command:

config sys set mgmt-virtual-ip <*ipaddr/mask*>

Note: When you assign an IP address to the virtual management port, that IP address provides access to both switch management modules. The master management module replies to all management requests sent to the virtual IP address, as well as to requests sent to its management port IP address. If the master management module fails and the standby management module takes over, the virtual management port IP address continues to provide management access to the switch.

Note: This feature is not supported in a switch with mixed Passport 8000 Series 8190SM modules and Passport 8000 Series 8691SF modules.

Configuration example

This configuration example uses the above commands to set an IP address for the virtual management port, save the configuration file to the standby management module, assign IP addresses to the physical management ports (see *Getting Started*).

```
Passport-8610:5# config sys set mgmt-virtual-ip 47.140.54.40/
255.255.255.0
Physical and Virtual IP must be in the same subnet
Passport-8610:5# save config file config1 standby standby1
Save config to file config1 successful.
Passport-8610:5# config bootconfig net mgmt ip 47.140.54.40/
255.255.255.0
Passport-8610:5#
```

Setting individual system level switch parameters

To set individual system-level switch parameters, use the following command:

`config sys set`

This command includes the following options:

`config sys set` followed by:	
`info`	Displays current system settings.
`clock-sync-time` *`<minutes>`*	Configures the RTC-to-system clock synchronization time. • *`minutes`* is 15 to 3600 minutes.
`contact` *`<contact>`*	Sets the contact information for the switch. • *`contact`* is an ASCII string from 1 to 1024 characters (for example a phone extension or email address).
`ecn-compatibility` *`<enable|disable>`*	Enables or disables explicit congestion notification, as defined in Experimental RFC 2780. This feature is not currently supported on the Passport 8000 Series switch.
`global-filter` *`<enable|disable>`*	Enables or disables global filtering on the switch. When this command is enabled, you must disable source MAC VLANs (**`config sys set vlan-bysrcmac disable`**). The system will not allow you to enable global filtering and source MAC-based VLANs at the same time. This command is available only on Passport 8600 switches.
`location` *`<location>`*	Sets the location information for the switch. • *`location`* is an ASCII string from 1 to 1024 characters (for example, Finance).
`mroute-stream-limit` *`<enable|disable>`*	Enables or disables multicast stream limiting.
`mgmt-virtual-ip` *`<ipaddr/mask>`*	Configures the virtual management port. • `ipaddr/mask` is the ip address and mask of the virtual management port.
`msg-control` *`<enable|disable>`*	Enables or disables the system message control. Enable this command to suppress duplicate error messages.

`config sys set` followed by:	
`mtu <`*`bytes`*`>`	Enables Jumbo frame support. • *`bytes`* is the Ethernet frame size, either 1950 (default) or 9600 bytes.
`name <`*`prompt`*`>`	Sets the box or root level prompt name for the switch. • *`prompt`* is an ASCII string from 1 to 1024 characters (for example, LabSC7 or Closet4).
`portlock <`*`on|off`*`>`	Turns port locking on or off. To specify the ports to be locked, use the **`config ethernet <`*`ports`*`> lock`** command (refer to *Configuring Routing Operations for the Passport 8000 Series Switch Using the Command Line Interface Release 3.1.2*).
`sendAuthenticationTrap <true|false>`	Sets whether or not to send authentication failure traps.
`smlt-on-single-cp <enable|disable> [timer <`*`value`*`>]`	Enables or disables SMLT on the single CP feature. Optional parameter: `timer` *`value`* is the timer value for SMLT on the single CP feature timer. Valid options are 1 to 3.
`topology <on|off>`	Turns the topology feature on or off. The topology feature generates topology packets used by Optivity* network management software. When this feature is off, the topology table is not generated. The default is on.
`udpsrc-by-vip <enable|disable>`	Enables or disables virtual IP as the UDP source.
`vlan-bysrcmac <enable|disable>`	Enables or disables the ability to configure source MAC VLANs on the switch. The default is disable. If you enable this command, you must disable the global filter command (**`config sys set global-filter disable`**). The system will not allow you to enable global filtering and source MAC-based VLANs at the same time. This command is available only on Passport 8600 switches.

Configuration example

This configuration example uses the above commands to set the following system-level switch parameter: contact, location, message control, and authentication trap. The example also uses the **`info`** command to display information about the switch parameters.

```
Passport-8610:5# config sys set
Passport-8610:5/config/sys/set# contact cbfw
Passport-8610:5/config/sys/set# location Marketing
Passport-8610:5/config/sys/set# msg-control enable
Passport-8610:5/config/sys/set# sendAuthenticationTrap true
Passport-8610:5/config/sys/set# info
Sub-Context: action flags record-reservation snmp ssh
Current Context:
   mgmt-virtual-ip : 0.0.0.0/0.0.0.0
   contact : cbfw
   location : Marketing
   name : Passport-8610
   msg-control : enable
   portlock : off
   sendAuthenticationTrap : true
   topology : on
   globalFilter : enable
   vlanBySrcMac : disable
   ecn-compatibility : enable
   System MTU : 1950
Passport-8610:5/config/sys/set#
```

Showing system status and parameter configuration

To show system status and parameter configuration, use the following command:

`show sys`

This command includes the following options:

`show sys` followed by:	
`dns`	Displays primary and secondary DNS server status.
`eapol`	Displays EAP status.

show sys followed by:	
`info [card] [asic] [mda]`	Displays system status and technical information about the switch hardware components. • `card` displays information about all the installed modules. • `asic` displays information about the ASICS installed on each module. • `mda` displays information about installed MDAs.
`mcast-mlt-distribution`	Displays the settings for multicast over MLT.
`mcast-software-forwarding`	Displays the settings for multicast software forwarding.
`msg-control`	Displays the system message control function status (enabled or disabled).
`perf`	Displays system performance information, such as CPU utilization, switch fabric utilization, NVRAM size, and NVRAM used. The information is updated once per second, so it is no more than one second from real time.
`record-reservation`	Displays the number of reserved records and usage information for each record type. Record types include filter, IPMC, MAC, and static route.
`sw`	Displays the version of software running on the switch, the last update of that software, and the Boot Config Table. The Boot Config Table lists the current system settings and flags.
`topology`	Displays the topology table. This table shows the information that is being sent to Optivity network management software for creating network displays.

Configuration example

This configuration example uses the above commands to display information about the following parameters: message control, system performance, system software, and system topography.

```
Passport-8610:5# show sys msg-control

                 msg-control : enable

Passport-8610:5# show sys perf

                      CpuUtil: 0%
             SwitchFabricUtil: 0%
        OtherSwitchFabricUtil: 0%
                   BufferUtil: 0%
                    DramSize: 64 M
                    DramUsed: 67%
                    DramFree: 21155 K
Passport-8610:5# show sys sw

System Software Info :

Default Runtime Config File : /flash/config
Default Boot Config File : /flash/boot.cfg
Config File :
Last Runtime Config Save : THU APR 15 19:50:19 1999
Last Runtime Config Save to Slave : 0
Last Boot Config Save : SAT MAR 06 21:07:10 1999
Last Boot Config Save on Slave : 0

Boot Config Table
Slot# : 5
Version : Build REL3.3.0.0_B069 on Build REL3.3.0.0_B069 on Fri Mar
29 14:05:52 EST 2002
LastBootConfigSource : /flash/boot.cfg
LastRuntimeImageSource : /flash/p80a3300b069.img
LastRuntimeConfigSource : /flash/config
PrimaryImageSource : /flash/p80a3300b069.img
PrimaryConfigSource : /flash/config
SecondaryImageSource : /flash/p80a3000.img
SecondaryConfigSource : /flash/config.cfg
TertiaryImageSource : 0.0.0.0:
TertiaryConfigSource : /flash/config.cfg
EnableAutoBoot : true
EnableFactoryDefaults : false
```

```
             EnableDebugMode : false
             EnableHwWatchDogTimer : false
             EnableRebootOnError : true
             EnableTelnetServer : true
             EnableRloginServer : false
             EnableFtpServer: true
             EnableTftpServer : true
             Passport-8610:5# show sys topology
============================================================================
                           Topology Table
============================================================================
SLOT  IP_ADDR       SEG MAC_ADDR     CHASSIS      BKPL   LOCAL CURSTATE
PORT                ID               TYPE         TYPE   SEG
----------------------------------------------------------------------------
0/0 47.140.54.40   0 00:04:dc:6c:00:00 Passport8610 enetFastGigEnet true  heartbeat
```

Controlling link state changes

Link flap detection allows you to control link state changes on a physical port. You can set thresholds for the number and frequency of changes allowed and take action if the thresholds are exceeded. If the link state change thresholds are exceeded, a log entry is generated. The possible configuration actions are to send a trap and to bring down the port.

This feature allows you to detect when the link is going up and down rapidly (that is, flapping) on a port. This action can be detrimental to network stability because it could trigger spanning tree and routing table recalculation.

To control link state changes, use the following command:

`config sys link-flap-detect`

The **`config sys link-flap-detect`** command includes the following options:

`config sys link-flap-detect` followed by:	
`info`	Shows the link-flap-detect settings.

`auto-port-down`
`<enable|disable>`
	Enables or disables automatic disabling of the port if the link-flap threshold is exceeded; the default is `enable`.

config sys link-flap-detect followed by:	
frequency *<frequency>*	Sets the number of changes that are allowed during the time specified by the **interval** command. The default is 10. *frequency* is from 1 to 9999.
interval *<interval>*	Sets the link-flap-detect interval in seconds. The default is 60. *interval* is from 2 to 600.
send-trap *<enable|disable>*	Enables or disables sending traps. The default is enable.

Configuration example

This configuration example uses the above commands to enable automatic disabling of the port, set the link-flap-detect interval, and enable sending traps. The example also uses the **info** command to display the link-flap settings.

```
Passport-8610:5# config sys link-flap-detect
Passport-8610:5/config/sys/link-flap-detect# auto-port-down enable
Passport-8610:5/config/sys/link-flap-detect# interval 20
Passport-8610:5/config/sys/link-flap-detect# send-trap enable
Passport-8610:5/config/sys/link-flap-detect# info

 Auto Port Down : enable
 Send Trap      : enable
 Interval       : 20
 Frequency      : 10

Passport-8610:5/config/sys/link-flap-detect#
```

Note: The **show sys link-flap-detect general-info** command displays the same information as the **config sys link-flap-detect info** command

Enabling the administrative status of a module

To enable or disable the administrative status of the module, use the following command:

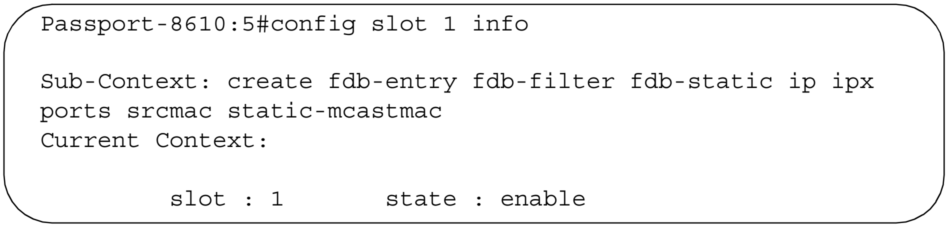
```
config slot <slots> state <enable|disable>
```

To display the administrative status of the module, enter the following command:

```
config slot <slots> info
```

Figure 40 shows output from the **config slot info** command.

Figure 40 config slot info command



```
Passport-8610:5#config slot 1 info

Sub-Context: create fdb-entry fdb-filter fdb-static ip ipx
ports srcmac static-mcastmac
Current Context:

         slot : 1        state : enable
```

Chapter 5
Configuring DHCP and UDP using the CLI

This chapter describes the Run-Time CLI commands that are used to configure DHCP and UDP functions in the Passport 8000 Series switch. This section includes the following topics:

- "Roadmap of IP commands," next
- "DHCP relay commands" on page 128
- "UDP commands" on page 134

Roadmap of IP commands

The following roadmap lists some of the IP commands and their parameters. Use this list as a quick reference or click on any command or parameter entry for more information.

Command	Parameter
`config ip dhcp-relay`	`info`
	`create-fwd-path agent <value> server <value> [mode <value>] [state <value>]`
	`enable-fwd-path agent <value> server <value>`
	`delete-fwd-path agent <value> server <value>`
	`disable-fwd-path agent <value> server <value>`
	`mode <mode> agent <value> server <value>`

Command	Parameter
`config ethernet <ports> ip dhcp-relay`	`info`
	`broadcast <enable|disable>`
	`disable`
	`enable`
	`max-hop <max-hop>`
	`min-sec <min-sec>`
	`mode <mode>`
`config vlan <vid> ip dhcp-relay`	`info`
	`broadcast <enable|disable>`
	`disable`
	`enable`
	`max-hop <max-hop>`
	`min-sec <min-sec>`
	`mode <mode>`
`config ip udpfwd protocol <udpport>`	`info`
	`create <protoname>`
	`delete`
`config ip udpfwd portfwd`	`info`
	`add-portfwd <udpport> <ipaddr>`
	`remove-portfwd <udpport> <ipaddr>`
`config ip udpfwd portfwdlist <fwdlistid>`	`info`

Command	Parameter
	add-portfwd <udpport> <ipaddr>
	create
	delete
	name <name>
	remove-portfwd <udpport> <ipaddr>
config ip udpfwd interface <ipaddr>	info
	broadcastmask <ipaddr>
	create <fwdlistid>
	delete
	maxttl <maxttl>
	udpportfwdlist <fwdlistid>
show ip dhcp-relay fwd-path	
show ip dhcp-relay counters	
show ports info dhcp-relay [<ports>]	
show ports stats dhcp-relay [<ports>]	
show vlan info dhcp-relay [<vid>]	
show ip udpfwd interface info [<ipaddr>]	
show ip udpfwd portfwd info	
show ip udpfwd portfwdlist info [<fwdlistid>]	
show ip udpfwd protocol info	

DHCP relay commands

Dynamic Host Configuration Protocol (DHCP), an extension of the Bootstrap Protocol (BootP), is used to dynamically provide host configuration information to the workstations. Use the port DHCP relay commands to set DHCP relay behavior on a port and the VLAN DHCP commands to set DHCP relay behavior on a VLAN.

DHCP relay must be enabled on the path for port or VLAN configuration to take effect.

Configuring DHCP relay

To view and configure DHCP parameters globally, use the following command:

`config ip dhcp-relay`

This command includes the following options:

`config ip dhcp-relay` followed by:	
`info`	Displays current DHCP global configuration on the switch.
`create-fwd-path agent <`*`value`*`> server <`*`value`*`> [mode <`*`value`*`>] [state <`*`value`*`>]`	Configures the forwarding path from the client to the server. • `agent` *`value`* is the IP address configured on an interface (a locally configured IP address). • `server` *`value`* is the IP address of the DHCP server in the network. If this IP address corresponds to the locally configured IP network, the DHCP packet is broadcast out the interface. • `mode` *`value`* is to forward BootP messages only, DHCP messages only, or both {bootp | dhcp | bootp_dhcp}. • `state` *`value`* enables or disables the forwarding path.

config ip dhcp-relay followed by:	
enable-fwd-path agent <*value*> server <*value*>	Enables DHCP relaying on the path from the IP address to the server. • agent *value* is the IP address configured on an interface (a locally configured IP address). • server *value* is the IP address of the DHCP server in the network. If this IP address corresponds to the locally configured IP network, the DHCP packet is broadcast out the interface.
delete-fwd-path agent <*value*> server <*value*>	Deletes the forwarding path from the client to the server. • agent *value* is the IP address configured on an interface (a locally configured IP address). • server *value* is the IP address of the DHCP server in the network.
disable-fwd-path agent <*value*> server <*value*>	Disables DHCP relaying on the path from the IP address to the server. This is the default. • agent *value* is the IP address configured on an interface (a locally configured IP address). • server *value* is the IP address of the DHCP server in the network.
mode <*mode*> agent <*value*> server <*value*>	Modifies DHCP mode to forward BootP messages only, DHCP messages only, or both. The default is both. • *mode* is [bootp | dhcp | bootp_dhcp]. • agent *value* is the IP address configured on an interface (a locally configured IP address). • server *value* is the IP address of the DHCP server in the network.

Showing DHCP relay information

To display information about DHCP routes and counters, use the following commands:

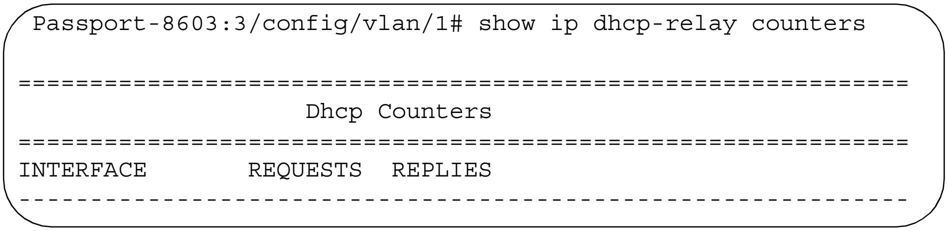
```
show ip dhcp-relay fwd-path
show ip dhcp-relay counters
```

The **show ip dhcp-relay fwd-path** command displays DHCP routing information, including interface, server, enabled or disabled, and mode (forward BootP messages only, DHCP messages only, or both).

The **show ip dhcp-relay counters** command displays DHCP counter information, including the number of requests and the number of replies for each interface.

Figure 41 shows sample output for the **show ip dhcp-relay counters** command.

Figure 41 show ip dhcp-relay counters command output



```
 Passport-8603:3/config/vlan/1# show ip dhcp-relay counters

==============================================================
                    Dhcp Counters
==============================================================
INTERFACE       REQUESTS  REPLIES
--------------------------------------------------------------
```

Configuring DHCP relay on a port

To view and configure DHCP parameters on the specified port(s), use the following command:

config ethernet *<ports>* **ip dhcp-relay**

where:
ports is the port or list of ports on which you are running the command {slot/port[-slot/port][, ...]}.

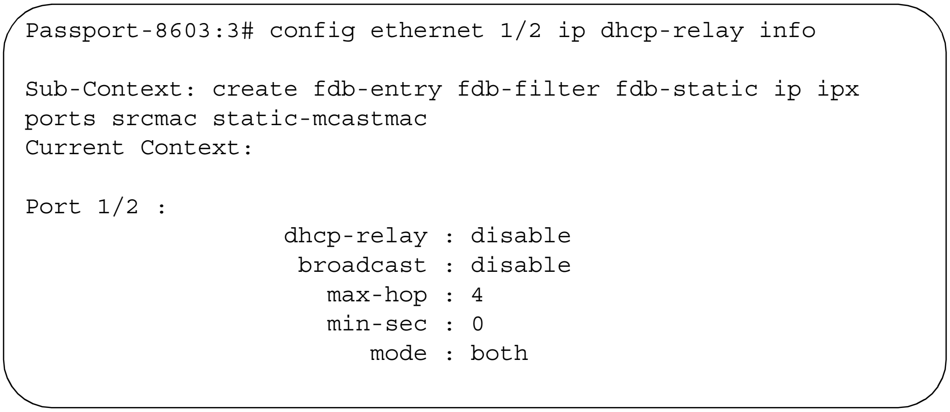
This command includes the following options:

config ethernet ***<ports>*** **ip dhcp-relay** followed by:	
info	Displays current DHCP configuration on the port (Figure 42).
broadcast *<enable|disable>*	Sets whether or not the server reply is sent as a broadcast or unicast back to the end station.
disable	Disables DHCP relaying on the port.This is the default state.
enable	Enables DHCP relaying on the port.

config ethernet <*ports*> ip dhcp-relay followed by:	
max-hop <*max-hop*>	Sets the maximum number of hops before a BootP/DHCP packet is discarded (1 to 16). The default is 4.
min-sec <*min-sec*>	Sets the minimum seconds count set for DHCP. If the “secs” field in the BootP/DHCP packet header is greater than this value, the switch relays or forwards the packet; otherwise, the packet is dropped (0 to 65535). The default is 0 seconds.
mode <*mode*>	Sets DHCP mode to forward BootP messages only, DHCP messages only, or both. The default is both.

Figure 42 shows a sample of the **config ethernet ip dhcp-relay info** command.

Figure 42 config ethernet ip dhcp-relay info command output



```
Passport-8603:3# config ethernet 1/2 ip dhcp-relay info

Sub-Context: create fdb-entry fdb-filter fdb-static ip ipx
ports srcmac static-mcastmac
Current Context:

Port 1/2 :
                  dhcp-relay : disable
                   broadcast : disable
                     max-hop : 4
                     min-sec : 0
                        mode : both
```

Showing DHCP relay information for a port

To display information about DHCP on one or more ports, use the following two commands:

show ports info dhcp-relay [<*ports*>]
show ports stats dhcp-relay [<*ports*>]

The **show ports info dhcp-relay** command displays the DHCP parameters for a specified port or all ports.

The **`show ports stats dhcp-relay`** command displays DHCP statistics for a specified port or for all ports.

Figure 43 shows an example of the **`show ports info dhcp-relay`** command.

Figure 43 show ports info dhcp-relay command (partial output)

```
Passport-8610# show ports info dhcp-relay

================================================================
                           Port Dhcp
================================================================
PORT_NUM ENABLE   MAX_HOP  MIN_SEC  MODE  ALWAYS_BROADCAST
----------------------------------------------------------------
9/1      false    4        0        both  false
9/2      true     4        0        both  false
9/3      false    4        0        both  false
9/4      false    4        0        both  false
9/5      false    4        0        both  false
9/6      false    4        0        both  false
9/7      false    4        0        both  false
```

Figure 44 shows sample output for the **`show ports stats dhcp-relay`** command.

Figure 44 show ports stats dhcp-relay command (partial output)

```
Passport-8610# show ports stats dhcp-relay

===============================================================
                       Port Stats Dhcp
===============================================================
PORT_NUM NUMREQUEST NUMREPLY
---------------------------------------------------------------
1/1      0          0
3/1      0          0
3/2      0          0
3/3      0          0
3/4      0          0
3/5      0          0
```

Configuring DHCP relay on a VLAN

To configure DHCP routing on a VLAN, use the following command:

```
config vlan <vid> ip dhcp-relay
```

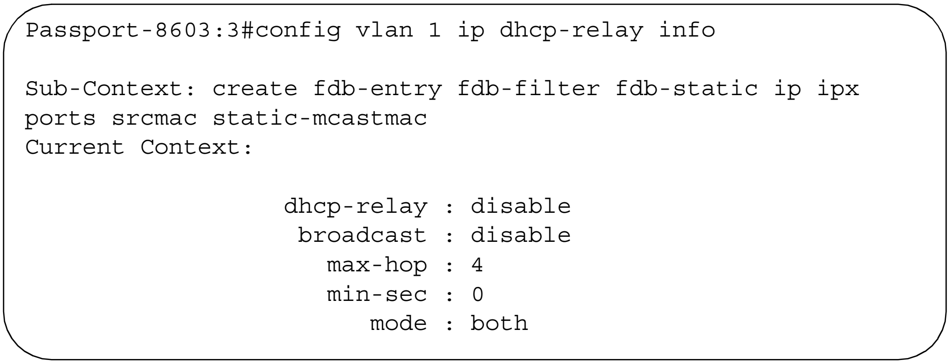
where:
vid refers the VLAN ID, which is a value from 1 to 4094.

This command includes the following options:

config vlan <*vid*> ip dhcp-relay followed by:	
info	Displays DHCP characteristics on the VLAN.
broadcast <*enable*|*disable*>	Sets whether or not the server reply is sent as a broadcast back to the end station.
disable	Disables DHCP relaying on the VLAN. This state is the default state.
enable	Enables DHCP relaying on the VLAN.
max-hop <*max-hop*>	Sets the maximum number of hops before the BootP/DHCP packet is dropped (1 to 16).
min-sec <*min-sec*>	Sets the minimum seconds count for DHCP. If the secs field in the packet header is greater than this value, the switch forwards the packet; otherwise it is dropped (0 to 65535).
mode <*mode*>	Sets DHCP mode to forward BootP messages only, DHCP messages only, or both. The default is both.

Figure 45 shows sample output for the **config vlan ip dhcp-relay info** command.

Figure 45 config vlan ip dhcp-relay info command output



```
Passport-8603:3#config vlan 1 ip dhcp-relay info

Sub-Context: create fdb-entry fdb-filter fdb-static ip ipx
ports srcmac static-mcastmac
Current Context:

                  dhcp-relay : disable
                   broadcast : disable
                     max-hop : 4
                     min-sec : 0
                        mode : both
```

Showing DHCP relay information for a VLAN

To display the DHCP parameters for all VLANs or for the specified VLAN, use the following command:

`show vlan info dhcp-relay` `[<`*`vid`*`>]`

where:
`vid` refers the VLAN ID, which is a value from 1 to 4094.

The interface index (IF Index) is assigned as the VLAN is created. Numbers 1 to 256 are ports; numbers above 257 are VLANs.

UDP commands

Some network applications, such as the NetBIOS name service, rely on a User Data Protocol (UDP) broadcast to request a service or to locate a service. By default, broadcasts are not forwarded by a router. UDP broadcast forwarding is a generalized mechanism for the router to selectively forward UDP broadcasts.

The basic procedure for setting up UDP broadcast forwarding is:

- To enter protocols in a protocol table, use the **`config ip udpfwd protocol`** command, next.

- To add or remove a port forward entry, use the **config ip udpfwd portfwd** command (page 135).
- To create and name the port forward list and assign protocols and servers to the port forward list, use the **config ip udpfwd portfwdlist** command (page 136).
- To apply the port forward list to the appropriate interfaces, use the **config ip udpfwd interface** command (page 137).
- To display the current UDP forwarding configuration, use the **show ip udpfwd** command (page 138)

Configuring UDP protocols

To configure a UDP protocol, use the following command:

```
config ip udpfwd protocol <udpport>
```

where:
udpport refers to the UDP protocol port number {1..65535}.

This command includes the following options:

config ip udpfwd protocol <*udpport*> followed by:	
info	Displays created and/or deleted UDP protocols.
create <*protoname*>	Creates a new UDP protocol. • *protoname* is the UDP protocol name {string}.
delete	Deletes a UDP port protocol.

Configuring a UDP port forward entry

To add or remove a port forward entry, use the following command:

```
config ip udpfwd portfwd
```

The **`config ip udpfwd portfwd`** command includes the following options:

`config ip udpfwd portfwd` followed by:	
`info`	Displays the current configuration for the port forward list ID.
`add-portfwd <udpport> <ipaddr>`	Adds a UDP protocol port to the specified port forwarding list. • *udpport* is a UDP protocol port {1..65535}. • *ipaddr* is an IP address in dotted decimal format.
`remove-portfwd <udpport> <ipaddr>`	Removes a protocol port forwarding entry and IP address from the list. • *udpport* is a UDP protocol port {1..65535}. • *ipaddr* is an IP address in dotted decimal format.

Configuring the UDP port forward list

To create and name the port forward list and assign protocols and servers to the port forward list, use the following command:

`config ip udpfwd portfwdlist` *`<fwdlistid>`*

`where:`
fwdlistid refers to the port forwarding list number {1..1000}.

This command includes the following options:

`config ip udpfwd portfwdlist <fwdlistid>` followed by:	
`info`	Displays the current configuration for the port forward list ID.
`add-portfwd <udpport> <ipaddr>`	Adds a UDP protocol port to the specified port forwarding list. • *udpport* is a UDP protocol port {1..65535}. • *ipaddr* is an IP address in dotted decimal format.
`create`	Creates a UDP port forwarding list.

config ip udpfwd portfwdlist <fwdlistid> followed by:	
delete	Deletes a port forwarding list ID.
name <*name*>	Assigns a name to the UDP port forwarding list. • *name* is an alphabetical string.
remove-portfwd <*udpport*> <*ipaddr*>	Removes a protocol port forwarding entry and IP address from the list. • *udpport* is a UDP protocol port {1..65535}. • *ipaddr* is an IP address in dotted decimal format.

Configuring UDP forward interfaces

To apply the port forward list to the appropriate interfaces, use the following command:

config ip udpfwd interface *<ipaddr>*

where:
ipaddr indicates the IP address of the selected interface.

This command includes the following options:

config ip udpfwd interface <*ipaddr*> followed by:	
info	Displays the current configuration of the UDP interface.
broadcastmask <*ipaddr*>	Sets the interface broadcast mask (the *interface broadcast* mask may be different than the interface mask). • *ipaddr* is an IP address.
create <*fwdlistid*>	Assigns a forwarding list ID {1..1000} to an interface IP address.
delete	Removes the forwarding list from the IP address.
maxttl <*maxttl*>	Sets maximum time-to-live for the UDP broadcast forwarded by the interface.
udpportfwdlist <*fwdlistid*>	Changes the port forwarding list {1..1000}.

Showing UDP forward information

The **`show ip udpfwd`** command displays information about the UDP forwarding characteristics of the switch. The command has four options: interface info, portfwd info, portfwdlist info, and protocol info.

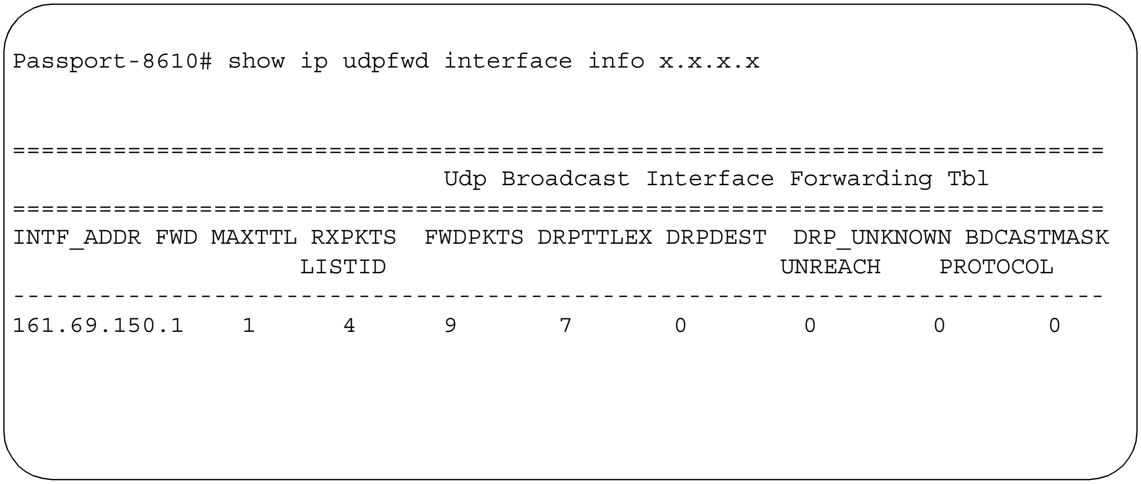
Showing UDF forward interface information

To display information about the UDP interface for all IP addresses or a specified IP address, use the following command:

`show ip udpfwd interface info` `[<`*`ipaddr`*`>]`

Figure 46 shows sample output for this command.

Figure 46 show ip udpfwd interface info command output



```
Passport-8610# show ip udpfwd interface info x.x.x.x


============================================================================
                              Udp Broadcast Interface Forwarding Tbl
============================================================================
INTF_ADDR FWD MAXTTL RXPKTS  FWDPKTS DRPTTLEX DRPDEST  DRP_UNKNOWN BDCASTMASK
                    LISTID                           UNREACH     PROTOCOL
----------------------------------------------------------------------------
161.69.150.1    1      4      9       7       0        0        0       0
```

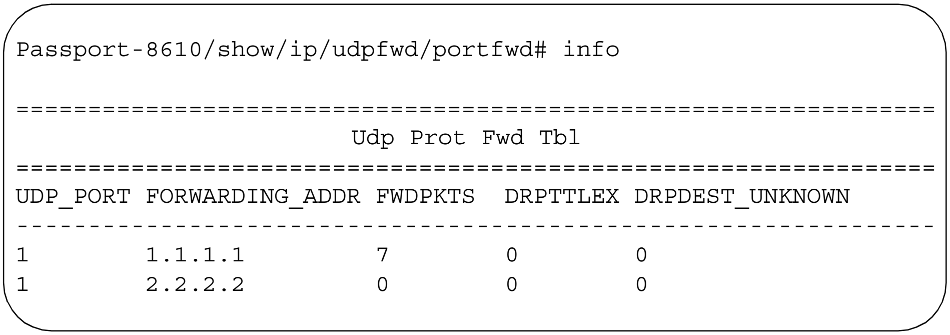
Showing the UDF port forwarding table information

To display the UDP port forwarding table, use the following command:

`show ip udpfwd portfwd info`

Figure 47 shows sample output for this command.

Figure 47 show ip udpfwd portfwd info command output



```
Passport-8610/show/ip/udpfwd/portfwd# info

================================================================
                       Udp Prot Fwd Tbl
================================================================
UDP_PORT FORWARDING_ADDR FWDPKTS  DRPTTLEX DRPDEST_UNKNOWN
----------------------------------------------------------------
1        1.1.1.1         7        0        0
1        2.2.2.2         0        0        0
```

Showing the UDP port forwarding list table information

To display the UDP port forwarding list table for the specified list or all lists on the switch, use the following command:

`show ip udpfwd portfwdlist info` `[<`*`fwdlistid`*`>]`

where:
`fwdlistid` is a list id number with a range of 1 to 1000.

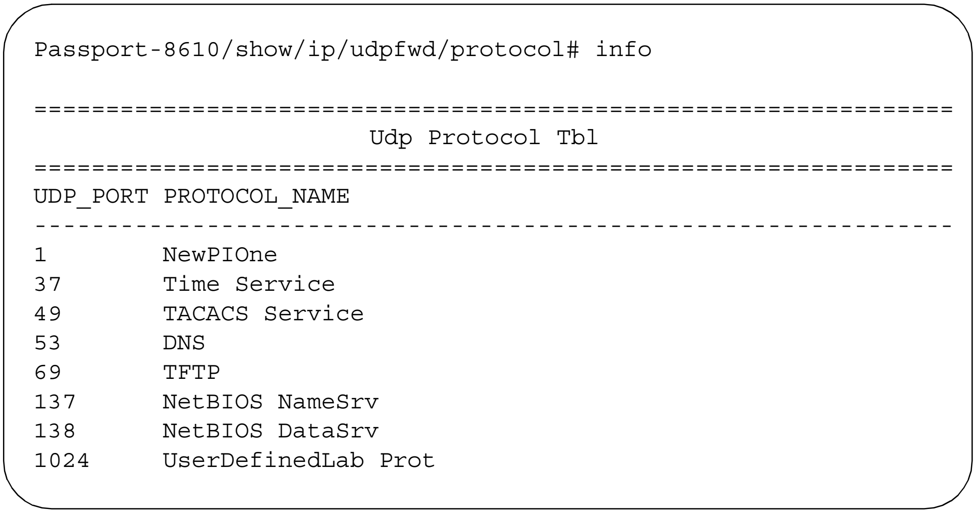
Showing the UDP protocol table information

To display the UDP protocol table with the UDP port numbers for each supported or designated protocol, use the following command:

`show ip udpfwd protocol info`

Figure 48 shows sample output for this command.

Figure 48 show ip udpfwd protocol info command output



```
Passport-8610/show/ip/udpfwd/protocol# info

================================================================
                       Udp Protocol Tbl
================================================================
UDP_PORT PROTOCOL_NAME
----------------------------------------------------------------
1        NewPIOne
37       Time Service
49       TACACS Service
53       DNS
69       TFTP
137      NetBIOS NameSrv
138      NetBIOS DataSrv
1024     UserDefinedLab Prot
```

Chapter 6
Configuring BootP/DHCP and UDP using Device Manager

This chapter describes how to use Device Manager for configuration and router management of BootP/DHCP relay and UDP forwarding. It includes the following topics:

- "Supporting BootP/DHCP relay," next
- "Configuring UDP broadcast forwarding" on page 146

For conceptual information on DHCP and UDP management, see Chapter 1, "System Platform Overview."

Supporting BootP/DHCP relay

Dynamic Host Configuration Protocol (DHCP), an extension of the Bootstrap Protocol (BootP), is used to dynamically provide host configuration information to workstations. To lower administrative overhead, network managers prefer to configure a small number of DHCP servers in a central location. Using few DHCP servers requires the routers connecting to the subnets or bridge (or VLANs) domains to support the BootP/DHCP relay function so that hosts can get the configuration information from servers several router hops away.

Note: BootP/DHCP relays are supported on only IP routed port-based VLANs and protocol-based VLANs. BootP/DHCP relays are not supported on IP subnet-based VLANs.

Configuring DHCP on a brouter port

Use the DHCP tab when setting the DHCP behavior on a brouter port. The DHCP tab is not applicable unless the port (or VLAN) is routed (i.e., assigned an IP address).

BootP/DHCP relay must be enabled first on a port (or VLAN), and then enabled globally.

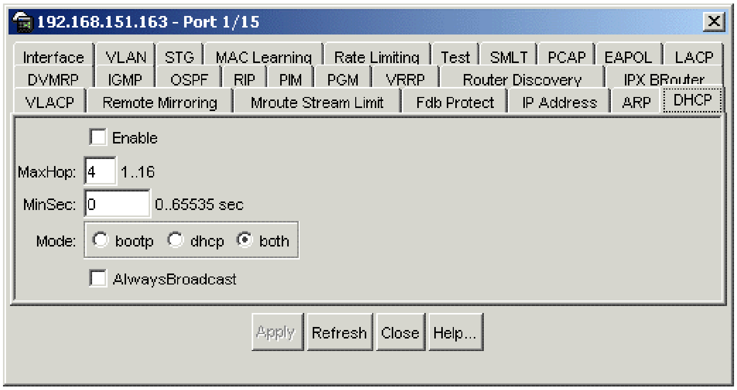
To enable BootP/DHCP on a port:

1. Select a port.
2. From the Device Manager menu bar, choose Edit > Port.

   The Port dialog box opens with the Interface tab displayed.
3. Click the DHCP tab.

   The DHCP tab opens (Figure 49).

Figure 49 Port dialog box—DHCP tab



192.168.151.163 - Port 1/15

☐ Enable

MaxHop: 4 1..16

MinSec: 0 0..65535 sec

Mode: ○ bootp ○ dhcp ● both

☐ AlwaysBroadcast

Table 2 describes the DHCP tab fields.

Table 2 DHCP tab fields

Field	Description
Enable	Enables or disables BootP/DHCP on the port. The default is disable.
MaxHop	Sets the maximum number of hops before a BootP/DHCP packet is discarded (1 to 16). The default is 4.
MinSec	The “secs” field in the BootP/DHCP packet header represents the elapsed time since the client first sent the message. If the “secs” field in the packet header is greater than this value, the switch relays or forwards the packet; otherwise, the packet is dropped. The default is 0 seconds.
Mode	Sets the interface to process only BootP, only DHCP, or both types of packets. The default is both.
AlwaysBroadcast	When enabled, the server reply is sent as a broadcast back to the end station. The default is disable.

4 Click Enable to select the DHCP option.

The default is disable.

5 Enter the appropriate values.

6 Click Apply.

Configuring BootP/DHCP on VLANs

The procedure for configuring BootP/DHCP relay on a routed VLAN is the same as that for configuring DHCP relay for a brouter port.

To configure the DHCP behavior for a routed VLAN:

1 From the Device Manager menu bar, select VLAN > VLANs > Basic.

The VLAN dialog box opens, with the Basic tab displayed.

2 Select a VLAN.

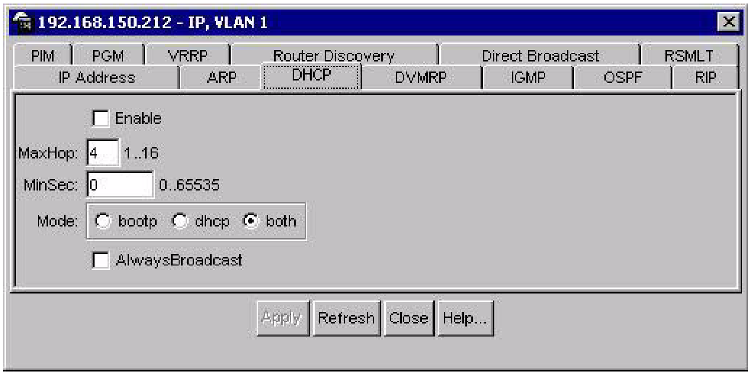
3 Click IP.

The IP, VLAN dialog box opens with the IP Address tab displayed.

4 Select the DHCP tab.

The DHCP tab opens (Figure 50).

Figure 50 IP, VLAN dialog box—DHCP tab



□ Enable

MaxHop: 4 1..16

MinSec: 0 0..65535

Mode: ○ bootp ○ dhcp ● both

□ AlwaysBroadcast

5 Select Enable and enter the appropriate values.

6 Click Apply.

Configuring forwarding policies

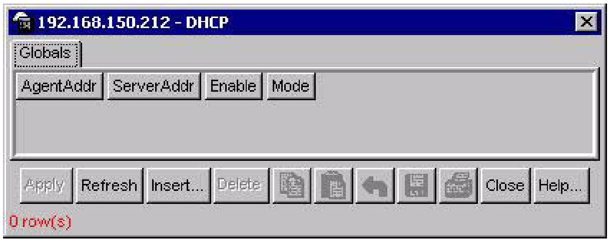
After configuring the BootP/DHCP relay on an IP interface, you can configure forwarding policies to indicate where packets are to be forwarded. The forwarding policies are based on the type of packet and where the packet is received.

To set up a forwarding policy for BootP/DHCP packets received on a virtual interface (brouter or VLAN) enabled for DHCP relaying:

1 From the Device Manager menu bar, choose IP Routing > DHCP.

The DHCP dialog box opens (Figure 51).

Figure 51 DHCP dialog box



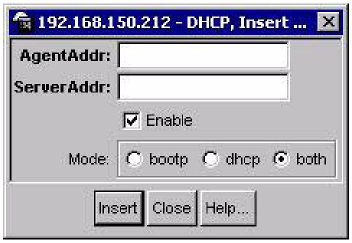
AgentAddr	ServerAddr	Enable	Mode

0 row(s)

2 Click Insert.

The DHCP, Insert Globals dialog box opens (Figure 52).

Figure 52 DHCP, Insert Globals dialog box



192.168.150.212 - DHCP, Insert ...

AgentAddr:

ServerAddr:

☑ Enable

Mode: ○ bootp ○ dhcp ● both

Table 3 describes the fields in the DHCP, Insert Globals dialog box.

Table 3 DHCP, Insert Globals dialog box fields

Field	Description
AgentAddr	IP address of the input interface (agent) on which the relaying of received BootP/DHCP packets must be enabled.
ServerAddr	This parameter is either the IP address of the BootP/DHCP server or the address of another local interface of the switch. • If it is the address of the BootP/DHCP server, then the request is unicast to the server's address. • If the address is one of the IP addresses of an interface on the switch, then the BootP/DHCP requests will be broadcast out of that local interface.
Enable	Enables BootP/DHCP relay on the routing switch.
Mode	Specifies the type of messages relayed: • None • Only BootP • Only DHCP • Both types of packets

3 In the AgentAddr box, type in the agent address.

This parameter specifies the IP address of the IP interface on which the BootP/DHCP request packets are received for forwarding. This address is the IP address of either a brouter port or a VLAN for which forwarding is enabled.

4 In the ServerAddr list, type in the server address.

This parameter is either the IP address of the BootP/DHCP server or the address of another local IP interface of the switch. If it is the address of the BootP/DHCP server, then the request is unicast to the server's address. If the address is one of the IP addresses of an interface on the switch, then the BootP/DHCP requests will be broadcast out of that local interface.

5 Click Enable to turn on BootP/DHCP relay, or click Enable to clear the option.

Each agent server forwarding policy can be enabled or disabled. The default is enabled.

6 In the Mode field, select the type of messages to be relayed.

What determines which packets get forwarded is both, the mode setting for the DHCP interface and the mode setting for the agent interface. The default is to forward both BootP and DHCP messages.

7 Click Insert.

Configuring UDP broadcast forwarding

Some network applications, such as the NetBIOS name service, rely on a User Data Protocol (UDP) broadcast to request a service or to locate a server. By default, broadcasts are not forwarded by a router. UDP broadcast forwarding is a generalized mechanism for the router to selectively forward UDP broadcasts.

The basic steps for setting up UDP broadcast forwarding are:

1 Enter protocols into a table.

2 Create policies (protocol/server pairs).

3 Assemble these policies into lists or profiles.

4 Apply the list to the appropriate interfaces.

5 Enter a name for the protocol.

6 Click Insert.

The protocol is added to the Protocol table. Once created, a protocol name or number cannot be changed. The protocol must be deleted first and then added with a new name and number.

The following sections describe using Device Manager to manage UDP forwarding protocols:

- “Managing UDP forwarding protocols,” next
- “Managing UDP forwarding” on page 149
- “Creating the forwarding profile” on page 151
- “Managing the broadcast interface” on page 152

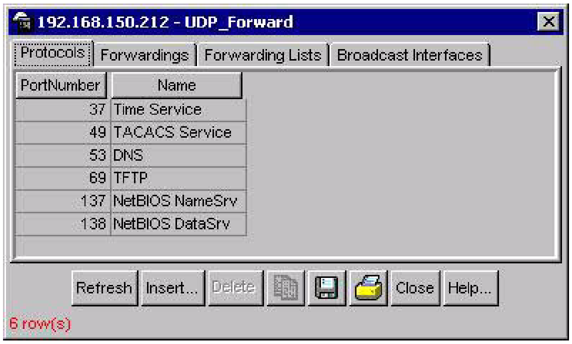
Managing UDP forwarding protocols

To enter protocols into the UDP Forwarding Protocols table:

1 From the Device Manager menu bar, choose IP Routing > UDP Forwarding.

The UDP_Forward dialog box opens with the Protocols tab (Figure 53) open, listing the UDP protocols with broadcasts that can be forwarded.

Figure 53 UDP_Forward dialog box—Protocols tab



PortNumber	Name
37	Time Service
49	TACACS Service
53	DNS
69	TFTP
137	NetBIOS NameSrv
138	NetBIOS DataSrv

6 row(s)

The Passport 8000 Series is configured with the following well-known protocols:

- Time Service
- TACACS Service
- DNS
- TFTP

- NetBIOS NameSrv
- NetBIOS DataSrv

Note: These protocols cannot be deleted. You may add to the list of protocols.

2 Click Insert.

The UDP_Forward, Insert Protocols dialog box opens (Figure 54).

Figure 54 IUDP_Forward, Insert Protocols dialog box

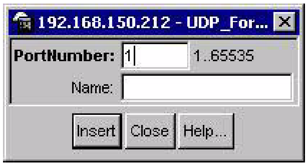


Table 4 describes the Protocols tab and the UDP_Forward, Insert Protocols dialog box fields.

Table 4 Protocols tab and UDP_Forward, Insert Forwarding dialog box fields

Field	Description
Id	Value that uniquely identifies this list of entries (1 to 1000).
Name	An administratively assigned name for this list (0 to 15 characters).
FwdIdList	The zero or more port forwarding entries associated with this list. Each list identifier is stored as 2 bytes in this array, starting from 0 bytes (size=64). Clicking on the ellipses (...) in this field displays the ID list.

3 In the PortNumber text box, type a port number (UDP port).

This number defines the port (UDP port) used by the server process as its contact port.The range is from 1 to 65535 and cannot be one of the well-known UDP port numbers or a number previously assigned.

4 In the Name text box, type a name for the protocol.

5 Click Insert.

The protocol is added to the Protocol table.

Note: Once created, a protocol name or number cannot be changed.

Managing UDP forwarding

You can define the destination addresses for the UDP protocol. To do so:

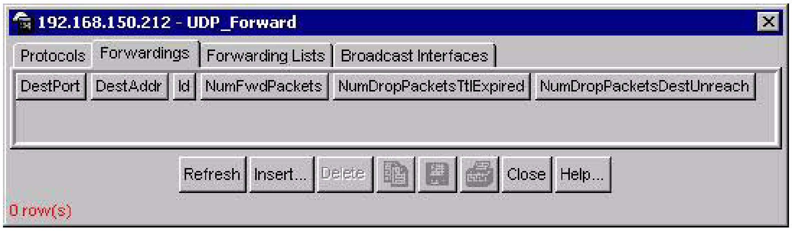
1 From the Device Manager menu bar, choose IP Routing > UDP Forwarding

The UDP_Forward dialog box opens (Figure 53 on page 147).

2 Click the Forwardings tab.

The Forwardings tab opens (Figure 55).

Figure 55 UDP_Forward dialog box—Forwardings tab



192.168.150.212 - UDP_Forward

Protocols | Forwardings | Forwarding Lists | Broadcast Interfaces

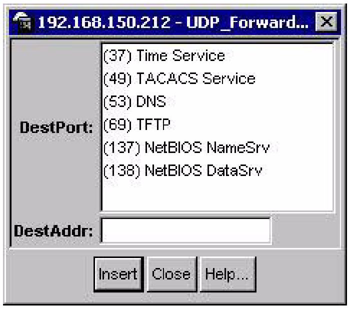
DestPort	DestAddr	Id	NumFwdPackets	NumDropPacketsTtlExpired	NumDropPacketsDestUnreach

0 row(s)

3 Click Insert.

The UDP_Forward, Insert Forwardings dialog box opens (Figure 56).

Figure 56 UDP_Forward, Insert Forwardings dialog box



192.168.150.212 - UDP_Forward...

DestPort:

(37) Time Service
(49) TACACS Service
(53) DNS
(69) TFTP
(137) NetBIOS NameSrv
(138) NetBIOS DataSrv

DestAddr:

4 Select a destination UDP port from the defined protocols.

5 Enter a destination IP address.

The destination address can be any IP server address for the given protocol application or the IP address of an interface on the router.

- If the address is that of a server, the packet will be sent as a unicast packet to this address.
- If the address is that of an interface on the router, the frame will be rebroadcast.

6 Click Insert.

The information is added to the Forwarding tab.

Table 5 describes UDP_Forward, Insert Forwardings dialog box and Forwarding tab fields.

Table 5 UDP_Forward, Insert Forwardings dialog box tab fields

Field	Description
DestPort	The well-known port number defined for UDP, depending upon the protocol type.
DestAddr	The destination address can be any IP server address for the given protocol application or the IP address of an interface on the router. • If the address is that of a server, the packet will be sent as a unicast packet to this address. • If the address is that of an interface on the router, the frame will be rebroadcast.

Table 5 UDP_Forward, Insert Forwardings dialog box tab fields (continued)

Field	Description (continued)
Id (Forwarding tab only)	Integer used to identify this entry internally.
NumFwdPackets (Forwarding tab only)	The total number of UDP broadcast packets forwarded using this policy.
NumDropPacketsTtlExpired (Forwarding tab only)	The total number of UDP broadcast packets dropped because the time to live (TTL) has expired.
NumDropPacketsDestUnreach (Forwarding tab only)	The total number of UDP broadcast packets dropped because the specified destination address was unreachable.

Creating the forwarding profile

You can create a forwarding profile, which is a collection of port and destination pairs. To do so:

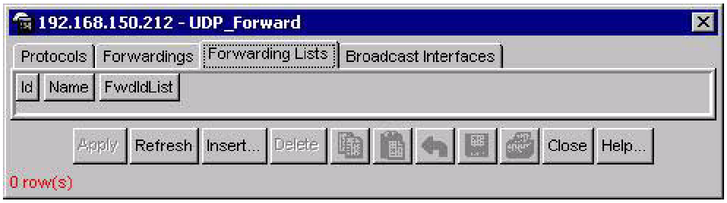
1 From the Device Manager menu bar, choose IP Routing > UDP Forwarding.

The UDP_Forward dialog box opens (Figure 53 on page 147).

2 Click the Forwarding Lists tab.

The Forwarding Lists tab opens (Figure 57).

Figure 57 UDP_Forward dialog box—Forwarding Lists tab



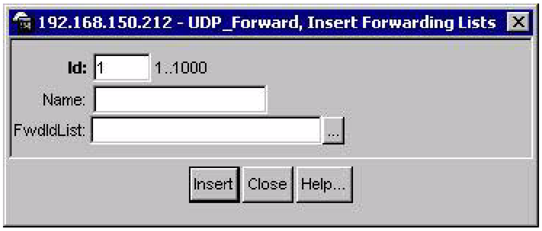
0 row(s)

3 To add a new list, click Insert.

When configuring UDP forwarding list entries, be sure to first configure the UDP forwarding list. Then, configure your UDP forwarding list entries and assign them to a UDP forwarding list. If you do not assign a UDP forwarding list entry to at least one UDP forwarding list, the UDP forwarding list will be lost after a reboot.

The UDP_Forward, Insert Forwarding Lists dialog box opens (Figure 58).

Figure 58 UDP_Forward, Insert Forwarding Lists dialog box



192.168.150.212 - UDP_Forward, Insert Forwarding Lists

Id: 1 1..1000

Name:

FwdIdList:

4 In the Id text box, type the forwarding list Id.

5 In the Name text box, type the name of the forwarding list (optional).

6 The forwarding list is displayed in the FwdIdList text box.

Table 6 describes the Forwarding Lists tab and UDP_Forwarding Forwarding Lists dialog box fields.

Table 6 Forwarding Lists tab and UDP_Forward, Insert Forwarding Lists dialog box fields

Field	Description
Id	Value that uniquely identifies this list of entries (1 to 1000).
Name	An administratively assigned name for this list (0 to 15 characters).
FwdIdList	The zero or more port forwarding entries associated with this list. Each list identifier is stored as 2 bytes in this array, starting from 0 bytes (size=64). Clicking on the ellipses (...) in this field displays the ID list.

Managing the broadcast interface

You can specify and display which router interfaces will receive UDP broadcasts to be forwarded.

To add a UDP broadcast interface:

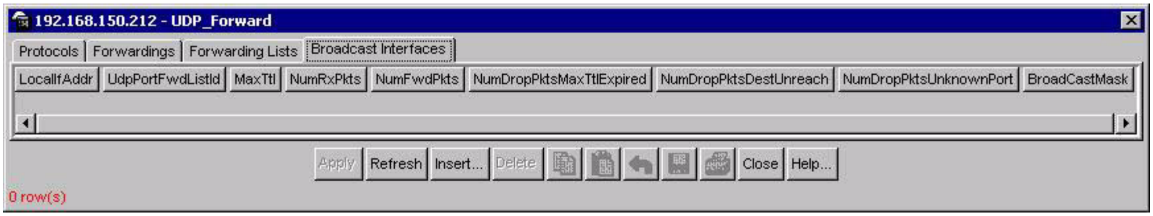
1 From the Device Manager menu bar, choose IP Routing > UDP Forwarding.

The UDP_Forward dialog box opens (Figure 53).

2 Click the Broadcast Interface tab.

The Broadcast Interfaces tab opens (Figure 59).

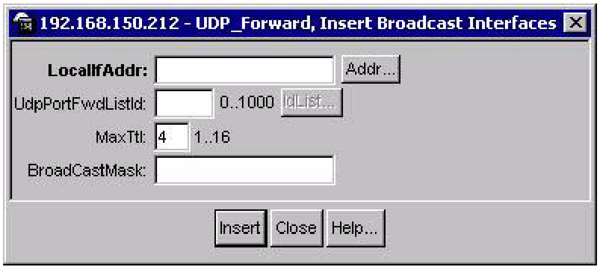
Figure 59 UDP_Forward dialog box—Broadcast Interfaces tab



3 Click Insert.

The UDP_Forward, Insert Broadcast Interfaces dialog box opens (Figure 60).

Figure 60 UDP_Forward, Insert Broadcast Interfaces dialog box



LocalIfAddr:

UdpPortFwdListId: 0..1000

MaxTtl: 4 1..16

BroadCastMask:

4 In the LocalIfAddr text box, type a local interface IP address; or click the Addr button to select an address from the list.

5 In the UdpPortFwdListId text box, type the forwarding list ID; or choose an ID from the list.

6 In the MaxTtl field, type the maximum number of hops an IP broadcast can take from the source device to the destination device (the default is 4; the range is 1 to 16).

7 In the BroadCastMask text box, enter the subnet mask of the local interface that is used for broadcasting the UDP broadcast packets.

When configuring the UDP forwarding broadcast mask, the broadcast mask should be less specific (shorter in length) or equally specific (equal in length) to the subnet mask of the IP interface it is configured upon. If the UDP forwarding broadcast mask is configured to be more specific than the subnet mask of the corresponding IP interface, then UDP forwarding will not function properly.

Table 7 describes the Broadcast Interface tab and UDP_Forward, Insert Broadcast Interface dialog box fields.

Table 7 UDP_Forward, Insert Broadcast Interface dialog box fields

Field	Description
LocalIfAddr	The IP address of the local router interface that will receive UDP broadcast packets that are forwarded.
UdpPortFwdListId	The number of the UDP lists/profiles that this interface is configured to forward (0 to100). A value of 0 indicates that the interface will not forward any UDP broadcast packets.
MaxTtl	The maximum number of hops an IP broadcast packet can take from the source device to the destination device (the default is 4; the range is 1 to 16).
BroadCastMask	The subnet mask of the local interface that is used for broadcasting the UDP broadcast packets.
NumRxPkts	The total number of UDP broadcast packets received by this local interface.
NumFwdPkts	The total number of UDP broadcast packets forwarded by this local interface.
NumDropPacketsTtlExpired	The total number of UDP broadcast packets dropped because the time to live (TTL) has expired.
NumDropPacketsDestUnreach	The total number of UDP broadcast packets dropped because the destination was unreachable.
NumDropPacketsUnknownPort	The total number of UDP broadcast packets dropped because the destination port/protocol specified has no matching forwarding policy.

Chapter 7
Configuring chassis operations

This section includes the following topics:

Enabling Jumbo frames

The standard 1518 bytes Ethernet frame size was designed to protect against the high bit error rates of older physical-layer Ethernet components. But computer processing power has increased by an order of magnitude, and the use of switched Ethernet over unshielded twisted pair or fiber media has significantly lowered Ethernet errors.

In addition, the speed and capacity of the Ethernet are pushing the processor limits of many installed servers, and more data is being transferred between servers. For these reasons, increasing Ethernet's frame size has become a logical option. The 8000 series switch now supports Ethernet frames as large as 9600 bytes, compared to the standard 1518 bytes, in order to transmit large amounts of data efficiently and minimize the task load on a server CPU.

Tagged VLAN support

A port with VLAN tagging enabled can send tagged frames. If you plan to use Jumbo frames in a VLAN, make sure that the ports in the VLAN are configured to accept Jumbo frames and that the server or hosts in the VLAN do not send frames that exceed 9600 bytes. For more information about configuring VLANs, refer to *Configuring Layer 2 Operations: VLANs, Spanning Tree, Multilink Trunking*.

Modules and Interfaces that support Jumbo frames

The following 8000 series modules and interfaces support Jumbo frames:

- Gig Fiber and Gig Copper ports in 8608SX, 8608SX-E, 8608GBIC, 8608GBIC-E, 8632TX, 8632TX-E, 8608GT, and 8608GT-E
- 10GB interfaces

Note: The Web Switching Module (WSM) supports Jumbo frames of up to 9018 octets. For instructions on configuring Jumbo frames for this module, see *Configuring the Web Switching Module Using Device Manager.*

When you enable Jumbo frame support on the chassis, the port interfaces that support the Jumbo frames feature are set to an MTU size of 9600 bytes. The port interfaces that do not support the Jumbo frames feature will retain the default MTU of 1950 bytes. Any changes that you make to the MTU size are dynamic; that is, they take place immediately.

Enabling Jumbo frames using the CLI

When you enable Jumbo frame support on the chassis, the port interfaces that support the Jumbo frames feature are set to an MTU size of 9600 bytes. The port interfaces that do not support the Jumbo frames feature will retain the default MTU of 1950 bytes.

To enable Jumbo frame support on the chassis, use the following command:

```
config sys set mtu <bytes>
```

where *bytes* is the Ethernet frame size, either 9600 bytes or 1950 bytes (default).

Showing the MTU for the system

To display the MTU value for the system, use the following command:

show sys info

Figure 61 shows sample output for this command.

Figure 61 show sys info command output

```
8000:5# show sys info

General Info :

        SysDescr     : Passport-8610 (3.3.0.0)
        SysName      : Passport-8610
        SysUpTime    : 1 day(s), 16:08:25
        SysContact   : support@nortelnetworks.com
       SysLocation  : 4401 Great America Parkway, Santa Clara,
CA 95054

Chassis Info :

        Chassis     : 8010
        Serial#     : SSNM00137R
        HwRev       : A
        NumSlots    : 10
        NumPorts    : 36
        GlobalFilter: enable
        VlanBySrcMac: disable
        Ecn-Compatib: enable
        BaseMacAddr : 00:01:81:2c:90:00
        MacAddrCapacity : 1024
        Temperature : 30 C
        MgmtMacAddr : 00:01:81:2c:93:f4

        System MTU  : 9600
```

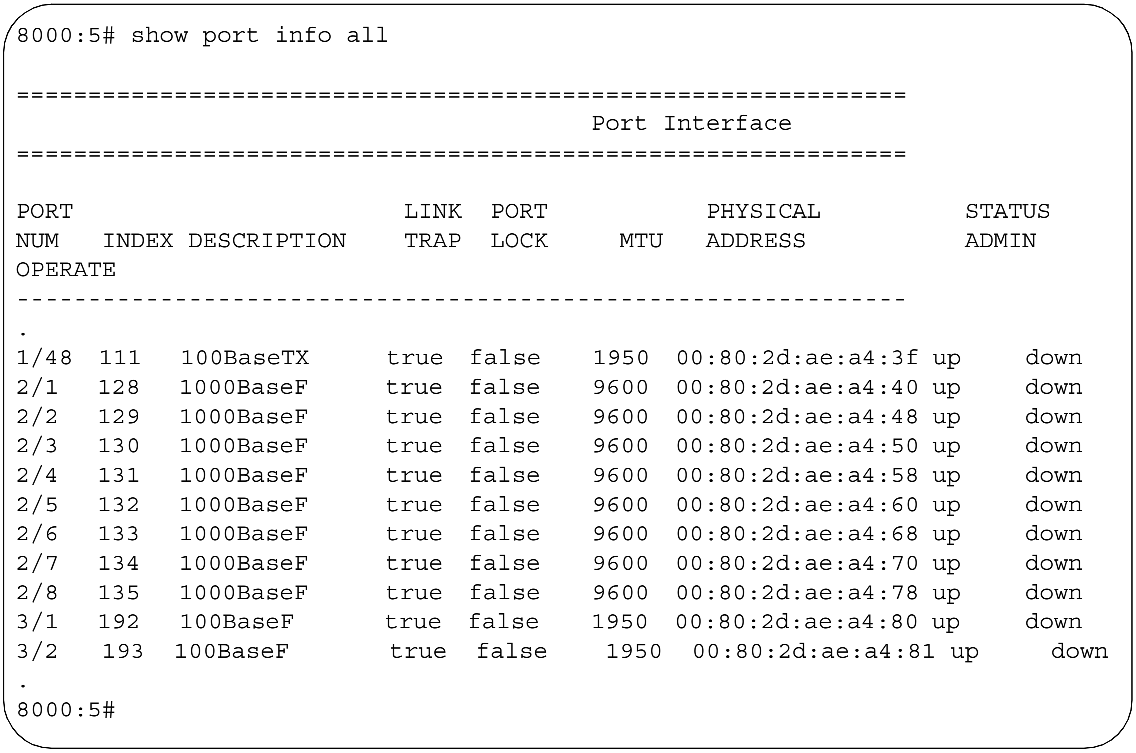
Showing the MTU for all ports

To display the MTU values for all ports on the chassis, use the following command:

`show port info all`

Figure 62 shows sample output for this command.

Figure 62 show sys info command output



```
8000:5# show port info all

==============================================================
                                        Port Interface
==============================================================

PORT                           LINK  PORT           PHYSICAL            STATUS
NUM    INDEX DESCRIPTION       TRAP  LOCK      MTU    ADDRESS            ADMIN
OPERATE
--------------------------------------------------------------
.
1/48  111   100BaseTX      true  false    1950  00:80:2d:ae:a4:3f up     down
2/1   128   1000BaseF      true  false    9600  00:80:2d:ae:a4:40 up     down
2/2   129   1000BaseF      true  false    9600  00:80:2d:ae:a4:48 up     down
2/3   130   1000BaseF      true  false    9600  00:80:2d:ae:a4:50 up     down
2/4   131   1000BaseF      true  false    9600  00:80:2d:ae:a4:58 up     down
2/5   132   1000BaseF      true  false    9600  00:80:2d:ae:a4:60 up     down
2/6   133   1000BaseF      true  false    9600  00:80:2d:ae:a4:68 up     down
2/7   134   1000BaseF      true  false    9600  00:80:2d:ae:a4:70 up     down
2/8   135   1000BaseF      true  false    9600  00:80:2d:ae:a4:78 up     down
3/1   192   100BaseF       true  false    1950  00:80:2d:ae:a4:80 up     down
3/2    193   100BaseF        true   false    1950   00:80:2d:ae:a4:81 up     down
.
8000:5#
```

Enabling Jumbo frames using Device Manager

When you enable Jumbo frame support on the chassis, the port interfaces that support the Jumbo frames are set to an MTU size of 9600 bytes. The port interfaces that do not support the Jumbo frames feature retain the default MTU of 1950 bytes.

To enable Jumbo frame support on the chassis:

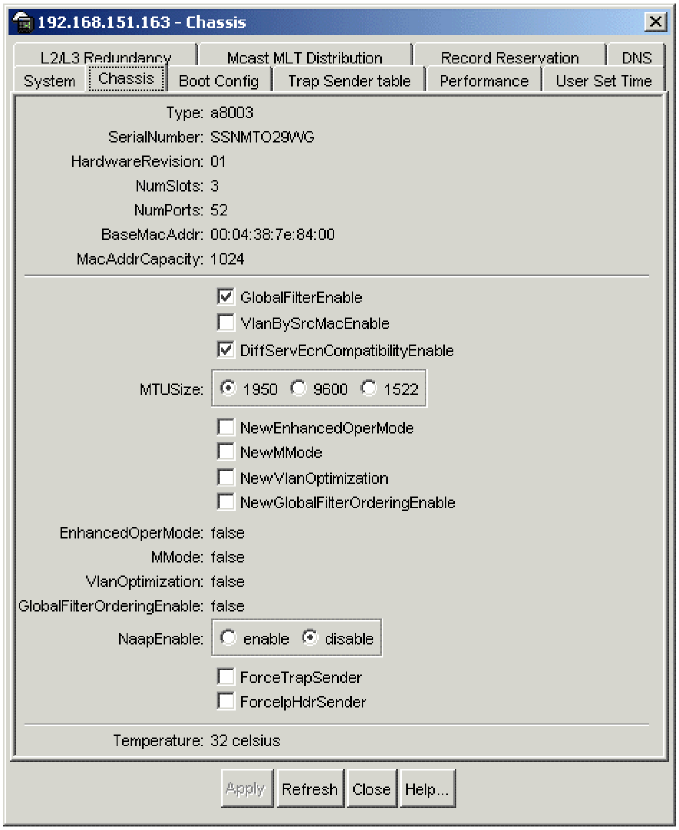
1 From the Device Manager menu bar, choose Edit > Chassis.

The System dialog box opens with the System tab displayed.

2 Click on the Chassis tab.

The Chassis dialog box opens with the Chassis tab displayed (Figure 63).

Figure 63 Chassis tab



Type: a8003
SerialNumber: SSNMTO29WG
HardwareRevision: 01
NumSlots: 3
NumPorts: 52
BaseMacAddr: 00:04:38:7e:84:00
MacAddrCapacity: 1024

☑ GlobalFilterEnable
□ VlanBySrcMacEnable
☑ DiffServEcnCompatibilityEnable

MTUSize: ● 1950 ○ 9600 ○ 1522

□ NewEnhancedOperMode
□ NewMMode
□ NewVlanOptimization
□ NewGlobalFilterOrderingEnable

EnhancedOperMode: false
MMode: false
VlanOptimization: false
GlobalFilterOrderingEnable: false
NaapEnable: ○ enable ● disable

□ ForceTrapSender
□ ForceIpHdrSender

Temperature: 32 celsius

3 Click MTU size: 9600.

4 Click Apply.

5 Click Close.

Showing the MTU for the system

To show the MTU configured for the entire system:

1. From the Device Manager menu bar, choose Edit > Chassis.

   The System dialog box opens with the System tab displayed.

2. Click on the Chassis tab.

   The Chassis dialog box opens with the Chassis tab displayed (Figure 63).

3. Check that 9600 is selected for MTU size.

Showing the MTU for each port

To show the MTU for each port:

1. From the Device View, click on the port for which you want to display information.

   To select more than one port, click on the first port. Then, while holding down the Ctrl key, click on the ports for which you want to display information.

2. From the Device Manager menu bar, choose Edit > Port.

   The Port dialog box opens with the Interface tab displayed.

3. Check the MTU field to verify the MTU size for each port.

Enabling M mode (128K mode)

The 8600 modules support 128K hardware records, which is the maximum allowed with the existing ASIC. This means that the hardware capacity has increased to handle as many as 100K routes in hardware. For information on reserving records, see *Configuring Network Management.*

Keep the following points in mind when configuring your switch:

- If your CPU module is a single 8690, it does **not** support the 128K M Mode. The operation mode is always 32K.

- If your CPU module is 8691 or higher, you can configure the chassis to operate either in 32K (default) or 128K M mode.
- I/O (Legacy I/O and E-Modules) modules support 32K mode only (non-MMode).
- If your system has both 128K and 32K modules, refer to Table 8 for configuration information so that the switch reboots in the desired mode.

Note: If all modules are currently in non-Mmode, with module 1 as the master and module 2 as the standby, and you enable MMode on module 1, save the configuration, and reboot, module 2 comes up as the master and module 1 as the standby. If you then enable MMode on the new master (module 2), the standby (module 1) goes offline and remains offline.

The boot mode is determined by the modules in the chassis and whether 128K mode status is enabled.

To see how to configure your switch, refer to Table 8.

Table 8 Boot mode at startup

If the configuration is:	**And 128K mode status at startup is:**	**Then:**
All M-modules	Enabled	System starts in 128K mode.
Mixed configuration: • M-modules, • E-modules and • Legacy modules	Enabled	System starts in 128K mode. • M-modules enabled. • E-modules disabled. • Legacy modules disabled.
All E-modules and/or Legacy modules	Enabled	All modules are disabled.
All 128K modules	Disabled	System starts in 32K mode. All modules are enabled.
Mixed (32K and 128K) modules	Disabled	System starts in 32K mode. All modules are enabled.
All E-modules and/or Legacy modules	Disabled	System starts in 32K mode. All modules are enabled.

When you insert a module into a running chassis, the 128K mode status determines the module's initialization mode (Table 9).

Table 9 Inserting 32K and 128K modules into a running chassis

If you insert this module into a running chassis:	And 128K mode status is:	Then:
M-module (128K)	Enabled	The module is initialized in M mode (128K).
E-module or Legacy module (32K)	Enabled	The module is **not** initialized. A trap is sent and an error is logged to the console.
M-module (128K)	Disabled	The module is initialized as a 32K module.
E-module or Legacy module (32K)	Disabled	The module is initialized as a 32K module.

The following sections describe how to enable M mode using the CLI and Device Manager. Once you have configured your switch for M mode, to synchronize the operating mode of the master and slave CPUs, reset the switch.

Enabling M mode with the CLI

If you decide to change the configuration while you are operating the switch, you can use the following CLI command to modify boot.cfg:

To enable M mode, enter:

```
config sys set flags m-mode true
```

To disable M mode, enter:

```
config sys set flags m-mode false
```

Note: If you have 8690 SF/CPU modules in your switch, and you attempt to activate any 128K features using the CLI, the following error message appears: `This feature will not be enabled with 8690 SF/CPU cards.`

Enabling M mode with Device Manager

To enable the M mode, use the following steps:

1 From the Device Manager menu bar, choose Edit > Chassis.

The Chassis dialog box opens with the System tab displayed.

2 Click the Chassis tab.

3 Check the NewMMode box.

4 Click Apply.

A warning message appears, advising you to reboot.

5 Click OK.

➡ **Note:** If you have enabled M mode and you are using Device Manager, you cannot edit or apply changes on the Boot tab on the standby CPU. Configuration is possible if you are in non-M mode.

Enabling enhanced operational mode

The enhanced operational mode increases the maximum number of VLANs when using MLT (1980) and SMLT (989). This mode requires 8600 E modules. For a list of E-modules, see Table 1 on page 24.

The scaling numbers are reduced by multicast MAC filters. Scaling figures remain unaffected for VLANs not using MLT. Scaling numbers are also reduced if you use IST and SMLT. With IST and SMLT, you can create maximum 989 VLANs.

Table 10 shows new VLAN scaling limitations, with and without enhanced operational mode enabled.

Table 10 Maximum numbers of port/protocol based VLANs

VLAN type	Enhanced Operational Mode enabled	Enhanced Operational Mode disabled
MLT	1980	240
IST/SMLT	989	120

Caution: When enhanced operational mode is enabled, only E-modules and M-modules are initialized (legacy modules are taken offline). Either replace any legacy module or move the network connections to an E- or M-module to avoid losing modules and network connectivity.

The boot mode is determined by the modules in the chassis and whether the enhanced operational mode is enabled. To see how to configure your switch, refer to Table 11.

Table 11 Boot mode at startup

If the configuration is:	And enhanced operational mode is:	Then:
All M-modules and/or E-modules	Enabled	System starts in enhanced operational mode. All modules are initialized and can be configured with up to 1980 VLANs with MLT.
Mixed configuration: • M-modules, • E-modules and • Legacy modules	Enabled	System starts in enhanced operational mode. • M-modules enabled. • E-modules enabled. • Legacy modules disabled.
All Legacy modules	Enabled	System starts in NON-enhanced operational mode. All modules are disabled.
All M-modules and/or E-modules	Disabled	System starts in NON-enhanced operational mode. All modules are enabled.
Mixed configuration: • M-modules, • E-modules and • Legacy modules	Disabled	System starts in NON-enhanced operational mode. All modules are enabled.
All Legacy modules	Disabled	System starts in NON-enhanced operational mode. All modules are enabled.

When you insert a module into a running chassis, the enhanced operational mode status determines the module's initialization mode (Table 12).

Table 12 Inserting modules into a running chassis

If you insert this module into a running chassis:	And enhanced operational mode status is:	Then:
M-module or E-module	Enabled	The module is initialized in enhanced operational mode.
Legacy module	Enabled	The module is not initialized. A trap is sent and an error is logged to the console.
M-module or E-module	Disabled	The module is initialized in NON-enhanced operational mode.
Legacy module	Disabled	The module is initialized in NON-enhanced operational mode.

Enabling enhanced operational mode with the CLI

If you decide to change the configuration while you are operating the switch, you can use the following CLI command to modify boot.cfg:

To enable the enhanced operational mode, enter:

```
config sys set flags enhanced-operational-mode true
```

To disable the enhanced operational mode, enter:

```
config sys set flags enhanced-operational-mode false
```

Enabling enhanced operational mode with Device Manager

To enable the enhanced operational mode, use the following steps:

1. From the Device Manager menu bar, choose Edit > Chassis.

   The Chassis dialog box opens with the System tab displayed.

2 Click the Chassis tab.

3 Check the NewEnhancedOperMode button.

Note: For the changes to take effect, you must save the configuration and reboot the chassis.

For more information on the parameter settings, see *Configuring Layer 2 Operations: VLANs, Spanning Tree, Multilink Trunking.*

Enabling CPU high-availability mode

CPU high-availability (HA) mode enables switches with two CPUs to recover quickly from a failure of one of the CPUs.

- In HA mode, also called “hot standby,” the two CPUs are synchronized. This means the CPUs are compatible and configured in the same mode.
- In non-HA mode, also called “warm standby,” the two CPUs are **not** synchronized. Either the CPUs are incompatible or one of them is configured in a mode that it cannot support.

Synchronization also applies to software parameters. Table 13 shows what features are supported in Release 3.2 and 3.3 or later.

Table 13 Release 3.2 and 3.3 or later synchronization capabilities in HA mode

Synchronization of:	**in Release 3.2**	**in Release 3.3 or later**	**in Release 3.7 or later**
Layer 1			
Port configuration parameters	Yes	Yes	
Layer 2			
VLAN parameters	Yes	Yes	
QoS parameters	Yes	Yes	
Layer 3		Yes	
VLAN virtual interface	Yes	Yes	
ARP entries	No	Yes	

Table 13 Release 3.2 and 3.3 or later synchronization capabilities in HA mode

Synchronization of:	**in Release 3.2**	**in Release 3.3 or later**	**in Release 3.7 or later**
Static and default routes	No	Yes	
Enabling CPU high-availability mode with the CLI			No
Enabling CPU high-availability mode with Device Manager			No

HA mode support for 8690SF and 8691SF CPUs

Table 14 shows the hardware and software dependencies that are required to support HA mode with 8690SF and 8691SF CPUs. The boot mode is determined by the types of CPU in the chassis and whether M Mode is enabled.

In the following configurations, assume that CPU high-availability mode is enabled. However, you can see in some cases that HA mode is impossible because one of the CPUs was taken off-line due to a hardware or software incompatibility.

Table 14 M Mode and switch fabric dependencies in HA mode

	Master CPU			
Slave CPU	**8690 in 32K (non M Mode)**	**8690 in 128K (M Mode)**	**8691 in 32K (non M Mode)**	**8691 in 128K (M Mode)**
8690 in 32K (non M Mode)	32K	32K W1, n/a[1]	32K	128K 8690 off-line E1, E2
8690 in 128K (M Mode)	32K n/a, W1	32K W1,W1	32K n/a, W1	128K 8690 off-line E1, W1&E2
8691 in 32K (non M Mode)	32K	32K W1&W2, I1	32K	Mismatch W4, W4
8691 in 128K (M Mode)	Mismatch W5, W3	32K W1&W3, W3	Mismatch	128K

[1] The following list shows the error and warning messages for each configuration. Messages for the master CPU are shown first and then the slave separated by a comma.

Information message:

I1: Configuration mismatch of M mode on master and slave. Rectify master's configuration.

Error messages (caused by hardware incompatibility):

E1: Peer CPU is 8690 which cannot support M mode (128K mode), ->offline

E2: 8690 slave cannot support master's M mode (128K mode), ->offline

Warning messages (caused by configuration incompatibility):

W1: 8690 cannot support M mode (128K mode), operating in 32K mode

W2: Slave (8691) can support configured M mode. For 128K mode of operation, check slave's configuration as reset/switch-over.

W3: Master (8690) cannot support configured M mode. For 128K mode of operation, reset Master.

W4: Master and Slave have mismatching M mode configuration.

W5: Configuration and HW mismatch: master does not have configuration or capability to support M mode. Slave has both. Switch over if M mode is needed.

HA mode support for Dual CPUs

If your switch supports Dual CPU modules, refer to Table 15 to use the CPU high-availability mode. The boot mode is determined by the types of CPUs in the chassis and whether the CPU high-availability mode is enabled.

Table 15 Boot mode at startup for Dual CPU configurations

If the configuration is:	**And CPU high-availability mode is:**	**Then:**
Two Dual CPU modules	Enabled	System starts in CPU high-availability mode.
One Dual CPU module and One Single CPU module	Enabled	If the Single CPU boots first, the CPU reboots so the Dual CPU can be Master and the Single CPU goes offline. If the Dual CPU boots first, the system starts in CPU high-availability mode and the Single CPU goes offline.
Two Single CPU modules	Enabled	System does not boot and stays in monitor mode.
Two Dual CPU modules	Disabled	System starts in single CPU mode.
One Dual CPU module and One Single CPU module	Disabled	System starts in single CPU mode.
Two Single CPU modules	Disabled	System starts in single CPU mode.

When you insert a module into a running chassis, the CPU high-availability mode status determines the module’s initialization mode (Table 16).

Table 16 Inserting single and dual CPU modules into running chassis

If you insert this module into a running chassis:	**And CPU high-availability mode status is:**	**Then:**
Dual CPU module	Enabled	The module is activated as a backup.
Single CPU module	Enabled	The module is not activated. A trap is sent and an error is logged to the console.
Dual CPU module	Disabled	The module is activated in single CPU mode.
Single CPU module	Disabled	The module is activated in single CPU mode.

Removing a master CPU with CPU-HA mode enabled

To remove the master CPU without loss of traffic when CPU-HA is enabled:

1. Software reset the master CPU, which then becomes the standby.
2. Remove what is now the standby CPU.

   The master is removed. Because CPU-HA is enabled, no traffic data is lost during reset.

➡ **Note:** Reinserting a CPU module before the HA-enabled CPU becomes the master CPU, may cause the master CPU to remain in a booting state.

Chapter 8
Configuring NTP using the CLI

This chapter describes how to configure the Network Time Protocol (NTP) using the CLI and includes the following topics:

- “Configuration prerequisites,” next
- “Configuring NTP” on page 171

Configuration prerequisites

Before you can configure NTP, you must do the following:

- Configure an IP interface on the Passport 8000 Series switch and be sure that the NTP server is reachable through this interface. For instructions, see *Configuring IP Routing Operations*.
- Ensure that the Real Time Clock is present on the CPU board.

Note: NTP server MD5 authentication does not support passwords (keys) that start with a special character or contain a space between characters.

Configuring NTP

This section includes the following topics:

- “Enabling NTP globally,” next
- “Creating an NTP server” on page 174
- “Configuring authentication keys” on page 176

- "Showing NTP server status" on page 178

Enabling NTP globally

When you enable NTP, default values are in effect for most parameters. You can customize NTP by modifying parameters. To enable or disable NTP globally on the Passport 8000 Series switch, use the following command.

```
config ntp
```

The **config ntp** commands include the following options:

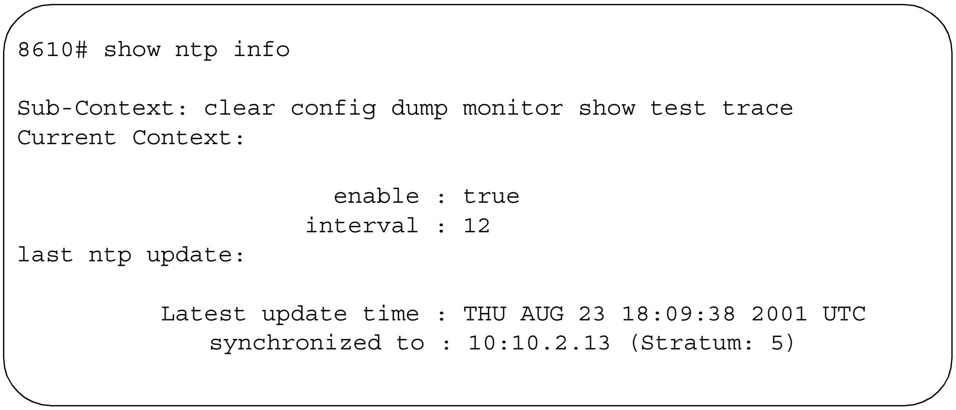
config ntp followed by:	
`info`	Displays current NTP settings on this NTP server.
`enable <true|false>`	Globally enables or disables NTP. The default is false. You cannot enable NTP unless RTC has been installed on the CPU boards.
`interval <value>`	Specifies the time interval (10 to 1440 minutes) between successive NTP updates. The default is 15 minutes. • *value* is the time interval in minutes. **Note:** If NTP is already enabled, this setting will not take effect until you disable NTP and then reenable it.

Configuration example

This configuration example uses the above commands to enable NTP. The example also uses the **`show ntp info`** command to display the NTP global status.

```
8610:5# config ntp
8610:5/config/ntp# enable true
8610:5/config/ntp# show ntp info

Sub-Context: key server
Current Context:

                      enable : true
                    interval : 15
last ntp update:


8610:5/config/ntp#
```

Figure 64 show ntp info command output



```
8610# show ntp info

Sub-Context: clear config dump monitor show test trace
Current Context:

                      enable : true
                    interval : 12
last ntp update:

          Latest update time : THU AUG 23 18:09:38 2001 UTC
             synchronized to : 10:10.2.13 (Stratum: 5)
```

As shown in Figure 64, the *latest update time* field indicates the most recent update to the NTP server. The *synchronized to* field displays the NTP server address from which the Passport 8000 Series switch received time. The *stratum* field indicates the current stratum value of the Passport 8000 Series switch.

Creating an NTP server

To create an NTP server or modify existing NTP server parameter, use the following command.

```
config ntp server
```

Note: You can configure a maximum of 10 time servers.

The **`config ntp server`** command includes the following options:

`config ntp server` followed by:	
`info`	Displays NTP server configuration settings on the switch.
`create <ipaddr> [enable <value>] [auth <value>] [key <value>]`	Adds an NTP server. • *`ipaddr`* is the IP address of the NTP server. NTP adds this address to a list of servers. The local NTP server consults this list of servers for time information. • `enable` *`value`* enables (true) or disables (false) the NTP server. The default is enable. • `auth` *`value`* enables (true) or disables (false) MD5 authentication on this NTP server. The default is no MD5 authentication. • `key` *`value`* specifies the key id value used to generate the MD5 digest for this NTP server. • The value range is an integer from 1 to 214743647. The default value is 0, which indicates that authentication is disabled.

config ntp server followed by:	
delete <*ipaddr*>	Deletes the NTP server. • *ipaddr* is the IP address of the NTP server you want to delete.
set <*ipaddr*> [enable <*value*>] [auth <*value*>] [key <*value*>]	Allows you to modify NTP server parameters. • *ipaddr* is the IP address of the NTP server. • enable *value* enables (true) or disables (false) the NTP server. The default is enable. • auth *value* enables (true) or disables (false) MD5 authentication on this NTP server. The default is no MD5 authentication. • key *value* specifies the key id value used to generate the MD5 digest for this NTP server. • The value range is an integer from 1 to 214743647. The default value is 0, which indicates that authentication is disabled.

Configuration example

This configuration example uses the above commands to create an NTP server, enable the server, assign authentication, and assign a key. The example also uses the **info** command to display information about the NTP server.

```
8610:5# config ntp server create 47.140.53.187 enable true
8610:5# config ntp server
8610:5/config/ntp/server# info

Sub-Context:
Current Context:

         create :

Server Ip         Enabled Auth    Key Id
47.140.53.187     true    false   0

         delete : N/A
            set : N/A

8610:5/config/ntp/server# set 47.140.53.187 auth true
8610:5/config/ntp/server# set 47.140.53.187 key 15
8610:5/config/ntp/server# info

Sub-Context:
Current Context:

                      create :

Server Ip         Enabled Auth    Key Id
47.140.53.187     true    true    15

                      delete : N/A
                         set : N/A

8610:5/config/ntp/server#
```

Note: The **`show ntp server config`** command displays the same information as the **`config ntp server info`** command.

Configuring authentication keys

To configure NTP authentication keys, use the following command:

`config ntp key`

The **`config ntp key`** command includes the following options:

`config ntp key` followed by:	
`info`	Display NTP authentication key configuration settings.

`create`
`<`*`authentication key value`*`>`
`<`*`secret key value`*`>`
	Adds a MD5 authentication key entry to the list where:
	• *`authentication key value`* is the key id used to generate the MD5 digest. Specify a value between 1 and 214743647. The default is 0.
	• *`secret key value`* is the MD5 key ID used to generate the MD5 digest. Specify an alphanumeric string between 0 and 8.

`delete`
`<`*`authentication key value`*`>`
	Delete a MD5 authentication key entry from the list.
	• *`authentication key value`* is the key id used to generate the MD5 digest.

`set`
`<`*`authentication key value`*`>`
`<`*`secret key value`*`>`
	Modifies a MD5 authentication key value where:
	• *`authentication key value`* is the key id used to generate the MD5 digest. Specify a value between 1 and 214743647. The default is 0.
	• *`secret key value`* is the MD5 key ID used to generate the MD5 digest. Specify an alphanumeric string between 0 and 8.

Configuration example

This configuration example uses the above commands to configure and NTP authentication key. The example also uses the **`show ntp key config`** command to display information about the NTP key configuration setup.

```
8610:5# config ntp key
8610:5/config/ntp/key# create 5 18
8610:5/config/ntp/key#
8610:5/config/ntp/server# show ntp key
8610:5/config/ntp/key# info

Sub-Context:
Current Context:

                      create :

MD5_Key_Id  MD5 Key
5           18

                      delete : N/A
                         set : N/A

8610:5/config/ntp/key#
```

Showing NTP server status

The **`show ntp server stat`** command displays the NTP server status. This information includes:

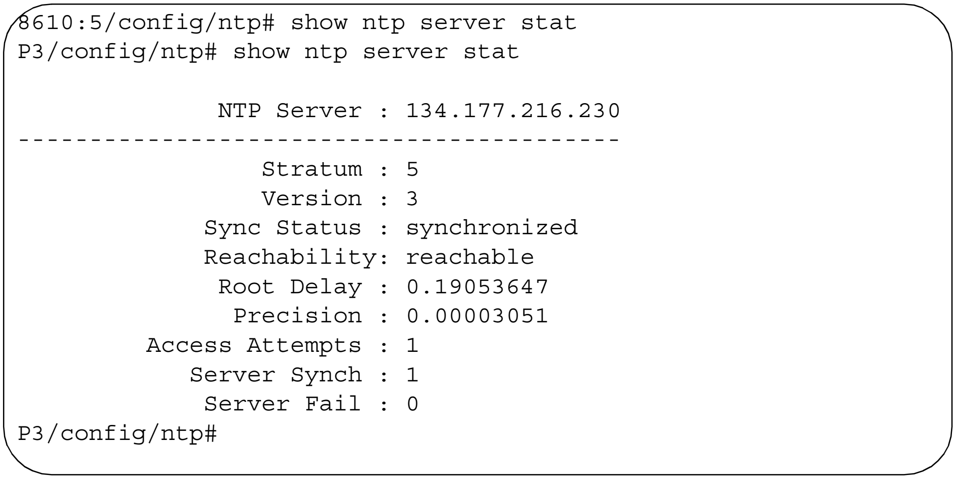
- Number of NTP requests sent to this NTP server,
- Number of times this NTP server was selected to update the time
- Number of times this NTP server was rejected from updating the time
- Stratum
- Version
- Sync Status
- Reachability
- Root Delay
- Precision

To display the NTP server status, use the following command:

`show ntp server stat`

Figure 65 shows sample command output.

Figure 65 show ntp server stat command sample output



```
8610:5/config/ntp# show ntp server stat
P3/config/ntp# show ntp server stat

              NTP Server : 134.177.216.230
------------------------------------------
                 Stratum : 5
                 Version : 3
             Sync Status : synchronized
             Reachability: reachable
              Root Delay : 0.19053647
               Precision : 0.00003051
         Access Attempts : 1
            Server Synch : 1
             Server Fail : 0
P3/config/ntp#
```

Chapter 9
Configuring NTP using Device Manager

This chapter describes how to configure the Network Time Protocol (NTP) using Device Manager. It includes the following topics:

- "Configuration prerequisites," next
- "Configuring NTP" on page 182

Configuration prerequisites

Before you can configure NTP, you must do the following:

- Configure an IP interface on the Passport 8000 Series switch and ensure that the NTP server is reachable through this interface. For instructions, see *Configuring IP Routing Operations*.
- Make sure that the Real Time Clock is present on the CPU board.

Note: NTP server MD5 authentication does not support passwords (keys) that start with a special character or that contain a space between characters.

Configuring NTP

This section describes how to use Device Manager to perform the following tasks:

- "Enabling NTP globally," next
- "Adding an NTP server" on page 183
- "Assigning a NTP key" on page 185

Enabling NTP globally

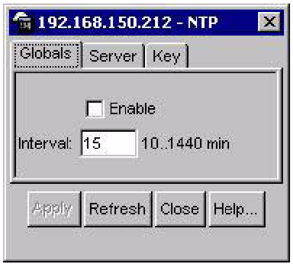
When you enable NTP globally on the Passport 8000 Series switch, default values are in effect for most NTP parameters.

To enable NTP globally:

1 From the Device Manager menu bar, select Edit > NTP.

The NTP dialog box opens with the Global tabs displayed (Figure 66).

Figure 66 NTP dialog box—Globals tab



192.168.150.212 - NTP

□ Enable

Interval: 15 10..1440 min

2 Select the Enable check box.

3 Click Apply.

Table 17 describes the NTP Globals tab fields.

Table 17 Global tab fields

Field	Description
Enable	Enables (true) or disables (false) NTP. You cannot enable NTP if RTC has not been installed on the CPU boards. By default, NTP is disabled.
Interval	Specifies the time interval (10 to 1440 minutes) between successive NTP updates. The default interval is 15 minutes. **Note:** If NTP is already enabled, this setting will not take effect until you disable NTP and then reenable it.

Adding an NTP server

After you enable NTP globally on the Passport 8000 Series switch, you can add a remote NTP server by specifying it's IP address. NTP adds this IP address to a list of servers, which the local NTP client uses when querying remote time servers for time information. The list of qualified servers is referred to as a peer list.

You can configure a maximum of 10 time servers.

To specify an IP address for an NTP server:

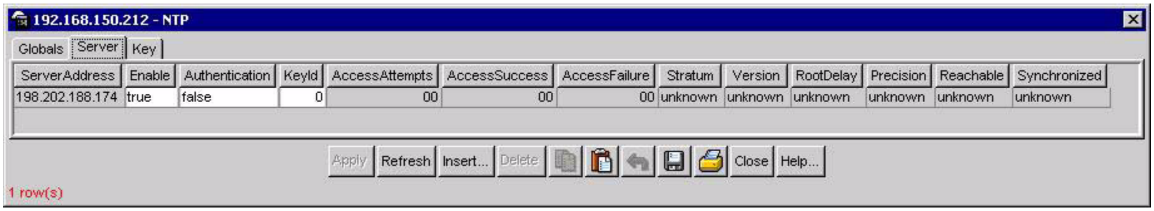
1. From the Device Manager menu bar, select Edit > NTP.

   The NTP dialog box opens with the Globals tab displayed (Figure 66 on page 182).

2. Click the Server tab.

   The Server tab opens (Figure 67).

Figure 67 Server tab



ServerAddress	Enable	Authentication	KeyId	AccessAttempts	AccessSuccess	AccessFailure	Stratum	Version	RootDelay	Precision	Reachable	Synchronized
198.202.188.174	true	false	0	00	00	00	unknown	unknown	unknown	unknown	unknown	unknown

Table 18 describes the Server tab fields.

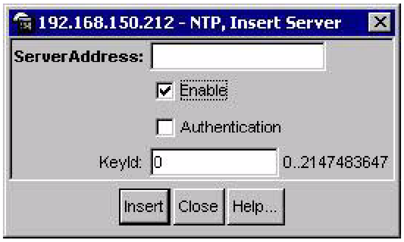
Table 18 Server tab fields

Field	**Description**
ServerAddress	Specifies the IP address of the remote NTP server.
Enable	Enables or disables the remote NTP server.
Authentication	Enables or disable MD5 authentication on this NTP server. MD5 produces a message digest of the key. MD5 verifies the integrity of the communication, authenticates the origin, and checks for timeliness. The default is no MD5 authentication.
KeyId	Displays the key id used to generate the MD5 digest for this NTP server. You must specify a number between 1 and 214743647. The default is 0, which indicates that authentication is disabled.
AccessAttempts	Displays the number of NTP requests sent to this NTP server.
AccessSuccess	Displays the number of times this NTP server was selected to update the time.
AccessFailure	Displays the number of times this NTP server was rejected from updating the time.
Stratum	This is the Stratum of the server.
Version	This field is the NTP version of the server.
RootDelay	This is the Root Delay of the server.
Precision	This is the NTP precision of the server in seconds.
Reachable	This is the NTP reach ability of the server.
Synchronized	This is the status of synchronization with the server.

3 Click Insert.

The NTP, Insert Server dialog box opens (Figure 68).

Figure 68 NTP, Insert Server dialog box



192.168.150.212 - NTP, Insert Server

ServerAddress:

☑ Enable

□ Authentication

KeyId: 0 0..2147483647

4 Specify the IP address of the NTP server.

5 Click Insert.

The IP address of the NTP server that you configured is displayed in the Server tab of the NTP dialog box.

Table 19 describes the NTP, Insert Server dialog box dialog box fields.

Table 19 NTP, Insert Server dialog box fields

Field	**Description**
ServerAddress	The IP address of the remote NTP server.
Enable	Enables or disables the remote NTP server.
Authentication	Enables or disables MD5 authentication on this server. If you enable authentication on a server but do not specify a value for the public key, the server is assumed disabled. The default is no MD5 authentication.
KeyId	Specifies the key id used to generate the MD5 digest for this server. By default, the key ID is 0, which indicates that MD5 authentication is disabled.

Assigning a NTP key

If you enable MD5 authentication on the server, you must assign an NTP key.

To assign an NTP key:

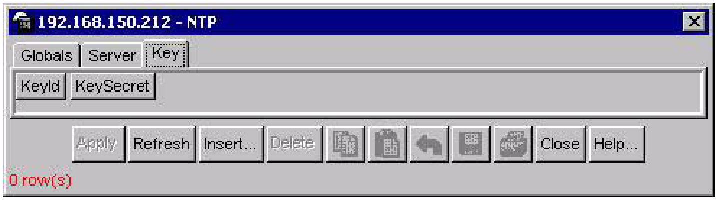
1 From the Device Manager menu bar, select Edit > NTP.

The NTP dialog box opens with the Global tab displayed (Figure 66).

2 Click the Key tab.

The Key tab opens (Figure 69).

Figure 69 NTP dialog box—Key tab



192.168.150.212 - NTP

0 row(s)

Table 20 describes Key tab fields.

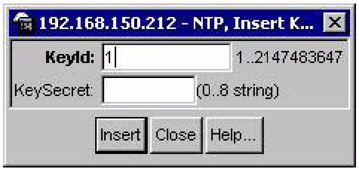
Table 20 Key tab fields

Field	**Description**
KeyId	This field is the key id used to generate the MD5 digest. You must specify a value between 1 and 214743647. The default value is 0, which indicates that authentication is disabled.
KeySecret	This field is the MD5 key used to generate the MD5 Digest. You must specify an alphanumeric string between 0 and 8. **Note:** You cannot specify an “#” as a value in the KeySecret field. The NTP server interprets the “#” as the beginning of a comment and truncates all text entered after the “#”. This is a limitation of xntpd version 3 or lower.

3 Click Insert.

The NTP, Insert Key dialog box opens (Figure 70).

Figure 70 NTP, Insert Key dialog box



192.168.150.212 - NTP, Insert K...

KeyId: 1 1..2147483647

KeySecret: (0..8 string)

Table 21 describes the fields in the NTP, Insert Key dialog box.

Table 21 NTP, Insert Key dialog box fields

Field	Description
KeyId	The key id used to generate the MD5 digest for this NTP server. You must specify a value between 1and 214743647. The default value is 0, which indicates that authentication is disabled.
KeySecret	The MD5 key ID used to generate the MD5 digest for this NTP server. **Note:** You cannot specify an "#" as a value in the KeySecret field. The NTP server interprets the "#" as the beginning of a comment and truncates all text entered after the "#". This is a limitation of xntpd version 3 or lower.

4 Click Insert.

The values that you specified for the key id and the MD5 key id are displayed in the Key tab of the NTP dialog box.

Chapter 10
CLI command logging

This chapter describes how to configure the CLI command logging feature using CLI.

This section includes the following topics:

- "Roadmap of CLI logging commands," next
- "Configuration commands" on page 190
- "Show commands" on page 193
- "Save command" on page 194

Roadmap of CLI logging commands

The following roadmap lists the commands used for enabling CLI command logging.

Command	Parameter

`config cli clilog enable`	`<true>`
	`<false>`

`config cli clilog maxfilesize`	`<value>`
`config cli clilog info`	
`show cli clilog info`	

Command	Parameter

`show clilog file`	`<tail>`
	`grep <text to be grepped>`

`save clilog file`	`<value>`

Configuration commands

This section includes configuration commands for the following topics:

- "Enabling CLI logging," next
- "Setting the maximum allowable file size for the clilog.txt file in PCMCIA" on page 191
- "Info command output on config clilog" on page 192

Enabling CLI logging

To enable CLI logging on the switch, enter the following command:

```
config cli clilog enable <true/false>
```

This command includes the following options:

config cli clilog enable followed by:	
<true>	Enables CLI command logging.
<false>	Disables CLI command logging.

Figure 71 shows sample output for the **config cli clilog enable** command.

Figure 71 config cli clilog enable <true/false> command output

```
Passport-8610:5/config/cli/clilog# enable true
Passport-8610:5/config/cli/clilog# info

Sub-Context:
Current Context:

                    enable : TRUE
               maxfilesize : 500
```

Setting the maximum allowable file size for the clilog.txt file in PCMCIA

To configure the maximum allowable file size for the clilog.txt file, enter the following command:

config cli clilog maxfilesize *<value>*

This command includes the following options:

config cli clilog maxfilesize followed by:	
<value>	The maximum allowable file size in KBs for the clilog.txt file in the PCMCIA. The minimum configurable value is 64KB and the maximm configurable value is 256MB. The default value is 256KB. **Note:** You can configure maxFileSize value of the clilog.txt file below the previously configured value. In this situation, if the filesize has already become bigger than the newly configured value, the clilog.txt file will start wrapping at the present size. Similar behaviour can be observed on failover scenarios, if the clilog.txt file exceeds the configured maxFileSize while failing over.

Figure 72 shows sample output for the **config cli clilog maxfilesize** command.

Figure 72 config cli clilog maxfilesize command output

```
Passport-8610:5/config/cli/clilog# maxfilesize 500
Passport-8610:5/config/cli/clilog# info

Sub-Context:
Current Context:

                      enable : TRUE
                 maxfilesize : 500
```

Note: If a secondary CPU is present in the chassis, the configuration commands take effect in the secondary CPU as well, when they are executed from the primary. While inserting a secondary CPU, the status of the clilog feature is checked and if the feature is enabled in the primary, the secondary takes the values of the global parameters from the primary CPU. However, the primary CPU and the secondary CPU work as separate CLI logging mechanisms, logging the commands independently on the primary and secondary PCMCIAs.

Info command output on config clilog

To view the clilog command settings, enter the following command:

`config cli clilog info`

Figure 73 shows sample output for the **`config cli clilog info`** command.

Figure 73 config cli clilog info command output

```
Passport-8610:5/config/cli/clilog# info

Sub-Context:
Current Context:

                      enable : TRUE
                 maxfilesize : 500
```

Show commands

This section includes show commands for the following topics:

- "clilog global info show," next
- "Command for viewing the decrypted log" on page 193

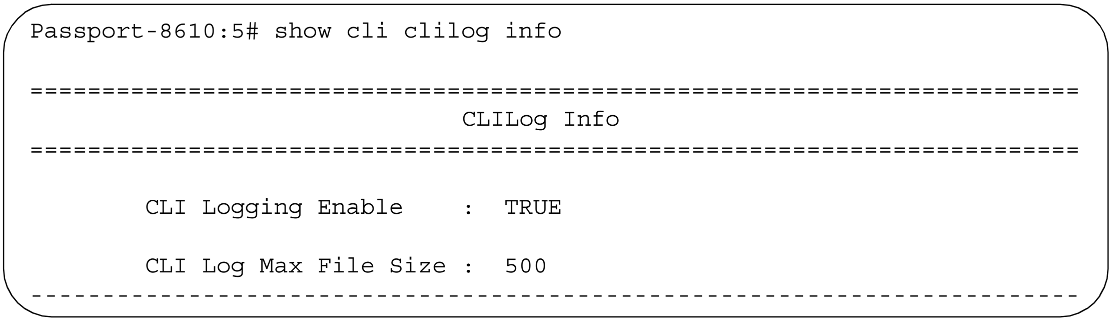
clilog global info show

To display status of the clilog global parameters, enter the following command:

show cli clilog info

Figure 74 shows sample output for the **show cli clilog info** command.

Figure 74 show cli clilog info command output



```
Passport-8610:5# show cli clilog info

==========================================================================
                              CLILog Info
==========================================================================

        CLI Logging Enable    :  TRUE

        CLI Log Max File Size :  500
--------------------------------------------------------------------------
```

Command for viewing the decrypted log

To decrypt the clilog.txt file in the PCMCIA and display the log in a user readable form, enter the following command:

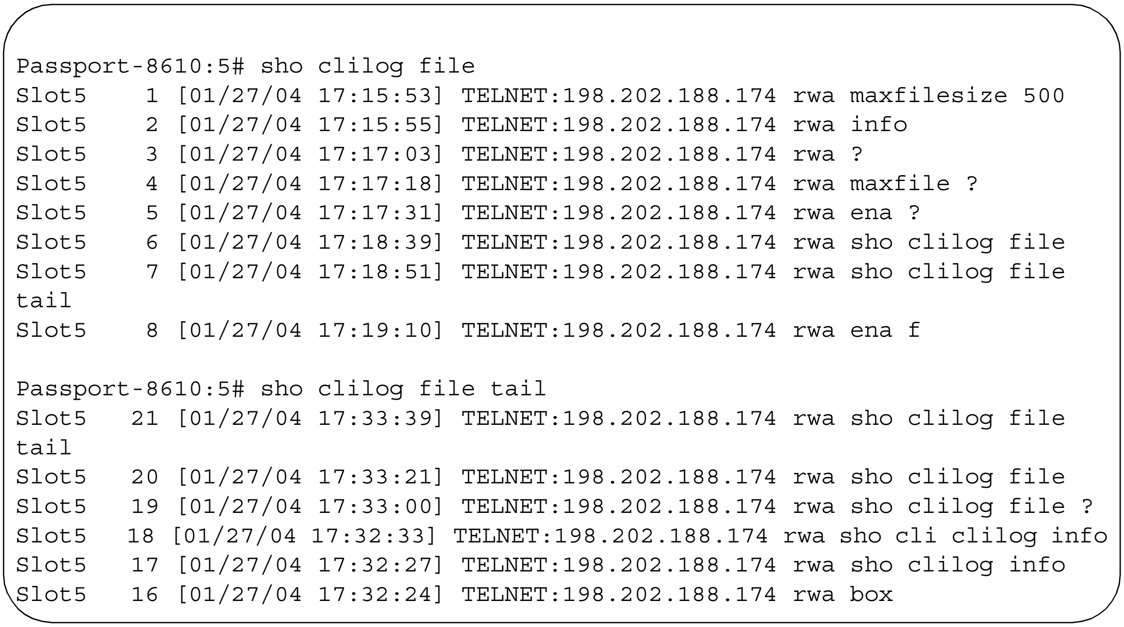
show clilog file

This command includes the following options:

show clilog file followed by:	
<tail>	Displays the log file from the bottom.
grep *<text to be grepped>*	Enables you to grep on the text specified and displays only the logs matching the text.

Figure 75 shows sample output for the **show clilog file <tail> grep <text to be grepped>** command.

Figure 75 show clilog file command output



```
Passport-8610:5# sho clilog file
Slot5    1 [01/27/04 17:15:53] TELNET:198.202.188.174 rwa maxfilesize 500
Slot5    2 [01/27/04 17:15:55] TELNET:198.202.188.174 rwa info
Slot5    3 [01/27/04 17:17:03] TELNET:198.202.188.174 rwa ?
Slot5    4 [01/27/04 17:17:18] TELNET:198.202.188.174 rwa maxfile ?
Slot5    5 [01/27/04 17:17:31] TELNET:198.202.188.174 rwa ena ?
Slot5    6 [01/27/04 17:18:39] TELNET:198.202.188.174 rwa sho clilog file
Slot5    7 [01/27/04 17:18:51] TELNET:198.202.188.174 rwa sho clilog file
tail
Slot5    8 [01/27/04 17:19:10] TELNET:198.202.188.174 rwa ena f

Passport-8610:5# sho clilog file tail
Slot5   21 [01/27/04 17:33:39] TELNET:198.202.188.174 rwa sho clilog file
tail
Slot5   20 [01/27/04 17:33:21] TELNET:198.202.188.174 rwa sho clilog file
Slot5   19 [01/27/04 17:33:00] TELNET:198.202.188.174 rwa sho clilog file ?
Slot5   18 [01/27/04 17:32:33] TELNET:198.202.188.174 rwa sho cli clilog info
Slot5   17 [01/27/04 17:32:27] TELNET:198.202.188.174 rwa sho clilog info
Slot5   16 [01/27/04 17:32:24] TELNET:198.202.188.174 rwa box
```

Save command

To save the decrypted log file into a device (PCMCIA, Flash or tftp server), enter the following command:

save clilog file *<value>*

This command includes the following options:

save clilog file followed by:	
<value>	Specifies the destination file. The destination can be flash, PCMCIA or a remote tftp server.

Figure 76 shows sample output for the **save clilog file** command.

Figure 76 save clilog file command output

```
Passport-8610:5# save clilog file /flash/clilog.txt
```

Chapter 11
DNS Client

Every equipment interface connected to a TCP/IP network is identified with a unique IP address. A name can be assigned to every machine having an IP address. The TCP/IP protocol does not require the usage of names, but these names make the task easier for network managers:

- An IP client can contact a machine with its name, the name being converted to an IP address, based on a mapping table. All applications using this specific machine are not dependant anymore on the addressing scheme. The IP addressing scheme of the servers can be modified (moving, network modification ….) without any disruption of the clients.
- It is easier to remember a name than a full IP address.

Two methods are used to establish the mapping between an IP name and an IP address:

- “/etc/hosts” file. This file gives the mapping between names and IP addresses.
- DNS (Domain Name Service). It is a hierarchical database that can be distributed on several servers (for backup and load sharing). When a new Hostname is added, the network administrator updates this database. At this time, the information is sent to all the different hosts: an IP client which resolves the mapping between the Hostname and the IP address sends a request to one of the database servers, to do the name resolution.

Mapping of IP name and IP address modifies the application to use a hostname instead of IP address. The hostname is converted to IP address by the switch.

- Local database file (/etc/hosts) file is queried to translate the hostname to IP address. The file can be stored in flash or in PCMCIA. Flash is queried first. This file should be in the same format as that of UNIX.

The form for each entry is:

```
<internet address>    <official hostname> <aliases>
```

The application looks for the entry in this file for translating the hostname to IP address.

- If the entry for translating the hostname to IP address is not found in the host file, the switch queries the configured DNS server for the mapping from hostname to IP address. You can configure up to 3 different DNS servers – Primary, Secondary and Tertiary. First Primary Server is queried, then secondary and finally tertiary server will be queried.

Ping, Telnet, and Copy applications are modified. You can either enter a hostname or an IP address for invoking Ping, Telnet, and Copy applications.

Note: The DNS query to remote host will NOT be done if the application is invoked from boot monitor. Only /etc/hosts file lookup is done for translating the hostname to IP address when invoked from boot monitor.

In non-HA mode, user can configure separate DNS server for master and slave CPUs. In HA mode, user can configure DNS server only from master CPU.

A log/debug will be generated for all the DNS requests send to DNS servers and all successful DNS responses received from the DNS servers.

This section includes the following topics:

- "Roadmap of DNS client commands," next
- "Configuration commands" on page 199
- "Show commands" on page 201

Roadmap of DNS client commands

The following roadmap lists the commands used for enabling DNS client feature.

Command	Parameter
`config sys dns`	`primary-create <ip address>`
	`secondary-create <ip address>`
	`tertiary- create <IP address>`
	`delete < primary | secondary | tertiary>`
	`domain-name <string>`
	`info`
`show sys dns`	
`show host <ipaddress/hostname>`	

Configuration commands

This section includes configuration commands for the following topics:

- “Configuring DNS client,” next
- “Info command output on conf sys dns” on page 201

Configuring DNS client

To enable DNS client on the switch, enter the following command:

```
config sys dns
```

This command includes the following options:

config sys dns followed by:	
primary-create <ip address>	Sets the primary DNS server IP address.
secondary-create <ip address>	Sets the secondary DNS server IP address.
tertiary- create <IP address>	Set the tertiary DNS server IP address.
delete < primary | secondary | tertiary>	Deletes specified primary/secondary/tertiary DNS server IP address.
domain-name <string>	Set the default domain name.
info	Displays the list of dns servers, with the status (active/non active).

Figure 77 shows sample output for the config sys dns command.

Figure 77 config sys dns create command output

```
Passport-8603:3# conf sys dns
Passport-8603:3/config/sys/dns# primary-create 198.202.188.134
Passport-8603:3/config/sys/dns# secondary-create 10.10.10.10
Passport-8603:3/config/sys/dns# tertiary-create 198.202.188.174
Passport-8603:3/config/sys/dns# info
        DNS Default Domain Name :
        Primary DNS server details:
        ===========================
                 IP address : 198.202.188.134
                 Status     : active
        Secondary DNS server details:
        ===========================
                 IP address : 10.10.10.10
                 Status     : Inactive
        Tertiary DNS server details:
        ===========================
                 IP address : 198.202.188.174
                 Status     : active
```

Info command output on conf sys dns

To view the config sys dns command settings, enter the following command:

`config sys dns info`

Figure 78 shows sample output for the config sys dns info command.

Figure 78 config sys dns info command output

```
Passport-8603:3/config/sys/dns# info
        DNS Default Domain Name :
        Primary DNS server details:
        ===========================
                 IP address : 198.202.188.134
                 Status     : active
        Secondary DNS server details:
        ===========================
                 IP address : 10.10.10.10
                 Status     : Inactive
        Tertiary DNS server details:
        ===========================
                 IP address : 198.202.188.174
                 Status     : active
```

Show commands

This section includes show commands for the following topics:

- "show sys dns," next
- "show host <ipaddress/hostname>" on page 202

show sys dns

To display system dns status, enter the following command:

`show sys dns`

This command displays the DNS configurations, DNS server status (active/ inactive), number of DNS request send to each server and the number of Successful response received from each server.

Figure 79 shows sample output for the show sys dns command.

Figure 79 show sys dns command output

```
Passport-8603:3# show sys dns
        DNS Default Domain Name :
        Primary DNS server details:
        ===========================
                 IP address : 198.202.188.134
                 Status     : active
                 Total DNS Number of request made to this server : 1
                 Number of Successful DNS : 1
        Secondary DNS server details:
        ===========================
                 IP address : 10.10.10.10
                 Status     : Inactive
                 Total DNS Number of request made to this server : 0
                 Number of Successful DNS : 0
        Tertiary DNS server details:
        ===========================
                 IP address : 198.202.188.174
                 Status     : active
                 Total DNS Number of request made to this server : 0
                 Number of Successful DNS : 0
```

show host <ipaddress/hostname>

To get the DNS host information, enter the following command:

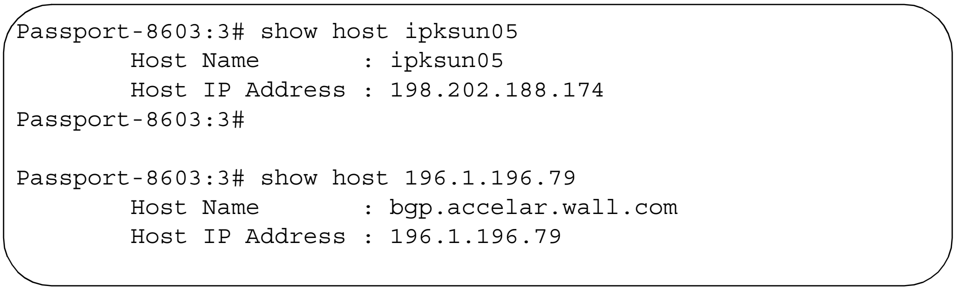
show host *<ipaddress/hostname>*

where
<ipaddress> is the ip address of the host dns server, and
<hostname> is the name of the host dns server.

You can enter either a hostname or an IP address. If you enter the hostname, this command will get the IP address corresponding to the hostname and if you enter an IP address, this command gets the hostname for the IP address.

Figure 80 shows sample output for the show host command.

Figure 80 show host ipksun05 command output



```
Passport-8603:3# show host ipksun05
        Host Name       : ipksun05
        Host IP Address : 198.202.188.174
Passport-8603:3#

Passport-8603:3# show host 196.1.196.79
        Host Name       : bgp.accelar.wall.com
        Host IP Address : 196.1.196.79
```

Appendix A
Port numbering and MAC address assignment

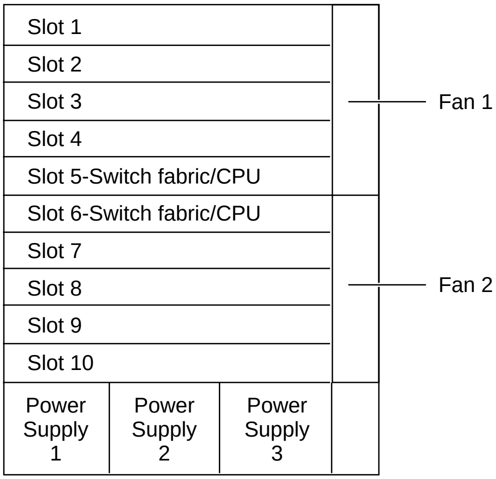
This appendix includes information about the following topics:

- "Port numbering," next
- "Interface indexes" on page 206
- "MAC address assignment" on page 207

Port numbering

A port number includes the slot location of the module in the chassis, as well as the port's position in the I/O module. In the Passport 8000 Series switches, slots are numbered from top to bottom. Figure 81 shows slot numbering for an 8010 chassis.

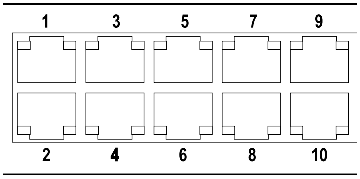
Figure 81 8010 chassis slots



9539EA

Ports are numbered generally from left to right beginning with 1 for the far left port. On high-density modules with two rows of ports, such as the 8648TX module, ports in the top row are assigned sequential odd numbers, and ports in the bottom row are assigned sequential even numbers (Figure 82).

Figure 82 Port numbers on high-density modules



9494EA

Interface indexes

Interface indexes are used in SNMP to identify ports, VLANs, and Multi-Link Trunks.

The interface index of a port is computed using the following formula:

inIndex = (64 x slot number) + (port number – 1)

where:

Slot number is a value between 1 and 10, inclusive.

Port number is a value between 1 and 48, inclusive.

For example, the interface index of port 1/1 is 64, and the interface index of port 10/48 is 687.

The interface index of a VLAN is computed using the following formula:

ifIndex = 2048 + VLAN’s MGID

where:

MGID is the multicast group ID number.

Because the default VLAN always has an MGID value of 1, its interface index is always 2049.

The interface index of a Multi-Link Trunk (MLT) is computed using the following formula:

ifIndex = 4096 + MLT ID number

MAC address assignment

Understanding how MAC addresses are assigned is important when you define static ARP entries for IP addresses in the switch and when you use a network analyzer to decode network traffic.

Each [Model #] module is assigned a base of 1024 MAC addresses. Within the switch, these MAC addresses are assigned as follows:

- 512 addresses for ports in the switch (physical MAC addresses)
- 500 addresses for VLANs in the switch (virtual MAC addresses)
- 8 addresses for CPU interfaces
- 4 addresses for use by other Passport 8000 Series modules

A MAC address has the format shown in Figure 83.

Figure 83 Parts of a MAC address

```
47                   24 23        10 9 8        0
| -------------------- | ---------- | | ------- |
```

The MAC address is divided into the following parts:

- Bits 47–24: IEEE OUI (for example, 00-80-2d)
- Bits 23–10: Chassis ID

- Bit 9: Type of MAC address in the switch:
  - 0 = Port address (physical MAC address)
  - 1 = VLAN address (virtual MAC address)
- Bits 8–0: Unique port or VLAN address

Physical MAC addresses

Physical MAC addresses are addresses assigned to the physical interfaces or ports visible on the device. The physical MAC addresses are used in the following types of frames:

- Spanning Tree Protocol BPDUs sent by the switch
- Frames to or from an isolated routing port’s physical interface

BPDUs are sent using the physical MAC address as the source because identifying which physical port sent the BPDU is critical to how the Spanning Tree Protocol works.

The ports on the switch fabric/CPU module have the following last bytes:

- Management port in slot 5: 0xf4
- CPU port (an internal port) in slot 5: 0xf5
- Management port in slot 6: 0xf6
- CPU port in slot 6: 0xf7

Virtual MAC addresses

Virtual MAC addresses are the addresses assigned to VLANs. A virtual MAC address is assigned to a VLAN when it is created. The MAC address for a VLAN IP address is the virtual MAC address assigned to the VLAN.

Index