Part No. 313189-C Rev 00
April 2003

4655 Great America Parkway
Santa Clara, CA 950540

Getting Started

Passport 8000 Series Software Release 3.5

NORTEL NETWORKS™

Copyright © 2003 Nortel Networks

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks Inc.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

Trademarks

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

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

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

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 MERCHANTABILITY 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

Figures

Tables

Preface

The Nortel Networks* Passport* 8000 Series switch is a flexible and multifunctional switch that supports a wide range of network architectures and protocols. This guide provides procedures for setting up and starting the Passport 8000 Series switch.

Before you begin

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

- Basic knowledge of networks, Ethernet bridging, and IP and IPX routing
- Familiarity with networking concepts and terminology
- Basic knowledge of network topologies
- 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`.
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:

BootP	Bootstrap Protocol
FTP	File Transfer Protocol
IP	Internet Protocol
MAC	media access control
MAU	media access unit
MDI-X	medium dependent interface crossover
NBMA	nonbroadcast multi-access
OSPF	Open Shortest Path First
PPP	Point-to-Point Protocol
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TELNET	Network Virtual Terminal 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
Setting up the switch

This chapter describes how to connect a terminal and modem to the switch, log on to the switch software, configure the switch using the Setup Utility, reboot the switch using the command line interface (CLI), and perform basic tasks. It includes the following topics:

The Passport 8000 Series switch supports two CLIs:

- Boot Monitor CLI
- Run-Time CLI

The Boot Monitor CLI allows you to configure and manage the boot process. You 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 only through a console session. Within the Boot Monitor CLI, you can change the boot configuration, including boot choices and boot flags.

You access the Run-Time CLI through a direct serial-port connection to the switch or through a Telnet, SSH or rlogin session (if the flags for Telnet and rlogin are set to allow remote access). Passport 8000 Series modules support one CLI session at the console serial port or up to eight Telnet/SSH sessions. You can open a Telnet session from Device Manager by clicking on the Telnet button on the toolbar or choosing Device > Telnet from the menu bar.

For more information about the Boot Monitor and Run-Time CLIs, see *Managing Platform Operations and Using Diagnostic Tools*. For more information about Device Manager, see *Installing and Using Device Manager.*

You can use any terminal or personal computer (PC) with a terminal emulator as the CLI console station. For instructions to connect the computer or terminal, see the next section, “Connecting a terminal.”

Connecting a terminal

The serial console interface is an RS-232 port that enables a connection to a PC or terminal for monitoring and configuring the switch. The port is implemented as a DB-9 connector that can operate as either data terminal equipment (DTE) or data communication equipment (DCE). The default communication protocol settings for the Console port are:

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

To use the Console port, you need the following equipment:

- A terminal or TTY-compatible terminal, or a portable computer with a serial port and terminal-emulation software
- A UL-listed straight-through RS-232 cable with a female DB-9 connector for the Console port on the switch

  The other end of the cable must have a connector appropriate to the serial port on your computer or terminal. (Most computers or terminals use a male DB-25 connector.)

  Any cable connected to the Console port must be shielded to comply with emissions regulations and requirements.

To connect a computer or terminal to the Console port:

1. Set the terminal protocol as follows:
   - 9600 baud
   - 8 data bits
   - 1 stop bit
   - No parity
2. Connect the RS-232 cable to the Console port.
3. Connect the other end of the cable to the terminal or computer serial port.
4. Turn on the terminal.
5. Log on to the CLI (see "Logging on to the system" on page 20).

Connecting a modem

You can access the CLI through a modem connection to the Passport 8690SF module or the Passport 8190SM module. This section describes how to connect a modem to the Modem port on the module.

To set up modem access, you need a DTE-to-DCE cable (straight or transmit cable) to connect the Passport 8000 Series switch to the modem. Table 1 shows the DTE-to-DCE pin assignments.

Table 1 DTE-to-DCE straight-through pin assignments

Signal	Switch	Modem	
	Pin number	DCE DB-9 pin number	DCE DB-25 pin number
RXD	2	2	3
TXD	3	3	2
DTR	4	4	20
GND	5	5	7
DSR	6	6	6
RTS	7	7	4
CTS	8	8	5

The Modem port is a data terminal equipment (DTE) device operating at 9600 baud, 8 data bits, no parity, and one stop bit. Because the Modem port expects to receive Data Set Ready (DSR) and Clear To Send (CTS) signals before transmitting, these control lines are required in the cables. The Modem port does not support any inbound flow control; that is, the port does not toggle control lines to indicate the input buffer is full.

To connect a modem to a Passport 8000 Series switch you may need to set up the Modem port first using another type of connection to the CLI.

Note: Nortel Networks recommends that you use the default settings for the Modem port for most modem installations.

To set up the Modem port:

1. In the Run-Time CLI, enter the following command:

   ```
   config bootconfig sio modem
   ```

   Now you can enter options for this command level without retyping the first part of the command.

2. Use the following commands to set port parameters, based on the requirements of the modem:

- **baud <*rate*>**

  where *rate* is the baud rate for the modem. The default is 9600.

- **8databits <true|false>**

  where:

  false sets the number of data bits per byte to 8. This setting is the default.

  true sets the number of data bits per byte to 7.

- **mode <ascii|slip|ppp>**

  where:

  ascii is the default setting. This setting is recommended for most modem connections.

  slip sets the port for serial line IP (SLIP) operation.

  ppp sets the port for point-to-point protocol (PPP) operation.

For information about the configuration requirements of your modem, refer to the documentation that was shipped with the modem.

Caution: Nortel Networks recommends that you not set the Modem port for SLIP or PPP operation unless you are already thoroughly familiar with the operation of these protocols.

3 If you set the port mode to slip, use the following commands to set other SLIP parameters:

- **slip-compression <true|false>** to enable or disable TCP/IP header compression. The default is false.
- **slip-rx-compression <true|false>** to enable or disable TCP/IP header compression on the receive packet. The default is false.

4 If you set the port mode to ppp, use the following commands to set other PPP parameters:

- **mtu <*bytes*>** to set the maximum transmission unit for the point-to-point link. The default is zero (0).
- **my-ip <*ipaddr*>** to set the near-end IP address on the point-to-point link. The default is 0.0.0.0.

- **peer-ip <*ipaddr*>** to set the peer IP address on the point-to-point link. The default is 0.0.0.0.
- **pppfile <*file*>** to identify the file to use for PPP initialization parameters.

5 On the modem, turn off echo mode and return code messaging.

6 Connect the modem to the modem port using a cable with the connector described in Table 1.

Logging on to the system

The basic switch configuration procedures in this chapter use the Run-Time CLI. When the switch completes its boot sequence, the login prompt appears. The default values for login and password for the console and Telnet sessions are shown in Table 2.

Table 2 Access levels and default login values

Access level	Description	Default login	Default password
Read-only	Allows only viewing configuration and status information. Is equivalent to SNMP read-only community access.	ro	ro
Layer 1read/write	Allows viewing most switch configuration and status information and changing physical port settings.	l1	l1
Layer 2 read/write	Allows viewing and changing configuration and status information for layer 2 (bridging/switching) functions.	l2	l2
Layer 3 read/write (8600 switches only)	Allows viewing and changing configuration and status information for layer 2 and layer 3 (routing) functions.	l3	l3

Table 2 Access levels and default login values

Access level	Description	Default login	Default password
Read/write	Allows viewing and changing configuration and status information across the switch; does not allow changing security and password settings. Is equivalent to SNMP read-write community access.	rw	rw
Read/write/all	Allows all the rights of Read-Write access *and* the ability to change security settings, including the CLI and Web-based management user names and passwords and the SNMP community strings.	rwa	rwa

Modifying the CLI login and passwords

If you have read/write/all access permission, you can modify the CLI login and passwords using the **`config cli password`** command. You can also change the CLI login and passwords using Device Manager. For complete instructions on changing the CLI login and password using the CLI or Device Manager, see *Configuring and Managing Security.*

Configuring the switch with the Setup Utility

To enhance the functionality of 8000 Series switches, Nortel Networks offers a growing list of hardware modules. Since the latest modules have advanced features, they work in certain operation modes that earlier modules do not support. The Setup Utility monitors system requirements and obtains the highest system performance.

The Setup Utility helps you configure your switch by asking you a series of questions. Then it saves the information in the boot and runtime configuration files. This ensures that your switch reboots in the desired operating mode. The Setup Utility also displays error and warning messages to advise you of the ramifications of certain hardware and software configurations.

This section describes how to use the Setup Utility to configure the boot and runtime configuration files. For detailed information about the supported operating modes, see *Managing Platform Operations and Using Diagnostic Tools*.

Running the Setup Utility

The Setup Utility prompts you through the configuration process by asking a series of questions. Answer each question or accept the default by pressing Enter. Each question shows the default in brackets and the acceptable parameter options in parenthesis. For more information about the individual prompts, see Table 3 on page 26.

To start and use the 8000 Series Setup Utility, enter the following command:

```
install
```

Note: After running the Setup Utility, remember to reboot the switch. See the following section, “Rebooting or resetting the switch,” for instructions.

Configuration example

This configuration example shows sample output from the setup utility. In this example, the defaults have been accepted.

```
8610:6# install
######################################################################
Welcome to the Passport 8000 setup utility. You are about to
configure initial configuration of the switch. Part of the data
will be stored in the file /flash/boot.cfg and part will be stored
in runtime configuration file. Please reboot the switch after
initial configuration.

Several of these commands do not require a reboot and can be
applied dynamically through CLI.
######################################################################
Do you want to continue (y/n)?
######################################################################
System Parameters
######################################################################
Please provide primary config-file path [/flash/factorydef.cfg]:
Please provide primary image-file path [p80a.img]:
Please add system prompt [8610]:
Please select CPU Master slot (5/6) [5]:
Master CPU mgmt port: autonegotiation [n] (y/n) ?
speed (10/100) [10]:
Do you want to enable automatic savetostandby mode [n] (y/n) ?
Do you want to enable m-mode support [n] (y/n) ?
Do you want to enable enhanced operation mode support [n] (y/n) ?
Do you want to enable CPU High Availability mode [n] (y/n) ?
#
1 - Primary configuration file path (/flash/dvmrp_pol.cfg)->/flash/
dvmrp_pol.cfg
2 - Primary image file path (134.177.160.114:/home/username/images/
test128k_4.img)->134.177.160.114:/home/username/images/
test128k_4.img
3 - CLI prompt (8610)->8610
4 - Master CPU selection (5)->5
5 - Master CPU Mgmt port autonegotiation (true)->false
6 - Master CPU Mgmt port speed (10)->10
7 - Automatic save to Standby (false)->false
8 - Support for M-mode (false)->false
9 - Support for enhanced operation mode (false)->false
10- High Availability mode
#
Please type the line-number you want to change
OR "0" to save & quit at this stage
```

```
OR hit return to continue [-1]:
Syncing autoneg
HA-CPU change will be applied at the end of this session only if you
choose to
save configuration
########################################################################
System Services
########################################################################
#
Do you want to enable FTP [n] (y/n) ?
Do you want to enable RLOGIN [n] (y/n) ?
Do you want to enable TELNET [n] (y/n) ?
Do you want to enable TFTP [n] (y/n) ?
Do you want to enable WEB server service [n] (y/n) ?
#
1 - FTP server service (false)->false
2 - RLOGIN server service (false)->falseservice (false 3 - TELNET
server service (true)->false
4 - TFTP server service (false)->false
5 - WEB server service (true)->false
#
Please type the line-number you want to change
OR "0" to save & quit at this stage
OR hit return to continue [-1]:
########################################################################
IP Network connectivity
########################################################################
IP Address for mgmt port in first CPU Slot [0.0.0.0/0.0.0.0]:
IP Address for mgmt port in second CPU Slot [10.10.43.98/
255.255.255.0]:
IP Address for mgmt-virtual-ip [0.0.0.0/0.0.0.0]:
First net mgmt route [134.177.160.0:10.10.43.1]:
Second net mgmt route [0.0.0.0:0.0.0.0]:
Third net mgmt route [0.0.0.0:0.0.0.0]:
Fourth net mgmt route [0.0.0.0:0.0.0.0]:
IP address of the default VLAN [0.0.0.0/0.0.0.0]:
#
1 - Management port Ip Address for first CPU slot (0.0.0.0/
0.0.0.0)->0.0.0.0/0.0.0.0
2 - Management port Ip Address for second CPU slot (10.10.43.98/
255.255.255.0)->10.10.43.98/255.255.255.0
3 - Virtual management port Ip Address (0.0.0.0/0.0.0.0)->0.0.0.0/
0.0.0.0
4 - First static route for management port
(134.177.160.0:10.10.43.1)->134.177.160.0:10.10.43.1
5 - Second static route for management port
(0.0.0.0:0.0.0.0)->0.0.0.0:0.0.0.0
6 - Third static route for management port
```

```
(0.0.0.0:0.0.0.0)->0.0.0.0:0.0.0.0
7 - Fourth static route for management port
(0.0.0.0:0.0.0.0)->0.0.0.0:0.0.0.0
8 - IP address of the default VLAN (0.0.0.0/0.0.0.0)->0.0.0.0/
0.0.0.0
#
Please type the line-number you want to change
OR "0" to save & quit at this stage
OR hit return to continue [-1]:
Do you want to save the changes
[Saving the parameters will update the files /flash/boot.cfg and /
flash/dvmrp_pol.cfg] (y/n) ?
########################################################################
```

Table 3 Setup utility prompt descriptions

Prompt	Description/Action
`Please provide primary config-file path [/flash/ factorydef.cfg]:.`	**Description:** Indicates the name of the primary configuration file. **Action:** Press Enter to accept the default, /flash/ factorydef.cfg, or enter a different file name for the primary configuration file. Specifying the path to the file is optional.
`Please provide primary image-file path [p80a.img]:`	**Description:** Indicates the name of the primary image file. **Action:** Press Enter to accept the default, p80a.img, or enter a different file name for the primary image file. Specifying the path to the file is optional.
`Please add system prompt [8610]:`	**Description:** Specifies the text for the prompt. **Action:** Press Enter to accept the default 8610, or enter a different string, up to 20 characters.
`Please select CPU Master slot (5/6) [5]:`	**Description:** Indicates the slot number of the master CPU. **Action:** Press Enter to accept the default, 5, or specify 6 for the master CPU slot.
`Master CPU mgmt port: autonegotiation [n] (y/n) ?`	**Description:** Specifies whether you want the master CPU management port to use autonegotiation. **Action:** Enter **n** to accept the default, no, or enter **y** to indicate that you want the master CPU management port to use autonegotiation.
`speed (10/100) [10]:`	**Description:** Specifies the line speed in Mbps. **Action**: Press Enter to accept the default, 10 Mbps, or specify 100 Mbps.
`Do you want to enable automatic savetostandby mode [n] (y/n) ?`	**Description:** Specifies whether you want the boot and runtime configuration files to be saved on the backup CPU. **Action:** Enter **y** if you want the boot and runtime configuration files to be saved on the backup CPU. Accept the default, **n**, if you want the boot and runtime configuration files to be saved on the primary CPU.
`Do you want to enable m-mode support [n] (y/n) ?`	**Description:** Specifies whether you want the chassis to run in 128K mode. To run in 128K mode, the CPU module must be an 8691 or higher and the switch must have at least one 8600 module (128K module). For more information about enabling M mode support, see *Managing Platform Operations and Using Diagnostic Tools*. **Note:** If you enable m-mode support and you have a mixed configuration of modules, the E-modules and legacy modules will be disabled. **Action:** Enter **y** if you want the chassis to run in 128K M mode. Accept the default, **n**, if you want it to run in 32K mode only.

Prompt	Description/Action
`Do you want to enable enhanced operation mode support [n] (y/n) ?`	**Description:** Specifies whether you want to enable enhanced operation mode. Enhanced operation mode increases the maximum number of VLANs when using MLT (1980) and SMLT (989). This mode requires 8600 E- or M-modules. For more information about enabling enhanced operational mode, see *Managing Platform Operations and Using Diagnostic Tools*. **Note:** If you enable enhanced operation mode and you have a mixed configuration of modules, the legacy modules (non E- and non M-modules) will be disabled. **Action:** Enter **y** is you want to enable enhanced operation mode. Accept the default, **n**, if you do not want to enable enhanced operation mode.
`Do you want to enable CPU High Availability mode [n] (y/n) ?`	**Description:** Specifies whether you want to enable CPU-high availability (HA) mode. CPU 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, meaning that the CPUs are compatible and configured in the same mode. For more information about high-availability mode, see *Managing Platform Operations and Using Diagnostic Tools.* **Action:** Specify **y** is you want to enable CPU high availability (HA) mode. Accept the default, **n**, if you do not want to enable it.
`Do you want to enable FTP [n] (y/n) ?`	**Description:** Specifies whether you want users to access the switch using FTP. **Action:** Enter **y** if you want to enable FTP for remote users. Accept the default, **n**, if you do not want to enable FTP.
`Do you want to enable RLOGIN [n] (y/n) ?`	**Description:** Specifies whether you want users to access the switch using rlogin **Action:** Enter **y** if you want to enable rlogin for remote users. Accept the default, **n**, if you do not want to enable rlogin.
`Do you want to enable TELNET [n] (y/n) ?`	**Description:** Specifies whether you want users to access the switch using Telnet. **Action:** Enter **y** if you want to enable Telnet. Accept the default, **n**, if you do not want to enable Telnet.
`Do you want to enable TFTP [n] (y/n) ?`	**Description:** Specifies whether you want user to access the switch using TFTP. **Action:** Enter **y** if you want to enable TFTP. Accept the default, **n**, if you do not want to enable TFTP.

Prompt	Description/Action
`Do you want to enable WEB server service [n] (y/n) ?`	**Description:** Specifies whether you want to enable the Web server service. The Web server service allows you to monitor statistics for the switch using your web browser. **Action:** Enter **y** if you want to enable WEB server service. Accept the default, **n**, if you do not want to enable it.
`IP Address for mgmt port in first CPU Slot [0.0.0.0/ 0.0.0.0]:`	**Description:** Indicates the IP address for the management port in the specified CPU slot. **Action:** Enter the IP address of the management port in the first CPU slot.
`IP Address for mgmt port in second CPU Slot [0.0.0.0/ 0.0.0.0]:`	**Description:** Indicates the IP address for the management port in the specified CPU slot. **Action:** Enter the IP address of the management port in the first CPU slot.
`IP Address for mgmt-virtual-ip [0.0.0.0/0.0.0.0]:`	**Description:** Indicates the IP address for the virtual management port. **Action:** Enter the IP address of the virtual management port. Accept the default, 0.0.0.0/0.0.0.0, if you do not want to specify an IP address.
`First net mgmt route [134.177.160.0:10.10.43.1]:`	**Description:** Specifies the IP address of the first network management route (static route from the network management port to a device in the network). **Action:** Enter the IP address of the first network management route.
`Second net mgmt route [0.0.0.0:0.0.0.0]:`	**Description:** Specifies the IP address of the second network management route. **Action:** Enter the IP address of the second network management route (static route from the network management port to a device in the network).
`Third net mgmt route [0.0.0.0:0.0.0.0]:`	**Description:** Specifies the IP address of the third network management route. **Action:** Enter the IP address of the third network management route (static route from the network management port to a device in the network).
`Fourth net mgmt route [0.0.0.0:0.0.0.0]:`	**Description:** Specifies the IP address of the fourth network management route. **Action:** Enter an IP address of the fourth network management route (static route from the network management port to a device in the network).

Prompt	Description/Action
`IP address of the default VLAN [0.0.0.0/0.0.0.0]:`	**Description:** Specifies the IP address of the default virtual LAN. **Action:** Enter the IP address of the default virtual LAN (VLAN).
`Do you want to save the changes [Saving the parameters will update the files /flash/boot.cfg and /flash/dvmrp_pol.cfg] (y/n) ?`	**Description:** Allows you to save your changes to the boot and runtime configuration files. **Action:** Enter **y** to save the boot and runtime configuration files. Enter **n** if you do not want to save your changes.

Rebooting or resetting the switch

When you reboot the system, you can specify the boot source (flash, PCMCIA card, or TFTP server) and file name. If you do not specify a device and file, the Run-Time CLI uses the software and configuration files on the primary boot device that is defined by the Boot Monitor **`choice`** command.

To reboot the system, use the following system command:

`boot [<`*`file`*`>] [config <`*`value`*`>] [-y]`

where:

- *`file`* is the software image device and file name in the format [a.b.c.d:]<file> | /pcmcia/<file> | /flash/<file>. The file name, including the directory structure, can be up to 1024 characters.
- `config <`*`value`*`>` is the software configuration device and file name in the format [a.b.c.d:]<file> | /pcmcia/<file> | /flash/<file>. The file name, including the directory structure, can be up to 1024 characters.
- `-y` suppresses the confirmation message before the switch reboots. If you omit this parameter, you are asked to confirm the action before the switch reboots.

To boot the switch using the BootStrap Protocol (BootP), use the following command:

```
boot 0.0.0.0
```

Note: Entering the **boot** command with no arguments causes the switch to boot using the current boot choices defined by the **choice** command (next).

You can reset the switch by using the following command:

```
reset
```

When you reset the switch, the most recently saved configuration file is used to reload the system parameters.

Cold boot/warm boot trap messages

When the switch reboots normally, a cold trap is sent within 45 seconds after a reboot. In the event of a SSF switchover, a warm-start management trap is sent within 45 seconds of a reboot.

Setting system identification

System identification parameters specify the system name, contact person, and location.

To set the system identification:

1. Specify the system name by entering:

   config sys set name <*prompt*>

   where *prompt* is an ASCII string specifying the system name.

2. Specify the name of the contact person for the switch by entering:

   config sys set contact <*contact*>

   where *contact* is an ASCII string specifying the name of the person.

3 Define the location for the system with the command:

config sys set location <*location*>

where *location* is an ASCII string specifying the system location.

Managing files

The CLI includes file management commands for working with the switch files. These commands allow all the basic operations of any file system. The commands take the general form of **command** <*arguments*>. Both the commands and the arguments can be abbreviated as long as the abbreviation is not ambiguous. Table 4 summarizes the file system commands.

Table 4 File system commands

Command	Description
directory	Lists contents of onboard flash memory or a PCMCIA card.
copy	Copies a file.
rename	Renames a file.
save	Saves the running configuration to a file.

Displaying a directory

To display the contents of the flash and PCMCIA memory, use the following command:

directory [<*dir*>] [-l>]

where:
dir specifies either flash or PCMCIA, in the form /flash or /pcmcia.
-l displays file details if you specify a path name.

When you invoke the `directory` command with no arguments, it displays the contents of all flash devices. When you specify flash or PCMCIA, `directory` displays only the contents of that device.

Note: When using the **`dir`** command, the CLI displays all filenames under the parent directory, rather than the sub directory.

Copying files

To copy a file, use the following command:

```
copy <srcfile> <dstfile>
```

where:
srcfile is the source file; *dstfile* is the destination file, that is, the copy.

For the **copy** command, the source and destination are specific file names in the form:

```
[<ipaddr>:] <filename>
```

where:
ipaddr can specify a TFTP server location for the file.
filename is the name of the file in the form /flash/xxx or /pcmcia/xxx.

You can use the **copy** command to copy a run-time image to flash memory from a TFTP server. The command format for this operation is:

```
copy <ip_address>:<filename> <destination>
```

where:
ip_address:*filename* is the source argument that specifies the IP address of the TFTP server and the name of the file to be copied.
destination specifies the name of the copied file in its new location.

Saving the configuration to a file.

To save the running configuration to a file, use the following command:

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

where:

- *savetype* specifies the type of file to save; options are `config`, `bootconfig`, `log`, and `trace`.
- `file <value>` is the file name.

- `verbose` saves default and current configuration. If you omit the [verbose] parameter, only the current configuration is 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.

Getting Help

When you navigate through the Boot Monitor and Run-Time CLI, online Help is available at all levels. From any level of the tree, you can access Help in one of these four ways:

- Typing **`help`** *<command>* explains what the command does and gives its syntax (Figure 1).

Figure 1 Result of typing “help clear”

```
8610:6# help clear
clear commands
atm             clear atm stats
ip              clear ip information
ports           clear port stats
telnet          kill telnet sessions
```

- Typing the word **`help`** at the system prompt provides an explanation of the available help (Figure 2).

Figure 2 Result of typing “help”

```
8610# help
Eight forms of help are available in the system.
1. Typing "help" describes help features
2. Typing "help commands" provides a list of commands you can enter from the
   current prompt.
3. Typing "help ttychars" provides a list of special terminal editing characters.
4. Typing "syntax" displays a path list of commands and parameters available from
   the current prompt or <command> forward.
5. Typing "help <command>" or "<command> help" describes a specific command or
   provides a list of sub-commands you can enter from with-in <command>.
6. Typing "?" displays the sub and current context commands available from the
   current prompt.
7. Typing "<command> ?" displays the sub and current context commands available
   from the current prompt if the command is a intermediate node in the command
   tree structure, otherwise, displays parameter help for the the command.
8. Typing "<command?>" displays a list of commands that will match the characters
   entered.
```

- Typing <*command*> **`syntax`** displays a list of commands and parameters available for that command (Figure 3).

Figure 3 Result of typing “test syntax”

```
8610:6# clear syntax
atm port-stats [<ports>]
atm elan-stats <vlan id>
ip arp ports <port>
ip arp vlan <vid>
ip route ports <port>
ip route vlan <vid>
ip vrrp ports <ports> vrid <value>
ip vrrp vlan <vid> vrid <value>
ports stats [<ports>]
telnet <session id>
```

- Typing a question mark (?) at the prompt results in a list of all commands in that command context and the subcontext of that command.

Pinging a device

When you ping a device, an Internet Control Message Protocol (ICMP) packet is sent from the switch to the target device. If the device receives the packet, it sends a ping reply. When the switch receives the reply, it displays a message indicating that the specified IP address is alive. If no reply is received, a message indicates that the address is not responding.

To test the connection between the Passport 8000 Series switch and another network device, use the following command:

```
ping <ipaddr> [datasize <value>] [count <value>] [-s] [-I
<value>] [-t <value>] [-d]
```

where:

- *ipaddr* is the IP address of the other network device.
- `datasize` *value* is the size of ping data sent in bytes (16 to 4076).
- `count` *value* is the number of times to ping (1 to 9999).
- `-s` sets the continuous ping at the interval rate defined by the `[-I]` parameter.
- `-I` *value* is the interval between transmissions in seconds (1 to 60).
- `-t` *value* is the no-answer timeout value in seconds (1 to 120).
- `-d` sets ping debug mode.

To specify a count for the ping operation, you must also specify a size. For example:

```
ping 10.5.5.5 1600 5
```

Figure 4 shows output from the **`ping`** command.

Figure 4 ping command output

```
monitor# ping 10.10.81.18
10.10.81.18 is alive
```

You can test an IPX network connection by using the following command:

```
pingipx <ipxhost> [<count>] [-s] [-q] [-t <value>]
```

where:

- *ipxhost* is the IP address of the network node you are pinging.
- *count* is the number of times to ping the host (1 to 9999).
- -s is a continuous ping.
- -q is quiet output (same as nonverbose mode).
- -t *value* is the no-answer timeout value in seconds (1 to 120).

Setting and displaying the date

To set the calendar time in the form of month, day, year, hour, minute, and second, use the following command:

```
config setdate <MMddyyyyhhmmss>
```

You must be logged in as **rwa** to use this command.

Configuration example

This configuration example uses the above commands to set the system date.

```
8610:5# config setdate 06062002191200
local time: THU JUN 06 19:12:00 2002 UTC
utc time:   THU JUN 06 19:12:00 2002 UTC
8610:5#
```

To view the current date settings for the switch, use one of the following commands:

```
date
```

or

```
show date
```

Figure 5 shows sample output for the `date` command.

Figure 5 date command output

```
monitor# date
local time:    TUE NOV 02 09:32:26 1999 PST
hardware time: TUE NOV 02 17:32:26 1999 UTC
```

Accessing the standby CPU

To use Telnet or rlogin to access the standby CPU, use the following command:

```
peer <operation>
```

where *operation* is either Telnet or rlogin.

You can use this command to make changes to the standby CPU without reconnecting to the console port on that module.

Note: You must set an rlogin access policy on the standby CPU before you can use the peer command to access it from the master CPU using rlogin. To set an access policy on the standby CPU, connect a terminal to the Console port on the standby CPU. For more information about the access policy commands, see *Configuring and Managing Security.*

Exiting and re-entering the CLI

To end your CLI session, enter one of the following commands:

```
quit
logout
exit
```

To log back in to the CLI, use the **login** command.

Chapter 2
Setting up the switch for remote management

This chapter describes how to assign an IP address to the management port, configure SNMP settings, and enable remote management services. It includes the following topics:

Assigning an IP address to the management port

You must assign an IP address to the management port before you can use it for out-of-band management. In a switch with redundant 8190SM modules, each management port has a specific IP address. In addition, you can create a virtual management port with an IP address that is available to either management module.

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 backup management module takes over, the virtual management port IP address continues to provide management access to the switch.

To assign an IP address to the management port, use the following command:

```
config bootconfig net mgmt ip <ipaddr/mask> [cpu-slot
<value>]
```

where:

- *ipaddr/mask* specifies the IP address and subnet mask of the management port (for example, 10.10.10.1/24).
- *cpu-slot <value>* specifies the position of the 8190SM module, either slot 5 or slot 6. If you do not specify a slot number for the IP address, it is assigned to the currently active management module

To assign an IP address to the virtual management port, use the following command:

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

where:
ipaddr/mask is the IP address and subnet mask you are assigning.

Any time you change the boot configuration, you must save the changes to both the master and standby management modules.

To save the boot configuration:

1. Save the configuration to the master management module by entering:

   save bootconfig

2. Save the command to the standby management module by entering:

   save bootconfig standby *<boot.cfg>*

   where *boot.cfg* is the name of the configuration file.

3. Telnet to the standby management module and reset it by entering:

   telnet *<ipaddr>*

   reset

   where *ipaddr* is the IP address of the standby management module

Assigning a default gateway

When configuring IP on most layer 2 switches, you need to specify the IP address of the default gateway, as well as the IP address of the device. You can specify up to four separate static routes. For more information about static routes, see *Configuring IP Routing Operations*.

To specify a default gateway address/default route from the Boot Monitor CLI, use the following command:

```
net mgmt route net <netaddr> <gateway>
```

To specify a default gateway address/default route from the Run-Time CLI, use the following command:

```
config bootconfig net mgmt route net <netaddr> <gateway>
```

In each of these commands, the parameters are defined as follows:

netaddr is the IP address of the destination network
gateway is the IP address of the default gateway.

As an example, if the IP address of the management port is 10.125.2.11 and its next hop is 10.125.2.1, enter the following command to set up the management port correctly:

```
config bootconfig net mgmt route net 13.177.76.0 10.125.2.1
```

The value 13.177.76.0 represents the target subnet; the value 10.125.2.1 represents the gateway used to point to the target subnet.

To save the configuration, use the following command:

```
save config
```

Configuring the management Ethernet port

The management Ethernet port can communicate only with devices on its local subnet and on up to four statically configured remote subnets. The management Ethernet port does not support a default gateway or default route. The remote subnet is configured using the following CLI command, which requires knowledge of the next hop address:

```
config bootconfig net mgmt route add <a.b.c.d> <w.x.y.z>
```

For example, if the IP address of the management port is 10.125.2.11 and its next hop is 10.125.2.1, use the following command to correctly set up the management port:

```
config bootconfig net mgmt route add 13.177.76.0 10.125.2.1
```

Caution: This command uses the natural mask of the target subnet. Therefore, using this example, what you implement is the **`config bootconfig net mgmt route add 13.0.0.0 10.125.2.1`** command. Additionally, this route does not appear in the routing table of the Passport 8600 switch. If any 13.x.x.x networks are learned or configured for output by way of the I/O modules, connectivity issues may result.

Setting security features

System security parameters allow you to define login names and passwords for access to the switch management functions and to specify the access methods, such as through a Telnet session or through a Web browser.

You can use the CLI to set up passwords and community strings for access to all the management functions of the switch.

For more information about the security features available in the Passport 8000 Series switch software, see *Configuring and Managing Security.*

Configuring SNMP settings

To configure SNMP settings, including SNMP community strings and traps, use the following command:

```
config sys set snmp
```

This command includes the following options:

config sys set snmp followed by:	
`info`	Displays the current SNMP settings.
`community <ro|rw|l1|l2|l3|rwa> <commstr>`	Sets the SNMP community string for the selected community: • `ro` is read-only. • `rw` is read/write. • `l1` is layer 1 read/write. • `l2` is layer 2 read/write. • `l3` is layer 3 (and layer 2) read/write. • `rwa` is read/write/all. • *`commstr`* is the input community string. SNMP community strings are required for access to the switch using Device Manager or to other SNMP-based management software.
`del-trap-recv <ipaddr>`	Deletes the SNMP trap receiver. • *`ipaddr`* is the IP address of the trap receiver.
`trap-recv <ipaddr> <v1|v2c> <commstr>`	Sets an SNMP trap receiver. • *`ipaddr`* is the IP address of the trap receiver. • `v1|v2c` is the SNMP version; select version 1 or version 2c. • *`commstr`* is the input community string from 1 to 1024 characters.

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-8610:5# config sys set snmp
Passport-8610:5/config/sys/set/snmp# community rw community1
Passport-8610:5/config/sys/set/snmp# trap-recv 47.140.54.40 v1
community1
Passport-8610:5/config/sys/set/snmp# info

Sub-Context:
Current Context:

       community :
              ro - public
              rw - community1
              l1 - private
              l2 - private
              l3 - private
              rwa - secret
del-trap-recv : N/A
    trap-recv :
47.140.54.40 - v1 community1
47.153.248.81 - v1 public
192.32.229.150 - v1 public
192.32.229.172 - v1 public
Passport-8610:5/config/sys/set/snmp#
```

Enabling remote access services using the CLI

You enable or disable access services by setting flags, either from the Boot Monitor CLI or from the Run-Time CLI. You can access the boot monitor CLI while the switch is booting.

To enable an access service from the Boot Monitor CLI, use the following procedure:

1. While the switch is booting, press any key to interrupt the autoboot process.
2. Enable or disable the access service by using the following command:

```
flags <access-service> <true|false>
```

where:
access-service is ftpd, rlogind, telnetd, tftpd, or sshd.
`true` enables the access service.
`false` disables the access service.

To set up these access services from the Run-Time CLI, use the following command:

```
config bootconfig flags <access-service> <true|false>
```

where:
access-service is ftpd, rlogind, telnetd, tftpd, or sshd.
`true` enables the access service.
`false` disables the access service.

To save the state of the access services that you set up, use the following command:

```
save bootconfig
```

Enabling rlogin

When you enable an rlogin flag using the **`config bootconfig rlogind true`** command, you must configure an access policy and specify the name of the user who can have access to the switch.

The following sample configuration shows how to configure an access policy for rlogin. For more information about configuring access policies using the CLI and Device Manager, see *Configuring and Managing Security.*

```
8610:5# config sys access-policy policy 3 name "from subnet10"
8610:5# config sys access-policy policy 3 username "netadmin"
8610:5# config sys access-policy policy 3 network 10.0.0.0/
255.0.0.0
8610:5# config sys access-policy policy 3 service rlogin enable
```

Disabling a service

To disable one of the services on the switch, enter the following command:

```
config bootconfig flags <access-service> false
```

Note: When you enable or disable the flags, daemon behavior is changed immediately. You do not need to save the boot configuration file and reboot the system.

Monitoring the switch using Web management

The Passport 8000 Series switch includes a Web management interface that lets you monitor your switch through a World Wide Web browser from anywhere on your network. The Web interface provides many of the same monitoring features as the Device Manager software.

For configuration requirements and instructions for installing the help files, enabling the web server using Device Manager, and accessing the web interface, see *Configuring Network Management*.

Managing the switch using Device Manager

Device Manager is an SNMP-based graphical user interface (GUI) tool designed to manage single devices. To use Device Manager, you must have network connectivity to a management station running Device Manager in one of the supported environments.

For instructions on installing and starting Device Manager, refer to *Installing and Using Device Manager*.

Chapter 3
Providing switch reliability

As system resources become more widely distributed, the reliability of network nodes is even more important since it affects connectivity in the entire network. While reliability ensures that the software and hardware components of a node are robust, they are still prone to failures. Protecting the node from failure of any of its components makes the node *highly available.*

Many high availability features are built in at all levels of the Passport 8000 Series switch, including the following:

- Port-level and slot-level redundancy in the form of MultiLink Trunking (MLT)
- Silicon Switch Fabric redundancy and load-sharing
- Split Multi-Link Trunking (SMLT)
- Hot-swappable I/O modules
- Router redundancy through VRRP
- Redundant fans and power supply units
- Basic CPU availability — *warm standby*
- High CPU availability — *hot standby*

For more information about MLT, SMLT, and VRRP, see *Configuring Layer Operations: VLANs, Spanning Tree, and MultiLink Trunking*.

In the event that the primary SSF/CPU module fails, the backup SSF/CPU assumes the primary role.

Note: During a CPU fail over, do not hot swap I/O modules until the new CPU becomes the master CPU.

You can configure CPU redundancy to provide either basic availability or high availability.

In *warm standby* redundancy mode, if the primary CPU fails, the backup CPU must initialize all input/output modules and load switch configurations, causing delays and disrupting operations. In *hot standby* redundancy mode, both CPUs maintain synchronized configuration and operational databases, enabling very quick recovery and high availability.

If you enable layer 2 CPU redundancy you automatically disable layer 3 routing operations on the switch and will be unable to configure routing parameters.

When you enable layer 2 CPU redundancy, both the primary and backup CPUs synchronize their database structures following initialization. This process, which takes a little time, need only be performed on initialization.

Index

L

M

N

P

Q

R

S

T

V

W