Part No. 315023-C Rev 00
May 2004

4655 Great America Parkway
Santa Clara, CA 95054

Using the Packet Capture Tool (PCAP)

Passport 8000 Series Software Release 3.7

NORTEL NETWORKS™

Copyright © 2004 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

This guide provides information about using the features and capabilities of the Packet Capture Tool* (PCAP) for configuring packet capture filters on port interfaces and the PCAP engine. The guide also provides sample examples and instructions for using the CLI to perform basic setup of filters.

For more information about using a Nortel Networks Passport 8000 Series switch, a list of publications can found in the Related Publications section of the release notes that accompany this release.

Before you begin

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

- Basic knowledge of networks, Ethernet bridging, and IP 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`.
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:

ATM	asynchronous transfer mode
CPU	central processing unit
HA	High Availability
IP	Internet Protocol
MAC	media access control
PCAP	Packet Capture
POS	packet-over-SONET

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
Packet Capture Tool (PCAP) overview

The Packet Capture Tool* (PCAP) is a data packet capture tool, capable of capturing ingress and egress (E-modules or M-modules only) packets on selected I/O ports. Captured packets are then analyzed for troubleshooting purposes. This feature is based on the mirroring capabilities of the I/O ports. Packets can be captured based on port mirroring or exchange flow with packet filters. This feature also allows software filters to be configured which will limit the number of packets captured by PCAP.

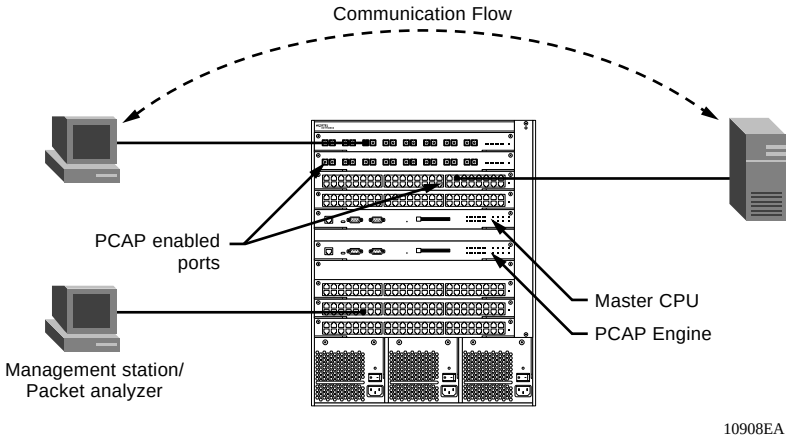
All captured packets are stored in the PCAP engine. The primary CPU maintains its protocol handling and will not be affected by any PCAP capture activity. Packets captured by PCAP can be saved and downloaded from the PCAP engine to be analyzed offline.

This chapter includes the following topics:

Packet capture flow

Figure 1 shows how the PCAP tool allows you to configure PCAP capture filters and enable them on ports. By default, PCAP uses port mirroring. If a filter set is applied, flow mirroring is used. If further filtering is required, PCAP software filters are applied. Captured packets are stored in the PCAP engine DRAM (PCAP00), on a PCMCIA device, or on the network. The packets may then be downloaded to an offline analyzer tool (such as EtherReal* or Sniffer Pro*) using FTP.

Figure 1 PCAP tool packet flow



Supported PCAP features

This release of PCAP supports the following features:

- PCAP uses the secondary CPU as the PCAP engine.
- PCAP can be used with HA-CPU mode.
- PCAP supports activating packet capture on one or multiple ports.
- PCAP captures packets on ingress, egress*, or both* directions. (*E-modules only).
- PCAP can be used with existing IP traffic filters so that only packets that match this filter criteria will be captured.

- PCAP can be used with existing MAC (fdb) filters so that only packets that match this filter criteria will be captured.
- PCAP supports software filters, which provide a way to filter the packets in the PCAP engine.
- PCAP captured packets can be stored on a PCMCIA device or on the network. The packets are stored in Sniffer Pro file format.

Using PCAP with High Availability (HA) mode

In release 3.7, PCAP can now be enabled when the switch is running in HA mode. The changes to the existing behavior include the ability to:

- Modify the HA flag from the standby CPU.
- Execute PCAP commands from the primary CPU in HA mode, provided that the standby CPU is in warm stand-by mode.

If you want to capture packets while the switch is in HA mode, follow these steps:

1. Disable the HA flag in the standby CPU.
2. Reboot the standby CPU in warm stand-by mode.
3. Configure IP/MAC filters, if necessary, from the primary CPU.
4. Enable PCAP on the port from the primary CPU.
5. Configure capture filters, if necessary, and enable PCAP globally. This can be done from either the primary or the standby CPU.
6. Capture packets.
7. Save the packets for analysis.
8. Disable PCAP on the port from the primary CPU.
9. Remove IP/MAC filters, if configured, from the primary CPU.
10. Re-enable HA mode in the standby CPU.
11. Reboot the standby CPU. The standby CPU comes up in HA mode.

You can now capture packets without interfering with the function of the primary CPU.

Note: If packets are being captured and the primary CPU in HA mode reboots, the HA switchover to the standby CPU will not occur. Instead, the standby CPU will go through a warm standby switchover and become the primary CPU.

Using PCAP with IP filter sets

A method to limit the amount of data traffic sent to the PCAP engine is the use of IP traffic filter sets. The PCAP engine is the device that is actively capturing data packets.

Using IP filter sets will affect data network traffic depending on the action taken at the filter and port level. Applying IP filter sets will have the same affect on network traffic as configuring filter sets to ports using PCAP parameters. For routed IP traffic, use Source/Destination IP filter sets, for bridged IP traffic use Global IP filter sets.

To reference how to configure and enable IP traffic filters, refer to *Configuring IP Routing Operations*.

Using PCAP capture filter sets

The PCAP capture filters allow for selectively configuring match criteria to capture or drop frames. Refer to "Configuring PCAP capture filters" on page 32." The parameters configured are used to determine which filter to apply to a given frame. The default behavior is to accept the frame. In addition to this, the user can set trigger filters to start and stop packet capturing globally.

Using PCAP with MAC filters

You may also use PCAP to capture packets that match criteria based on MAC address filters. Using PCAP with MAC filters is recommended because it reduces traffic flow on the PCAP engine.

Accessing the PCAP engine

The PCAP engine is the secondary CPU. You can gain access to the PCAP engine through a direct console or modem connection to the secondary CPU, or by using a peer telnet session from the primary CPU. By issuing the command **`peer telnet`** a connection is made to the secondary CPU, which then prompts for the login and password.

Figure 2 is an example of accessing the PCAP engine using a peer telnet session.

Figure 2 Accessing the PCAP engine

```
8606:5# peer telnet
Trying 127.0.0.6 ...
                    Connected to 127.0.0.6

*****************************************
* Copyright (c) 2004 Nortel Networks, Inc.  *
* All Rights Reserved                       *
* Passport 8006                             *
* Software Release 3.7.0.0                  *
*****************************************

Login: rwa
Password: ***

8606:6#
```

Supported PCAP options

This section describes some options that are available when configuring PCAP capture filters. The CLI commands show how to configure the option.

- The option to enable (true) or disable (false) PCAP globally.

  ```
  config diag pcap enable true
  ```

  ```
  config diag pcap enable false
  ```

- The option to start or stop packet capture based on the protocol type of the packet. In this example, TCP packets (`protocol-type 6`) are captured.

Note: While this capture filter specifies to capture TCP packets, the default action is to capture all packets. A PCAP capture filter with action drop would first need to be configured to drop all packets to achieve the desired result.

```
config diag pcap enable false
config diag pcap capture-filter 7 create
config diag pcap capture-filter 7 action capture
config diag pcap capture-filter 7 protocol-type 6
config diag pcap capture-filter 7 enable true
```

- The option to capture packets for a pre-defined time period. When the *`trigger-on`* option is used, packet capture starts when the first packet that matches the *`protocol-type`* criteria is processed and continues for the length of the *`timer`* value.

```
config diag pcap capture-filter 7 create
config diag pcap capture-filter 7 action trigger-on
config diag pcap capture-filter 7 protocol-type 6
config diag pcap capture-filter 7 timer 10
config diag pcap capture-filter 7 enable true
```

- The option to drop all IP broadcast packets.

```
config diag pcap capture-filter 8 create
config diag pcap capture-filter 8 action drop
config diag pcap capture-filter 8 dstip 255.255.255.255
config diag pcap capture-filter 8 enable true
```

- The option to capture packets for a pre-defined number of packets.

```
config diag pcap capture-filter 7 create
config diag pcap capture-filter 7 action trigger-on
config diag pcap capture-filter 7 srcip 10.10.10.10
config diag pcap capture-filter 7 packet-count 1000
config diag pcap capture-filter 7 enable true
```

- The option to stop packet capture when the PCAP engine buffer is full.

  ```
  config diag pcap buffer-wrap false
  ```

- The option to save packets captured after the PCAP engine buffer is full.

  ```
  config diag pcap auto-save true file-name pcap_test.cap device
  pcmcia
  ```

- The option to configure the PCAP engine buffer size, which is the amount of DRAM allocated in megabytes for storing packets.

  ```
  config diag pcap buffer-size 10
  ```

- The option to configure the fragment size, which is the number of bytes of each captured packet that will be captured.

  ```
  config diag pcap fragment-size 200
  ```

Implementing PCAP packet capture

The following basic steps are required to set the PCAP parameters, enable PCAP on a port, enable PCAP, and copy the captured packets to a remote machine. See Chapter 5, “PCAP examples,” on page 67 for more detailed examples.

1 Enable PCAP parameters.

```
config diag pcap auto-save true file-name
pcap_test.cap device pcmcia
```

2 Enable PCAP on a port, by MAC address, or IP filter.

```
config ether 2/10 pcap enable true mode {rx|tx|both}
```

or

```
config ether 2/10 pcap enable true mode rxFilter
```

```
config vlan 2 fdb-filter pcap 00:08:07:60:89:D6
enable
```

or

```
config ether 2/10 pcap enable true mode rxFilter
```

```
config ip traffic-filter create global src-ip
10.10.10.10/32 dst-ip 10.10.20.20/32 id 5
```

3 Enable PCAP globally.

```
config diag pcap enable true
```

4 Configure a PCAP filter that only allows TCP ports that are not in 20 to 21.

```
config diag pcap capture-filter 7 tcp-port 20 to 21 not
```

5 Display all PCAP statistics.

```
show diag pcap stats
```

6 Disable PCAP at the port level.

```
config ether 2/10 pcap enable false
```

7 Copy captured packets to a file.

```
copy PCAP00 /pcmcia/pcap_packets.cap
```

8 Use Ethereal or Sniffer Pro to analyze the packets.

Chapter 2
Configuring PCAP with CLI

This chapter describes the CLI commands that support all PCAP configuration through the primary CPU and the PCAP engine.

This chapter includes the following topics:

Roadmap of PCAP CLI commands

The following table lists all the PCAP commands and their parameters. Use this list as a quick reference or click on any entry for more information:

Command	Parameter
`config {ethernet|atm|pos} <slot/port> pcap`	`info`
	`add set <value>`
	`enable <true|false> [mode <value>]`
	`remove set <value>`

Command	Parameter
config diag pcap	info
	auto-save <true|false> [file-name <value>] [device <value>] [ip <value>]
	buffer-size <2...256>
	buffer-wrap <true|false>
	enable <true|false>
	ethertype-for-svlan-level <EtherType for hex vlan level>
	fragment-size <64...9600>
	pcmcia-wrap <true|false>
	reset-stat
config diag pcap capture-filter <listid>	info
	action <capture|drop|trigger-on|trigger-off>
	create
	delete
	dscp <dscp> [to <value>] [match-zero <value>] [not]
	dstip <ipaddr/mask> [to <value>] [not]
	dstmac <DstMac> [mask <value>] [not]
	enable <true|false>
	ether-type <Ethertype> [to <value>] [not]
	packet-count <PacketCount>
	pbits <Pbits> [to <value>] [match-zero <value>] [not]
	protocol-type <protocoltype> [to <value>] [not]

Command	Parameter
	refresh-timer <RefreshTimer>
	srcip <ipaddr> [to <value>] [not]
	srcmac <SrcMac> [mask <value>] [not]
	tcp-port <tcport> [to <value>] [not]
	timer <Timer>
	udp-port <udpport> [to <value>] [not]
	user-defined <0..9600> <data> [not]
	vlan-id <Vlanid> [to <value>] [not]
show diag pcap dump	
show diag pcap capture-filter [id <value>]	
show diag pcap info	
show diag pcap port	
show diag pcap stats	
copy PCAP00 /<device>/<filename>	
config diag pcap enable false	
config diag pcap reset-stat	

Enabling PCAP on a port

PCAP is enabled on Ethernet, ATM, or POS ports. IP traffic filter sets can be added and removed. Creating the IP Filter sets (Global or Source/Destination) must occur prior to adding them to a PCAP enabled port.

To enable PCAP on Ethernet, ATM, or POS ports, use the following CLI command:

```
config {ethernet|atm|pos} <slot/port> pcap
```

where:
slot/port specifies the ports on which you want to enable PCAP in port list form: {slot/port [-slot/port][, ...]}.

This command includes the following options.

config {ethernet|atm|pos} <ports> pcap followed by:	
`info`	Displays the current PCAP configuration information (Figure 3).
`add set <value>`	Allows you to add an IP filter set (Global or Source Destination) to a port. The IP filter set must be created prior to performing this function. Filter Global Set ID values are in the range of 1 to 100 and Source/Destination sets are in the range of 300 to 1000. This will cause the following to happen: • Create an IP traffic filter for a port if one does not already exist; otherwise, disable the IP traffic filter. • Add the IP traffic filter set to the port. • Set the mirror bit for all the filters in the set. • Restore the “default-action” of the port. If “default-action” was not set, set to “forwarding.” • Enable the traffic filter on the port.

config {ethernet|atm|pos} <ports> pcap followed by:	
`enable <true|false> [mode <value>]`	Enable or disable PCAP on the port. The default PCAP mode will only capture ingress packets in rx mode. • [mode <*value*>] value is rx, tx, both, or rxFilter. If PCAP is enabled in rxFilter mode, then only ingress packets which match the filter criteria will be captured.
`remove set <value>`	Allows you to remove a filter. *value* is the number of the filter set. The Source/Destination set is a value from 1 to 100. The Global set is a value from 300 to 1000. This will cause the following to happen: • Disable the IP traffic filter. • Remove the IP traffic filter set from the port.

Figure 3 shows sample output for the **config {ethernet|atm|pos} pcap info** command. Each command is issued from the primary CPU. To use IP traffic filter sets (Global or Source/Destination), PCAP must be enabled in rxFilter mode. The default mode, rx, will result with the packets captured containing PCAP filtered or all the packets.

Figure 3 config {ethernet|atm|pos} pcap info command sample output

```
Passport-8606:5# config ethernet 1/44 pcap enable true mode
rxFilter
Passport-8606:5# config ethernet 1/44 pcap info
                      enable : true
                        mode : rxFilter
                     add set :

Passport-8606:5# config ethernet 1/46 pcap enable true mode tx
Passport-8606:5# config ethernet 1/46 pcap info
                      enable : true
                        mode : tx
                     add set :


Passport-8606:5# config ethernet 1/48 pcap enable true mode both
Passport-8606:5# config ethernet 1/48 pcap info
                      enable : true
                        mode : both
                     add set :

Passport-8606:5# config atm 9/1 pcap enable true mode rx
Passport-8606:5# config atm 9/1 pcap info
                      enable : true
                        mode : rx
                     add set :

Passport-8606:5# config pos 7/1 pcap enable true mode rxFilter
Passport-8606:5# config pos 7/1 pcap info
                      enable : true
                        mode : rxFilter
                     add set :
```

Enabling PCAP with MAC (fdb) filters

Note: Nortel Networks recommends using PCAP with IP or MAC address filters to reduce traffic flow on the PCAP engine.

To capture packets that match criteria based on MAC address filters:

1. Enable PCAP with the mode option set to rxFilter.
2. Enable PCAP with fdb-filters on a VLAN.

To enable PCAP for an fdb-filter by MAC address, use the following command:

```
config vlan <vid> fdb-filter pcap <mac> enable
```

where:
vid identifies the VLAN
mac is the MAC address

For information about the other options available from the **`config vlan <vid> fdb-filter`** command, see *Configuring VLANs, Spanning Tree, and Link Aggregation*.

Configuring PCAP global parameters

Global parameters are configured to define where captured frames are to be stored, the size of the buffer required to store frames, the size of the packet to be captured, and whether or not to reset statistical counters. The command syntax is:

```
config diag pcap
```

Note: All of the following commands can be executed only when PCAP is globally disabled. All commands can be executed from the primary CPU or PCAP engine.

To configure PCAP global parameters, use the command **`config diag pcap`** with the following options:

`config diag pcap` followed by:	
`info`	Displays the current PCAP configuration (Figure 4).
`auto-save <true|false> [file-name <value>] [device <value>] [ip <value>]`	When enabled, saves the captured frames into the device specified and continues to capture frames. Default is enable. If this option is disabled, packets are stored in the DRAM buffer only. • `file-name value` is the name of the file where captured frames are to be saved. • `device value` is the device name (i.e., PCMCIA or network). • `ip value` is the IP address to be used. This is used only if the device is "network."
`buffer-size <2...256>`	This is the size of the buffer that needs to be allocated for storing data. The maximum buffer size is 40MB for a 8690 CPU and 104MB for a 8691 CPU. Default is 32 MB.
`buffer-wrap <true|false>`	When this parameter is set to true and the buffer becomes full, the capture will continue by wrapping the buffer. If this parameter is set to false and the buffer becomes full, the packet capture will stop. The default value is set to true. A log message is generated when the buffer is wrapped.
`enable <true|false>`	Use to enable or disable PCAP globally. The default is false.
`ethertype-for-svlan-level <EtherType for hex vlan level>`	Specifies the Ethernet type for SVLAN packets. With this information, PCAP can identify and capture the tag information of packets received from SVLAN ports. `ethertype-for-svlan-level` is a hexadecimal value. The default is 0x8100.
`fragment-size <64...9600>`	The number of bytes of each frame that will be captured. The default is set to capture the first 64 bytes of each frame.

config diag pcap followed by:	
pcmcia-wrap <true|false>	When this parameter is set to true and the autosave device is PCMCIA, this will cause an overwrite of the present file on the PCMCIA during an autosave. If this parameter is set to false, the present file will not be overwritten. A log is generated when the file is overwritten on the PCMCIA.
reset-stat	This command resets the PCAP engine DRAM buffer, as well as all software counters used for PCAP statistics. This command can be executed in the Primary and PCAP engine.

Figure 4 shows sample output for the **config diag pcap info** command. The command can be issued from both the primary CPU or the PCAP engine.

Figure 4 config diag pcap info command

```
Passport-8606:6# config diag pcap info
       enable = TRUE
       buffer-wrap = TRUE
       pcmcia-wrap = TRUE
       buffer-size = 32 MB
       fragment-size  = 64 Bytes
       auto-save = FALSE
       AutoSaveFilename = pcap.cap
       AutoSaveDevice = pcmcia
       ether-type-for-svlan-level = 0x8100
```

Configuring PCAP capture filters

Use PCAP capture filters to better define the match criteria used on packets. This is done to further narrow the scope of the types of packets to be captured.

Note: Nortel Networks highly recommends using PCAP with IP or MAC filters to reduce the load on the PCAP engine that has a capturing capability that can be exceeded by a gigabit port mirrored traffic stream. IP filter sets affect network traffic and is dependent on the action taken by the filter on the port.

To configure a capture filter with match criteria, use the following CLI command:

```
config diag pcap capture-filter <listid>
```

where:
listid represents a unique filter. The valid range is 1 to 1000.

This command includes the following options. The command can be issued from both the primary CPU and the PCAP engine.

config diag pcap capture-filter <listid> followed by:	
`info`	Displays the current PCAP filter configuration. (Figure 5).
`action <capture|drop|trigger-on|trigger-off>`	This option determines the action to be taken by the filter. • `capture` indicates that the packet will be captured. • `drop` indicates that the packet will be dropped. • `trigger-on` indicates to start capturing the packet when a packet matches this filter. PCAP will be enabled globally and the trigger filter will get disabled. • `trigger-off` indicates to stop capturing the packet when a packet matches this filter. PCAP will be disabled globally and the trigger filter will get disabled.
`create`	Creates a new PCAP capture filter.

config diag pcap capture-filter <listid> followed by:	
`delete`	Deletes an existing filter.
`dscp <dscp> [to <value>] [match-zero <value>] [not]`	This is the DSCP value of the packet. • *dscp* can be one or a range of DSCP values. The default is 0 which means this option is disabled. • `to` *value* is used to specify a range. • `match-zero` *value* is either `true` or `false`. When this option is set to true, 0 is considered a valid value. When it is set to false, 0 is considered a disable value. • `not` means that the filter matches for ALL other values than the range of values defined.
`dstip <ipaddr/mask> [to <value>] [not]`	The destination IP address. • *ipaddr/mask* can be one or a range of IP addresses. The default is 0.0.0.0, which means this option is disabled. • *to value* is used to specify a range. • `not` means that the filter matches for ALL other values than the range of values defined.
`dstmac <DstMac> [mask <value>] [not]`	The MAC address of the destination. If the mask is set, then only the first few bytes will be compared. • *DstMac* is used to represent a range of MAC addresses. The default is 00:00:00:00:00:00 which means this option is disabled. • `mask <value>` destination MAC address mask. This is used to specify an address range. • `[not]` NOT means that the filter matches for ALL other values than the range of values defined.
`enable <true|false>`	Used to enable or disable the filter. Default is disable.
`ether-type <Ethertype> [to <value>] [not]`	This is the Ethernet type of the packet. • *Ethertype* can be one or a range of ether-type values. The default is 0, meaning that this option is disabled. • `to` *value* is used to specify a range. • `not` means that the filter matches for ALL other values than the range of values defined.

config diag pcap capture-filter <listid> followed by:	
packet-count *<PacketCount>*	When set, PCAP will stop after capturing the specified value of packets. This is similar to the refresh- timer option, once this is invoked, the filter is disabled. This option is active only when the action parameter is set to trigger-on. The default value is 0 which means this option is disabled.
pbits *<Pbits>* [to *<value>*] [match-zero *<value>*] [not]	This is the priority bit of the packet. • *Pbits* can be one or a range. The default is 0 which means this option is disabled. • to *value* is used to specify a range. • match-zero *value* is either true or false. When this option is set to true, 0 is considered a valid value. When it is set to false, 0 is considered a disable value. • not means that the filter matches for ALL other values than the range of values defined.
protocol-type *<protocoltype>* [to *<value>*] [not]	The protocol of the packet. • *protocoltype* can be one or a range of protocol-type values. The default is 0 which means this option is disabled. • to *value* is used to specify a range. • not means that the filter matches for ALL other values than the range of values defined.
refresh-timer *<RefreshTimer>*	When set, this will start or reset a timer. If another packet is not received within the specified time, PCAP will be disabled globally. This option is active only when the action parameter is set to 'trigger-on'. To delete this option, set it to 0. The default value is 0.
srcip *<ipaddr>* [to *<value>*] [not]	The source IP address. • *ipaddr* can be one or a range of IP addresses. The default is 0.0.0.0, which means this option is disabled. • to *value* is used to specify a range. • not means that the filter matches for ALL other values than the range of values defined.

config diag pcap capture-filter <listid> followed by:	
srcmac *<SrcMac>* [mask *<value>*] [not]	The MAC address of the source. • *SrcMac* is the source MAC address. If the mask is set, then only the first few bytes will be compared. The default is 00:00:00:00:00:00 which means this option is disabled. • mask *value* is the mask of the destination MAC address. This is used to specify an address range. • not means that the filter matches for ALL other values than the range of values defined.
tcp-port *<tcport>* [to *<value>*] [not]	This is the TCP port of the packet. • *tcport* can be one or a range of TCP port values. The default is 0 which means this option is disabled. • to *value* This is used to specify a range. • not means that the filter matches for ALL other values than the range of values defined.
timer *<Timer>*	When set, PCAP will be invoked when the first packet is matched and stopped after the set value of time. After starting the timer, the filter will be disabled. This option is active only when the action parameter is set to trigger-on. • *Timer* is a value from 100 to 3600000 milliseconds. The default value is 0. Setting the value to 0 disables the timer.
udp-port *<udpport>* [to *<value>*] [not]	The UDP port of the packet. • *udpport* can be one or a range of UDP port values. The default is 0 which means this option is disabled. • to *value* is used to specify a range. • not means that the filter matches for ALL other values than the range of values defined.

config diag pcap capture-filter <listid> followed by:	
`user-defined <0..9600> <data> [not]`	This parameter is used to set the user defined value to match the packet. The user can define a pattern in hex or character to match in the packet. The user can also specify the offset to start the match. The default value of pattern is null (‘’) which means this field will be discarded. To disable this option set the pattern to null (‘’). • `not` means that the filter matches for ALL other values than the range of values defined.
`vlan-id <Vlanid> [to <value>] [not]`	The VLAN ID of the packet. • *`Vlanid`* can be one or a range of VLAN IDs. The default is 0 which means this option is disabled. • `to` *`value`* is used to specify a range. • `not` means that the filter matches for ALL other values than the range of values defined.

Figure 5 shows sample output for the **`config diag pcap capture-filter info`** command. The command can be issued from both the primary CPU and the PCAP engine.

Figure 5 config diag pcap capture-filter info command

```
Passport-8606:6# config diag pcap capture-filter 10 info
        Id : 10
        action : capture
        enable : false
        srcmac : 00:00:00:00:00:00 Mask = 6
        dstmac : 00:00:00:00:00:00 Mask = 6
        srcip : 0.0.0.0 to 0.0.0.0
        dstip : 0.0.0.0 to 0.0.0.0
        vlan-id : 0 to 0
        pbits : 0 to 0
        ether-type : 0x0 to 0x0
        protocol-type : 0 to 0
        dscp : 0 to 0
        udp-port : 0 to 0
        tcp-port : 0 to 0
        user-defined: Offset: 0 Data:
        timer : 0 ms
        packet-count : 0
        refresh-timer : 0 ms
```

Displaying PCAP information with the CLI

This section describes the commands used to display PCAP information and defines if they are to be used on the primary CPU or the PCAP engine.

Showing all captured packets

The **`show diag pcap dump`** command displays all captured packets. This command is allowed only from the PCAP engine and only when PCAP is disabled.

Note: Dumping a large number of captured packets is CPU intensive. The switch will not respond to any commands while the dump is in progress. Nortel Networks recommends to use this command only when it is absolutely necessary. However, there is no degradation in the normal traffic handling or switch failover.

To display information about all captured packets, use the following command:

```
show diag pcap dump
```

Figure 6 shows sample output for the **show diag pcap dump** command. The command is issued from the PCAP engine.

Figure 6 show diag pcap dump command output

```
Passport-8606:6# show diag pcap dump
 cc dd ee ff aa bb aa bb cc dd ee ff 81 00 00 0a 08 00 45 00 00
2a 00 00 00 00 4
0 11 48 92 0c 0c 0c 0c 0d 0d 0d 0d c0 20 00 07 00 16 0d 69 00 00
00 00 00 00 00
00 00 00 00 00 00 00
 cc dd ee ff aa bb aa bb cc dd ee ff 81 00 00 0a 08 00 45 00 00
2a 00 00 00 00 4
0 11 48 92 0c 0c 0c 0c 0d 0d 0d 0d c0 20 00 07 00 16 0d 69 00 00
00 00 00 00 00
00 00 00 00 00 00 00
 cc dd ee ff aa bb aa bb cc dd ee ff 81 00 00 0a 08 00 45 00 00
2a 00 00 00 00 4
0 11 48 92 0c 0c 0c 0c 0d 0d 0d 0d c0 20 00 07 00 16 0d 69 00 00
00 00 00 00 00
00 00 00 00 00 00 00
```

Showing capture filter information

The **show diag pcap capture-filter [id <value>]** command displays all capture filter information. If Id is not specified, then all configured filters will be displayed. This command can be issued from both the primary CPU or the PCAP engine.

To display information about capture filters, use the following command:

```
show diag pcap capture-filter [id <value>]
```

where:
id <value> is the filter id.

Figure 7 shows sample output for the **show diag pcap capture-filter** command.

Figure 7 show diag pcap capture-filter command output

```
Passport-8606:6# show diag pcap capture-filter

================================================================
                                        PCAP Capture-filters
================================================================
        Id : 10
        action : capture
        enable : false
        srcmac : 00:00:00:00:00:00 Mask = 6
        dstmac : 00:00:00:00:00:00 Mask = 6
        srcip : 0.0.0.0 to 0.0.0.0
        dstip : 0.0.0.0 to 0.0.0.0
        vlan-id : 0 to 0
        pbits : 0 to 0
        ether-type : 0x0 to 0x0
        protocol-type : 0 to 0
        dscp : 0 to 0
        udp-port : 0 to 0
        tcp-port : 0 to 0
        user-defined: Offset: 0 Data:
        timer : 0 ms
        packet-count : 0
        refresh-timer : 0 ms
```

Showing PCAP global parameters

The **show diag pcap info** command displays PCAP global parameter values in the PCAP engine. This command can be issued from both the primary CPU and the PCAP engine.

To display all global information, use the following command:

```
show diag pcap info
```

Figure 8 shows sample output for the **show diag pcap info** command.

Figure 8 show diag pcap info command output

```
Passport-8606:6# show diag pcap info
       enable = FALSE
       buffer-wrap = TRUE
       pcmcia-wrap = TRUE
       buffer-size = 32 MB
       fragment-size  = 64 Bytes
       auto-save = TRUE
       AutoSaveFilename = pcap.cap
       AutoSaveDevice = pcmcia
       ether-type-for-svlan-level = 0x8100
```

Showing PCAP port information

The **show diag pcap port** command displays all PCAP ports that are enabled.

To display information about PCAP ports, use the following command:

```
show diag pcap port
```

Figure 9 shows sample output for the **show diag pcap port** command. This command is issued from the primary CPU.

Figure 9 show diag pcap port command output

```
Passport-8606:5# show diag pcap port
        Port      mode
        ====      ====
          2/20    rx
```

Showing all PCAP information

The **`show diag pcap show-all`** command displays the output from all **`show diag pcap`** commands.

To display all information related to PCAP, use the following command:

```
show diag pcap show-all [file <value>]
```

where:
value is the filename to which the output will be redirected.

Figure 10 and Figure 11 show sample output for the **`show diag pcap show-all`** command. This command can be issued from both the primary CPU and the PCAP engine.

Figure 10 show diag pcap show-all command output

```
Passport-8606:6# show diag pcap show-all

# show diag pcap dump

        Command not allowed in Primary CPU

# show diag pcap capture-filter

================================================================
                                          PCAP Capture-filters
================================================================

        Id : 7
        action : capture
        enable : true
        srcmac : 00:00:00:00:00:00 Mask = 6
        dstmac : 00:00:00:00:00:00 Mask = 6
        srcip : 0.0.0.0 to 0.0.0.0
        dstip : 0.0.0.0 to 0.0.0.0
        vlan-id : 0 to 0
        pbits : 0 to 0

        ether-type : 0x0 to 0x0
        protocol-type : 6 to 6
        dscp : 0 to 0
        udp-port : 0 to 0
        tcp-port : 0 to 0
        user-defined: Offset: 0 Data:
        timer : 0 ms
        packet-count : 0
        refresh-timer : 0 ms
```

Figure 11 show diag pcap show-all command output (continued)

```
============================================================

# show diag pcap info

        enable = FALSE
        buffer-wrap = TRUE
        pcmcia-wrap = TRUE
        buffer-size = 32 MB
        fragment-size  = 64 Bytes
        auto-save = TRUE
        AutoSaveFilename = pcap.cap

        AutoSaveDevice = pcmcia
        ether-type-for-svlan-level = 0x8100


# show diag pcap port

          port        mode
          ====        ====
           4/1    rxFilter


# show diag pcap stats

        Stat Information for PCAP
        =========================
        Packet Capacity Count : 363636
        Number of packets received in PCAP engine : 0
        Number of packets accumulated in PCAP engine : 0
        Number of packets dropped in PCAP engine by filters : 0
        Number of packets dropped in Hardware : 0
Passport-8606:6#
```

Showing PCAP statistics

The **`show diag pcap stats`** command displays PCAP port statistics.

To display all PCAP statistic information, use the following command:

```
show diag pcap stats
```

Figure 12 shows sample output for the **`show diag pcap stat`** command. This command can be executed in the Primary and the PCAP engine.

Figure 12 show diag pcap stat command output

```
Passport-8606:6# show diag pcap stats
        Stat Information for PCAP
        =========================
        Packet Capacity Count : 340909
        Number of packets received in PCAP engine : 10
        Number of packets accumulated in PCAP engine : 10
        Number of packets dropped in PCAP engine by filters : 0
        Number of packets dropped in Hardware : 0
```

Table 1 defines the show diag pcap stats counters.

Table 1 PCAP statistic counters

Statistic	Description
Packet Capacity Count:	This is the maximum number of packets that currently can be stored in the PCAP engine buffer. Reset-stat will not reset this value.
Number of packets received in PCAP engine:	This is the number of packets currently in the PCAP engine buffer. When buffer-wrap occurs, this is set to 0 and the count starts again. **Note:** When buffer-wrap occurs, the second field is set to 0 and the third field is not set to zero. From the capture log, the user can determine how many times buffer-wrap has occurred.

Table 1 PCAP statistic counters

Statistic	Description
Number of packets accumulated in PCAP engine:	This is the number of packets accumulated in the PCAP engine. **Note:** When buffer-wrap occurs, the second field is set to 0 and the third field is not set to zero. From the capture log, the user can determine how many times buffer-wrap has occurred.
Number of packets dropped in PCAP engine by filters:	The number of packets dropped when ingress packets match the filter criteria and the PCAP *action* is set to **drop**.
Number of packets dropped in Hardware:	The number of packets dropped by the PCAP engine hardware when the amount of packets being forwarded can not be processed.

Copying captured packets to a remote machine

If PCAP is used with `autosave` disabled, captured packets will be stored in the PCAP engine DRAM buffer. To copy the packets captured to a file for later viewing, use the CLI `copy` or FTP `get` commands. These commands can be executed in the Primary CPU.

To use the CLI copy command, use the following:

```
copy PCAP00 /<device>/<filename>
```

where:
`PCAP00` indicates the DRAM buffer.
`device` is pcmcia, flash, or an IP host.
`filename` is (filename.cap).

To use the FTP get command, use the following command:

```
ftp> get PCAP00 <filename>
```

where:
`PCAP00` indicates the DRAM buffer.
`filename` is in the format *`filename`*.cap.

Resetting the PCAP DRAM buffer

To reset the PCAP engine DRAM buffer, use the following command sequence from the PCAP engine:

```
config diag pcap enable false
config diag pcap reset-stat
```

The **`reset-stat`** command can be issued only after disabling PCAP. Issuing the command clears the DRAM buffer and the PCAP counters.

Chapter 3
Configuring PCAP with Device Manager

Device Manager supports PCAP configuration commands. Device Manager commands are supported through the primary CPU. The user needs to connect to the primary CPU to perform PCAP configuration.

This chapter includes the following topics:

Enabling PCAP globally

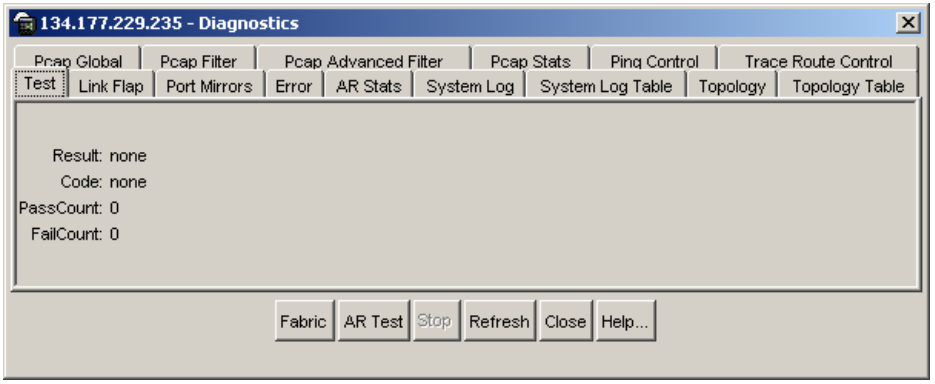
Global parameters are configured to define among other things, where captured frames are to be stored, the size of the DRAM buffer required to store frames, the frame size of the captured packet, and other characteristics of the frame set.

To configure PCAP global parameters:

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

The Diagnostics dialog box opens with the Test tab displayed (Figure 13).

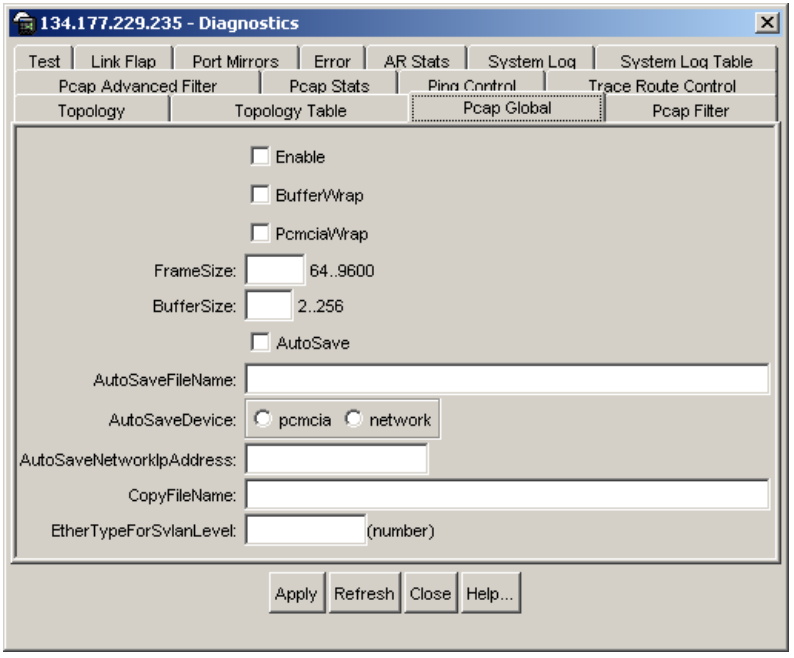
Figure 13 Diagnostics dialog box—Test tab



2 Click the PcapGlobal tab.

The PcapGlobal tab opens (Figure 14).

Figure 14 Diagnostics dialog box—PcapGlobal tab



3 Enter the appropriate information.

4 Click Apply.

Table 2 describes the PcapGlobal tab fields.

Table 2 PcapGlobal tab fields

Field	Description
Enable	Enable or Disable PCAP globally on the PCAP engine.
BufferWrap	This is used to enable buffer wrap-around when the buffer is full. When set, PCAP will continue to capture packets, otherwise packet capturing stops.
PcmciaWrap	When enabled, this will cause an overwrite of the present file in the PCMCIA during auto-save.
FrameSize	The number of bytes of each packet that will be captured.
BufferSize	The amount of memory to be allocated for storing data.
AutoSave	Set this parameter to save data automatically when the buffer is full.
AutoSaveFilename	The name of the file in which packets are stored.
AutoSaveDevice	The type of device used to store the captured packets. If the device is network, the user also needs to enter an IP address.
AutoSaveNetworkIpAddress	This is the IP address of the remote host where the data needs to be stored. This field is valid only if the device is network.
CopyFileName:	The file name to use when copying the PCAP capture file from the PCAP engine DRAM or a PCMCIA device, to a remote client (user's local machine).
EtherTypeForSvlanLevel	Specifies the Ethernet type for SVLAN packets. With this information, PCAP can identify and capture the tag information of packets received from SVLAN. The value for this field is a hexadecimal number.

Enabling PCAP on a port

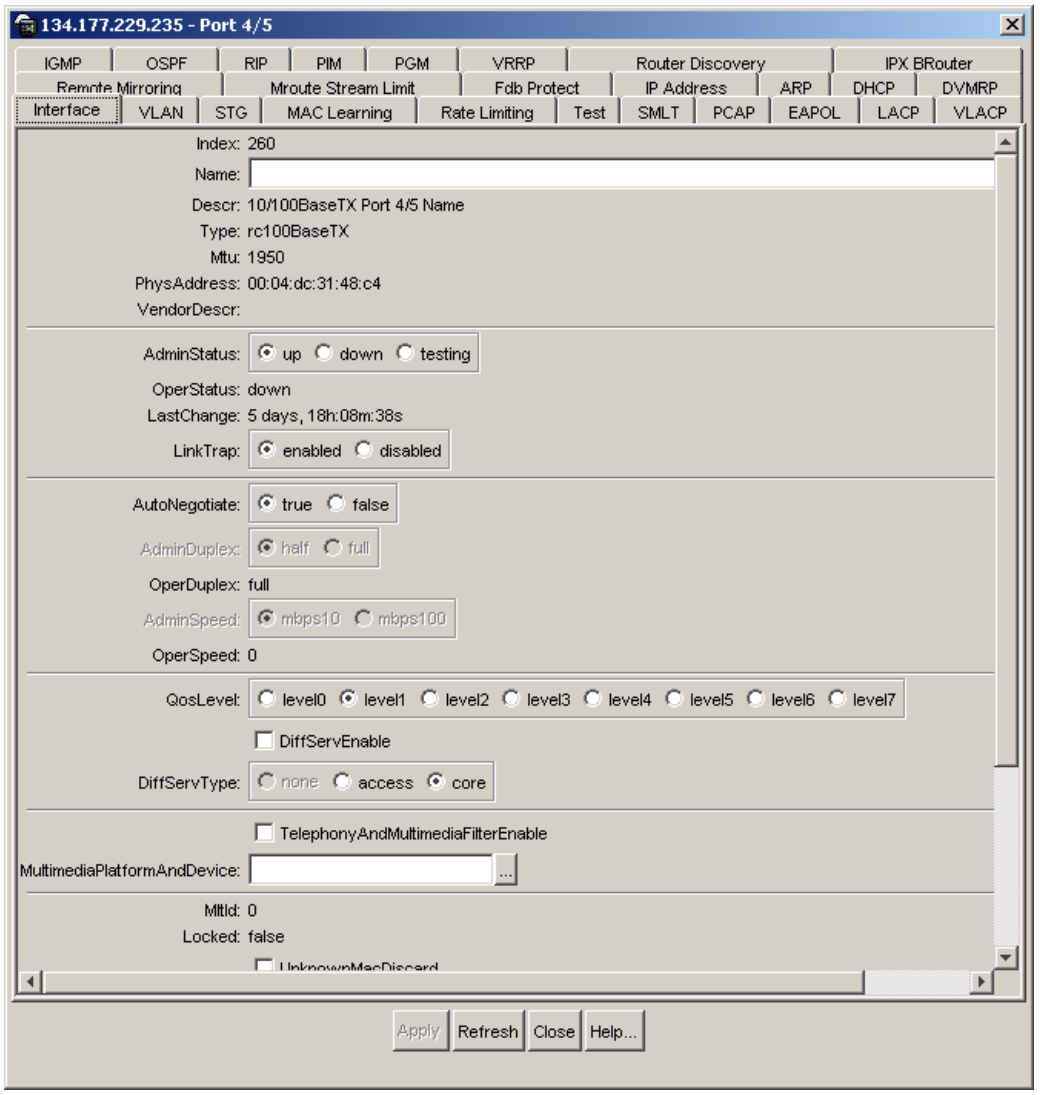
PCAP is enabled on an Ethernet, ATM, or POS ports. IP traffic filter sets are created, added, and enabled.

To configure PCAP 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 (Figure 15).

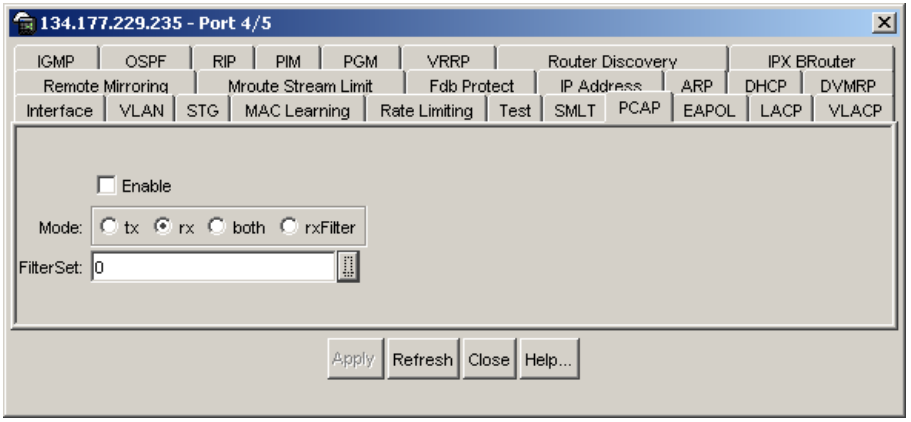
Figure 15 Port dialog box—Interface tab



3 Click the PCAP tab.

The PCAP tab opens (Figure 16).

Figure 16 Port dialog box—PCAP tab



4 Click Enable.

5 Select a mode.

6 Click the FilterSet button and select a filter set.

7 Click Apply.

Table 3 describes the PCAP tab fields.

Table 3 PCAP tab fields

Field	Description
Enable	Enable or Disable PCAP for the port.
Mode	Sets the mode in which PCAP is enabled. The valid values are rx, tx, both, or rxFilter. When PCAP is enabled in rxFilter mode, only ingress packets which match the filter criteria will be captured. The default is rx.
FilterSet	Adds an IP filter set (Global or Source Destination) to a port. The IP filter set must be created prior to performing this function. Filter Global Set ID values are in the range of 1…100 and Source/ Destination sets are in the range of 300…1000.

Configuring PCAP filters

You can use Device Manager to define the match criteria used to capture packets. This is done to further narrow the scope of the types of packets to be captured.

To configure match criteria used to capture packets:

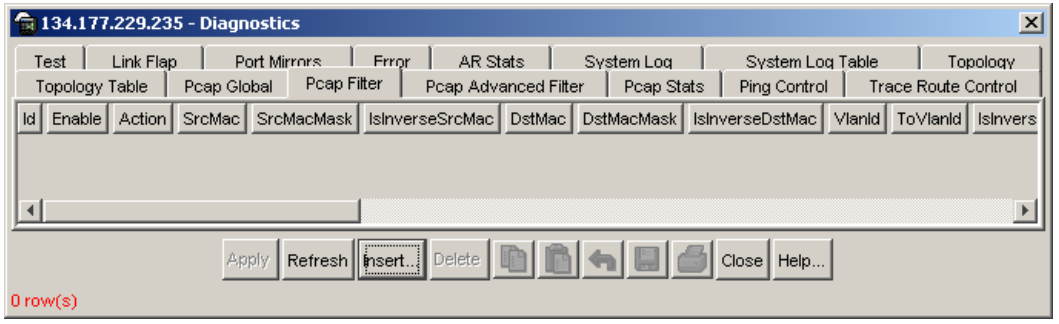
1. From the Device Manager menu bar, choose Edit > Diagnostics.

   The Diagnostics dialog box opens with the Test tab displayed (Figure 13).

2. Click the PcapFilter tab.

   The PcapFilter tab opens (Figure 17).

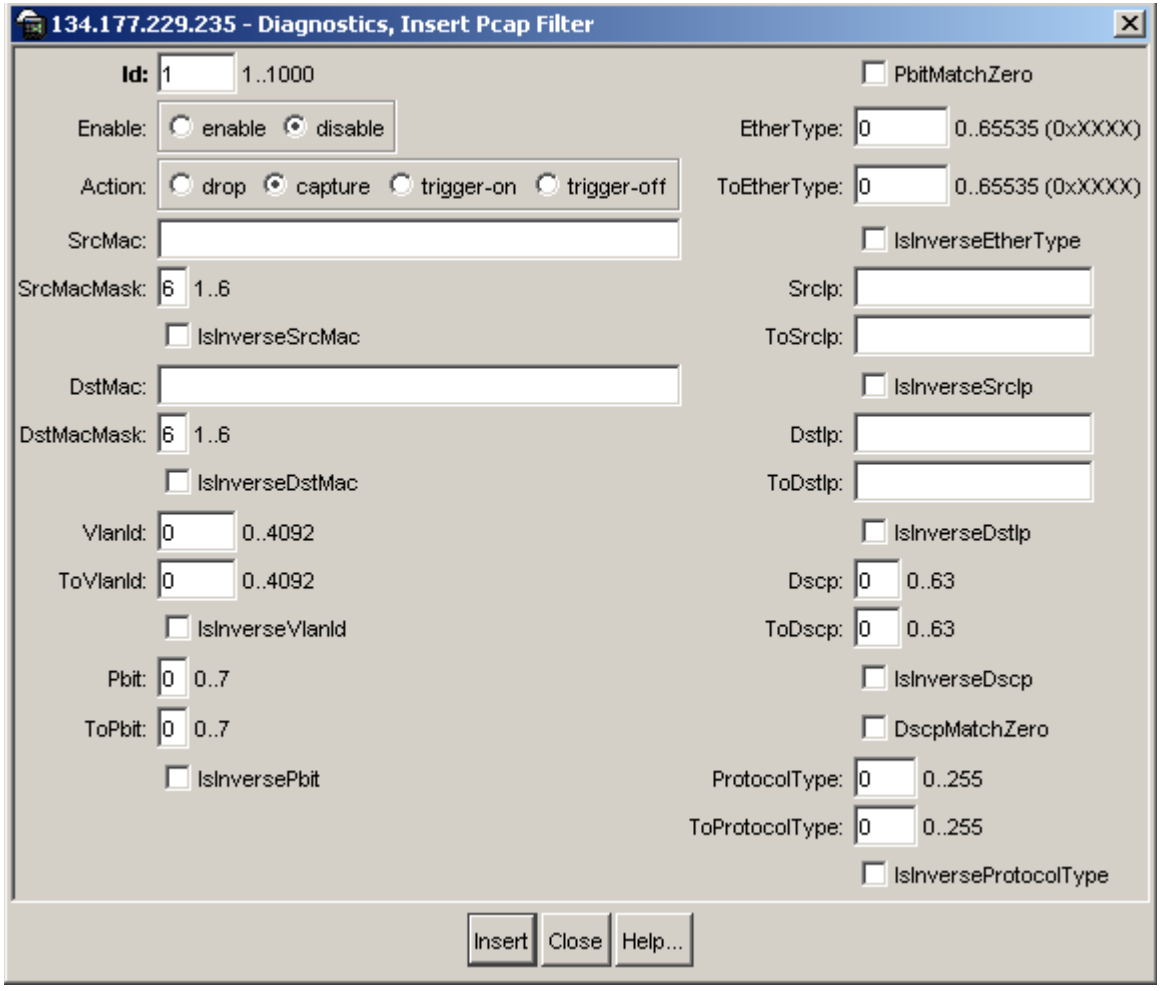
Figure 17 Diagnostics dialog box—PcapFilter tab



3. Click Insert.

   The Diagnostics, Insert PcapFilter dialog box opens (Figure 18).

Figure 18 Diagnostics, Insert PcapFilter dialog box



4 Click Insert.

Table 4 describes the PcapFilter dialog box fields.

Table 4 PcapFilter dialog box fields

Field	Description
Id	The unique ID that represents the filter.
Enable	This field is used to enable or disable the filter.
Action	The action to be taken when the policy is matched.

Table 4 PcapFilter dialog box fields

Field	Description
SrcMac	The Source MAC address to match.
SrcMacMask	The Source MAC address mask. This is used to specify an address range.
IsInverseSrcMac	The Source MAC address inverse. When this is set, the MAC addresses other than the one specified are matched.
DstMac	The Destination MAC address.
DstMacMask	The Destination MAC address mask. This is used to specify an address range.
IsInverseDstMac	The Destination MAC address inverse. When this is set, the MAC addresses other than the one specified are matched.
VlanId	The VLAN ID of the packet to be matched.
ToVlanId	The destination VLAN ID. This is used to specify a range.
IsInverseVlanId	The VLAN ID inverse. When this is set, the VLAN ID other than the one specified are matched.
Pbit	The Pbit of the packet to be matched.
ToPbit	This is used to specify a Pbit range.
IsInversePbit	The Pbit inverse. When this is set, the Pbit other than the one specified are matched.
PbitMatchZero	When this is set, 0 is considered a valid value. Otherwise, 0 is considered a disable value.
EtherType	The EtherType of the packet to be matched.
ToEtherType	This is used to specify an EtherType range.
IsInverseEtherType	The EtherType inverse. When this is set, the EtherType other than the one specified are matched.
SrcIp	The source IP address of the packet to be matched.
ToSrcIp	This is used to specify an SrcIp range.
IsInverseSrcIp	The SrcIp inverse. When this is set, the SrcIp other than the one specified are matched.
DstIp	The destination IP address of the packet to be matched.
ToDstIp	This is used to specify a DstIp range.
IsInverseDstIp	The DstIp inverse. When this is set, the DstIp other than the one specified are matched.
Dscp	The DSCP value of the packet to be matched.
ToDscp	This is used to specify a Dscp range.

Table 4 PcapFilter dialog box fields

Field	Description
IsInverseDscp	The Dscp inverse. When this is set, the Dscp other than the one specified are matched.
DscpMatchZero	When this is set, 0 is considered a valid value. Otherwise, 0 is considered a disable value.
ProtocolType	The ProtocolType of the packet to be matched.
ToProtocolType	This is used to specify a ProtocolType range.
IsInverseProtocolType	The ProtocolType inverse. When this is set, the ProtocolType other than the one specified are matched.

Using advanced PCAP capture filters

To use advanced PCAP capture filter parameters:

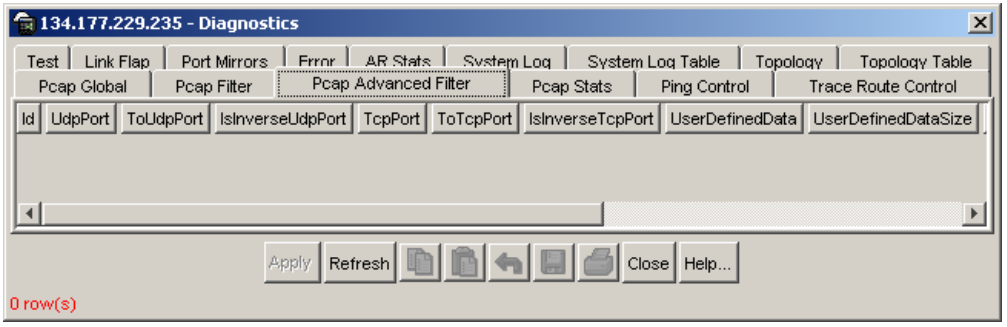
1 From the Device Manager menu bar, choose Edit > Diagnostics.

The Diagnostics dialog box opens with the Test tab displayed (Figure 13).

2 Click the PcapAdvancedFilter tab.

The PcapAdvancedFilter tab opens (Figure 19).

Figure 19 Diagnostics dialog box—PcapAdvancedFilter tab



3 Enter the appropriate fields.

4 Click Apply.

Table 5 describes the PcapAdvanceFilter dialog box fields.

Table 5 PcapAdvanceFilter dialog box fields

Field	Description
Id	The unique ID that represents the filter.
UdpPort	The UDP port of the packet to be matched. UdpPort can be one or a range of UDP port values.
ToUdpPort	Specifies a range of UDP ports.
IsInverseUdpPort	Indicates that all other values other than the specified range of UDP ports are matched.
TcpPort	The TCP port of the packet to be matched.
ToTcpPort	Specifies a range of TCP ports.
IsInverseTcpPort	Indicates that all other values other than the specified range of TCP ports are matched.
UserDefinedData	Specifies the user-defined data to match with the packets received.
UserDefinedDataSize	The length of user-defined data.
UserDefinedOffset	The offset from which the match must start.
IsInverseUserDefined	Indicates that all other data other than the specified user-defined data is matched.
Timer	When set, PCAP will be invoked when the first packet is matched and stopped after the set value of time. After starting the timer, the filter will be disabled. This option is active only when action parameter is set to “trigger-on.” The default value is 0.
PacketCount	When set, PCAP will stop after capturing the specified value of packets. This is similar to the refresh- timer option, once this is invoked, the filter is disabled. This option is active only when the action parameter is set to trigger-on. To delete this option, set it to 0. The default value is 0.
RefreshTimer	When set, this will start or reset a timer. If another packet is not received within the specified time, PCAP will be disabled globally. This option is active only when the action parameter is set to ‘trigger-on’. To delete this option, set it to 0. The default value is 0.

Enabling PCAP with MAC (fdb) filters

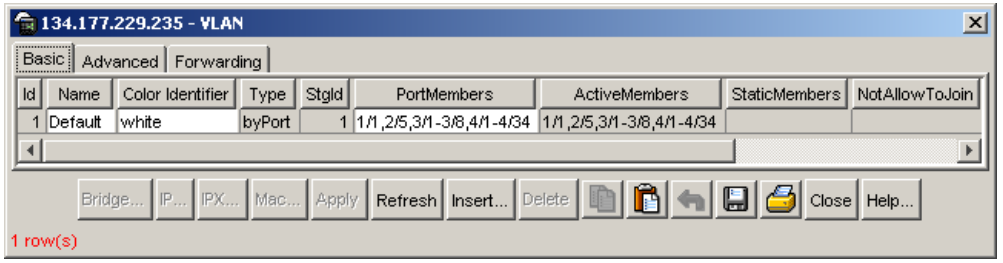
Note: Nortel Networks recommends using PCAP with IP or MAC address filters to reduce traffic flow on the PCAP engine.

To capture packets that match criteria based on MAC address filters:

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

The VLAN dialog box opens with the Basic tab displayed (Figure 20).

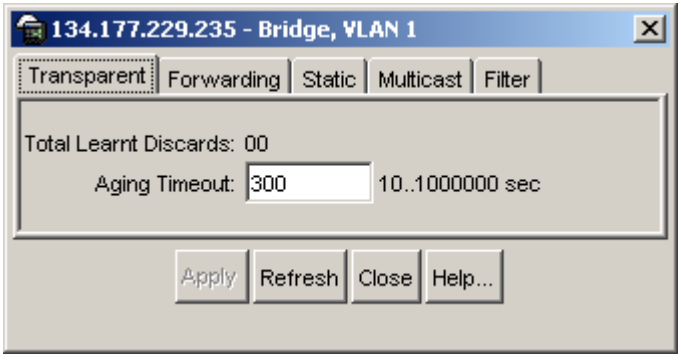
Figure 20 VLAN dialog box—Basic tab



2 In the VLAN dialog box, select a VLAN and click Bridge.

The Bridge, VLAN dialog box opens with the Transparent tab displayed (Figure 21).

Figure 21 Bridge, VLAN dialog box—Transparent tab



3 In the Bridge, VLAN dialog box, click Filter.

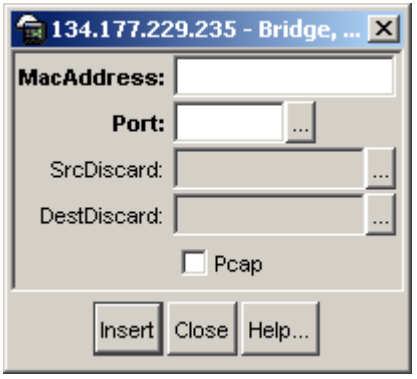
The Filter tab opens (Figure 22).

Figure 22 Bridge, VLAN dialog box—Filter tab

4 Click Insert.

The Bridge, VLAN, Insert Filter dialog box opens (Figure 23).

Figure 23 Bridge, VLAN Insert Filter dialog box



5 Select PCAP.

This field is used to enable or disable PCAP for the fdb-filter.

6 Click Insert.

For information about the other fields on the Bridge, VLAN Insert Filter dialog box, see *Configuring VLANs, Spanning Tree, and Link Aggregation*.

Accessing the PCAP captured frames file

Once packets have been captured in a file, analysis can be performed to determine the cause of network problems.

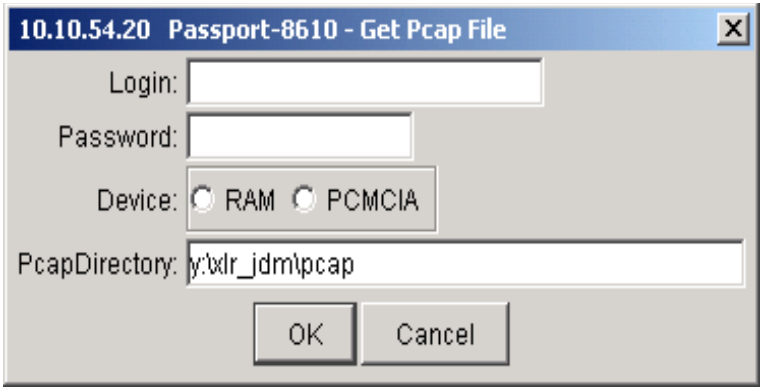
Note: The procedure described below requires that the secondary CPU have a management IP address assigned, and that your JDM client has access to that management network. If either of these conditions are not met, this process will not be successful, and the file will need to be obtained using the CLI. See "Copying captured packets to a remote machine" on page 45.

To access the PCAP captured packets file:

1. From the Device Manager menu bar, choose Actions > Get PCAP File.

   The Get Pcap File dialog box opens (Figure 24).

Figure 24 Get Pcap dialog box



2. Enter your login name and password for the PCAP engine (secondary CPU).
3. Click RAM or PCMCIA.

   If you click RAM, the PCAP file is copied from RAM. If you click PCMCIA, the PCAP file is copied from a PCMCIA device.

4. In the PcapDirectory field, enter the directory path where you want the file to be stored.

5 Click OK.

Table 6 describes the Get Pcap File dialog box fields.

Table 6 Get Pcap File dialog box fields

Field	Description
Login	The rwa (read-write-all) user name for the PCAP engine (secondary CPU).
Password	The password for the read-write-all account.
PcapDirectory	The directory name to use when copying the PCAP capture file from the PCAP engine DRAM or a PCMCIA device, to a remote client (user's local machine). If you leave this field blank, when you transfer the PCAP capture file, the files are saved in the JDM root directory (for example, y:/JDM) on the local machine.

Viewing PCAP statistics

To view PCAP statistics:

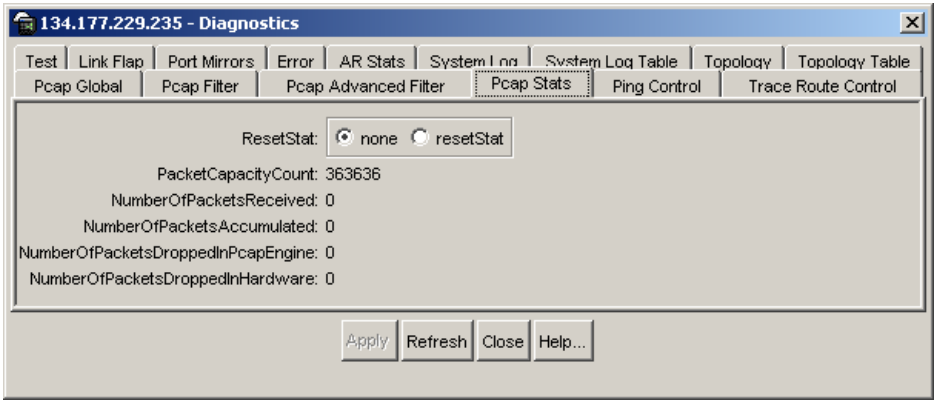
1 From the Device Manager menu bar, choose Edit > Diagnostics.

The Diagnostics dialog box opens with the Test tab displayed (Figure 13).

2 Click the PcapStat tab.

The PcapStat tab opens (Figure 25).

Figure 25 Diagnostics dialog box—PcapStat tab



3 If you want to clear the statistics counter, select resetStat and then click Apply. To display current statistics, click Refresh.

Table 7 describes the PcapStat tab fields.

Table 7 PcapStat tab fields

Field	Description
ResetStat	Resets the PCAP engine DRAM buffer, as well as all software counters used for PCAP statistics.
PacketCapacityCount	This is the maximum number of packets that currently can be stored in the PCAP engine buffer. ResetStat will not reset this value.
NumberOfPacketsReceived	This is the number of packets currently in the PCAP engine buffer. When buffer-wrap occurs, this is set to 0 and the count starts again. **Note:** When buffer-wrap occurs, the second field is set to 0 and the third field is not set to zero. From the capture log, the user can determine how many times buffer-wrap has occurred.
NumberOfPacketsAccumulated	This is the number of packets accumulated in the PCAP engine. **Note:** When buffer-wrap occurs, the second field is set to 0 and the third field is not set to zero. From the capture log, the user can determine how many times buffer-wrap has occurred.

Table 7 PcapStat tab fields

Field	Description
NumberOfPacketsDroppedInPcapEngine	The number of packets dropped when ingress packets match the filter criteria and the PCAP action is set to drop.
NumberOfPacketsDroppedInHardware	The number of packets dropped by the PCAP engine hardware when the amount of packets being forwarded cannot be processed.

Chapter 4
PCAP limitations and considerations

This chapter describes the limitations and considerations of the PCAP tool.

- PCAP is now compatible with HA-CPU.
- Flow control packets may be issued if port performance is affected while PCAP is enabled.
- As the PCAP feature is based on the mirroring capabilities of the I/O ports, limitations that apply to port mirroring also apply to PCAP. These limitations include:
  - — Egress packet capture is supported only with Passport E-modules.
  - — PCAP can not be enabled on a port that has port mirroring currently enabled.
  - — PCAP can not be enabled if PCAP or port mirroring is enabled on any other port on the same Octapid. For 10/100 ports, there is one Octapid for every 8 ports. Therefore, ports 1-8 use one Octapid, ports 9-16 use another Octapid, ports 17-24 use another Octapid, and so on. For all Gigabit, ATM, and POS ports, each port has its own Octapid. The only exception is the Passport 8616 module, which has 2 Gigabit ports for each Octapid. For this module, ports 1 and 2 share an Octapid, ports 3 and 4 share an Octapid, and so on.
  - — Control packets that are copied to the primary CPU will not be captured using non Passport E-modules
- When setting capture-filter parameters for PCAP, a value of ‘0’ when used in setting the range of values will be accepted. The value of ‘0’ will cause the filter parameter to be disabled (a value of ‘0’ means the filter parameter is disable). Do not use '0' in setting a range of values in a filter parameter. (Q00518533)

- When the secondary CPU cycles in the PCAP engine are used for packet capturing and if the packet incoming rate is high (about 200 Mbps), the log messages and certain CLI commands executed in the secondary CPU will be queued. This will be recovered once the packet capturing is completed. For immediate recovery, disable PCAP on the individual ports in the primary CPU on which packets are to ingress. The packets captured until this time will be stored in the buffer. (Q00537576)
- To autosave using an anonymous FTP session to a Windows system, first create a "/pub" sub-directory in "c:" directory or the drive which is default for the FTP server. (Q00524278)
- Data traffic captured from the 8672ATM or 8683POS ports does not contain any ATM or POS encapsulation information. Only the Ethernet frame format is available in the capture file. (Q00522183)
- PCAP uses two levels of filtering to capture packets: one at the hardware level and one at the software level. The hardware level uses the existing IP filters; the software level uses capture filters. The **`config ethernet <ports> pcap add set`** command allows you to add IP filters for the specified port for PCAP and for regular IP traffic filtering. Therefore, when you use the **`config ethernet <ports> pcap info`** command, you may see filter set values that are specific to IP traffic filters only.

  The **`config ethernet <ports> pcap enable`** command allows you to enable or disable PCAP on the port. When you use the **`config ethernet <ports> pcap info`** command, the information displayed for the enable parameter refers to PCAP only (that is, if enable is set to true, this means that PCAP is enabled for the specified interface). (Q00614444)
- If you use an IP filter as a PCAP filter to capture packets, then you disable PCAP globally and at the port level, the IP filter remains active. (Q00624142)

- If you want your PCAP config file to be restored after a CPU-failover, you must source the config file after the standby CPU becomes the master. Otherwise, the PCAP config file will not be loaded. (Q00632891)
- If you globally disable PCAP, the number of packets dropped in hardware will continue to go up unless you also disable PCAP on the port. To disable PCAP on the port, use the **config {ethernet|atm|pos} <*ports*> pcap** command. (Q00630688)

Chapter 5
PCAP examples

This chapter provides examples showing how PCAP is used to solve common network problems. It provides a sample network configuration and includes examples of PCAP CLI commands used to solve these problems. For a complete description of all available CLI commands you can use to configure PCAP, including those shown in this chapter, refer to Chapter 2, “Configuring PCAP with CLI,” on page 23.

Problem definition

You are the network administrator at a large multi-national software company. A user calls and states they are trying to download some data from an FTP server to their client machine. However, they are having a problem connecting to the FTP server. The FTP client resides on client 1 and the FTP server is on client 2.

The FTP server is connected to a Passport 8600 switch (R1) through port interface 2/10, see Figure 26.

Hardware configuration

This section describes the hardware configurations that are assumed for each PCAP solution example.

- One Passport 8600 series switch (R1), with dual CPU modules.
- Each CPU module contains a PCMCIA card.
- Two clients.
- I/O cards are E-modules.

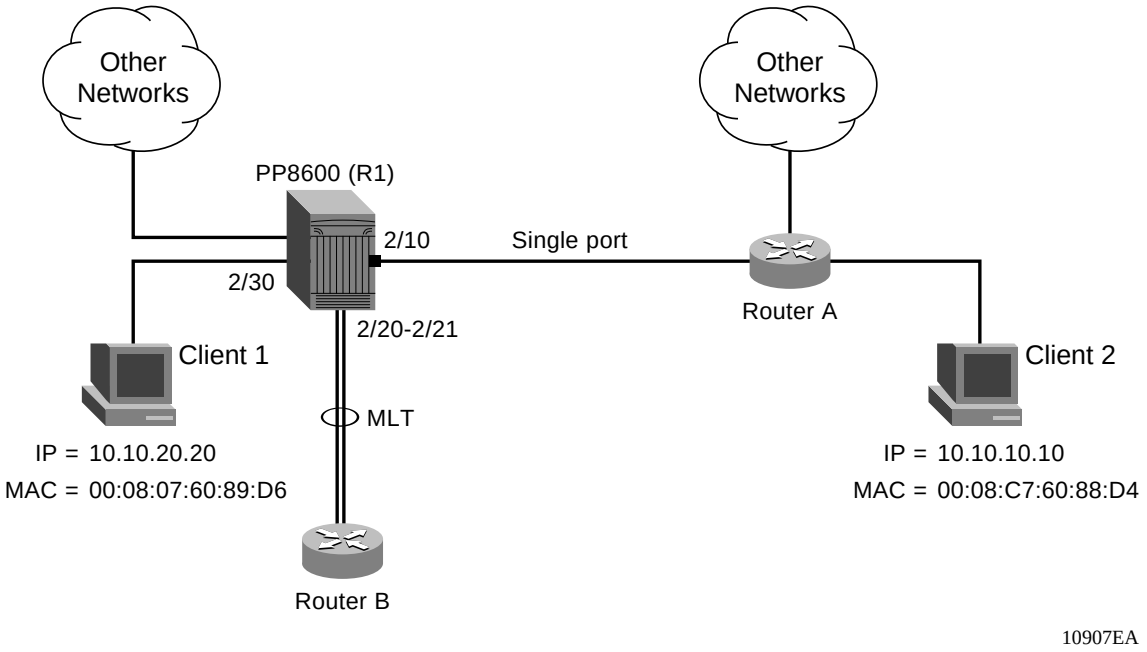
Software configuration

This section describes the software configurations that are assumed for each PCAP solution example.

- An ftp and tftp daemon running on a client server
- Sniffer network software.

Figure 26 shows a sample network configuration used for solving the above problem definition.

Figure 26 Sample Network configuration



Solution 1

In this solution PCAP is configured to capture all packets on port interface 2/10 and have the packets saved on a PCMCIA device. The file containing captured packets is then copied using FTP for analysis at a later time.

To enable PCAP and capture all packets on a port interface complete the following steps:

1 Enable PCAP on ports.

This step will enable PCAP in receive mode on R1, port interface 2/10, to capture all ingress packets and confirm that it is enabled (see Figure 27).

Figure 27 Configure and show command output

```
Passport-8606:6# config ether 2/10 pcap enable true
Passport-8606:6# show diag pcap port
        Port      mode
        ====      ====
          2/10    rx
```

2 Configure PCAP global parameters.

Configure the PCAP parameter `auto-save` (see Figure 28) to automatically save the captured packets, assign a `file-name`, and set the `device to` PCMCIA. All other parameters will use default values. See “Configuring PCAP global parameters” on page 29.

Figure 28 Configuring PCAP global parameters

```
Passport-8606:5# config diag pcap auto-save true file-name
pcap_test.cap device pcmcia
```

3 Enable PCAP.

Enable the PCAP and display the parameter values. Packet capture begins when PCAP is enabled. Figure 29 displays that the following parameters are set:

auto-save = True

file-name = pcap_test.cap

Device = PCMCIA

Figure 29 Enable PCAP

```
Passport-8606:5# config diag pcap enable true
Passport-8606:5# show diag pcap info
enable = TRUE
buffer-wrap = TRUE
pcmcia-wrap = TRUE
buffer-size = 32 MB
fragment-size = 64 Bytes
auto-save = TRUE
AutoSaveFilename = pcap_test.cap
AutoSaveDevice = pcmcia
ether-type-for-svlan-level = 0x8100
```

4 Show PCAP statistics.

Connect to the PCAP engine and display the packet capture statistics (see Figure 30).

Figure 30 The show diag pcap stats command output

```
Passport-8606:5# show diag pcap stats
        Stat Information for PCAP
        =========================
        Packet Capacity Count: 363636
        Number of packets received in PCAP engine : 1042
        Number of packets accumulated in PCAP engine : 1042
        Number of packets dropped in PCAP engine by filters : 0
        Number of packets dropped in Hardware : 0
```

5 Copy the captured packets.

After you have disabled PCAP you can copy the captured packets stored in memory to any device using the commands in Figure 31. The filename **`PCAP00`** is an internal name that refers to packets stored the PCAP engine DRAM.

Figure 31 The copy PCAP00 command output

```
Passport-8606:6# copy PCAP00 /pcmcia/pcap_packets.cap
Passport-8606:6# dir -l /pcmcia
  size          date       time       name
--------       ------     ------    --------
171992    APR-22-1998  02:22:02   /pcmcia/pcap_packets.cap

total: 16039936 used: 389120 free: 15650816 bytes
```

You may also copy captured packets stored in the PCAP engine memory to a remote client using the FTP commands in Figure 32.

Figure 32 The FTP get PCAP00 command output

```
C:\WINDOWS\DESKTOP>ftp 10.10.42.54
Connected to 10.10.42.54.
220 Passport FTP server ready
User (10.10.42.54:(none)): rwa
331 Password required
Password:
230 User logged in
ftp> bin
200 Type set to I, binary mode
ftp> hash
Hash mark printing On (2048 bytes/hash mark).
ftp> get PCAP00 pcap_ftp.cap
200 Port set okay
150 Opening BINARY mode data connection
##################################################################
###########
226 Transfer complete
171992 bytes received in 0.38 seconds (452.61 Kbytes/sec)
```

Solution 2

In solution 1 the number of captured packets is quite large. In this case it is necessary to try and capture fewer packets.

In this solution PCAP is configured to further refine the type of packets to be captured. This solution uses IP traffic filters to only capture packets with a source IP address of 10.10.10.10 and a destination IP address of 10.10.20.20. In addition to procedures followed in solution 1, perform the following steps:

1 Configure IP traffic filters.

This step shows how to configure a global IP traffic filter, set the action of the filter to forward, and display the results (see Figure 33).

Figure 33 Configuring IP traffic filters

```
Passport-8606:5# config ip traffic-filter create global src-ip
10.10.10.10/32 dst-ip 10.10.20.20/32 id 5
Global filter 5 is created.
Passport-8606:5# config ip traffic-filter filter 5 action mode
forward
Passport-8606:5# show ip traffic-filter global 5

=========================================================
                                        Ip Traffic-filter Global
Filters
=========================================================

ID  NAME            TYPE            SRC_OPTION DST_OPTION
PROTOCOL        MIRROR
5  global-5      global        ignore    ignore    ignore
false

    DST_ADDR        DST_MASK        DSTPT SRC_ADDR
SRC_MASK        SRCPT
    10.10.20.20     255.255.255.255 0     10.10.10.10
255.255.255.255 0

    TCPCONNECT      MODE                  STOP_ON_MATCH
    false           forward               true

    DS_MT_DS_FIELD  DS_MT_DS_RSVED  DS_MD_8021P     DS_MD_DSCP
    000000          00:disable      0:disable
000000:disable

    DS_PRO_ID       M_ICMP_REQ      M_IP_FRAG       STATISTICS
    0               false           false           disable

    N_H_FORWARD_IP  N_H_UNREACHABLEDROPE
    0.0.0.0         false
```

2 Create a filter set.

This step shows how to create and name an IP filter set (see Figure 34).

Figure 34 Creating a filter set

```
Passport-8606:5/config/ip/traffic-filter/global-set/5# box
Passport-8606:5# config ip traffic-filter global-set 5 create
name pcap_set
Passport-8606:5# config ip traffic-filter global-set 5
add-filter 5
Passport-8606:5# config ip traffic-filter global-set 5 info
Sub-Context: clear config dump monitor show test trace wsm
Current Context:

                     create :
                                  name - pcap_set
                     delete : N/A
                 add-filter : 5
              remove-filter : N/A
```

3 Apply a filter set to the port.

This step adds the filter set to the port 2/10, sets the mode to rxFilter, and displays the information (see Figure 35).

Figure 35 Adding a filter set to a port

```
Passport-8606:5# config ether 2/10 pcap add set 5
Passport-8606:5# config ether 2/10 pcap enable true mode
rxFilter
Passport-8606:5# config ether 2/10 pcap info
                     enable : true
                       mode : rxFilter
```

If the amount of traffic flowing between client 1 and client 2 is still to large for analysis, define a filter by `protocol-type` as shown in solution 3.

Solution 3

In this solution PCAP filters are configured on the PCAP engine to drop all IP packets that are not protocol type 6 and are not FTP packets. In effect this captures all TCP/FTP packets. When used in conjunction with IP filters this narrows down the number of packets captured to TCP/FTP packets flowing from client 2 to client 1 (see Figure 36).

In addition to procedures followed in solution 1, perform the following steps.

Figure 36 Configuring PCAP protocol-type filters

```
Passport-8606:5# config diag pcap capture-filter 7 create

Passport-8606:5# config diag pcap capture-filter 7 action drop

Passport-8606:5# config diag pcap capture-filter 7
protocol-type 6 not
Passport-8606:5# config diag pcap capture-filter 7 tcp-port 20
to 21 not
Passport-8606:5# config diag pcap capture-filter 7 enable true
Passport-8606:5# config diag pcap capture-filter 7 info
        Id : 7
        action : drop
        enable : true
        srcmac : 00:00:00:00:00:00 Mask = 6
        dstmac : 00:00:00:00:00:00 Mask = 6
        srcip : 0.0.0.0 to 0.0.0.0
        dstip : 0.0.0.0 to 0.0.0.0
        vlan-id : 0 to 0
        pbits : 0 to 0
        ether-type : 0x0 to 0x0
        protocol-type : 6 to 6 [not]
        dscp : 0 to 0
        udp-port : 0 to 0
        tcp-port : 20 to 21 [not]
        user-defined: Offset: 0 Data:
        timer : 0 ms
        packet-count : 0
        refresh-timer : 0 ms
```

If the amount of traffic flowing between client 1 and client 2 continues to be to large for analysis, define a filter using the `action` parameter as shown in solution 3.

Solution 4

In this solution PCAP is configured to start packet capture when the first TCP/FTP packet arrives at the port which also enables PCAP automatically. This is done by setting the `trigger-on` parameter. Prior setting the trigger-on filter, PCAP should be disabled. PCAP is disabled after the first 1000 packets are captured by setting the `packet-count` parameter (see Figure 37).

In addition to procedures followed in solution 1, perform the following.

Figure 37 Configuring PCAP trigger filters

```
Passport-8606:5# config diag pcap enable false
Passport-8606:5# config diag pcap  capture-filter 10 create
Passport-8606:5# config diag pcap capture-filter 10
protocol-type 6
Passport-8606:5# config diag pcap capture-filter 10 tcp-port 20
to 21
Passport-8606:5# config diag pcap capture-filter 10 action
trigger-on
Passport-8606:5# config diag pcap capture-filter 10 enable true
Passport-8606:5# config diag pcap capture-filter 10
packet-count 1000
Passport-8606:5# config diag pcap capture-filter 10 info
        Id : 10
        action : trigger-on
        enable : true
        srcmac : 00:00:00:00:00:00 Mask = 6
        dstmac : 00:00:00:00:00:00 Mask = 6
        srcip : 0.0.0.0 to 0.0.0.0
        dstip : 0.0.0.0 to 0.0.0.0
        vlan-id : 0 to 0
        pbits : 0 to 0
        ether-type : 0x0 to 0x0
        protocol-type : 6 to 6
        dscp : 0 to 0
        udp-port : 0 to 0
        tcp-port : 20 to 21
        user-defined: Offset: 0 Data:
        timer : 0 ms
        packet-count : 1000
        refresh-timer : 0 ms
```

Index

R

S

T

U

V