Part No. 317359-A Rev 0.00
May 2004

4655 Great America Parkway
Santa Clara, CA 95054

Using Diagnostic Tools

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

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

Before you begin

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

- 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`.
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:

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.

You can purchase printed books and documentation sets from Vervante. To order printed documentation, go to Vervante at the www.vervante.com/nortel URL.

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 one of the following Nortel Networks Technical Solutions Centers:

Technical Solutions Center	Telephone
Europe, Middle East, and Africa	(33) (4) 92-966-968
North America	(800) 4NORTEL or (800) 466-7835
Asia Pacific	(61) (2) 9927-8800
China	(800) 810-5000

Additional information about the Nortel Networks Technical Solutions Centers is available from the www.nortelnetworks.com/help/contact/global URL.

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
Diagnostic Tools Overview

This chapter provides overview information about diagnostic tools. Specifically, it includes information about the following topics:

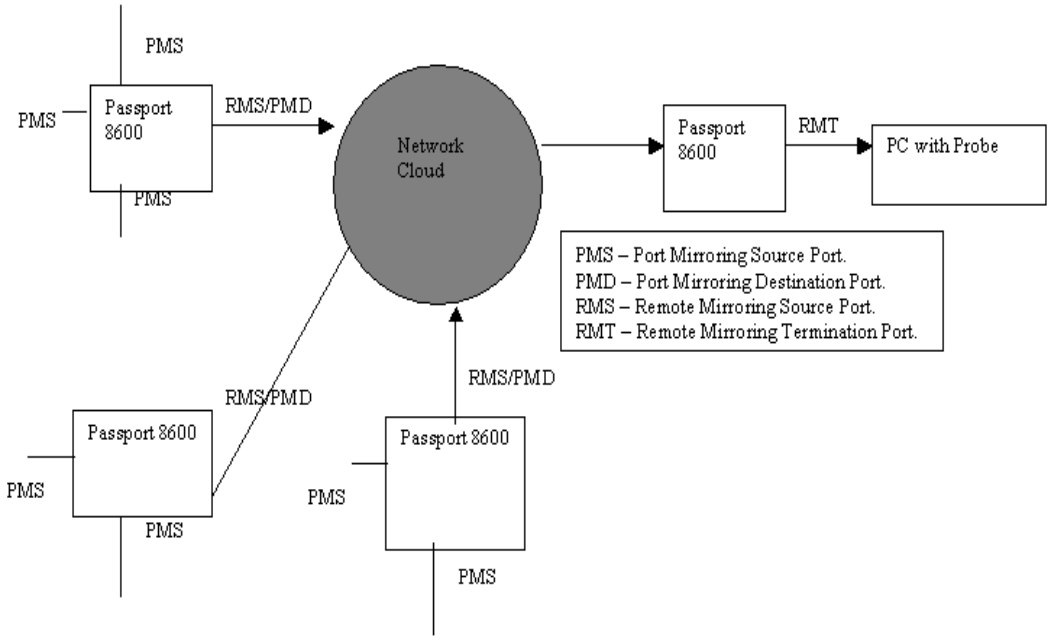
Syslog

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

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

Remote Mirorring

Remote mirroring provides the feature to steer mirrored traffic through a switch cloud to a network analysis probe located on a remote switch. In a network, this feature allows the user, to monitor many ports from different switches using one network probe device. This function is achieved by encapsulating mirrored packets in a Remote Mirroring Encapsulation “wrapper”. The encapsulated frame can be bridged though the network to the remote diagnostic termination port. Remote mirroring Encapsulation “wrapper” is 20 bytes in length and consists of a Layer 2 Destination Address, Layer 2 Source Address, Monitor Tag, Monitor EtherType, and Monitor Control. The original CRC-32 is stripped from a mirrored packet, and a new CRC-32 is computed over the entire encapsulated frame. When the mirrored frame is 1522 bytes (1518 plus 4-byte 802.1p/q tag), the resulting maximum frame length is 1542 bytes. To support this, all the nodes in the network should have the capability to handle packets of size 1542. At the termination port, the encapsulation is removed before sending it out of the port. Source port for Remote Mirroring is called Remote Mirroring Source (RMS) and the destination port is called Remote Mirroring Termination (RMT).



Remote Mirrored Packet Format

The Mirror Destination Address (Mirror DA), Mirror Source Address (Mirror SA) (The three least significant bits of the Mirror SA byte are derived from the port number) and mirror etherType are user configurable parameters under remote-mirroring node. The Mirror Tag field is generated from the “IEEE VLAN ID” configured under port mirroring.

6 Bytes	6 Bytes	4 Bytes	2 Bytes	2 Bytes	6 Bytes	6 Bytes	1506 Bytes	4 Bytes
MirrorDA	MirrorSA	MirrorTag	MirrorEtherType	MirrorControl	Original DA	Original SA	Mirrored Frame	CRC-32

Behavior

When an RMS receives a mirrored packet from switch fabric, before sending it out on the port, the octapid will encapsulate the packet with remote mirroring wrapper as the packet is being transmitted on the port. This header will have remote mirroring Encapsulation Wrapper. So the packet will be sent to the destination mac in this encapsulation. Remote mirrored packets sent out of RMS are always tagged (with Remote mirroring Tag).

When a RMT port receives an encapsulated frame from the switch fabric, it strips off the Remote Mirroring Encapsulation, as it is being transmitted on the port. Remote mirrored encapsulated frames are identified when the configured “remote mirroring destination mac Address” is detected as the “destination MAC address” in the packet. RMT sends dummy broadcast Layer-2 packets with “remote mirroring destination mac” as source mac so that all nodes in the network can learn this mac address. This is sent every 10 seconds (as the minimum value of FDB-aging timer is 10 seconds). When a port is configured as RMT, a static FDB entry is added to channel all traffic destined for the remote mirroring destination mac to RMT port. When an RMT port is removed from the all VLAN configured, the Remote Mirroring feature on the port is disabled.

- Only RWA user will be allowed to configure Remote mirroring.
- Remote mirrored packets will be sent with lowest priority (pBit value of 0).
- RMS port has to be a port mirror destination port. Only mirrored packets will be remote mirrored. This check is not done when RMS is enabled on the port. No error message will be generated while RMS is configured on a port, which is not a port mirroring destination port. If port mirroring is disabled, then no packets will be remote mirrored. Whenever user is using remote mirroring, user has to make sure that the port mirroring is enabled with RMS port as mirror destination Port.
- If RMS is a tagged port, then the remote mirroring packet will be sent with vlan id of that of mirrored packet (Original Packet).
- RMT has to be part of at least one port based VLAN.
- Packets will be captured as long as RMT is reachable.
- Whenever user enables/disables Remote mirroring, a Trap is sent to trap receiver and a SMP log message is generated stating that remote mirroring is enabled/disabled and the mode.

- When an I/O card is removed from a slot, RMS/RMT on all ports in the slot will be disabled. A SMP log message and a trap is generated for the same. The RMS/RMT will not be re-enabled even if the user re-inserts the same card. User has to enable Remote mirroring once the card is inserted back.
- The RMT switch should receive the remote mirroring packet with complete remote mirroring encapsulation (Including the remote mirroring tag).

Hardware Requirements or Dependencies

For Remote Mirroring packets, the I/O card hardware should support port mirroring and remote mirroring. E-Tickets cards are required to remotely capture Egress packets from a port. Remote mirroring encapsulation header size is 20 Bytes. When the mirrored frame is 1522 bytes (1518 plus 4-byte 802.1p/q tag), the resulting maximum frame length is 1542 bytes. To support this, all the nodes in the network should have the capability to handle packets of size 1542.

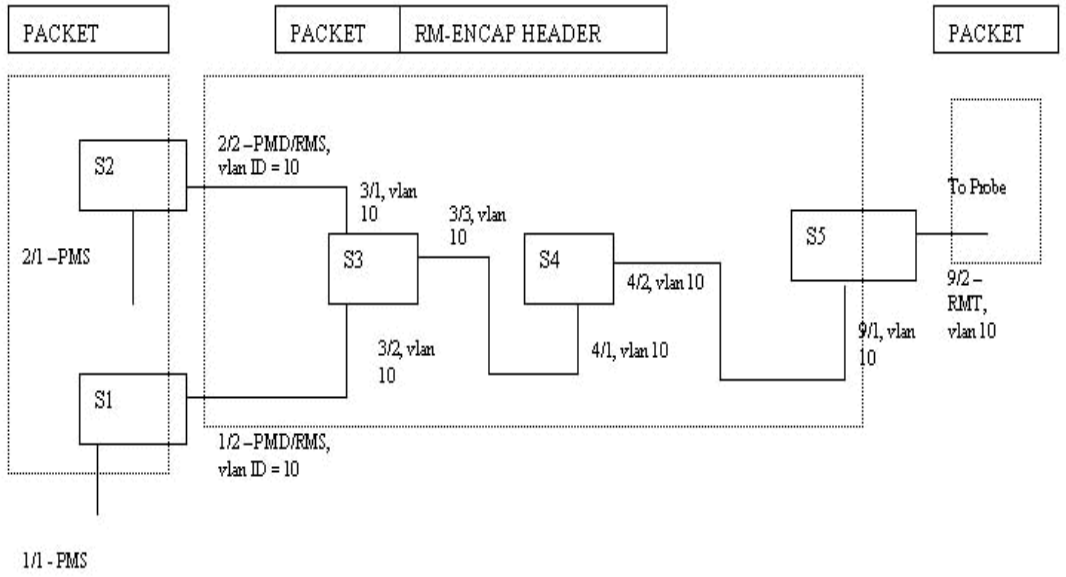
Limitations and restrictions

- Maximum of 16 RMTs can be configured in a switch.
- RMT can be enabled in only one port in an octapid.
- For a port to function as RMS, it has to be a destination Port of port mirroring. Octapid has a limitation of only one port as port mirror destination port. So RMS can be enabled in only one port in an octapid.

Configuration Sequence

To remote mirror a packet, following are the recommended sequence of configuration:

Consider the following network configuration. Requirement is to send the traffic from port 1/1 in Switch S1 and from port 2/1 in Switch S2 to Probe connected to port 9/2 of switch S5.First configure the RMT information in switch S5.



Configurations in Switch S5:

Following are the steps to do the configuration in Switch S5:

- Create a separate port based vlan – say vlan 10 (config vlan 10 create byport <stg id>)
- Add ports RMT and the port in which remote mirrored packet enters the switch to this vlan. In this example ports 9/1 and 9/2 to this vlan (vlan 10). If port 9/1 is already a member of another port based VLAN, then it needs to be tagged before adding it to this vlan (config vlan 10 port add 9/1-9/2)
- Create remote mirroring in RMT port (config ethernet 9/2 remote-mirroring create)
- Add this vlan to remote mirroring configuration in RMT so that RMT switch will broadcast the dummy packets in this vlan. (config ethernet 9/2 remote-mirroring add-vlan-id 10)
- Set the mode to termination for RMT port (config ethernet 9/2 remote-mirroring mode termination)

- Enable RMT (config ethernet 9/2 remote-mirroring enable true). This enables RMT in the port.
- Get the dstmac of the RMT port. This is needed to configure RMS in other switches (config ethernet 9/2 remote-mirroring info).
- Now S5 start sending a L2 dummy packet with dstmac of RMT as source in vlan 10. So all nodes in vlan 10 will learn this MAC address and forward any packet coming to this MAC address to S5.

Note: It is highly recommended to create a separate port based VLAN to channel the remote mirroring traffic in the network.

Configure RMS ports:

Following are the steps to do the configuration in Switch S1:

- Create the remote mirror vlan (vlan 10) (config vlan 10 create byport <stgid>)
- Create port mirroring with RMS port as destination port. Source port is the port from which packets needs to be remotely mirrored (config diag mirror-by-port 1 create in-port 1/1 out-port ½).
- Add PMD port to vlan 10 (config vlan 10 port add 10).
- Set the remote-mirror-vlan to this port mirror entry so that the remote mirrored packets will be sent with this vlan ID in the monitor tag (We have configured vlan 10 in switch 5 for this) (config diag mirror-by-port 1 remote-mirroring-vlanid 10)
- Create remote mirroring in RMS port (config ethernet ½ remote-mirroring create)
- Set the dstmac for remote-mirroring in RMS port. This is the dstmac address of the RMT port from switch 5. (config ethernet ½ remote-mirror dstmac <mac>)
- If needed, set the ether-type for the remote mirroring packet in RMS (config ethernet ½ remote-mirroring ether-type <value>).
- Enable RMS. (config ethernet ½ remote-mirroring enable true)

Note: Similar configuration (as above) needs to be done in switch S2 also.

In switch S3 and S4, the remote mirrored packets are just bridged. Since remote-mirrored packets will be coming with vlan ID 10 (As configured in S1 and S2), the ports in the path should be part of vlan 10. In S3 and S4, create vlan 10 and add ports 3/1-3/3 in S3 and 4/1-4/2 in S4 to vlan 10.

In Switch S4, the port 4/2 should be a tagged port so that the remote mirroring tag will be send to RMT switch (Switch S5)

Packet Flow:

The packets from port 1/1 in Switch S1 (and 2/1 in Switch S2) will be remotely mirrored to port 9/2 in Switch S5.

- First packets entering/leaving port 1/1 (2/1 in Switch S2) will be mirrored to ports ½ in Switch S1 (2/2 in Switch S2) with port-mirroring feature.
- Since these ports (1/2 in Switch S1 and 2/2 in Switch S2) are configured as RMS, before going out of that port, the switch adds a remote mirroring encapsulation to the mirrored packets. The Monitor tag in remote mirroring encapsulation will have vlan-ID as 10 (as configured in port mirroring node) and DstMac of the remote mirroring Encapsulation header as the Remote mirroring DstMac of the RMT port of Switch S5 (As configured in RMS).
- This packet is bridged through Switch S3 and S4 to Switch S5. Switch S3 and S4 will have learned the Remote mirroring DstMac of RMT as Switch S5 sends a dummy L2 packets every 10 secs with this MAC address as SrcMac.
- Remote mirrored packets enter Switch S5 through port 9/1. In Switch S5, there will be a static FDB entry to bridge the packets coming to this Remote mirroring DstMac of RMT to port 9/2.
- The remote mirrored packets are bridged to port 9/2. As it goes out of port 9/2, the octapid removes the remote mirroring encapsulation header since we configure 9/2 as RMT. So to the probe connected to 9/2 of Switch S5, the packets will be exactly same as it enters 1/1 in Switch S1 & 2/1 in Switch S2.

Chapter 2
Using CLI diagnostic tools

This chapter describes the CLI diagnostic tools that you can run on a Passport 8000 Series switch. It includes the following topics:

Roadmap of CLI diagnostic commands

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

Command	Parameter
config diag	info
config diag mirror-by-port <id>	info
	create in-port <value> out-port <value> [mode <value>] [enable <value>>] [remote-mirroring-vlanid <vlan-id>]
	enable <true|false>
	delete
	mirrored-port <port>
	mirroring-port <port>
	mode <tx|rx|both|rxFilter>
show diag mirror-by-port	
show port stats routing	
show port stats dhcp-relay	
show port stats rmon	
show port stats stg	
config cli monitor	info
	duration <integer>
	interval <integer>
clear	atm elan-stats <vlan id>
	atm f5-stats [<ports>]
	atm port-stats [<ports>]
	ip arp ports <port>
	ip arp vlan <vid>
	ip route ports <port>

Command	Parameter
	ip route vlan <vid>
	`ip vrrp ports <ports> vrid <value>`
	`ip vrrp vlan <vid> vrid <value>`
	`mlt ist stats`
	ports stats [<ports>]
	telnet <session id>
`config sys syslog`	`info`
	host <id> address <ipaddr>
	host <id> create
	host <id> delete
	host <id> facility <facility>
	host <id> <enable|disable>
	host <id> info
	host <id> mapinfo <level>
	host <id> mapwarning <level>
	host <id> maperror <level>
	host <id> mapfatal <level>
	host <id> severity <info| warning| error|fatal> [<info|warning| error|fatal>]
	host <id> udp-port <port>
	max-hosts <maxhost>
	`state <enable|disable>`
`show sys syslog`	`general-info`
	host <id> info
dump ar <opid> <vlan|ip_subnet|mac_vlan|mac|arp|ip|ipx| ipmc|ip_filter|protocol|all> <verbosity>	
traceroute <ipaddr> [<datasize>] [-m <value>] [-p <value>] [-q <value>] [-w <value>] [-v]	

Command	Parameter
`trace auto-enable`	`info`
	add-module <modid> <level>
	`auto-trace <enable|disable>`
	high-percentage <percent>
	high-track-duration <seconds>
	low-percentage <percent>
	low-track-duration <seconds>
	remove-module <modid>
test loopback <ports> [<int|ext>]	
`config log`	`info`
	add-ports <ports>
	create src-ip <value> dst-ip <value>
	`delete`
	`enable <true|false>`
	remove-ports <ports>
`show log file [tail]`	
`config diag ping-snoop`	`info`
	add-ports <ports>
	create src-ip <value> dst-ip <value>
	`delete`
	`enable <true|false>`
	remove-ports <ports>
config ethernet <slot/port> remote-mirroring	`enable <true|false>`
	`mode<source|termination>`
	srcmac <mac>
	dstmac <mac>
	ether-type <ether-type>

Command	Parameter
	add-vlan-id <vlan-id>
	remove-vlan-id <vlan-id>

Configuring and monitoring port mirroring

You use port mirroring for troubleshooting and analyzing network traffic. When using port mirroring, you specify a destination port to see mirrored traffic and specify the source ports from which traffic is mirrored. Any packet ingressing or egressing the specified ports is forwarded normally, and a copy of the packet is sent out of the mirror port. When this feature is active, all packets received on the specified ports are copied to the port specified as out-port. The mirroring operation is nonintrusive.

Note: Ingress mirroring mirrors only packets with valid CRCs.

The Passport 8100 switch supports ingress and egress port mirroring; however egress mirroring is supported only in half-duplex mode.

On a Passport 8600 switch, ingress mirroring is supported by all modules; however, egress mirroring is supported only on Passport E-modules. Refer to the release notes for a list of E-modules.

You set up port mirroring using the **`config diag`** commands. For example, to monitor port 9/2 with output on port 9/3, use the following commands:

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

```
config diag mirror-by-port enable true
config diag mirror-by-port 1 create in-port 9/2 out-port 9/3
```

If you are using a network sniffer, connect the sniffer to port 9/3.

In addition, you can use the VLAN forwarding database feature to monitor traffic for MAC addresses where traffic with a given source or destination MAC address is copied to the mirror port. To avoid seeing unintended traffic, remove the mirroring (destination) port from all VLANs and spanning tree groups (STGs).

This section includes the following port mirroring commands:

Displaying port mirroring settings

To display information about the current port mirroring settings, use the following command:

```
config diag
```

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

`config diag` followed by:	
`info`	Displays information about the current port mirroring setting.

Configuring mirror-by-port entries

To diagnose the system by monitoring/mirroring a port, use the following command:

```
config diag mirror-by-port <id>
```

Note: The required parameter *`id`* is the mirror-by-port entry ID (1 to 383). You can configure one mirroring port and up to 10 mirrored ports.

This command includes the following options:

config diag mirror-by-port <*id*> followed by:	
`info`	Displays current port mirroring settings.
`create in-port` <*value*> out-port <*value*> [mode <*value*>] [enable <*value*>>] `[remote-mirroring-vlanid <vlan-id>]`	Creates a new mirror-by-port table entry. • `in-port` <*value*> is the mirrored port. • `out-port` <*value*> is the mirroring port. Optional parameters: • `mode` *value* sets the mirror mode (see description for `mode`). • `enable` *value* enables the mirroring port (see description for `enable`). • remote-mirroring-vlanid will set the vlan id for the remote mirrored packet.
`enable <true|false>`	Enables or disables a mirroring port already created in the mirror-by-port table.
`delete`	Deletes an entry from the mirror-by-port table.
`mirrored-port` <*port*>	Specifies the mirrored port.
`mirroring-port` <*port*>	Specifies the mirroring port. See "Mirroring ports/ destination ports" for more information.
`mode <tx|rx|both|rxFilter>`	Sets the mirroring mode. • `tx` mirrors transmit packets. • `rx` mirrors receive packets. • `both` mirrors both transmit and receive packets. • `rxFilter` mirrors and filters receive packets.
`remote-mirroring-vlanid <vlanid>`	Remote-mirroring-vlanid will set the vlan id for the remote mirrored packet.

Configuration example

This configuration example uses the above commands to monitor/mirror a port. Figure 1 also uses the **`info`** command to display information about the current port mirroring settings.

Figure 1 config diag command sample output

```
8610:5# config diag
8610:5/config/diag# mirror-by-port 2
8610:5/config/diag/mirror-by-port/2# info

Sub-Context:
Current Context:

8610:5/config/diag/mirror-by-port/2# enable
```

Mirroring ports/destination ports

The number of mirroring ports (also called “destination ports”) that you can configure depends on the type and quantity of modules you have in your system configuration.

The module’s switch fabric determines the quantity of mirrored (source) ports that can be supported by a single mirroring (destination) port, based on the OctaPID ID assignment for that module. For example, a 48-port 10/100TX module is assigned 6 OctaPID IDs, and each OctaPID ID supports up to 8 ports (6 x 8 = 48 ports). You can assign one destination port per OctaPID ID.

When you configure destination ports, the CLI interface automatically assigns the actual OctaPID ID assignment according to the switch fabric in specific Passport 8000 modules. The assignment of the OctaPID ID by the interface follows a fixed set of configuration rules based on the module type.

Source ports that are members of the same OctaPID ID can only be mirrored to the same destination port. If you try to assign source ports that are members of the same OctaPID ID to different destination ports, the CLI will prompt you with an error message. For more information on how the OctaPID ID is used for assigning destination ports, see Appendix D.

Displaying mirrored port information

To display information about mirrored ports on the switch, use the following command:

```
show diag mirror-by-port
```

Configuration example

Figure 2 uses the **show** command to monitor/mirror a port.

Figure 2 show diag mirror-by-port command sample output

```
Passport-8603:3# show diag mirror-by-port
================================================================================
                                        Diag Mirror-By-Port
================================================================================
ID   MIRRORED_PORT   MIRRORING_PORT  ENABLE     MODE REMOTE-MIRROR-VLAN-ID
1    9/2             9/3             true       rx
```

Showing port statistics

You can display port statistics using the CLI. This section includes the following port statistic commands:

Showing port routing statistics

To display routing statistics about ports on the switch, use the following command:

```
show port stats routing
```

Configuration example

Figure 3 uses the **show** command to display routing statistics.

Figure 3 show port stats routing command sample output

```
8610:5# show port stats routing
=============================================================
                      Port Stats Routing
=============================================================
PORT     IN_FRAME   IN_FRAME   IN         OUT_FRAME  OUT_FRAME
NUM      UNICAST    MULTICAST  DISCARD    UNICAST    MULTICAST
-----------------------------------------------------------------------------
8/1      0          0          0          0          0
8/2      0          0          0          0          0
8/3      0          0          0          0          0
8/4      0          0          0          0          0
8/5      0          0          0          0          0
8/6      0          0          0          0          0
8/7      0          0          0          0          0
8/8      0          0          0          0          0
9/1      0          0          0          0          0
9/2      0          0          0          0          0
9/3      0          0          0          0          0
9/4      0          0          0          0          0
9/5      0          0          0          0          0
9/6      0          0          0          0          0
9/7      0          0          0          0          0
9/8      0          0          0          0          0
9/9      0          0          0          0          0
9/10     0          0          0          0          0

8610:5#
```

Showing port DHCP relay statistics

To display DHCP relay statistics about ports on the switch, use the following command:

```
show port stats dhcp-relay
```

Configuration example

Figure 4 uses the **show** command to display DHCP relay statistics.

Figure 4 show port stats dhcp-relay command sample output

```
8610:5# show port stats dhcp-relay

================================================================
                  Port Stats Dhcp
================================================================
PORT_NUM NUMREQUEST NUMREPLY
----------------------------------------------------------------
8610:5#
```

Showing port RMON statistics

To display RMON statistics about ports on the switch, use the following command:

```
show port stats rmon
```

Configuration example

Figure 5 uses the **show** command to display RMON statistics.

Figure 5 show port stats rmon command sample output

```
Passport-8610:5# show port stats rmon

================================================================================
                          Port Stats Rmon
================================================================================
PORT  OCTETS     PKTS    MULTI   BROAD   CRC     UNDER   OVER    FRAG    COLLI
NUM                      CAST    CAST    ALLIGN  SIZE    SIZE    MENT    SION
--------------------------------------------------------------------------------
9/3   0          0       0       0       0       0       0       0       0

8610:5#
```

Showing port STG statistics

To display STG statistics about ports on the switch, use the following command:

```
show port stats stg
```

Configuration example

Figure 6 uses the **show** command to display STG statistics:

Figure 6 show port stats stg command sample output

```
8610:5# show port stats stg

================================================================================
                            Port Stats Stg
================================================================================
PORT      IN_CONFIG  IN_TCN     IN_BAD     OUT_CONFIG OUT_TCN
NUM       BPDU       BPDU       BPDU       BPDU       BPDU
--------------------------------------------------------------------------------
8/1       0          0          0          0          0
8/2       0          0          0          0          0
8/3       0          0          0          0          0
8/4       0          0          0          0          0
8/5       0          0          0          0          0
8/6       0          0          0          0          0
8/7       0          0          0          0          0
8/8       0          0          0          0          0
9/1       0          0          0          0          0
9/2       0          0          0          0          0
9/3       0          0          0          0          0
9/4       0          0          0          0          0
9/5       0          0          0          0          0
9/6       0          0          0          0          0
9/7       0          0          0          0          0
9/8       0          0          0          0          0

8610:5#
```

Monitoring port statistics

The **monitor** commands are self-updating **show** commands. To set the monitor duration and interval, use the following command:

```
config cli monitor
```

The **config cli monitor** command include the following options:

config cli monitor followed by:	
`info`	Displays current level parameter settings and next level directories.
`duration <integer>`	Sets the monitor time duration. To clear the display, type Ctrl/L. • <*integer*> is an integer value with a range of 1 to 1800 seconds.
`interval <integer>`	Sets the monitor time interval. To clear the display, type Ctrl/L. • <*integer*> is an integer value with a range of 1 to 600 seconds

Configuration example

This configuration example uses the above commands to set the monitor duration and set the monitor interval. Figure 7 also uses the **info** command to display the current level parameter settings and next level directories.

Figure 7 config cli monitor command sample output

```
8610:5# config cli monitor
8610:5/config/cli/monitor# info

Sub-Context:
Current Context:

                    duration : 300
                    interval : 5

8610:5/config/cli/monitor# duration 500
8610:5/config/cli/monitor# interval 10
8610:5/config/cli/monitor# info

Sub-Context:
Current Context:

                    duration : 500
                    interval : 10

8610:5/config/cli/monitor#
```

Table 1 lists the **monitor** commands.

Table 1 Monitor and show commands

monitor commands
monitor mlt error collision [<*mid*>*]*
monitor mlt error main [<*mid*>]
monitor mlt stats interface main [<*mid*>*]*
monitor mlt stats interface utilization [<*mid*>]
monitor ports error collision [<*ports*>] [from <*value*>]
monitor ports error extended [<ports>] [from <*value*>]
monitor ports error main [<*ports*>] [from <*value*>]
monitor ports stats bridging [<*ports*>] [from <*value*>]
monitor ports stats interface extended [<*ports*>] [from <*value*>]
monitor ports stats interface main [<*ports*>] [from <*value*>]

Table 1 Monitor and show commands (continued)

monitor commands
monitor ports stats interface utilization [<*ports*>] [from <*value*>]
monitor ports stats stg [<*ports*>] [from <*value*>]

The **monitor ports stats rmon [<*ports*>] [from <*value*>]** command is similar to the **config rmon etherstats info** command, which is described in *Managing the Passport 8000 Series Switch Using the Command Line Interface Release 3.2*.

Table 2 lists the monitor commands for routing functions.

Table 2 Routing monitor commands

routing monitor commands
monitor ports error ospf [<*ports*>] [from <*value*>]
monitor ports stats dhcp-relay [<*ports*>] [from <*value*>]
monitor ports stats ospf extended [<*ports*>] [from <*value*>]
monitor ports stats ospf main [<*ports*>] [from <*value*>]
monitor ports stats routing [<*ports*>] [from <*value*>]
monitor ports stats vrrp extended [<*ports*>] [from <*value*>]
monitor ports stats vrrp main [<*ports*>] [from <*value*>]

Configuration example

Figure 8 uses the above commands to monitor error collisions and to set the monitor port statistics.

Figure 8 config cli monitor ports error collision command sample output

```
8610:5/config/cli/monitor# monitor ports error collision

                        PORT COLLISION STATISTIC
Monitor Interval: 5sec | Monitor Duration: 300sec THU FEB 12 16:16:36 2004

PORT  -----------------COLLISIONS------------
NUM   SINGLE   MULTIPLE LATE     EXCESSIVE
-------------------------------------------------------------------
1/1   0        0        0        0
1/2   0        0        0        0
1/3   0        0        0        0
1/4   1        1        0        0
1/5   0        0        0        0
1/6   0        0        0        0
1/7   0        0        0        0
1/8   0        0        0        0
1/9   0        0        0        0
1/10  0        0        0        0
1/11  0        0        0        0
1/12  0        0        0        0
1/13  1        2        0        0
1/14  0        1        0        0
1/15  0        0        0        0

8610:5/config/cli/monitor# monitor ports stats interface utilization

PORT INTERFACE UTILIZATION

Monitor Interval: 5sec | Monitor Duration: 300sec THU FEB 12 16:16:36 2004


PORT_NUM IN_OCTETS  OUT_OCTETS IN_UTIL(%) OUT_UTIL(%)
-------------------------------------------------------------------
9/1      0          0          0          0
9/2      0          0          0          0
9/3      0          0          0          0
9/4      0          0          0          0
9/5      0          0          0          0
9/6      0          0          0          0
9/7      0          0          0          0
8610:5/config/cli/monitor#
```

Clearing statistics

To clear statistics from counters, flush entries from a table, or end a Telnet session, use the following command:

```
clear
```

This command includes the following options:

clear followed by:	
atm elan-stats <vlan id>	Clears ATM ELAN statistics • *vlan id* is a value from 1 to 4095.
atm f5-stats [<ports>]	Clears ATM F5 statistics. • *ports* specifies the ports for which you are entering the command in the form portlist {slot/port[-slot/port][, ...]}.
atm port-stats [<ports>]	Clears ATM port statistics. • *ports* specifies the ports for which you are entering the command in the form portlist {slot/port[-slot/port][, ...]}.
ip arp ports <*port*>	Clears ARP port entries from the ARP table. • *port* specifies the ports for which you are entering the command in the form portlist {slot/port[-slot/port][, ...]}.
ip arp vlan <*vid*>	Clears ARP VLAN entries from the ARP table. • *vid* is the VLAN ID.
ip route ports <*port*>	Clears route entries associated with the specified port. • *port* specifies the ports for which you are entering the command in the form portlist {slot/port[-slot/port][, ...]}.
ip route vlan <*vid*>	Clears route entries associated with the specified VLAN. • *vid* is the VLAN ID. The valid values are 0 to 255.

clear followed by:	
`ip vrrp ports <ports> vrid <value>`	Clears IP VRRP statistics for the specifed ports and virtual router. • *`ports`* specifies the ports for which you are entering the command in the form portlist {slot/port[-slot/port][, ...]}. • *`vrid`* specifies the virtual router. The valid values are 0 to 255.
`ip vrrp vlan <vid> vrid <value>`	Clears IP VRRP statistics for the specified VLAN and virtual router. • *`vid`* is the VLAN ID. The valid values are 1 to 4095. • *`vrid`* is the virtual router ID. The valid values are 0 to 255.
`mlt ist stats`	Clears MLT IST statistics.
`ports stats` [<*`ports`*>]	Clears port statistics from the switch counters. • *`ports`* specifies the ports for which you are entering the command in the form portlist {slot/port[-slot/port][, ...]}.
`telnet <session id>`	Ends the specified Telnet session. • *`session id`* is a number between 0 and 7.

Configuration Example

The following configuration example uses the above command to:

- Clears ATM ELAN statistics
- Clears ATM F5 statistics
- Clears ATM port statistics
- Clears ARP port entries from the ARP table

After configuring the parameters, use the info command to show a summary of the results.

```
Passport-8610:5# clear atm elan-stats ?
clear atm elan stats
Optional parameters:
<ports>          = portlist {slot/port[-slot/port][,...]}
```

```
<vlan id>        = VLAN ID {1..4095}
Command syntax:
elan-stats [<ports>] [<vlan id>]
Passport-8610:5# clear atm elan-stats 8/5 80
Passport-8610:5#
Passport-8610:5#
Passport-8610:5# clear atm f5-stats ?
clear atm f5 stats
Optional parameters:
<ports>          = portlist {slot/port[-slot/port][,...]}
Command syntax:
f5-stats [<ports>]
Passport-8610:5# clear atm f5-stats 8/5
Passport-8610:5#
Passport-8610:5#
Passport-8610:5# clear atm port-stats ?
clear port stats
Optional parameters:
<ports>          = portlist {slot/port[-slot/port][,...]}
Command syntax:
port-stats [<ports>]
Passport-8610:5# clear atm port-stats 8/5
Passport-8610:5#
Passport-8610:5# clear ip arp ports ?
clear specific port for arp
Required parameters:
<port>           = portnumber {slot/port[-slot/port][,...]}
Command syntax:
ports <port>
```

```
Passport-8610:5# clear ip arp ports 1/5
```

Configuring the syslog facility

The syslog facility in UNIX machines logs messages and assigns each message a severity level based on importance.

To configure the syslog facility, use the following command:

```
config sys syslog
```

The **`config sys syslog`** command includes the following options:

Note: For the syslog host ID, the range is from 1 to 10.

`config sys syslog` followed by:	
`info`	Displays the current syslog settings.
`host` *<id>* address *<ipaddr>*	Configures a host location for the syslog host. • *`address`* is the IP address of the UNIX system syslog host.
`host` *<id>* `create`	Creates a syslog host.
`host` *<id>* `delete`	Deletes a syslog host.
`host` *<id>* `facility` *<facility>*	Specifies the UNIX facility used in messages to the syslog host. • *`facility`* is the UNIX system syslog host facility (LOCAL0 to LOCAL7).
`host` *<id>* `<enable|disable>`	Enables or disables the syslog host.
`host` *<id>* `info`	Displays system log information for the specified host. This command results in the same output as the **`show sys syslog host <id> info`** command. The ID ranges from 1 to 10.
`host` *<id>* `mapinfo` *<level>*	Specifies the syslog severity level to use for Passport Information messages. • *`level`* is {`emergency|alert|critical|error|warning|notice|info|debug`}.
`host` *<id>* `mapwarning` *<level>*	Specifies the syslog severity to use for Passport Warning messages. • *`level`* is {`emergency|alert|critical|error|warning|notice|info|debug`}.

config sys syslog followed by:	
`host <id> maperror <level>`	Specifies the syslog severity to use for Passport Error messages. • *level* is {emergency|alert|critical|error|warning|notice|info|debug}.
`host <id> mapfatal <level>`	Specifies the syslog severity to use for Passport Fatal messages. • level is {emergency|alert|critical|error|warning|notice|info|debug}.
`host <id> severity <info| warning|error|fatal> [<info|warning|error|fatal>]`	Specifies the severity levels for which syslog messages should be sent for the specified modules. • severity is the severity for which syslog messages are sent.
`host <id> udp-port <port>`	Specifies the UDP port number on which to send syslog messages to the syslog host. • udp-port <*port*> is the UNIX system syslog host port number (514 to 530).
`max-hosts <maxhost>`	Specifies the maximum number of syslog hosts supported. • *maxhost* is the maximum number of enabled hosts allowed (1 to 10).
`state <enable|disable>`	Enables or disables sending syslog messages on the switch.

Configuration example

Figure 9 uses the above commands to create a host, specify a facility to log on syslog host, specify a syslog severity to use for Passport Warning messages, specify a syslog severity to use for Passport Fatal messages, and enable the sending of syslog messages. The example also uses the **`info`** command to display system log information for the specified host.

Figure 9 config sys syslog command sample output

```
Passport-8610:5# config sys syslog
Passport-8610:5/config/sys/syslog# host 1 create
Passport-8610:5/config/sys/syslog# host 1 facility local0
Passport-8610:5/config/sys/syslog# host 1 mapwarning alert
Passport-8610:5/config/sys/syslog# host 1 mapfatal alert
Passport-8610:5/config/sys/syslog# state enable
Passport-8610:5/config/sys/syslog# host 1 info

Sub-Context: host
Current Context:

                     address : 0.0.0.0
                      create : 1
                      delete : N/A
                    facility : local0
                        host : disable
                     mapinfo : info
                  mapwarning : alert
                    maperror : error
                    mapfatal : alert
                    severity : info|warning|error|fatal
                    udp-port : 514

Passport-8610:5/config/sys/syslog#
```

Configuration Example

The following configuration example uses the above command to:

- Configures a host location for the syslog host.
- Creates a syslog host
- Specifies the UNIX facility used in messages to the syslog host
- Enables or disables the syslog host

```
Passport-8610:5# config sys syslog
Passport-8610:5/config/sys/syslog# ?

Sub-Context: host
Current Context:
```

```
    info
    max-hosts <maxhost>
    state <enable|disable>

Passport-8610:5/config/sys/syslog# host 1
Passport-8610:5/config/sys/syslog/host/1# ?

Sub-Context:
Current Context:

    address <ipaddr>
    create
    delete
    facility <facility>
    host <enable|disable>
    info
    mapinfo <level>
    mapwarning <level>
    maperror <level>
    mapfatal <level>
    severity <info|warning|error|fatal> [<info|warning|error|fatal>]
[<info|warning|error|fatal>] [<info|warning|error|fatal>]
    udp-port <port>

Passport-8610:5/config/sys/syslog/host/1# create
Passport-8610:5/config/sys/syslog/host/1# address 10.143.163.200
Passport-8610:5/config/sys/syslog/host/1# facility ?
set unix system syslog host facility
Required parameters:
<facility>       = facility to log on syslog host
{local0|local1|local2|local3|local4|local5|local6|local7}
Command syntax:
facility <facility>
Passport-8610:5/config/sys/syslog/host/1# facility local6
Passport-8610:5/config/sys/syslog/host/1# host ?
```

```
Not enough required parameters entered
enable/disable syslog host
Required parameters:
<enable|disable> = operation {disable|enable}
Command syntax:
host <enable|disable>
Passport-8610:5/config/sys/syslog/host/1# host enable
Passport-8610:5/config/sys/syslog/host/1# info

Sub-Context:
Current Context:

                     address : 10.143.163.200
                      create : 1
                      delete : N/A
                    facility : local6
                        host : enable
                     mapinfo : info
                  mapwarning : warning
                    maperror : error
                    mapfatal : emergency
                    severity : info|warning|error|fatal
                    udp-port : 514


            Passport-8610:5/config/sys/syslog/host/1#
```

Displaying information about syslog features

To display information about the syslog features enabled on the switch, use the following command:

```
show sys syslog
```

The **`show sys syslog`** command includes the following options.

`show sys syslog` followed by:	
`general-info`	Displays general information about the system log
`host <id> info`	Displays system log information for a specified host.

Configuration example

Figure 10 uses the above commands to display general information about the system log, and to display information about a specified host.

Figure 10 show sys syslog general-info command sample output

```
Passport-8610:5# show sys syslog general-info

 Enable    : true
 Max Hosts : 5
 OperState : active
 Total number of configured hosts : 1
 Total number of enabled hosts : 0
 Configured host : 1
 Enabled host :

Passport-8610:5#
Passport-8610:5# show sys syslog host 1 info

                Id : 1
            IpAddr : 0.0.0.0
           UdpPort : 514
          Facility : local0
          Severity : info|warning|error|fatal
    MapInfoSeverity : info
 MapWarningSeverity : alert
   MapErrorSeverity : error
     MapMfgSeverity : notice
   MapFatalSeverity : alert
             Enable : false

Passport-8610:5#
```

Displaying hardware registers

The **`dump ar`** command allows you to display the hardware registers of the RaptARU attached to OctaPID. To display the hardware registers, use the following command:

```
dump ar <opid> <vlan|ip_subnet|mac_vlan|mac|arp|ip|ipx|
ipmc|ip_filter|protocol|all> <verbosity>
```

where:

- *`opid`* specifies the octaPID assignment, from 1 to 64. See *Configuring Network Management* for more information.
- `vlan|ip_subnet|mac_vlan|mac|arp|ip|ipx|ipmc|ip_filter|protocol|all` specifies a record type in the AR table.
- *`verbosity`* specifies the verbosity level, from 0 to 3. Higher numbers specify more verbosity.

Configuration example

Figure 11 uses the above commands to specify an octaPID and specify a record type in the AR table.

Figure 11 dump ar command sample output

```
Passport-8610:5# dump ar 4 all 3
Passport-8610:5#
```

Tracing the route to a remote host

To trace the route to a remote host, use the following command:

```
traceroute <ipaddr> [<datasize>] [-m <value>] [-p <value>]
[-q <value>] [-w <value>] [-v]
```

where:

- *ipaddr* is the IP address of the remote host.
- *datasize* is the size of the probe packet (1 to 1464).
- `-m <value>` is maximum time-to-live (TTL) value (1 to 255).
- `-p <value>` is the base UDP port number (0 to 4294967295).
- `-q <value>` is the number of probes per TTL (1 to 255).
- `-w <value>` is the wait time per probe (1 to 255).
- `-v` is the verbose mode (showing all).

This command is valuable for troubleshooting because it shows all the routes that are used or indicates that the remote network is not reachable.

Figure 12 shows output from the **`traceroute`** command.

Figure 12 traceroute command sample output

```
8610# traceroute 10.10.81.18
traceroute to 10.10.81.18, 30 hops max, 40 byte packets
 1  10.10.221.1  12 ms 1 ms 1 ms
 2  10.10.175.1  0 ms 0 ms 0 ms
 3  10.10.180.1  2 ms 1 ms 2 ms
 4  10.10.184.2  1 ms 1 ms 3 ms
 5  10.10.103.2  3 ms 2 ms 2 ms
 6   10.10.13.8   7 ms 4 ms 6 ms
 7  10.10.81.18  19 ms 17 ms 17 ms
```

Configuring an automatic trace

You can configure the switch to automatically enable a trace in the event CPU utilization reaches a pre-defined value.

To enable the trace auto-enable feature, use the following command:

```
trace auto-enable
```

This command includes the following parameters:

trace auto-enable followed by:	
`info`	Displays trace auto-enable information.
`add-module <modid> <level>`	Adds a module to be traced by the trace auto-enable feature. • *modid* identifies the module that you want to add. For example, 3 = Port Manager, 20 = Topology Discovery. For a complete list of module IDs, enter **trace auto-enable add-module ?**. • *level* identifies the level of detail you want in the trace. For example, 0 = Disabled, 1 = Very Terse. For a complete list of module IDs, enter **trace auto-enable add-module ?**.
`auto-trace <enable|disable>`	Enables or disables auto-trace. The default is disable.
`high-percentage <percent>`	Specifies the CPU utilization percentage above which auto trace should be enabled. • *percent* is a value from 60 to 100. The default is 90.
`high-track-duration <seconds>`	Specifies the time in seconds to monitor CPU utilization before triggering a trace. • *seconds* is a value from 3 to 10. The default is 5.
`low-percentage <percent>`	Specifies the CPU utilization percentage below which auto-trace should be disabled. • *percent* is a value from 50 to 90. The default is 75.
`low-track-duration <seconds>`	Specifies the time, in seconds, to monitor CPU utilization before disabling the trace. • *seconds* is a value from 3to 10. The default is 5.
`remove-module <modid>`	Removes a module from automatic tracing. • *modid* identifies the module for which you want to disable auto-trace. For example, 3 = Port Manager, 20 = Topology Discovery. For a complete list of module IDs, enter **trace auto-enable add-module ?**.

Note: The enabling or disabling of auto-trace is not saved to the configuration file. When a Passport 8000 Series switch re-boots, auto-trace functionality will be disabled.

Figure 13 shows sample output for the **`trace auto-enable info`** command.

Figure 13 trace auto-enable info command sample output

```
Passport-8606:5#/trace/auto-enable# info

Sub-Context:
Current Context:

        Auto-Trace Enable    : Enable
        High CPU Utilization : 90%
        High Track Duration  : 3 seconds
        Low CPU Utilization  : 75%
        Low Track Duration   : 5 seconds
        Modules Selected     : Module     ModId    Level
                               SNMP       1          4
                               OSPF       6          4
                               PORT_MGR   3          3
                               P2IP       14         4
```

Performing a loopback test

To perform a loopback test, use the following command:

`test loopback <ports> [<int|ext>]`

where:
`ports` specifies the ports for which you are entering the command in the form portlist {slot/port[-slot/port][, ...]}. `int/ext` is a string length between 1 and 1536.

Figure 14 show the warning message that appears when you perform a loopback test using the `test loopback` command.

Figure 14 test loopback warning message output

```
8610:5# test loopback 1

CPU utilization will dramatically increase with this diagnostic.
This could affect the performance of box.
Do you really want to loopback (y/n)?
```

Configuring and displaying log files

The **`log`** commands allow you to configure and display the log files for the switch. When the **`config bootconfig flags logging true`** command is saved in the configuration file, the log entries are written to the `/pcmcia/syslog.txt` file. If the logging flag is not set to true, the entries are stored in memory.

Writing log files

To write a log file, use the following command:

```
config log
```

The **`config log`** commands include the following options:

`config log` followed by:	
`info`	Displays the current log settings.
`clear`	Clears the log file.

config log followed by:	
`level` [<*`level`*>]	Shows and sets the logging level. *`level`* is one of these values: • 0 = Information; all messages are recorded. • 1 = Warning; only warning and more serious messages are recorded. • 2 = Error; only error and more serious messages are recorded. • 3 = Manufacturing; this parameter is not available for customer use. • 4 = Fatal; only fatal messages are recorded.
`screen` [<*`setting`*>]	Sets the log display on the screen to on or off. • *`setting`* is `off` or `on`.
`write` <*`str`*>	Writes the log file with the designated string. • *`str`* is the string or command that you append to the log file. If the string contains spaces, you must enclose the string in quotation marks.
`logToPCMCIA`	Enables or disables logging to the PCMCIA.

Configuration example

Figure 15 uses the above commands to write a log file, set the logging level, and turn on the screen display. The example also uses the **`info`** command to display log information.

Figure 15 config log command sample output

```
8610:5# config log
8610:5/config/log# write test
8610:5/config/log# level 0
8610:5/config/log# screen on
Screen logging is on
8610:5/config/log# info

Sub-Context:
Current Context:

                        clear : N/A
                        level : 0
                       screen : on
                        write : N/A
              LoggingToPcmcia : True


8610:5/config/log#
```

Displaying log information

To display log information for the switch, use the following command:

```
show log file [tail]
```

where:
`tail` displays the log file in reverse order, with the most recent information first.

Note: Issuing the `show log file tail` command shows only the log messages reported after the system comes up. This will avoid system problems when displaying a large (larger than 10MB) /pcmcia/syslog.txt file.

Configuration example

Figure 16 uses the above command to write a log file, where the `tail` option was entered to display the most recent information first.

Note: If the Passport 8000 Series switch has a real-time clock, the log file shows real time.

Figure 16 show log file tail command sample output

```
8610:5/config/log# show log file tail
[04/17/99 01:02:28] test
[04/16/99 23:09:54] WARNING Code=0x1ff0009 Task=tShell Blocked unauthorized
cli access
[04/15/99 19:50:19] Save config to file config1 successful.
[04/09/99 12:37:04] State 172.16.2.5: OPENCONFIRM --> ESTABLISHED

[04/09/99 12:37:04] State 172.16.2.5: OPENSENT --> OPENCONFIRM

[04/09/99 12:37:03] State 172.16.2.5: CONNECT --> OPENSENT

[04/09/99 12:37:03] State 172.16.2.5: IDLE --> CONNECT

[04/09/99 12:36:53] State 172.16.2.5: ESTABLISHED --> IDLE

[04/09/99 12:36:53] GLOBAL_ERROR PKT: receiving data: Conn is gone: nbr
172.16.2.5, conn 2

[04/09/99 12:36:27] PEER_ERROR EVENT:(172.16.2.5): svr conn: collision in
ESTABLISHED state

[04/09/99 12:35:49] State 172.16.2.5: OPENCONFIRM --> ESTABLISHED

[04/09/99 12:35:49] State 172.16.2.5: OPENSENT --> OPENCONFIRM

[04/09/99 12:35:49] State 172.16.2.5: CONNECT --> OPENSENT
```

Displaying level information

The **`show log level`** command displays the level of information being entered in the log. The level ranges from information (INFO), where all messages are entered, to FATAL, where only fatal errors are recorded. The manufacturing (MFG) level is for manufacturing purposes only and not available for customer use. To display the level information, use the following command:

```
show log level command
```

Configuration example

Figure 17 uses the above command to display level of information being entered in the log.

Figure 17 show log level command sample output

```
8610:5/config/log# show log level
Log Levels are:
 0 = INFO
 1 = WARNING
 2 = ERROR
 3 = MFG
 4 = FATAL
The Log Level is INFO
8610:5/config/log#
```

Configuring ping snoop

You can use the ping snoop feature to troubleshoot Multilink-trunking (MLT) and Split Multilink-trunking (SMLT) networks. This feature displays the path that IP traffic takes over an MLT or SMLT path. Ping snoop works by enabling a filter that copies ICMP messages to the CPU. The CPU then monitors the ICMP stream. The console displays the port that is used for each IP traffic flow, from source to destination station. There is no mechanism to prevent line rate ICMP traffic from going to the CPU as a result of enabling ping snoop.

You create a ping snoop filter by specifying a source and destination IP address. Then, you specify the ports on which you want to enable ping snoop. Only one ping snoop filter is supported on a port. If an ICMP request is received on any of the added ports, the source and destination IP address and the port on which the packet was received will be displayed on the management console.

Ping snoop uses one of the available global filters (0-7). If eight global filters are configured on a port prior to enabling ping snoop, then ping snoop cannot be enabled for a port. You must remove at least one of the global filters to enable ping snoop.

By design, ping snoop configurations are not saved to the config file and are deleted by resetting the switch. In addition, your ping snoop configuration will be erased if you log out and login under a different security level.

To configure and enable ping snoop, use the following command:

```
config diag ping-snoop
```

This command includes the following options.

`config diag ping-snoop` followed by:	
`info`	Displays the ping snoop filter and the ports on which it is applied (Figure 18).
`add-ports <`*`ports`*`>`	This is used to add ports to the ping snoop filter after the filter has been created. After adding a port, if an ICMP request is received on that port, the source and destination IP address, and the port on which the packet was received will be displayed on the management console. • *`ports`* specifies the port or range of ports when you apply the ping snoop filter.
`create src-ip <`*`value`*`> dst-ip <`*`value`*`>`	This command is used to create the ping snoop filter. It takes two arguments, the source IP address, and the destination IP address. To enable ping snoop, after you create the filter, you add ports using the `add-ports` option. • `src-ip` *`value`* the source IP address. • `dst-ip` *`value`* the destination IP address.

config diag ping-snoop followed by:	
`delete`	This command removes the ping snoop filter from any ports that were added and deletes the filter.
`enable <true|false>`	Enables or disables the ping snoop filter.
`remove-ports <ports>`	Used to delete the ping snoop filter on a particular port. • *ports* used to remove a port or range of ports from a ping snoop filter.

Figure 18 shows sample output for the **config diag ping-snoop info** command.

Figure 18 config diag ping-snoop info command

```
Passport-8600:5/config/diag/ping-snoop# info

                     src-ip : 1.1.1.0/255.255.255.0
                     dst-ip : 2.2.2.0/255.255.255.0
                  add_ports : 1/1
                     enable : true
```

Configuring and Displaying Remote Mirroring

Remote mirroring provides the feature to steer mirrored traffic through a switch cloud to a network analysis probe located on a remote switch. In a network, this feature allows the user, to monitor many ports from different switches using one network probe device. This function is achieved by encapsulating mirrored packets in a Remote Mirroring Encapsulation “wrapper”.

To set up remote mirorring, use the following command:

```
config ethernet <slot/port> remote-mirroring
```

This command includes the following options.

config ethernet <slot/port> remote-mirroring followed by:	
`create [enable <true|false>] [mode <source|termination>] [srcmac <mac>] [dstmac <mac>] [ether-type <ether-type>]`	Creates a remote mirroring entry for the port. User need to create an entry before setting any remote mirroring parameter on the port
`enable <true|false>`	Enable/disables the feature on the port. When RMT is enabled, the following things are done. • An FDB static entry for the dstmac is added. This is to send all the packets that are coming with remote mirroring dstmac to RMT port. • Switch periodically (once in 10 secs) transmits broadcast layer 2 packets in all the vlan added so that all nodes in the network can learn the dstmac
`mode<source|termination>`	Specifies whether the port is a RMT or RMS.
srcmac <mac>	Used to set the source mac for the remote mirroring encapsulation. The packet will be sent out of RMS with source mac derived from this. The source mac of the encapsulated frame will contain first 45 bits of this Mac address. The three least significant bits are derived from the port number of RMS port. Mac address of the port is used as default value.
dstmac <mac>	Used to set the destination mac for the remote mirroring encapsulation. The remote mirrored packet will be sent to this mac address. User configured dstmac is used only for RMS. For RMT, one of the unused Mac address from the switch Port Mac address range is used. To get the same dstmac for RMT across re-boot, this mac address is saved in configuration file and only when config file is restored, the dstmac of RMT is accepted from user.
ether-type <ether-type>	The ether-type of the remote mirrored packet. Default value is 0x8103
add-vlan-id <vlan-id> remove-vlan-id <vlan-id>	Used only for RMT. The user has to specify which vlan the remote mirror destination mac belongs to. This has to be a port based VLAN. When the RMT port is removed from the last vlan in the list, RMT will be disabled from the port.

config ethernet <slot/port> remote-mirroring followed by:	
info	Displays the Remote Mirorring configuration of the port.
delete	Deletes the Remote Mirorring configuration of the port.

Note: Parameters can be modified only if remote mirroring is disabled.

Figure 19 shows sample output for the **config ethernet <slot/port> remote-mirroring** command.

Figure 19 config ethernet <slot/port> remote-mirroring command

```
Passport-8603:3/config/ethernet/1/1/remote-mirroring# info
port 1/1
        Enable = FALSE
        Mode = source
        srcmac = 00:04:38:7e:84:00
        dstmac = 00:00:00:00:00:00
        ether-type = 0x8103
        vlan-id-list =
```

Use the following show command to display the remote mirroring related information of the port:

```
Show port info
 remote-mirroring [<port-num>] [mode <value>] [dstmac
<value>] [srcmac <value>] [vlan-id <value>]
```

Configuration Example

Figure 20 shows sample output for the Show port info show command.

Figure 20 Show port info show command

```
Passport-8603:3# show port info remote-mirroring
================================================================================
                          Port Remote Mirroring
================================================================================

PORT   Enable MODE       SourceMac         DestinationMac    EtherType
--------------------------------------------------------------------------------
1/1    false  source     00:04:38:7e:84:00 00:00:00:00:00:00 0x8103
```

Chapter 3
Using Device Manager diagnostic tools

This chapter describes the Device Manager diagnostic tools that you can run on a Passport 8000 Series switch. It includes the following topics:

Testing the switch fabric and address resolution table

The Test tab in Device Manager allows you to perform two tests. You can test the switch fabric and check the address resolution (AR) table for consistency.

The Fabric test causes the CPU to generate traffic and send it through the switch fabric. Given the forwarding rate of Passport 8000 Series switches, the CPU does not generate much traffic, but it performs a simple test of the switch fabric memory.

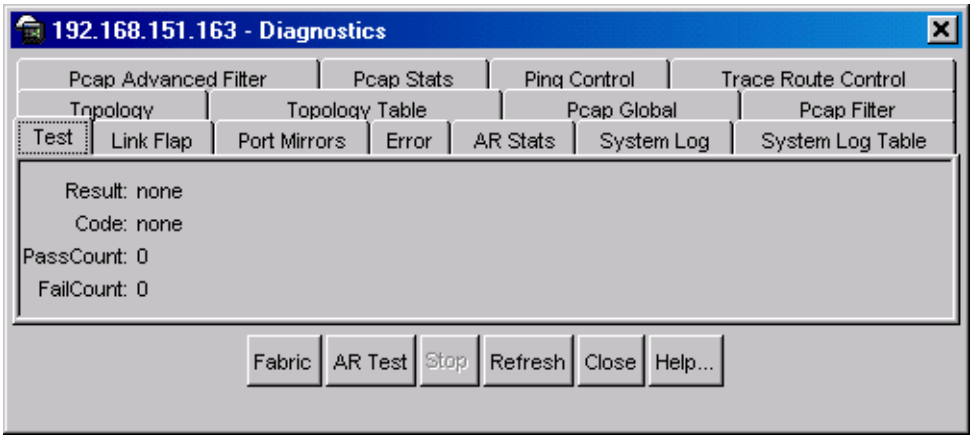
The AR table test performs a consistency check on address resolution table entries.

To test the fabric or address resolution table:

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

The Diagnostics dialog box opens with the Test tab displayed. (Figure 21)

Figure 21 Diagnostics dialog box—Test tab



The following test options are available:

- Test the Address Resolution Table (AR Test)
- Test the switch fabric (Fabric)
- Stop a test in progress

Table 3 describes the Test tab fields on the Diagnostics dialog box.

Table 3 Test tab fields

Field	Description
Result	The result of the most recently run (or current) test: • none • success • inProgress • notSupported • unAbleToRun • aborted • failed
Code	The code contains more specific information about the test result (for example, an error code after a failed test): • none • NoReceive (timeout on a send) • BadSeq (packets received out of sequence) • BadLen (packet length mismatch) • BadData (packet data mismatch)
PassCount	The number of iterations of the test case that completed successfully.
FailCount	The number of iterations of the test case that failed.

Monitoring how often a port goes down

You can monitor the number of times a link is going up or down rapidly (that is, flapping) on a port. This action can be detrimental to network stability because it could trigger spanning tree and routing table recalculation. If the number exceeds a given boundary during a specified interval, the port is forced out of service.

To monitor a port:

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

   The Diagnostics dialog box opens with the Test tab displayed.

2. Click the Link Flap tab.

   The Link Flap tab opens. (Figure 22)

Figure 22 Diagnostics dialog box—Link Flap tab

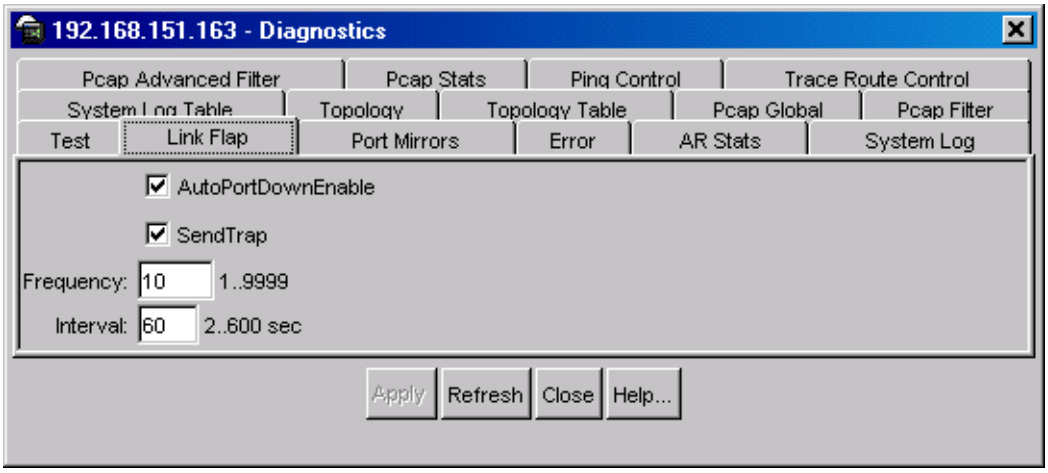


Table 4 describes the Link Flap tab fields on the Diagnostics dialog box.

Configuring and monitoring port mirroring

Table 4 Link Flap tab fields

Field	Description
AutoPortDownEnable	Enables or disables the Link Flap Detect feature.
SendTrap	Specifies whether or not a trap should be sent if the port is forced out of service.
Frequency	Specifies the number of times the port can go down. The default is 10.
Interval	Specifies the interval (in minutes). The default is 60.

You can use port mirroring to specify a destination port on which you want to see mirrored traffic and specify the source ports from which traffic is mirrored. Any packets entering or leaving the specified ports are forwarded normally and a *copy* of the packets is sent out the mirror port. You can configure up to 100 entries in the MirroredPort field for mirroring, and you can have up to 25 entries active

(enabled) at any given time. When the port mirroring feature is active, all packets received on the port(s) specified by the MirroredPort field are copied to MirroringPort. The mirroring operation is nonintrusive; mirrored traffic is always treated in the lowest priority queue.

You can also use the port mirroring feature to monitor traffic from MAC addresses where traffic with a given MAC source address (SA) or MAC destination address (DA) is copied to the mirror port. This feature is enabled by setting the Monitor field to true for a MAC address in the Forwarding dialog box.

Note: Monitoring of MAC address traffic must be within the context of a VLAN.

Configuring port mirroring ports

To configure ports for port mirroring:

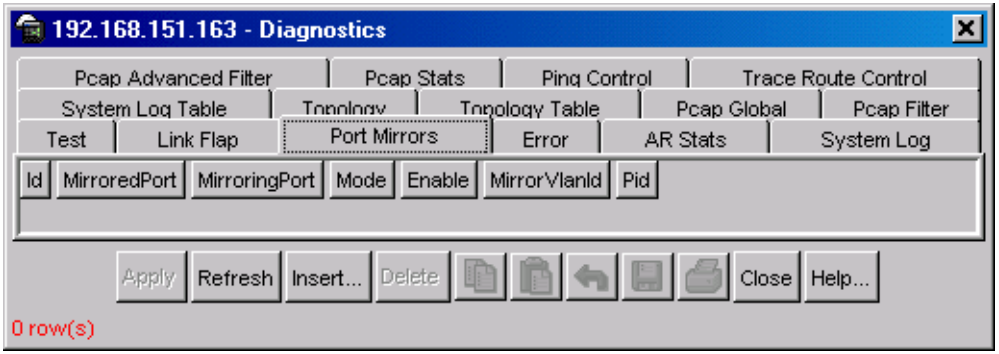
1. From the Device Manager menu bar, choose Edit > Diagnostics.

   The Diagnostics dialog box opens with the Test tab displayed. (Figure 21)

2. Click the Port Mirrors tab.

   The Port Mirrors tab opens. (Figure 23)

Figure 23 Diagnostics dialog box—Port Mirrors tab



3. Click Insert.

   The Diagnostics, Insert Port Mirrors dialog box opens. (Figure 24)

Figure 24 Diagnostics, Insert Port Mirrors dialog box

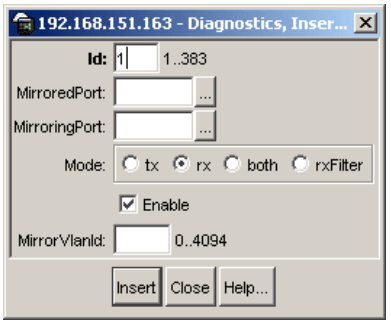


Table 5 describes the Diagnostics, Insert Port Mirrors dialog box fields.

Table 5 Diagnostics, Insert Port Mirrors dialog box fields

Field	Description
Id	An assigned identifier for the configured port mirroring instance.
MirroredPort	Allows you to specify a port to be mirrored (source port). You can select ports from any module in your configuration by clicking the ellipses button to the right of the field (Figure 24).
MirroringPort	Allows you to specify a destination port (the port to which the mirrored packets are forwarded). You can select ports from any module in your configuration by clicking the ellipses button to the right of the field (see "Selecting ports for mirroring," next).
Mode	Allows you to specify the traffic direction of the packet being mirrored—Rx, Tx, or both. The default configuration is Rx.
Enable	Allows you to enable or disable this port mirroring instance. The default value is Enable.
MirrorVlanId	Set the Remote Mirror VLAN Id.

Selecting ports for mirroring

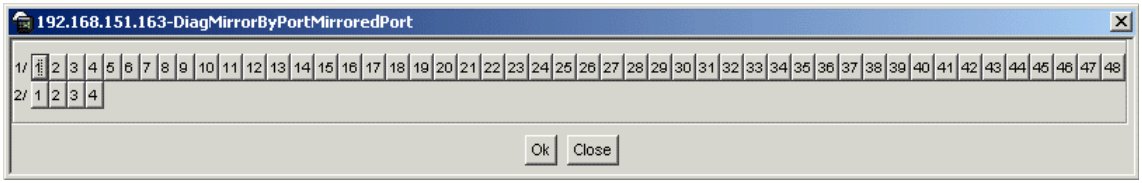
To select ports for port mirroring:

1 On the device view, select a mirrored (source) port:

a Click the ellipses button in the MirroredPort field.

The DiagMirrorByPortMirroredPort dialog box opens. (Figure 25)

Figure 25 DiagMirrorByPortMirroredPort dialog box



b Select a source port.

c Click Ok.

The Diagnostics, Insert Port Mirrors dialog box displays the new entry in the MirroredPort field.

2 Select a destination port.

a Click the ellipses button in the MirroringPort field.

The DiagMirrorByPortMirroringPort dialog box opens.

b Select a destination port.

c Click Ok.

The Diagnostics, Insert Port Mirrors dialog box displays the new entry in the MirroringPort field.

3 In the Diagnostics, Insert Port Mirrors dialog box, select the appropriate mode value (tx, rx, or both) to specify the traffic direction of the mirrored packet. The default configuration is rx.

4 Select the appropriate value (Enable or Disable) to enable or disable this instance of mirroring. The default value is Enable.

5 Click Insert to accept your configuration choices.

Editing existing port mirroring values

This section describes how to edit existing port mirroring values. The following topics are covered:

Sorting entries

You can click on the column heading of any entry listed in the Port Mirrors tab to sort the entries in ascending or descending numerical order, or you can sort to group entry values.

Displaying configured port mirroring entries

To display existing port mirroring entries:

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

The Diagnostics dialog box opens with the Test tab displayed. (Figure 21)

2 Click the Port Mirrors tab.

The Port Mirrors tab opens, displaying the configured port mirroring entries. (Figure 26)

Figure 26 Diagnostics dialog box—Port Mirrors tab

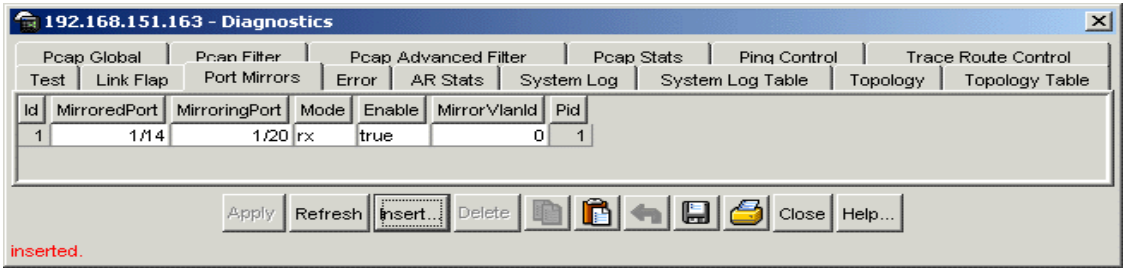


Table 6 describes the Port Mirrors tab fields on the Diagnostics dialog box.

Table 6 Port Mirrors tab fields

Field	Description
Id	Read-only field—displays the assigned identifier for the existing port mirroring instances.
MirroredPort	Displays existing port(s) from which packets are being copied (also referred to as *source* ports).
MirroringPort	Displays the existing port(s) that are performing the mirroring, that is, the port(s) to which the mirrored packets are forwarded (also referred to as *destination* ports).
Mode	Specifies the traffic direction of the packets being mirrored for each existing entry—Rx, Tx, or Both.
Enable	Specifies the status of existing entries—true (enabled) or false (disabled).
MirrorVlanId	Set the Remote Mirror VLAN Id.
Pid	Pid for a port

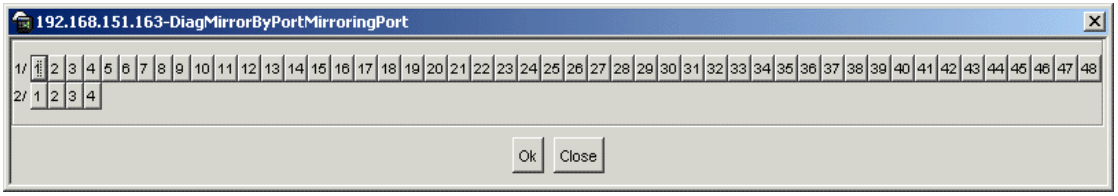
Editing existing mirrored or mirroring ports

To modify an existing mirrored or mirroring port:

1. From the Port Mirrors dialog box, double click on an entry you want to modify in the MirroredPort or MirroringPort column heading.

   The appropriate dialog box opens with the port you clicked to modify shown selected. (Figure 25)

Figure 27 MirroringPort dialog box



2. Click on the port you want as a replacement.
3. Click Ok.

   The entry in the Port Mirrors tab is replaced with the new port.

Editing the Mode field values

To modify an existing entry in the Mode field:

1. Click on the entry to display the pop up menu.

   A pop up widow displays the following options: Rx, Tx, or Both.

2. Click on the option you want for replacement.

   The Apply button becomes highlighted.

3. Click Apply to accept the option.

Editing the Enable field values

To modify an existing entry in the Enable field:

1. Click on the entry to display the pop up menu.

   A pop up widow displays the following options: true or false.

2. Click on the option you want for replacement.

   The Apply button is highlighted.

3. Click Apply to accept the option.

Trapping errors

You can specify that errors generate an SNMP trap. All errors detected are then sent to a log that you can view in Device Manager.

To trap errors:

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

   The Diagnostics dialog box opens with the Test tab displayed.

2. Click the Error tab.

   The Error tab opens. (Figure 28)

Figure 28 Diagnostics dialog box—Error tab

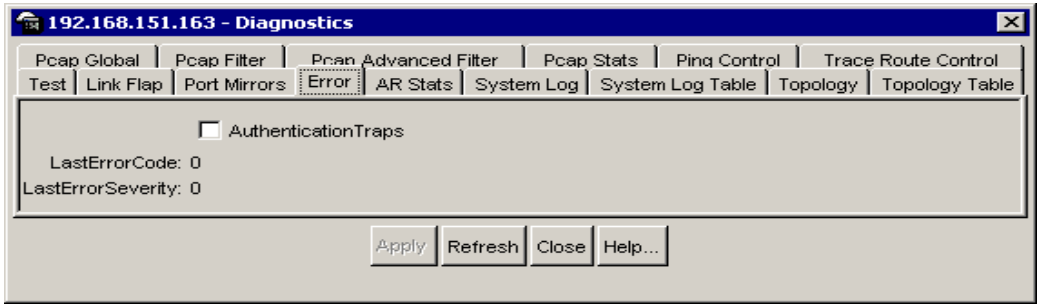


Table 7 describes the Error tab fields on the Diagnostics dialog box.

Table 7 Error tab fields

Field	Description
AuthenticationTrap	When enabled, sends a trap upon receiving an error in the system.
LastErrorCode	The last error reported in the system. This value is intended to help customer support personnel isolate system problems.
LastErrorSeverity	The last error reported in the system. The meanings of this value are: 0= Informative Information 1= Warning Condition 2= Error Condition 3= Manufacturing Information 4= Fatal Condition

Viewing address resolution statistics

The AR Stats tab shows statistics for the internal state of the address translation table. These statistics are debugging aids, and you should use them only when consulting with Nortel Networks support personnel.

The statistic of most interest is the NoSpace counter, which indicates the number of entries the address resolution (AR) table could not add because of lack of space.

To access the AR Stats tab:

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

   The Diagnostics dialog box opens with the Test tab displayed.

2. Click the AR Stats tab.

   The AR Stats tab opens. (Figure 29)

Figure 29 Diagnostics dialog box—AR Stats tab

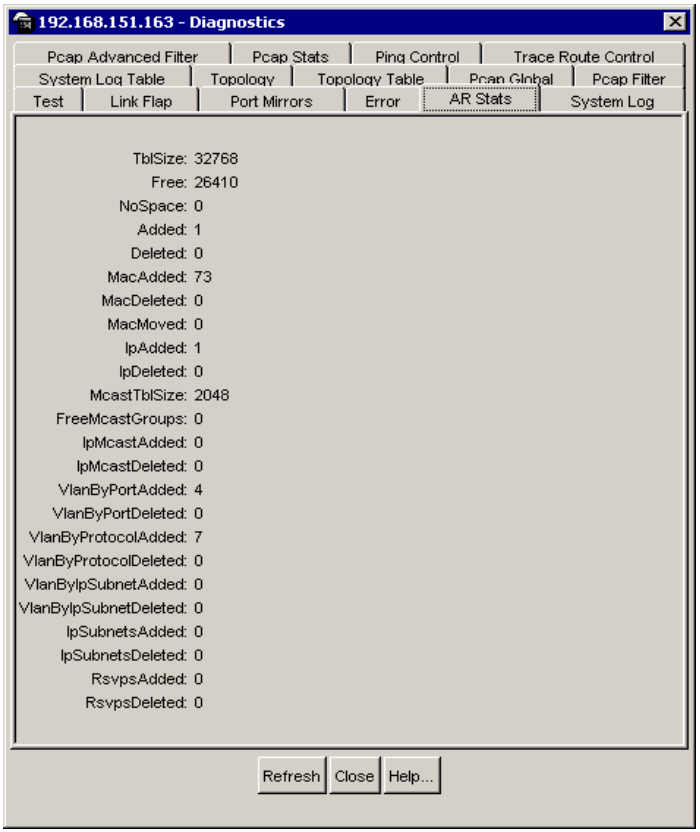


Table 8 describes the AR Stats tab fields on the Diagnostics dialog box.

Table 8 AR Stats tab fields

Field	Descriptions
TblSize	The size of the address resolution (AR) translation table.
Free	The number of free entries that are available in the AR translation table.
NoSpace	The number of entries that were not added to the AR translation table because of lack of space.
Added	The number of entries added to the AR translation table.
Deleted	The number of entries deleted from the AR translation table.
MacAdded	The number of MAC entries added to the AR translation table.
MacDeleted	The number of MAC entries deleted from the AR translation table.
MacMoved	The number of MAC entries moved in the AR translation table.
IpAdded	The number of IP entries added to the AR translation table.
IpDeleted	The number of IP entries deleted from the AR translation table.
McastTblSize	The size of the Multicast AR translation table.
FreeMcastGroups	The number of free multicast groups available in the AR table.
IpMcastAdded	The number of IP multicast entries added to the AR table.
IpMcastDeleted	The number of IP multicast entries deleted from the AR table.
VlanByPortAdded	The number of VLAN by Port entries added to the AR table.
VlanByPortDeleted	The number of VLAN by Port entries deleted from the AR table.
VlanByProtocolAdded	The number of VLAN by Protocol Type entries added to the AR table.
VlanByProtocolDeleted	The number of VLAN by Protocol Type entries deleted from the AR table.
VlanByIpSubnetAdded	The number of VLAN by IP Subnet entries added to the AR table.
VlanByIpSubnetDeleted	The number of VLAN by IP Subnet entries deleted from the AR table.
IpSubnetsAdded	The number of IP Subnet entries added to the AR table.
IpSubnetsDeleted	The number of IP Subnet entries deleted from the AR table.
RsvpsAdded	The number of RSVP entries added to the AR table.
RsvpsDeleted	The number of RSVP entries deleted from the AR table.

Enabling the system log

This section includes the following topics:

Enabling the system log globally

You can enable the system log feature globally to send messages to up to 10 syslog hosts. By default, five hosts are supported.

To enable the system log feature globally:

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

   The Diagnostics dialog box opens with the Test tab displayed.

2. Click the System Log tab.

   The System Log tab opens. (Figure 30).

Figure 30 Diagnostics dialog box—System Log tab

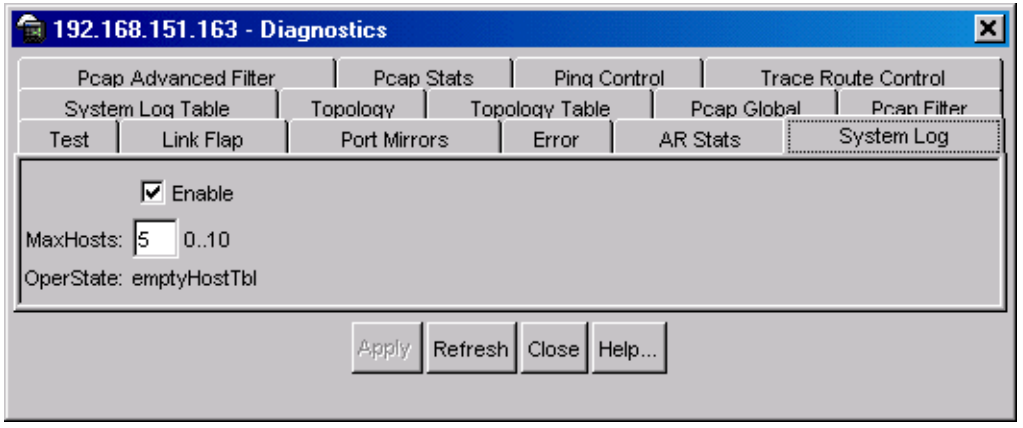


Table 9 describes the System Log tab fields on the Diagnostics dialog box.

Table 9 System Log tab fields

Field	Descriptions
Enable	Used to enable/disable the syslog feature. When enabled, this feature sends a message to a server on a network that is configured to receive and store diagnostic messages from this device. The type of messages sent is user configurable.
MaxHost	The maximum number of remote hosts considered active and able to receive messages from the syslog service.
OperState	The operational state of the syslog service.

Receiving system log messages

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

At a remote UNIX management workstation, the system log messaging feature does the following:

- Receives system log messages from the Passport 8000 Series switch
- Examines the severity code in each message
- Uses the severity code to determine appropriate system handling for each message
- Based on the severity code in each message, dispatches each message to any or all of the following destinations:
  - — Workstation display
  - — Local log file
  - — Designated printer

— One or more remote hosts

Internally the Passport 8000 Series switch has four severity levels for log messages:

- Info
- Warning
- Error
- Fatal

The system log feature supports eight different severity levels:

- Debug
- Info
- Notice
- Warning
- Error
- Critical
- Alert
- Emergency

Table 10 shows the default mapping of internal severity levels to syslog severity levels.

Table 10 Default severity levels and system log severity levels

UNIX system error codes	System log severity level	Internal Passport 8000 Series switch severity level
0	Emergency	Fatal
1	Alert	-
2	Critical	-
3	Error	Error
4	Warning	Warning
5	Notice	-
6	Info	Info
7	Debug	-

Changing the severity level mapping

To change the severity level mapping:

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

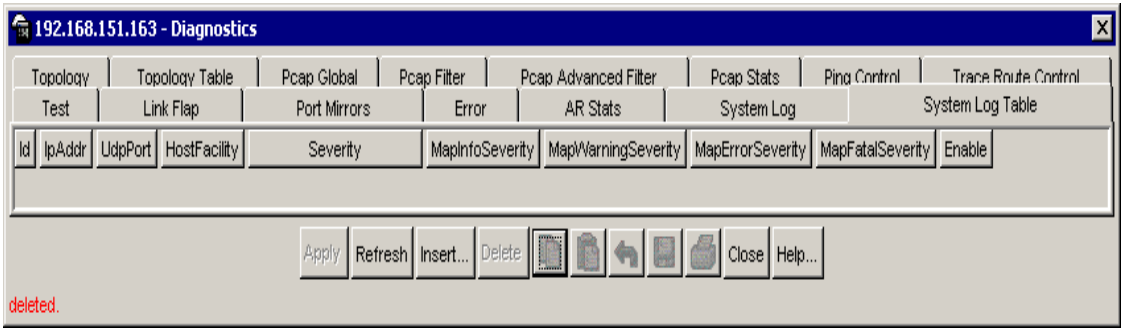
   The Diagnostics dialog box opens with the Test tab displayed.

2. Click the System Log Table tab.

   The System Log Table tab opens. (Figure 31)

3. For each severity type, use the MapWarningSeverity list to change the severity level.

Figure 31 Diagnostics dialog box—System Log Table tab



To insert a system log table member:

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

   The Diagnostics dialog box opens with the Test tab displayed.

2. Click the System Log Table tab.

   The System Log Table tab opens.

3. In the Diagnostics dialog box, click Insert.

   The Diagnostics, Insert System Log Table dialog box opens. (Figure 32)

4. Select the appropriate items.
5. Click Insert.

Figure 32 Diagnostics, Insert System Log Table dialog box

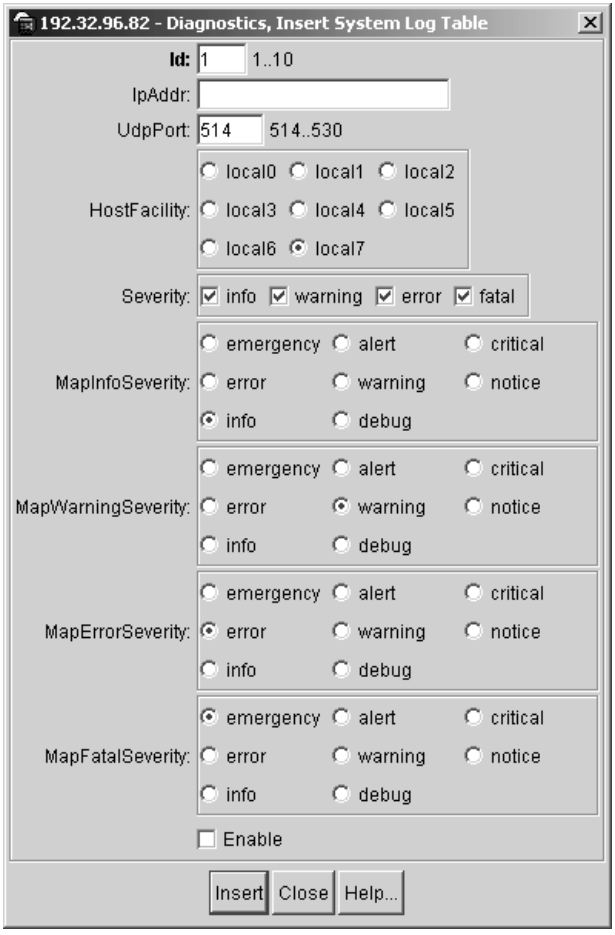


Table 11 describes the System Log Table tab fields and Diagnostics, Insert System Log Table dialog box.

Table 11 Diagnostics, Insert System Log Table dialog box fields

Field	Description
Id	ID for the syslog host being created.
IpAddr	IP address of the syslog host.
UdpPort	The UDP port to use to send messages to the syslog host (514 to 530).
HostFacility	The syslog host facility used to identify messages (LOCAL0 to LOCAL7)
Severity	The Passport 8000 Series switch message severity for which syslog messages will be sent.
MapInfoSeverity	The fields that map Passport 8000 Series switch severity levels to syslog severity.
MapWarningSeverity	The fields that map Passport 8000 Series switch warning severity levels to syslog severity.
MapErrorSeverity	The fields that map Passport 8000 Series switch error severity levels to syslog severity.
MapFatalSeverity	The fields that map Passport 8000 Series switch fatal severity levels to syslog severity.
Enable	Enables or disables sending messages to the syslog host.

Checking the MIB status

This section includes the following topics:

View topology status information

Use the Topology tab to view Nortel Management MIB (NMM) status information.

To view topology status information:

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

The Diagnostics dialog box opens with the Test tab displayed.

2 Click the Topology tab.

The Topology tab opens. (Figure 33)

Figure 33 Diagnostics dialog box—Topology tab

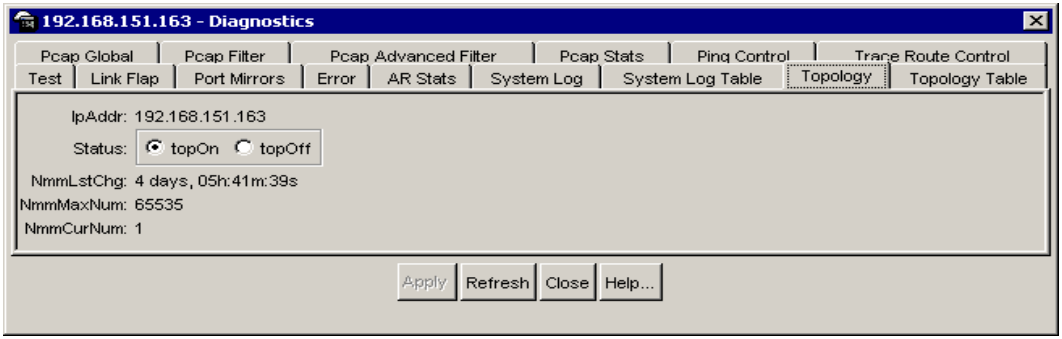


Table 12 describes the Topology tab fields on the Diagnostics dialog box.

Table 12 Topology tab fields

Field	Description
IpAddr	The IP address of the device.
Status	Whether Nortel Networks topology is on or off for the device.
NmmLstChg	The value of sysUpTime the last time an entry in the network management MIB (NMM) topology table was added, deleted, or modified. If the table has not changed since the last cold or warm start of the agent.
NmmMaxNum	The maximum number of entries in the NMM topology table.
NmmCurNum	The current number of entries in the NMM topology table.

Checking the details of the MIB status

Use the Topology Table tab to view details of Nortel Management MIB (NMM) status information.

To view topology table information:

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

   The Diagnostics dialog box opens with the Test tab displayed.

2. Click the Topology Table tab.

   The Topology Table tab opens. (Figure 34)

Figure 34 Diagnostics dialog box—Topology Table tab

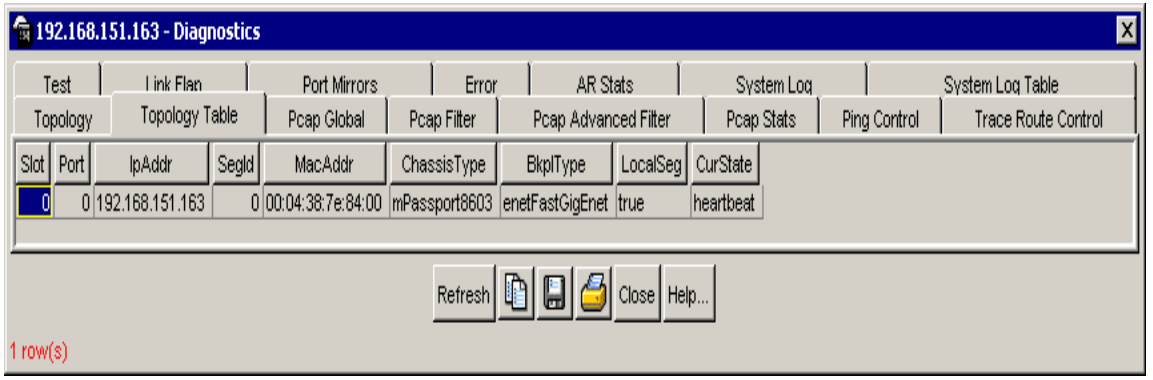


Table 13 describes the Topology Table tab fields.

Table 13 Topology Table tab fields

Field	Description
Slot	The slot number in the chassis in which the topology message was received.
Port	The port on which the topology message was received.
IpAddr	The IP address of the sender of the topology message.
SegId	The segment identifier of the segment from which the remote agent sent the topology message. This value is extracted from the message.
MacAddr	The MAC address of the sender of the topology message.
ChassisType	The chassis type of the device that sent the topology message.
BkplType	The backplane type of the device that sent the topology message.
LocalSeg	Indicates if the sender of the topology message is on the same Ethernet segment as the reporting agent.
CurState	The current state of the sender of the topology message. The choices are: • topChanged—Topology information has recently changed. • heartbeat—Topology information is unchanged. • new—The sending agent is in a new state.

Running Ping Test

This feature provides the functionality of running Ping operations remotely via management stations. This implementation is done using RFC 2925. The user can create Ping test entries and log the cumulative test result as well as the probe wise test results. The user also gets the flexibility to specify the frequency at which the test would run all over again. Target Address, Data Size, Probe Count, Time-Out period, Data Pattern are some other parameters, which can be specified by the user.

To run Ping:

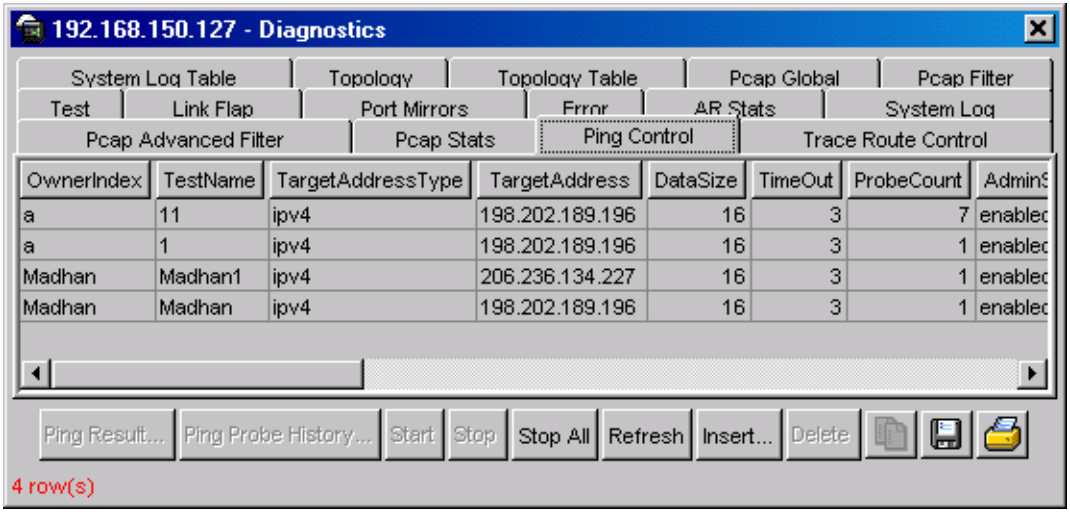
1 From the Device Manager menu bar, choose Edit > Diagnostics.

The Diagnostics dialog box opens with the Test tab displayed.

2 Click the Ping Control tab.

The Ping Control tab opens. (Figure 35)

Figure 35 Diagnostics dialog box - Ping Control tab



(Table 14) describes the Diagnostics, Ping Control box fields.

Table 14 Diagnostics, Ping Control dialog box fields.

Field	Description
OwnerIndex	Facilitates the provisioning of access control by a security administrator using the View-Based Access Control Model (VACM) for tables in which multiple users may need to independently create or modify entries.
TestName	The name of the Ping test.
TargetAddressType	The type of host address to be used at a remote host to perform a ping operation.
TargetAddress	The host address to be used at a remote host to perform a ping operation.
DataSize	The size of the data portion to be transmitted in a ping operation in octets.
TimeOut	The time-out value, in seconds, for a remote ping operation.
ProbeCount	The number of times to perform a ping operation at a remote host.
AdminStatus	The desired state that a Ping Control Entry should be in. the options are: • Enabled - Attempt to activate the test as defined by this Ping Control Entry. • Disabled - Deactivate the test as defined by this Ping Control Entry.
DataFill	Determines how to fill the data portion of a probe packet
Frequency	The number of seconds to wait before repeating a ping test as defined by the value of the various objects in the corresponding row
MaxRows	The maximum number of entries allowed in the PingProbeHistory table.
StorageType	The storage type for this conceptual row.

Field	Description
TrapGeneration	The value of this object determines when and if to, generate a notification for this entry. The options are: • ProbeFailure - Generates a PingProbeFailed notification subject to the value of pingCtlTrapProbeFailureFilter. The object pingCtlTrapProbeFailureFilter can be used to specify the number of successive probe failures that are required before a pingProbeFailed notification can be generated. • TestFailure - Generates a PingTestFailed notification. In this instance the object pingCtlTrapTestFailureFilter can be used to determine the number of probe failures that signal when a test fails. • TestCompletion - Generates a PingTestCompleted notification.
TrapProbeFailureFilter	Determines the generation of a PingProbeFailed notification.
TrapTestFailureFilter	Determines the generation of a PingTestFailed notification.
Type	Selects or reports the implementation method to be used for calculating a ping response time.
Descr	Desrciption of the remote ping test.
SourceAddressType	Specifies the type of the source address, PingCtlSourceAddress, to be used at a remote host when performing a ping operation.
SourceAddress	The specified IP address (which must be given in numeric form, not as a hostname) as the source address in outgoing probe packets.
IfIndex	Setting this object to an interface's ifIndex, prior to starting a remote ping operation, directs the ping probes to be transmitted over the specified interface.
ByPassRouteTable	Using this you can optionally enable bypassing the route table.
DSField	Specifies the value to store in the Differentiated Services (DS) field in the IP packet used to encapsulate the ping probe.

3 In the Edit>Diagonistics>Ping Control tab:

Click “Insert” and create an entry in the Ping Control table.

4 Select an entry in the Ping Control table and the “Ping Result” and the “Ping Probe History” buttons are enabled. “Start” is activated

5 You can click “Start” to run a Ping test. You can click on “Stop” to stop the Ping test

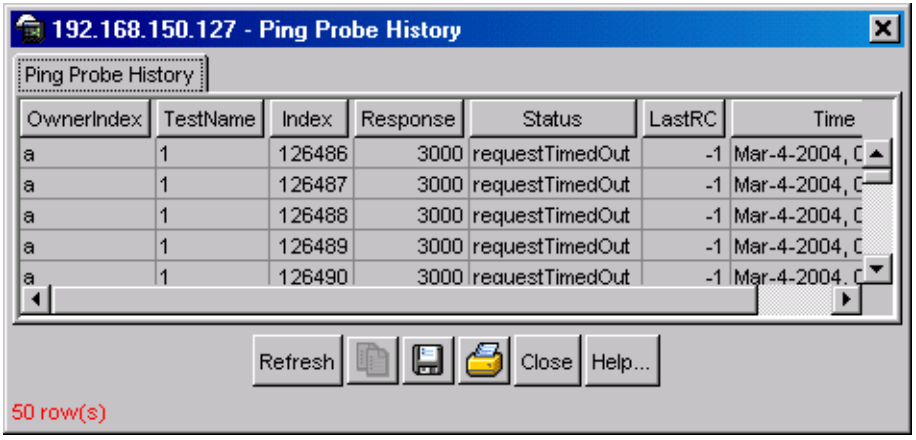
Ping Probe History

1 Click in any field in the Ping Control table. The Ping Probe History button is enabled.

2 Click Ping Probe History button.

The Ping Probe History screen opens. (Figure 36)

Figure 36 Ping Probe History screen



(Table 15) describes the fields.

Table 15 Ping Probe History fields

Field	Description
Ownerindex	Owner index
Testname	The name given to test.
Index	Index number
Response	The number of responses
Status	At what status the response stands

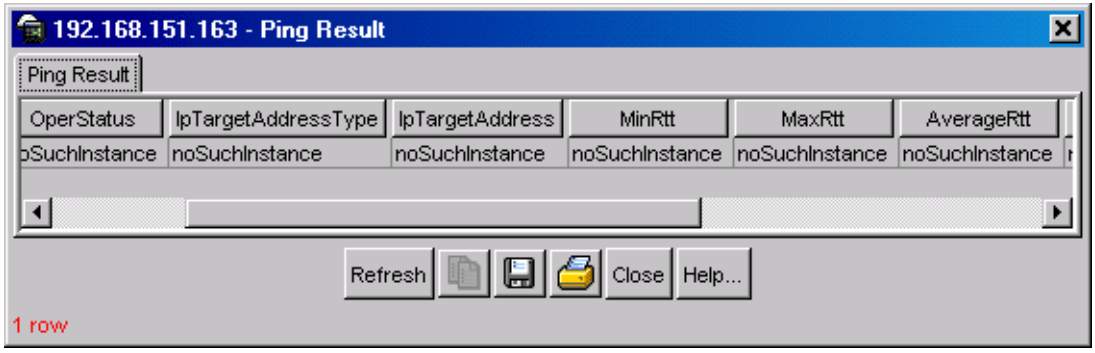
Table 15 Ping Probe History fields

Field	Description
LastRC	Last time recorded
Time	The time taken to respond.

Ping Result

Highlight an entry in the Ping control tab and the Ping result gets activated.

Figure 37 Ping Result



(Figure 16) describes the fields.

Table 16 Ping Result Ffields

Field	Description
OwnerIndex	Index owned
TestName	Test name
OperStatus	Status of operation
IPTargetAddressType	The address type of IP
IPTargetAddress	The address of IP
MinRtt	Minimum rtt
MaxRtt	Maximum rtt
AverageRtt	Average rtt

Table 16 Ping Result Ffields

Field	Description
ProbeResponses	Responses for probes
SentProbes	Probes that are sent
RttSumofSquares	The sum of squares of rtt
LastGoodProbe	Last good probe done.

Running TraceRoute Test

This feature provides the functionality of running TraceRoute operations remotely via management stations. This implementation is done using RFC 2925. The user can create TraceRoute the test entries and log the cumulative test result as well as the probe wise test results. The user also gets the flexibility to specify the frequency at which the test would run all over again. Target Address, Data Size, Probe Count, Time-Out period, Data Pattern are some other parameters, which can be specified by the user.

To run Trace Route:

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

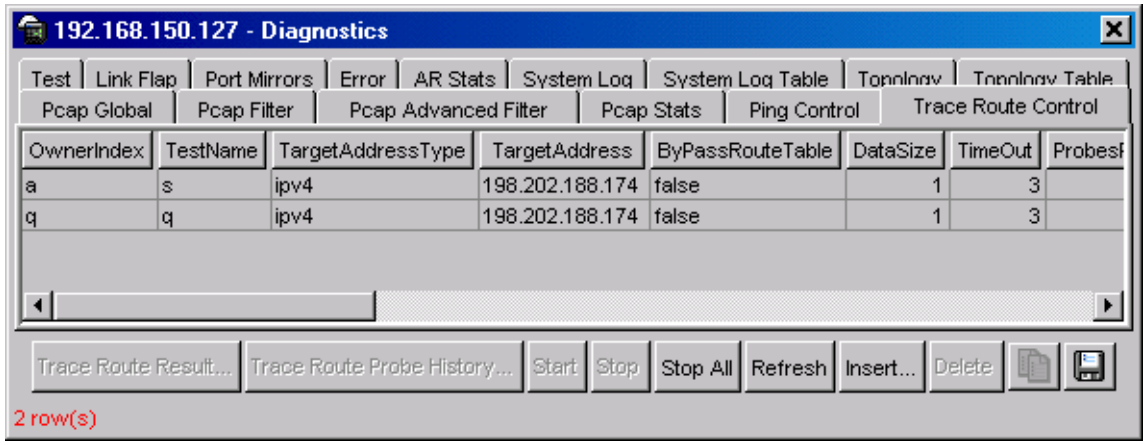
   The Diagnostics dialog box opens with the Test tab displayed.

2. Click the Trace Route Control tab.

   The Trace Route Control tab opens. (Figure 38)

3. Click “Insert” and create an entry in the Trace Route Control tab.

Figure 38 Diagnostics dialog box - Trace Route tab



(Table 17) describes the Diagnostics, TraceRoute Control box fields.

4 Highlight an entry in the Trace Route table and “Trace Route Result”, “Trace Route History” “Start” and “Stop” are activated.

5 Click “Start” to start a Trace Route operation and “Stop” to stop or “StopAll” to stop all operations.

Table 17 Diagnostics, TraceRoute Control box fields. fields.

Field	Description
OwnerIndex	Facilitates the provisioning of access control by a security administrator using the View-Based Access Control Model (VACM) for tables in which multiple users may need to independently create or modify entries.
TestName	The name of the TraceRoute test.
TargetAddressType	Specifies the type of host address to be used on the TraceRoute request at the remote host.
TargetAddress	Specifies the host address used on the TraceRoute request at the remote host.
ByPassRouteTable	Using this field you can optionally enable bypassing of the route table.
DataSize	Specifies the size of the data portion of a TraceRoute request in octets.
TimeOut	Specifies the time-out value, in seconds, for a TraceRoute request.
ProbesPerHop	Specifies the number of times to re-issue a traceroute request with the same time-to-live (TTL) value.
Port	Specifies the UDP port to which you need to send the TraceRoute request.
MaxTtl	Specifies the maximum time-to-live value.
DSField	Specifies the value to store in the Differentiated Services (DS) field in the IP packet used to encapsulate the TraceRoute probe.
SourceAddressType	Specifies the type of the source address, TraceRouteCtlSourceAddress, to be used at a remote host when you perform a TraceRoute operation.
SourceAddress	Use the specified IP address (which must be given as an IP number, not a hostname) as the source address in outgoing probe packets.
IfIndex	Setting this object to an interface's ifIndex, prior to starting a remote traceroute operation, directs the TraceRoute probes to be transmitted over the specified interface
MiscOptions	Enables an application to specify implementation dependent options.
MaxFailures	The value of this object indicates the maximum number of consecutive timeouts allowed before terminating a remote TraceRoute request.

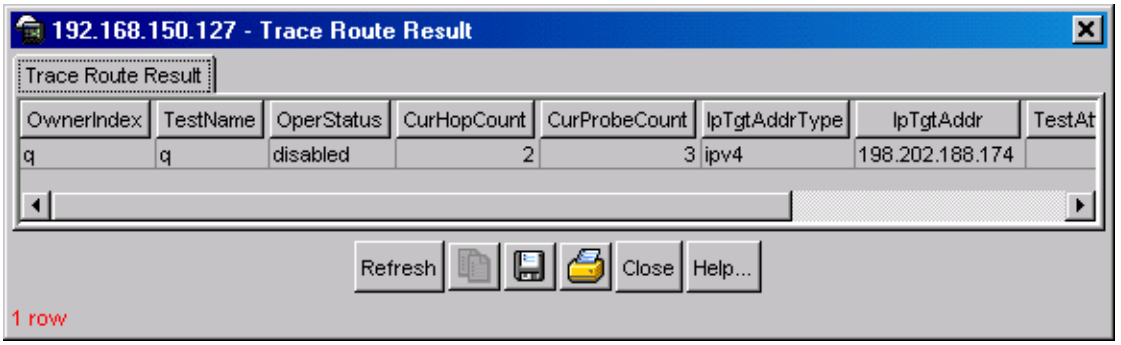
Field	Description
DontFragment	This field enables setting of the don't fragment flag (DF) in the IP header for a probe.
InitialTtl	Specifies the initial TTL value to use.
Frequency	The number of seconds to wait before repeating a TraceRoute test as defined by the value of the various objects in the corresponding row.
StorageType	The storage type for this conceptual row.
AdminStatus	The desired state that a TraceRouteCtlEntry should be in. The options are: • Enabled - Attempt to activate the test as defined by this TraceRouteCtlEntry. • Disabled - Deactivate the test as defined by this TraceRouteCtlEntry.
MaxRows	The maximum number of entries allowed in the traceRouteProbeHistoryTable.
TrapGeneration	The value of this object determines when to generate a notification for this entry. The options are: • PathChange - Generate a TraceRoutePathChange notification when the current path varies from a previously determined path. • TestFailure - Generate a TraceRouteTestFailed notification when the full path to a target can't be determined. • TestCompletion - Generate a TraceRouteTestCompleted notification when the path to a target has been determined.
Descr	Description of the remote TraceRoute test.
CreateHopsEntries	The current path for a TraceRoute test is kept in the TraceRouteHopsTable on a per hop basis when the value of this object is true(1).
Type	Use this field either to report or select the implementation method to be used for performing a TraceRoute operation

Trace Route Result

1. Click on a field and the Trace Route Result button is enabled.
2. Click on the Trace Route Result button.

The Trace Route Result screen displays. (Figure 39)

Figure 39 Trace Route Result screen



(Table 18) describes the Trace Route result fields.

Table 18 Trace Route Result fields

Fields	Description
Ownerindex	Index owner
Testname	name of the test
Operstatus	Operation status
CurHopCount	Current count of hops.
CurProbeCount	Current count of probe
IpTgtAddressType	IP target address type
IpTgtAddr	IP target address
TestAttempts	Number of test attempts
TestSuccesses	Number of successful test attempts
LastGoodPath	Time stamp of the last successful traceRoute operation for a particular Trace-Route Control Entry

Trace Route Probe History

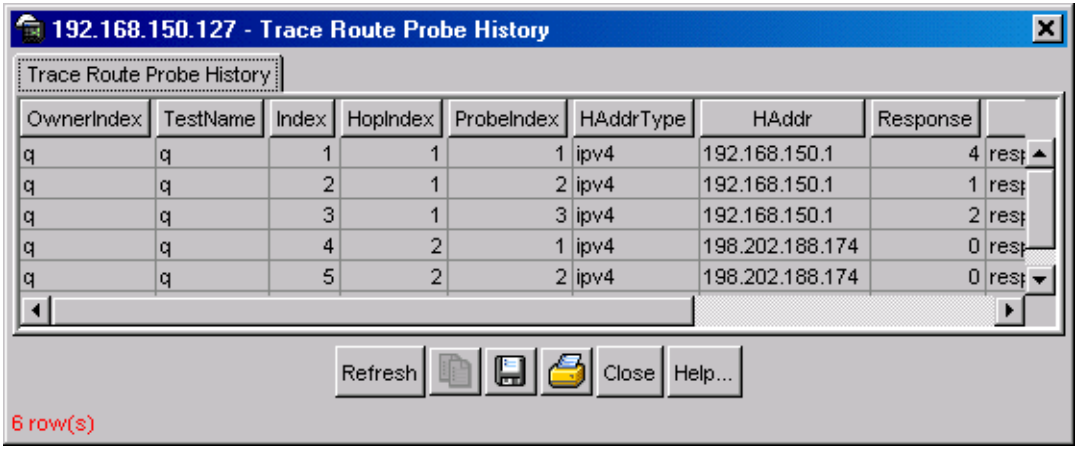
Contains probe information for the hops in the routing path.

Click a field and the trace Route Probe History button is enabled.

Click the Route Probe History button.

The Trace Route Probe History screen displays. (Figure 40)

Figure 40 Trace Route Probe History dialog



(Table 19) describes the Trace Route Probe History fields.

Table 19 Trace Route Probe History fields

Field	Description
Ownerindex	Owner Index
TestName	Test name
Index	Index
HopIndex	Per probe information
ProbeIndex	Index per probe
HAddrType	IP adress type of the hop to which this probe belongs.
Haddr	IP adress of the hop to which this probe belongs.
Response	Cumulative results at any time.
Status	Status of the probe.

Table 19 Trace Route Probe History fields

Field	Description
LastRC	When a new entry is added in the ProbeHistoryTable, the old entry is purged if the total number of entries exceeds the specified maximum number of entries in the Control Table Entry
Time	Response time of the probe.

Configuring and Displaying Remote Mirroring

Remote mirroring provides the feature to steer mirrored traffic through a switch cloud to a network analysis probe located on a remote switch. In a network, this feature allows the user, to monitor many ports from different switches using one network probe device. This function is achieved by encapsulating mirrored packets in a Remote Mirroring Encapsulation “wrapper”.

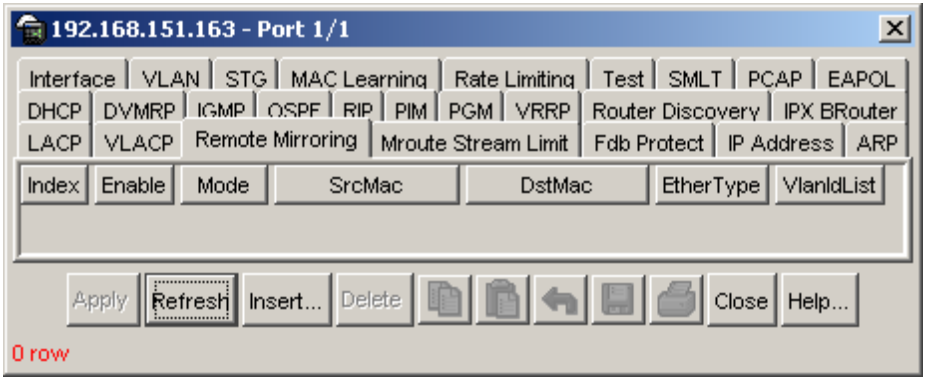
To configure ports for remote mirroring:

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

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

   The Remote Mirroring tab opens (Figure 41).

Figure 41 Port dialog box—Remote Mirroring tab



4 Click Insert to add an entry.

The Insert Remote Mirroring dialog box opens (Figure 42).

Figure 42 Insert Remote Mirroring dialog box

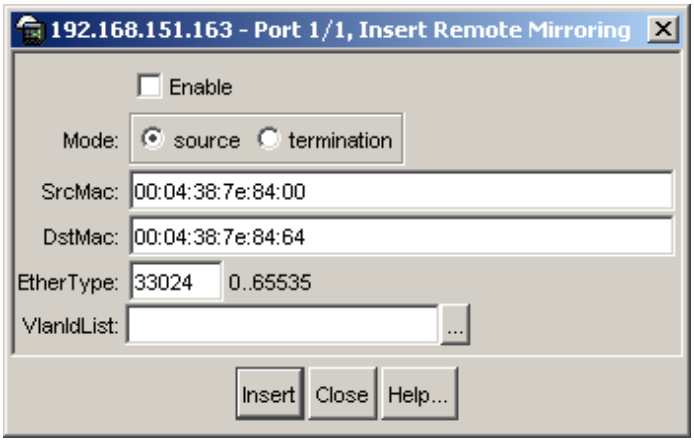


Table 20 describes the Remote Mirroring tab fields.

Table 20 Remote Mirroring tab fields

Field	Description
Enable	Enable/disables the feature on the port. When RMT is enabled, the following things are done. • An FDB static entry for the dstmac is added. This is to send all the packets that are coming with remote mirroring dstmac to RMT port. • Switch periodically (once in 10 secs) transmits broadcast layer 2 packets in all the vlan added so that all nodes in the network can learn the dstmac
mode<source|termination>	Specifies whether the port is a RMT or RMS.
srcmac	Used to set the source mac for the remote mirroring encapsulation. The packet will be sent out of RMS with source mac derived from this. The source mac of the encapsulated frame will contain first 45 bits of this Mac address. The three least significant bits are derived from the port number of RMS port. Mac address of the port is used as default value.
dstmac	Used to set the destination mac for the remote mirroring encapsulation. The remote mirrored packet will be sent to this mac address. User configured dstmac is used only for RMS. For RMT, one of the unused Mac address from the switch Port Mac address range is used. To get the same dstmac for RMT across re-boot, this mac address is saved in configuration file and only when config file is restored, the dstmac of RMT is accepted from user.

Table 20 Remote Mirroring tab fields (continued)

Field	Description
Ether Type	The ether-type of the remote mirrored packet. Default value is 0x8103.
VlanIdList	Used only for RMT. The user has to specify which vlan the remote mirror destination mac belongs to. This has to be a port based VLAN. When the RMT port is removed from the last vlan in the list, RMT will be disabled from the port.

5 Click Insert to insert the remote mirroring entry.

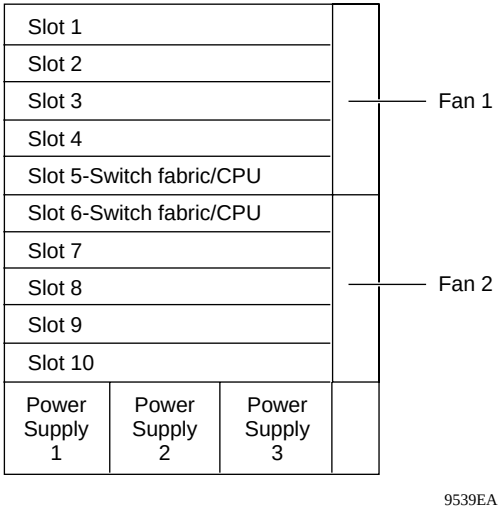
Appendix A
Port numbering and MAC address assignment

This appendix includes information about the following topics:

Port Numbering

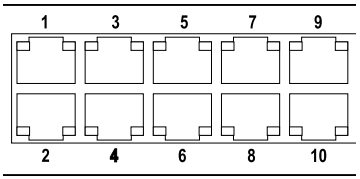
A port number includes the slot location of the module in the chassis, as well as the port's position in the I/O module. In the Passport 8000 Series switches, slots are numbered from top to bottom. Figure 43 shows slot numbering for an 8010 chassis.

Figure 43 8010 chassis slots



Ports are numbered generally from left to right beginning with 1 for the far left port. On high-density modules with two rows of ports, such as the 8648TX module, ports in the top row are assigned sequential odd numbers, and ports in the bottom row are assigned sequential even numbers (Figure 44).

Figure 44 Port numbers on high-density modules



Interface indexes

Interface indexes are used in SNMP to identify ports, VLANs, and Multi-Link Trunks.

The interface index of a port is computed using the following formula:

inIndex = (64 x slot number) + (port number – 1)

where:

Slot number is a value between 1 and 10, inclusive.

Port number is a value between 1 and 48, inclusive.

For example, the interface index of port 1/1 is 64, and the interface index of port 10/48 is 687.

The interface index of a VLAN is computed using the following formula:

ifIndex = 2048 + VLAN’s MGID

where:

MGID is the multicast group ID number.

Because the default VLAN always has an MGID value of 1, its interface index is always 2049.

The interface index of a Multi-Link Trunk (MLT) is computed using the following formula:

ifIndex = 4096 + MLT ID number

MAC address assignment

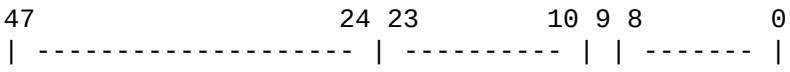
Understanding how MAC addresses are assigned is important when you define static ARP entries for IP addresses in the switch and when you use a network analyzer to decode network traffic.

Each [Model #] module is assigned a base of 1024 MAC addresses. Within the switch, these MAC addresses are assigned as follows:

- 512 addresses for ports in the switch (physical MAC addresses)
- 500 addresses for VLANs in the switch (virtual MAC addresses)
- 8 addresses for CPU interfaces
- 4 addresses for use by other Passport 8000 Series modules

A MAC address has the format shown in Figure 45.

Figure 45 Parts of a MAC address



The MAC address is divided into the following parts:

- Bits 47–24: IEEE OUI (for example, 00-80-2d)
- Bits 23–10: Chassis ID
- Bit 9: Type of MAC address in the switch:
  - 0 = Port address (physical MAC address)

  - 1 = VLAN address (virtual MAC address)
- Bits 8–0: Unique port or VLAN address

Physical MAC addresses

Physical MAC addresses are addresses assigned to the physical interfaces or ports visible on the device. The physical MAC addresses are used in the following types of frames:

- Spanning Tree Protocol BPDUs sent by the switch
- Frames to or from an isolated routing port's physical interface

BPDUs are sent using the physical MAC address as the source because identifying which physical port sent the BPDU is critical to how the Spanning Tree Protocol works.

The ports on the switch fabric/CPU module have the following last bytes:

- Management port in slot 5: 0xf4
- CPU port (an internal port) in slot 5: 0xf5
- Management port in slot 6: 0xf6
- CPU port in slot 6: 0xf7
- Virtual management IP address: 0xf8

Virtual MAC addresses

Virtual MAC addresses are the addresses assigned to VLANs. A virtual MAC address is assigned to a VLAN when it is created. The MAC address for a VLAN IP address is the virtual MAC address assigned to the VLAN.

Appendix B
Edit commands

To edit a file, type ESC to enter edit mode and use the commands listed in Table 21. The ESC key switches the shell to edit mode. The RETURN key always moves to the next line.

When you enter the editor, you are in edit mode.

Table 21 is a summary of the commands available in edit mode.

Table 21 Commands available in edit mode

Key Combination	Description
:q	Ends the editing mode without saving the changes made to a file.
:w	Quits and saves the file.
ZZ	Quits and saves the file.
	Movement and Search Commands
^L	Redraw screen.
^F	Display next screen.
^B	Display previous screen.
^D	Display next 1/2 screen.
^U	Display previous 1/2 screen.
<*n*>G	Go to command number *n*.
G	Go to last command line.
/<*s*>	Search for string *s* forward in file.
?<*s*>	Search for string *s* backward in file.
n	Repeat last search.
N	Repeat last search in opposite direction.

Table 21 Commands available in edit mode (continued)

Key Combination	Description
<*n*>k	Get *nth* previous line in file.
<*n*>-	Same as “k.”
<*n*>j	Get *nth* next line in file.
<*n*>+	Same as “j.”
RETURN	Same as “j.”
<*n*>h	Move left *n* characters.
^H	Same as “h.”
<*n*>l	Move right *n* characters.
SPACE	Same as “l.”
<*n*>w	Move *n* words forward.
<*n*>W	Move *n* blank-separated words forward.
<*n*>e	Move to end of the *nth* next word.
<*n*>E	Move to end of the *nth* next blank-separated word.
<*n*>b	Move back *n* words.
<*n*>B	Move back *n* blank-separated words.
f<*c*>	Find character *c*, searching forward.
F<*c*>	Find character *c*, searching backward.
^	Move cursor to first nonblank character in line.
$	Go to end of line.
0	Go to beginning of line.
	Insert Commands (Input is expected until an ESC is typed)
a	Append.
A	Append at end of line.
c SPACE	Change character.
cl	Change character.
cw	Change word.
cc	Change entire line.
c$	Change everything from the cursor to the end of the line.

Table 21 Commands available in edit mode (continued)

Key Combination	Description
C	Same as “c$.”
S	Same as “cc.”
i	Insert.
I	Insert at the beginning of the line.
R	Type over characters.
o	Open a line below current line.
O	Open a line above current line.
	Editing Commands
<*n*>r<*c*>	Replace the following *n* characters with *c*.
<*n*>x	Delete *n* characters starting at the cursor.
<*n*>X	Delete *n* characters to the left of the cursor.
d SPACE	Delete character.
dl	Delete character.

Note: The default value for <*n*> is 1.

Appendix C
Special terminal characters

Table 22 lists the special terminal characters.

Table 22 Special terminal characters

Key Combination	Command
^H	Backspace.
^D	Logout of cli.
^C	Abort line entry.
^P	Previous history command.
^N	Next history command.
^S	Output suspend.
^Q	Output resume.
^I	Command completion.
^B	Move cursor back one character.
^F	Move cursor forward one character.
^A	Move cursor to beginning of line.
^E	Move cursor to end of line.
ESC B	Move cursor back one word.
ESC F	Move cursor forward one word.
DEL	Erase character at cursor.
^K	Erase all characters from cursor to end of line.
^X	Erase all characters before the cursor to beginning of line.
^U	Erase or clear entire line.
^W	Erase word to left of cursor.
ESC D	Erase from cursor to end of word.
^L	Redisplay line.
^R	Redisplay line.

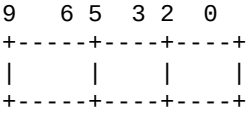
Table 22 Special terminal characters (continued)

Key Combination	Command
^T	Transpose the character to left of cursor with character at cursor.
ESC L	Change character at cursor to lowercase.
ESC U	Change character at cursor to uppercase.
;	Multiple command terminator.
"..."	Preserve white space in strings.

Appendix D
Tap and OctaPID assignment

The switch fabric in the Passport 8600 modules has nine switching taps, one for each of the eight I/O slots (1 to 4 and 7 to 10) and one for the CPU slots (5 and 6). Taps 0-7 map to the eight I/O slots and can support up to eight OctaPIDs. Each OctaPID can support up to eight ports.

In the Passport 8000 Series switch, a physical port number is 10 bits long and has the following format:



bits 9–6: Tap number (0–15)

bits 5–3: OctaPID number (0–7)

bits 2-0: MAC port number (0-7)

The Tap number bits and the OctaPID number bits combined (bits 9–3) are usually referred to as the OctaPID ID.

Table 23 lists the module types that are currently available, along with the associated OctaPID ID assignments for each module.

Table 23 Available module types and OctapPID ID assignments

Module type	Port type	OctaPID ID assignment
8608GBE and 8608GBM Modules	1000BASE-SX (GBIC)	Table 24 next
	1000BASE-LX (GBIC)	
	1000BASE-ZX (GBIC)	
	1000BASE-XD (GBIC)	
	1000BASE-TX (GBIC)	
8608GTE and 8608GTM Modules	1000BASE-T	Table 24 next
8608SXE Module	1000BASE-SX	Table 24 next
8616SXE Module	1000BASE-SX	Table 25 on page 119
8624FXE Module	100BASE-FX	Table 26 on page 120
8632TXE and 8632TXM Modules	10BASE-T/100BASE-TX	Table 27 on page 120
	1000BASE-SX (GBIC)	
	1000BASE-LX (GBIC)	
	1000BASE-ZX (GBIC)	
	1000BASE-XD (GBIC)	
	1000BASE- TX (GBIC)	
8648TXE and 8648TXM Modules	10/100 Mb/s	Table 28 on page 120
8672ATME and 8672ATMM Modules	OC-3c MDA	Table 29 on page 121
	OC-12c MDA	
	DS3	
8681XLR Module	10GBASE-LR	Table 30 on page 121
8681XLW Module	10GBASE-LW	Table 31 on page 122
8683POSM Module	OC-3c MDA	Table 32 on page 122
	OC-12c MDA	

Table 24 describes the OctaPID ID and port assignments for the 8608GBE, Passport 8608GBM, 8608GTE, 8608GTM, and 8608SXE modules.

Table 24 8608GBE/8608GBM/8608GTE/8608GTM, and 8608SXE modules

OctaPID ID assignment	Port assignment
OctaPID ID: 0	Port 1
OctaPID ID: 1	Port 2
OctaPID ID: 2	Port 3
OctaPID ID: 3	Port 4
OctaPID ID: 4	Port 5
OctaPID ID: 5	Port 6
OctaPID ID: 6	Port 7
OctaPID ID: 7	Port 8

Table 25 describes the OctaPID ID and port assignments for the 8616SXE Module.

Table 25 8616SXE module

OctaPID ID assignment	Port assignment
OctaPID ID: 0	Ports 1 and 2
OctaPID ID: 1	Ports 3 and 4
OctaPID ID: 2	Ports 5 and 6
OctaPID ID: 3	Ports 7 and 8
OctaPID ID: 4	Ports 9 and 10
OctaPID ID: 5	Ports 11 and 12
OctaPID ID: 6	Ports 13 and 14
OctaPID ID: 7	Ports 15 and 16

Table 26 describes the OctaPID ID and port assignments for the 8624FXE Module.

Table 26 8624FXE module

OctaPID ID assignment	Port assignment
OctaPID ID: 0	Ports 1 through 8
OctaPID ID: 1	Ports 9 through 16
OctaPID ID: 2	Ports 17 through 24

Table 27 describes the OctaPID ID and port assignments for the 8632TXE and 8632TXM Modules.

Table 27 8632TXE and 8632TXM modules

OctaPID ID assignment	Port assignment
OctaPID ID: 0	Ports 1 through 8
OctaPID ID: 1	Ports 9 through 16
OctaPID ID: 2	Ports 17 through 24
-	-
-	-
OctaPID ID: 5	Ports 25 through 32
OctaPID ID: 6	Port 33 (GBIC port)
OctaPID ID: 7	Port 34 (GBIC port)

Table 28 describes the OctaPID ID and port assignments for the 8648TXE and 8648TXM Modules.

Table 28 8648TXE and 8648TXM modules

OctaPID ID assignment	Port assignment
OctaPID ID: 0	Ports 1 through 8
OctaPID ID: 1	Ports 9 through 16
OctaPID ID: 2	Ports 17 through 24
-	-
-	-

Table 28 8648TXE and 8648TXM modules

OctaPID ID assignment	Port assignment
OctaPID ID: 5	Ports 25 through 32
OctaPID ID: 6	Port 33 through 40
OctaPID ID: 7	Port 41 through 48

Table 29 describes the OctaPID ID and port assignments for the 8672ATME and 8672ATMM Modules.

Table 29 8672ATME and 8672ATMM modules

OctaPID ID assignment	Port assignment
OctaPID ID: 0	• Ports 1 through 4 (with OC-3c MDA) • Port 1 (with OC-12c MDA) • Ports 1 through 2 (with DS-3 MDA)
OctaPID ID: 1	• Ports 5 through 8 (with OC-3c MDA) • Port 5 (with OC-12c MDA) • Ports 5 through 6 (with DS-3 MDA)
OctaPID ID: 2	Not used

Table 30 describes the OctaPID ID and port assignments for the 8681XLR Module.

Table 30 8681XLR module

OctaPID ID assignment	Port assignment
OctaPID ID: 0	Port 1
OctaPID ID: 1	
OctaPID ID: 2	
OctaPID ID: 3	
OctaPID ID: 4	
OctaPID ID: 5	
OctaPID ID: 6	
OctaPID ID: 7	

Table 31 describes the OctaPID ID and port assignments for the 8681XLW Module.

Table 31 8681XLW module

OctaPID ID assignment	Port assignment
OctaPID ID: 0	Port 1
OctaPID ID: 1	
OctaPID ID: 2	
OctaPID ID: 3	
OctaPID ID: 4	
OctaPID ID: 5	
OctaPID ID: 6	
OctaPID ID: 7	

Table 32 describes the OctaPID ID and port assignments for the 8683POSM Module.

Table 32 8683POSM module

OctaPID ID assignment	Port assignment
OctaPID ID: 0	• Ports 1 and 2 (with OC-3c MDA) • Port 1 (with OC-12c MDA)
OctaPID ID: 1	• Ports 3 and 4 (with OC-3c MDA) • Port 3 (with OC-12c MDA)
OctaPID ID: 2	• Ports 5 and 6 (with OC-3c MDA) • Port 5 (with OC-12c MDA)

Index

N

O

P

R

S

T

U

V