OptiView™ Protocol Expert

Users Manual

Note: Most figures in this manual are best viewed in PDF at 134%,
    Large figures at 200%

LIMITED WARRANTY AND LIMITATION OF LIABILITY

Fluke Networks, Inc. (Fluke Networks) warrants its products to be free from defects in material and workmanship under normal use and service for one (1) year, beginning on the date of shipment. This warranty extends only to the original buyer or end-user customer of a Fluke Networks authorized reseller, and does not apply to fuses, disposable batteries, or to any product which, in Fluke Network's opinion, has been misused, altered, neglected, contaminated, or damaged by accident or abnormal conditions of operation or handling. Fluke Networks warrants that software will operate substantially in accordance with its functional specifications for 90 days and that it has been properly recorded on non-defective media. Fluke Networks does not warrant that software will be error free or operate without interruption.

Fluke Networks authorized resellers shall extend this warranty on new and unused products to end-user customers only but have no authority to extend a greater or different warranty on behalf of Fluke Networks.

Fluke Networks' warranty obligation is limited, at Fluke Networks' option, to refund of the purchase price, free of charge repair, or replacement of a defective product which is returned to a Fluke Networks authorized service center within the warranty period.

To obtain warranty service, call Fluke Networks for instructions. Following warranty repair, the product will be returned to Buyer, transportation prepaid (FOB Destination). If Fluke Networks determines that failure was caused by neglect, misuse, contamination, alteration, accident, or abnormal condition of operation or handling, including over-voltage failures caused by use outside the product's specified rating, or normal wear and tear of mechanical components, Fluke Networks will provide an estimate of repair costs and obtain authorization before commencing the work. Following repair, the product will be returned to the Buyer transportation prepaid and the Buyer will be billed for the repair and return transportation charges (FOB Shipping Point).

Warranty service is available outside the United States only if product was purchased through a Fluke Networks Authorized Sales outlet in the country of use or the applicable Fluke Networks international price was paid. Product transported from the United States for which the applicable Fluke Networks International price was not paid must be returned to the U.S. to receive warranty service, at the shipment expense and risk of Buyer. Fluke Networks reserves the right to invoice Buyer for importation costs of repair/replacement parts when product purchased in one country is submitted for repair in another country.

THIS WARRANTY IS BUYER'S SOLE AND EXCLUSIVE REMEDY AND IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PAR-TICULAR PURPOSE. FLUKE NETWORKS SHALL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OR LOSSES, INCLUDING LOSS OF DATA, ARISING FROM ANY CAUSE OR THEORY.

Since some countries or states do not allow limitation of the term of an implied warranty, or exclusion or limitation of incidental or consequential damages, the limitations and exclusions of this warranty may not apply to every buyer. If any provision of this Warranty is held invalid or unenforceable by a court or other decision-maker of competent jurisdiction, such holding will not affect the validity or enforceability of any other provision.

Fluke Networks	Fluke Networks
P.O. Box 9090	P.O. Box 1186
Everett, WA 98206-9090	5602 BD Eindhoven
U.S.A.	The Netherlands

Note: Contact Fluke Networks Sales, Service, and Support Centers

To locate the nearest Fluke Networks distributor or Service Center, visit us on the World Wide Web at www.flukenetworks.com or email to info@flukenetworks.com or call:

USA: 1-800-283-5853
Anywhere in the world: +1-425-446-4519
Europe: +31 40-267-8300
Japan: +81-3-3434-0188
Singapore: +65-737-2922

Table of Contents

List of Tables

List of Figures

Figure   **Page**

Chapter 1
Introduction

Fluke Networks' fully distributed, full line rate performance network analysis products monitor, measure, analyze and troubleshoot 10/100/1000 Mbps Ethernet and VoIP. These products deliver unrivaled scalability, performance, accuracy and value to customers worldwide. Fluke Networks' OptiView™ Protocol Expert (OVP-PE) software is a Windows-based (95, 98, 2K, NT 4.x) software analyzer-plus-monitor application for 10/100/1000 Mbps Ethernet networks. OPV-PE provides users with the most robust, easy to use set of network analysis and monitoring tools in a single package. OPV-PE's features include full 7-layer packet decode and analysis, real-time network statistics, advanced alarm setting and actions, packet edit and slicing, multi-layer filtering, and automatic name table updating. Optional software modules provide multi-layer expert analysis, traffic generation and the ability to monitor remote segments.

Fluke Networks' newest software option, OPV-PE/VOIP, monitors, measures and analyzes QoS of VoIP (Voice Over IP) calls. It reports over 20 QoS metrics (jitter, packet loss, delay, etc.) and provides Call and Channel table summaries similar to Call Detail Records (CDRs) for standard VoIP protocols including H.323, SIP and Cisco SSP and SCCP calls. OPV-PE/VOIP is one of the first products to provide both network analysis and VoIP measurement and verification for Cisco AVVID (Architecture for Voice, Video and Integrated Data).

OPV-PE has expert features for automatic and very detailed problem diagnosis. Potential error conditions are automatically logged. Counters, addresses, protocols, and diagnostic information related to the detected network condition are displayed. You can also set alarms to be informed of any events detected by the Expert system.

OPV-PE can interface with one or more of Fluke Networks' hardware analyzer devices. OPV-PE can simultaneously capture, monitor and analyze multiple devices and analyze captured data. OPV-PE monitors local network segments, and the optional Remote Control software module allows OPV-PE to communicate with Fluke Networks hardware and access Fluke Networks products on remote segments.

OPV-PE's user interface provides both a comprehensive view of the network as well as the ability to easily drill down to a specific network segment. OPV-PE's main window provides a single, user-defined view for each of the segments being monitored. The user determines what information to view for each segment such as network utilization, protocol distribution, host table, etc. In this same window, the user can create alarms that monitor multiple segments simultaneously.

For test and development environments, a Traffic Generator software option provides advanced traffic generation and intelligent packet and file editing capabilities.

OPV-PE Functions

OPV-PE provides you with tremendous flexibility in performing the tasks required to monitor and troubleshoot your network. As your OPV-PE expertise grows you will find that the number of ways you can set up and apply the tool are virtually limitless.

The basic functions of OPV-PE are described in Table 1-1. Table 1-2 on the next page shows the additional options available with OPV-PE.

Table 1-1. OPV-PE Functions

Function	Description
Capture	Capture data from a network and place it in system memory space (buffer) on an analyzer device. OPV-PE lets you create and save special capture filters that direct analyzer devices to capture only the information you want to view and analyze.
Capture View	Look at the data in a way that is useful for network analysis and troubleshooting. OPV-PE lets you create and save special viewing filters. You use these filters to display only the information you want to analyze. The data can be viewed in numerous ways and from different perspectives. Display of the data can be either as graphical charts or row-and-column tables.
Expert Analysis	Expert analysis starts with the automatic logging of possible problems. Expert data views display counters, addresses, protocols, and diagnostic information related to the detected network condition. Expert alarms can be set to flag network error conditions. Actions can be performed when alarms are triggered.
Save	Move captured data from a capture buffer to a storage device on the OPV-PE host PC. OPV-PE enables you to store captured data onto your hard drive for later viewing, analysis, or transmission.

Table 1-1. OPV-PE Functions (continued)

Log	Record counter information. OPV-PE enables you to capture all byte, frame, and error counter values compiled during the capture or transmission of data.
Monitor	Real-time views for data seen on a network segment. The data can be viewed in numerous ways and from different perspectives. Display of the data can be either graphical charts or row-and-column tables.
Settings Alarms	Alarms can be set to flag network conditions. Actions can be performed when alarms are triggered.

Table 1-2. OPV-PE Software Options

Function	Description
Remote Control	All data collection and data management functions described in Table 1-1 are available from other devices in a distributed network.
Traffic Generator	Send data to a network. Traffic Generator lets you see what happens to your network under precisely controlled conditions. You can play back streams of captured data or you can transmit edited data. You can edit a stream of captured data by changing the sequence of the packets, deleting or adding (inserting) packets, creating bad packets, eliminating all packets of a certain type (protocol) and so on. Traffic Generator also gives you complete control of when, how fast, how long, and how often it transmits the data you want to send over the network.
Voice over IP (VoIP)	Decode H.323 or SCCP packets in an Ethernet environment and present the data in tables. Voice over IP data views display counters, call detail records showing QS statistics, addresses, and protocol conditions related to conversations and channels within the H.323 or Cisco SCCP protocol.

Hardware Devices

The full power of OPV-PE is realized through optional hardware analyzer cards available from Fluke Networks. Analyzer cards from Fluke Networks are installed in analyzer devices (DPI-1XX, GPI-1XX, and OPV-LA). The table below provides a brief summary of the Fluke Networks analyzer devices used by OPV-PE:

Table 1-3. Fluke Networks Analyzer Devices

Fluke Networks Device	Description
OPV-LA (OptiView Link Analyzer)	Analyzer device accessed remotely by OPV-PE. OPV-LA contains two synchronized IMM modules for analysis of full-duplex 10, 100, or Gigabit Ethernet traffic at full-line rate.
GPI-1XX	Analyzer device accessed remotely by OPV-PE. GPI-1XX contains two synchronized GMM modules for analysis of full-duplex Gigabit Ethernet traffic at full-line rate.
DPI-1XX	Analyzer device accessed remotely by OPV-PE. DPI-1XX 10/100 contains two synchronized PMM modules for analysis of full-duplex 10/100 Ethernet traffic at full-line rate.
IMM (Integrated Media Module)	Hardware card in OPV-LA for analyzing 10/100 Ethernet or Gigabit Ethernet networks.
GMM (Gigabit Media Module)	Hardware card in GPI-1XX for analyzing Gigabit Ethernet networks.
PMM (Protocol Media Module)	Hardware card in DPI-1XX for analyzing 10/100 Ethernet networks.

Protocols Supported

Table 1-4 and Table 1-5 on the following pages list the network and application protocols that OPV-PE can encode/decode. For a listing of protocol specifications and information, refer to Appendix C.

Note that Fluke Networks continually adds to the list of protocols it can decode. If you do not see a protocol on this list that you need, visit the Fluke Networks web site, www.fluke.com, or check with Customer Support for new additions.

Table 1-4. Protocols Supported in OPV-PE

MAC Layer	TCP/IP Suite	TCP/IP Suite (Cont.)	TCP/IP Suite (Cont.)
IEEE 802.2 (LLC)	ARP	IGMP	RPC
IEEE 802.3	BGP (Version 4)	IMAP	RTSP
Ethernet II	BOOTP	IMSP IP	SGCP
IEEE 802.5	CharGen	iSCSI	SLP
Loopback	DHCP	LDAP	SMTP
MAC Control Frame	Discard	MIME	SNMP (v1, v2, v3)
IEEE SNAP	DNS	Mobil_IP (A11)	TCP
IEEE 802.1X	Echo	MOUNT	TELNET
	EGP	NetBIOS	TFTP
PPP Suite	Finger	NFS	TPKT
PPPCHAP	FTP	NIS	UDP
PPPIPCP	GGP	NNTP	UNIX Remote Svcs
PPPIPX	Gopher	NTP	(lpr, rcp, rexec, login, rsh)
PPPLCP	HTTP	OSPF	VRRP
PPPNBFCP	HTTPS	PH	WebNFS
PPP over Ethernet	ICMP	POP3	WhoIs
	Ident	PORT MAPPER	XDR
Cisco Suite	iFCP	RARP	XDMCP
CDP	**IPX/SPX Suite**	RIP (Version 2)	Xwindows
DISL	Diagnostic	**IP Multicast**	
EIGRP	Error	DVMRP	**XNS**
HSRP	IPX	MOSPF	Echo Protocol
IGRP	IPX BCAST	PIM-DM	Error Protocol
ISL	IPX EIGRP	PIM-SM	IDP
RUDP	IPX Ping	RSVP	NetBOIS over SSP
SSP, SCCP	IPX RIP, IPX WAN		PEP
VTP	NBCAST		RIP
	NCP		SSP
	NDS		

Oracle Suite	IPX/SPX Suite (cont.)	LOA	Banyan Vines Suite
TNS (TCP/IP only)	NetBOIS	LOA	VARP
SQLNET	NLSP		VICP
AppleTalk Phase2	Packet Burst		VIP
AARP	SAP		VIPC
ADSP	Serialization	**Sybase Suite**	VRPC
AEP	SPX	TDS (TCP/IP only)	VRTP
AFP	SPX II		VSPP
ASP	Watchdog	**Fujitsu Suite**	
ATP	**DECnet Phase IV**	FNA	
AURP	CTERM	LNDFC	**SNA Protocol Suite**
DDP	DAP		3270
DDP EIGRP	DRP	**Applications**	FDC
LAP	FOUND	cc:Mail	FID2
NBP	LAT	Lotus Notes	FM
PAP	LAVC	Fluke Networks RSP	NC
RTMP	MOP	XWIN	XID
ZIP	NICE		SC
	NSP		
IPV6	**IpSec**	**VPN**	**Bridge Protocols**
DHCPng	AH	L2TP	BDPU
ICMPng	ESP	LDP	IEEE 802.1D
IDRPng	ISAKMP	PPPOEDS	IEEE 802.1Q VLAN
IPng	KERBEROS	PPPOESS	GARP (802.1p)
OSPFng	RADIUS		GMRP
RIPng	SOCKS	**Microsoft**	GVRP
RSVPng	SSH	NMPI	
	TACACS	SMB	
	TLS	SMB+ (CIFS)	
		WebNFS	

IBM	ISO	Intel	MPLS
NetBEUI	CLNP	MGCP	CR-LDP
NetBIOS	CONP	MTP2	RSVP-TE
	ESIS	MTP3	
	ISIS	RTSP	
	ISO	SCCP	
		SIP	
		TCAP	

Table 1-5. Supported Multi-Media Protocols

Multi-Media			
ITU H.323	**IETF**	**Cisco**	**Codec**
ASN.1	H.248 / Megaco	RUDP	CellB
GK DISC	MGCP	SCCP	G.711
H.225.0	RTCP	SSP	G.721
H.245	RTP		G.722
H.323v4	RTSP		G.723
H.450.1	SGCP		G.728
Q.921	SIP		G.729
Q.931			H.261
RAS			H.263
T.120			JPEG
T.38			MPEG (v1, v2)
			PCMU
			PCMA

What's New in Release 4.1

A synopsis of what's new in OPV-PE 4.1 is provided below.

Major VoIP Enhancements for Voice over IP

The graphical user interface has been improved. Calls are initially broken out by call metrics such as call jitter, call setup time, and dropped packets. Getting call details and sorting calls is easier. A direct interface is provided to set up and apply VoIP alarms. Utilization graphs are now available in monitor mode. Configuration is available from a single tab in the interface.

The SIP protocol is now supported. See New and Enhanced Protocol Decodes below for a complete list of all new protocols supported.

Call analysis for SCCP and H.323 have been improved. This includes gatekeeper awareness for the H.323 protocol.

Monitoring alarms are now supported. Note that VoIP monitoring alarms do not work with remote DPI-1XX analyzers, remote analyzer cards or NDIS cards running in systems with Protocol Inspector 3.2 or lower, or GMM analyzer cards.

Expert System Enhancements

The graphical user interface has been improved. The interface supports more views that are easier to access.

New symptoms have been added, including symptoms for HTTP server conditions, NCP server conditions, TNS server conditions, and transmission error rates.

Network analyses have been added to more clearly indicate severe network problems.

Expert symptoms are now available for VoIP protocols.

In monitor mode, the expert system does not work with remote DPI-1XX analyzers, GMM analyzer cards, or remote analyzer cards or NDIS cards running in systems with Protocol Inspector 3.2 or lower. Expert features will work on captures obtained from these devices.

Filter Enhancements

Filtering can now be done at the bit-level. A button on the Filter Design window allows you to enter bit values to filter on for any single byte in the filter.

Display filters now support up to 28 filters.

Alarm Action Enhancements

Additional actions are now possible when alarms are triggered. You can set the alarm to execute a command or send an SNMP trap to management stations.

Aliases Supported for Devices

You can now create/display a name for devices that appear in the resource browser. User-assigned names are created with a right-mouse click. Names are displayed by passing the mouse over the resource.

SNMP Support

OPV-PE now supports SNMP.

NTP Support

NTP support provides an OPV-LA with the ability to perform clock synchronization based on a dialogue with a network server. The frequency of updates can be controlled. If a network server is present, attached copies of OPV-PE will also synchronize via the OPV-LA.

Data Security for Packet Data Viewed During Analysis

A version of OPV-PE is available that shows only relevant decode fields during monitor/capture. Data fields are not visible. This option is not configurable. Contact Fluke Networks if you are interested in this secure version of OPV-PE.

New and Enhanced Protocol Decodes

The following protocol decodes are new or enhanced in version 4.1 of OPV-PE:

- iSCSI
- H.450.1
- Codecs: JPEG, MPEG
- MPLS: CR-LDP, RSVP-TE
- H.261, H.263
- ISIS
- CellB
- SIP

Performance Improvements

Performance improvements have been made to OPV-PE's monitoring capabilities. Fewer dropped packets result in better monitoring results.

Name Change

Protocol Inspector has been renamed OptiView Protocol Expert. In addition, the Distributed Protocol Inspector (DPI-212) has been renamed OptiView Link Analyzer. The following chart describes the change in model names and products.

Table 1-6. New Models/Products in Release 4.1

Old Models/Products	Replaced by New Models/Products
PIP-040 Protocol Inspector with Expert Option	OPV-PE/PRO OptiView Protocol Expert
PIP-100 Protocol Inspector with Remote Control, Traffic Generation and Expert options	OPV-PE/PLUS OptiView Protocol Expert Plus
PI-010 Remote Control Option and PI-020 Traffic Generation Option together	OPV-PE/EP Enhancement package that adds Remote Control and Traffic Generation options to OPV-PE/PRO
DPI-212 Distributed Protocol Inspector, 10/100/1000Mbps	OPV-LA OptiView Link Analyzer

Existing members of the Gold Support Program for Protocol Inspector software will receive the upgrade to OptiView Protocol Expert with the proper Installation Key(s) to turn on the appropriate functions. New Gold Support Program products for OptiView Protocol Expert are available to Protocol Inspector customers during program renewal.

Chapter 2
Installation

System Requirements

The system requirements for installing and running the OPV-PE software are shown in the table below.

Table 2-1. System Requirements

CPU	Pentium @ 233Mhz or greater recommended
Operating System Software	Windows 95C, Windows 98, Windows 98 Version 2, Windows 2000, or Windows NT 4.0 with Service Packs 3, 4, 5, and 6, and administrative privileges.
System Memory for Opening Capture Files	Capture Buffer Size, Local or Remote / Pentium Processor / RAM / Virtual Memory (see below)
Video Display	800x600 or higher resolution, 16-bit color
CDROM	CDROM drive is required to install OPV-PE software.
Disk Space	24MB of free disk space.
Network Adapters	NDIS-compatible Ethernet adapter or NDIS-compatible 4/16 Token Ring adapter card. • 10/100 Ethernet Adapters require an NDIS enhanced 16/32 bit driver and must be in promiscuous mode. • 4/16 Token Ring Adapters require an NDIS enhanced 16/32 bit driver. Adapters accessible through NDIS drivers must be compatible with the NIC 2.0 standard. Not all Token Ring adapters are supported.

System Memory for Opening Capture Files detail:

Capture Buffer Size, Local or Remote	Pentium Processor	RAM	Virtual Memory
16MB	PI	64MB	64MB
32MB	PII	128MB	500MB
64MB	PIII	256MB	600MB
128MB	PIII	512MB	700MB
256MB	PIII	1000MB	1000MB

See the Readme file for the latest system requirements for OPV-PE 4.1.

Upgrading OPV-PE

If you have Protocol Inspector, un-install the software before installing OPV-PE.

The format and name of the .ini file has changed. The file is now called OPV-PE.ini under the Windows directory. If you have customized the Protocol Inspector.ini file, you will be required to re-enter your changes to the OPV-PE.ini file once the software is installed. Other user-generated files such as filters (.cfd), capture files (.cap), and transmit specifications (.tsp) can be saved when you install OPV-PE in the same directory as the previous version.

OPV-PE 4.x has different table formats from Protocol Inspector. It is required that you upgrade all PCs and remote analyzer devices to the latest software version. Although remote communications with Protocol Inspector version 3.2 will work, you may see data that is out of order or missing in OPV-PE tables.

Installing OPV-PE

Begin by installing any local hardware analyzer cards and/or adapter cards.

Perform the following steps to install the OPV-PE software:

1. Insert the OPV-PE CD-ROM into your CD-ROM drive.

2. The Master Install program will start and display your install choices. Make your selection and follow the on-screen instructions.

If the program does not Autorun.

1. Click the "Start" button on the "Task Bar" and select "Run". Then type **d:/setup** (or replace 'd' with the letter of your CD-ROM drive) and click **OK**.

2. Make your selection and follow the on-screen instructions. Enter your software license key when prompted.

To use OPV-PE to access remote resources, make sure the OPV-PE software is installed at the remote host and the remote resources are connected to the network.

Chapter 3
Getting Started

The OPV-PE System

A complete OPV-PE system consists of OPV-PE software, an NDIS-compatible Ethernet adapter, and remote analyzer devices.

With Remote Control software option, you have access to other PCs containing NDIS adapters or other devices such as a DPI-1XX, an OPV-LA, or Multi-Port Tap. All remote devices must be properly installed before they can be accessed by Remote Control software.

Launching OPV-PE

Perform the following steps to set up your environment and launch the OPV-PE software:

1. Launch the OPV-PE program.
    Double-click on the OptiView Protocol Expert icon in the OptiView Protocol Expert group or other group where you installed the OPV-PE application.

2. With Remote Control software option installed, you are asked for an account name and password in the **Login** dialog box.

    OPV-PE provides two default accounts, **guest** and **su**. Table 3-1 shows the password and privileges associated with these accounts. Choose an account, complete the dialog box, and click **OK**.

Table 3-1. Default Account Names, Passwords and Privileges

Default Account Name	Password	Privileges
guest	public	full
su	manager	super-user

Normally, you can use either account to access all remote resources. If a remote resource will not permit access with either of these accounts, then get the user name and password from the resource owner and establish an account on that resource. To access a remote resource, you must have an account and password set up on the remote system containing the resource or use the remote system's guest account.

You can also password-protect local resources. See the section called "Protecting Local Resources" in the "Resources and Modes" chapter.

3. OPV-PE starts (arms) your local devices automatically the first time you start the software. For subsequent launches of OPV-PE or to start a remote resource, you must select a PMM, GMM, IMM, or Ethernet adapter to start monitor, capture, or transmit functions.

    From the Resource Browser, click on the button that corresponds to the PMM, GMM, or Ethernet adapter that you want to control with the OPV-PE software. The resource can be local or remote. A monitor window appears for the PMM, GMM, IMM, or Ethernet adapter you select.

4. IMM analyzer cards have two interfaces, RJ45 for 10/100 copper wire and a G-BIC for 1000 Mbps fiber optic. If you selected a IMM, you may need to change the interface. From the **Module** menu, choose **Interface**. **On Board RJ45** selects the bidirectional 10/100BASE-T port. The default is the **G-BIC** which selects the G-BIC send/receive port pair.

5. PMMs have two ports. If you selected a PMM, you may need to change the port. From the **Module** menu, choose **Interface** to set the port. **On Board RJ45** selects the 10/100BASE-T port.

    The MII port requires a 3rd party transceiver to connect to other Ethernet media types such as fiber, coaxial, and twisted-pair cable.

6. If you selected a PMM or IMM, you may need to set the Interface Mode. From the **Module** menu, choose **Interface Mode**.

Auto Negotiate places the resource in auto-detection (10Mbps or 100Mbps) mode. The interface mode can also force the module to only one speed. For PMMs, the mode can also be set to Full Duplex.

7. If you selected a GMM, you may need to force the link. **You must force the link if you are connected to GMM(s) through a tap device.** From the **Module** menu, choose **Link → Force Link**. For more information on forcing links, See "Establishing Links for GPI-1XX GMM and OPV-LA IMM" on page 19 of this chapter.

8. If you selected a IMM for Gigabit Ethernet, you may need to disable auto negotiation if you cannot establish a link. From the **Module** menu, choose **Fiber Link** and select the **No Auto-Negotiation** menu item. For more information on auto negotiation, See "Establishing Links for GPI-1XX GMM and OPV-LA IMM" on page 19 of this chapter.

Basic Navigation Tips

There are three main windows in OPV-PE:

• OPV-PE Main Window (Summary View)

• Detail View Window

• Capture View Window

Summary View is used primarily for monitoring, as it shows a single view of many different resources. It also contains the docking windows for selecting resources (Resource Browser), setting alarms (Alarm Browser), and viewing system messages (Message window).

Refer to the *OPV-PE Quick Start Guide* for pictures of the main windows used in OPV-PE.

Detail View is primarily for analyzing data from a single resource. You can look at the data from Detail View in many different ways.

To display a resource in Detail View, click on (highlight) the resource icon in the Resource Browser. Press the ▦ button to display Detail View for the resource.

Once you have data to analyze, stop the module and press ▦ from Detail View to bring up Capture View. Capture View provides full decode of data in a capture buffer. Capture View opens as a window within Detail View. Capture View has its own toolbar so you can view captured data in many different ways.

You can also access Capture View from Summary View to view a Capture file. From Summary View, click the ▣ button in the OPV-PE toolbar. The contents of the Capture file are displayed in the **Capture View** window.

You'll notice that many of the same functions can be performed from the different windows. This design allows you to perform all the tasks you might expect to do from any one of the major windows without having to switch to a different window.

Because of OPV-PE's flexibility, you can open many different windows and subwindows within the program. To avoid confusion, close windows you are not using.

Be sure to browse the Hints and Tips sections in the on-line Help system. There is a "Hints and Tips" section for each major functional area within the product. Over time, you'll find the ways that you like to use the product. We encourage you to contact us and let us know so we can include these tips in the help system and pass these tips on to other customers and to user groups.

Here are some tips to help you use the OPV-PE interface:

- Click on a resource in the Resource Browser to select that resource.

- Press the ▦ button to bring up Detail View for a resource. You can also bring up Detail View by double-clicking with the left mouse button on the active monitor view displayed within Summary View.

- Press the ▦ button from Detail View to bring up the **Capture Filter** window. Use this window to create/edit capture filters.

- Press the ▦ button from Detail View to bring up the **Display Filter** window. Use this window to create/edit display filters.

- Once a resource is stopped and you have captured data, press the ▦ button in Detail View to bring up Capture View for analyzing packets and full protocol decode.

- Press the ▦ button from Summary View to open a previously saved capture file and bring up Capture View.

- Use the buttons in the Data Views toolbar to open many views of the same resource within Detail View. Note: Due to the speed of the network, data views are limited when OPV-PE monitors Gigabit Ethernet traffic through a GMM.

- Double-click on device in the Reousrce Browser to set an alarm for the device.

- If you are running Traffic Generator, use the ▦ in Detail View to bring up the **Transmit Specification** dialog box to create data streams for transmit.

Buttons and Toolbars

OPV-PE Toolbar

Open button
Opens a file, typically a capture file (.CAP). A dialog box displays showing all files with extension .CAP in the current directory. From the Summary Viewer, selecting a capture file to open will bring up Capture View.

Save button
Saves the current contents of the capture buffer to a file. A dialog box displays to select the file name and directory.

Print button
Prints the contents of the current view.

Name Table button
Brings up the **Name Table** dialog box for editing the current name table, saving a name table to a file, or loading a name table from a file.

Help button
Displays the help contents.

Module Toolbar (Summary View)

Start button
Starts a module. The module captures or transmits packets, depending on whether the mode is set to transmit or capture.

Stop button
Stops a module. The module ceases to capture packets or transmit packets.

Capture Mode button
Places the currently selected resource in capture mode. This button is gray if the resource is currently active (started).

Monitor Mode button
Activates the monitor functions for the currently selected resource. If the resource does not support monitoring functions, the resource is put into capture mode. This button is gray if the resource is currently active (started).

Transmit Mode button
Places the currently selected resource in transmit mode.
(Traffic Generator only)

Detail View button
Brings up Detail View for the currently active resource.

Load Filter button
Brings up a dialog box to select a capture filter (`.CFD` extension). If a capture filter is opened, that filter is applied to the currently selected resource. This button is gray if the resource is currently active (started).

Unload Filter button
If a filter is loaded for the currently selected module, the filter is disabled. This button has no function if the currently selected resource is in transmit or monitor only mode. This button is gray if the resource is currently active (started).

Transmit button
Brings up a dialog box to select a transmit specification (`.TSP` extension) or a capture file (`.CAP` extension) for transmit. This button has no function if the currently selected resource is in capture or monitor mode. This button is gray if the resource is currently active (started). (Traffic Generator only)

Detail View Toolbar

	Save button Saves the current contents of the capture buffer to a file. A dialog box displays, allowing you to select the file name and directory.
	Print button Prints the contents of the current view.
	Start button Starts a module. The module captures or transmits packets, depending on the whether the mode is set to transmit or capture.
	Stop button Stops a module. The module ceases to capture packets or transmit packets.
	Capture Mode button Places the currently selected resource in capture mode. This button is gray if the resource is currently active (started).
	Monitor Mode button Activates the monitor functions for the currently selected resource. If the resource does not support monitoring functions, the resource is put into capture mode. This button is gray if the resource is currently active (started).
	Transmit Mode button Places the currently selected resource in transmit mode. This button is gray if the resource is currently active (started).
	Capture View button Selects Capture View mode for viewing captured information. You can see protocol decodes in this view. Capture View has its own toolbar to allow you to select other view of captured information.
	Capture Filter button Display the **Capture Filter** window. The window displays a previously opened filter or the default filter.

LOAD F — Load Filter button

Brings up a dialog box to select a capture filter (`.CFD` extension). If a capture filter is opened, that filter is applied to the currently selected resource. This button is gray if the resource is currently active (started).

Unload Filter button

If a filter is loaded for the currently selected module, the filter is disabled. This button has no function if the currently selected resource is in transmit or monitor only mode. This button is gray if the resource is currently active (started).

Display Filter button

Display the **Display Filter** window. The window displays a previously opened filter or the default filter.

Unload Display Filter button

Unloads the current display filter. All frames in the current capture will display.

Transmit Specification button

Brings up the **Transmit Specification** dialog box to define/load a transmit specification. (Traffic Generator only)

Transmit from Buffer button

Brings up a the dialog box to select a capture file and then load the capture file to the module for transmission. (Traffic Generator only)

Name Table button

Brings up the **Name Table** dialog box for editing the current name table or saving/loading a name table to/from a file.

Alarm List and Log button

Brings up a table showing all alarm groups assigned to this resource. It lists alarm groups by name and identifies the type of alarm group.

Help button

Displays the help contents. Prints the contents of the current view.

Data Views Toolbar

The data views toolbar will have a subset of the options below when using a GMM card. See the next toolbar description for a description of GMM options.
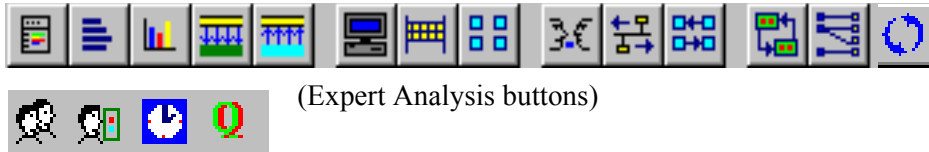
 (Expert Analysis buttons)

Ring Statistics View button (Token Ring Only)
Brings up tables showing information about the rings and the ring stations detected on the network. This button is available for Token Ring adapters only.

MAC Statistics View button
Brings up MAC Statistics View for graphically viewing packet and error counters. This view also contains module and capture buffer status information. The view displays appropriate error counters depending on the mode, capture or transmit.

Frame Size Distribution View button
Selects Frame Size Distribution View for viewing the distribution of frame sizes.

Protocol Distribution View button
Selects Protocol Distribution View for viewing a chart of the distribution of major protocols. Control buttons in this view allow you to customize the way you view the protocol distribution.

Utilization/Error View button (Rx)
Brings up a strip chart that plots utilization and number of errors over time. The table for this view contains packet counters and error counters for receive.

Utilization/Error View button (Tx)
Brings up a strip chart that plots utilization and number of errors over time. The table for this view contains packet counters and error counters for transmit. (Traffic Generator only)

Host Table View button
Selects Host Table View for viewing information. You can see MAC stations and their associated traffic in this view.

Network Layer Host Table View button
Selects Network Layer Host Table View for viewing information. You can see network (IP/IPX) stations and their associated traffic in this view.

Application Layer Host Table View button
Selects Application Layer Host Table View for viewing information. You can see application stations and their associated traffic in this view.

Host Matrix View button
Selects Host Matrix View for viewing information. You can see all conversations between MAC stations in this view.

Network Layer Matrix View button
Selects Network Layer Matrix View for viewing information. You can see all network layer conversations and their associated traffic in this view.

Application Layer Matrix View button
Selects Application Layer Matrix View for viewing information. You can see all application conversations and their associated traffic in this view.

VLAN View button
Brings up VLAN view for viewing network traffic on virtual LANs. Cisco's ISL protocol is the only VLAN currently recognized.

Address Mapping View button
Brings up Address Mapping View for viewing associations between MAC station names and addresses and network station names and addresses.

Refresh button
Update the information in all open views.

Duplicate Address Button
Brings up a table showing all duplicate IP and IPX addresses. The duplicate network and MAC addresses associated each duplicate are displayed.

Expert View Button
Brings up a table showing counts of all expert symptoms detected. All expert views can be accessed after pressing this button.

Application Response Time Button
Brings up a table showing the applications detected and their minimum, maximum, and average response times. The number of connections for each application is also displayed.

VoIP (VoIP software option only)
Brings up a table showing all VoIP calls. Multiple tables and views are available within the VoIP interface.

Data View Toolbar (Gigabit Ethernet Traffic Analysis)

OPV-PE does not support real-time views (which include Expert views) of Gigabit Ethernet traffic. While monitoring Gigabit Ethernet traffic, monitored using GPI-11X, OPV-PE provides the following buttons in the Data View toolbar.

(Gigabit Ethernet traffic analysis buttons)

MAC Statistics View button
Brings up MAC Statistics View for graphically viewing packet and error counters. This view also contains module and capture buffer status information. The view displays appropriate error counters depending on the mode, capture or transmit.

Frame Size Distribution View button
Selects Frame Size Distribution View for viewing the distribution of frame sizes.

Utilization/Error View button (Rx)
Brings up a strip chart that plots utilization and number of errors over time. The table for this view contains packet counters and error counters for receive.

Utilization/Error View button (Tx)
Brings up a strip chart that plots utilization and number of errors over time. The table for this view contains packet counters and error counters for transmit. (Traffic Generator only)

Refresh button
Update the information in all open views.

Filter Design Toolbar

Create Filter button
Creates a new filter. The default window appears for the **Filter Design** window.

Open Filter button
Opens a filter. A dialog box displays to select the file. Capture filters are designated with an extension of .CFD files and display filters with an extension of .DFD.

Save Filter button
Saves the current contents of the filter to a file. A dialog box displays to specify the file name and directory. Capture filters are saved as .CFD files and display filters as .DFD files.

Load Filter button
Load the current filter to the currently active module.

Disable Filter button
Disable the current filter. Subsequent starting of the module will capture all packets (use default filter).

Filter Window Toggle button
Brings up the **Filter States Design** window. The **Filter States Design** window is used to create advanced filters with multi-state logic.

Help button
Displays a help topic on filters.

Filter States Design Toolbar

Create Filter button
Creates a new filter. The default filter appears in the **Filter States Design** window.

Open Filter button
Opens a filter. A dialog box displays to select the file. Capture filters are designated with an extension of `.CFD` files and display filters with an extension of `.DFD`.

Save Filter button
Saves the current contents of the **State** window to a file. A dialog box displays to specify the file name and directory. Capture filters are saved as `.CFD` files and display filters as `.DFD` files.

Load Filter button
Load the contents of the **Filter States Design** window to the currently active module (capture) or apply the filter to current active display (display filter).

Disable Filter button
Disable the current capture filter. Subsequent starting of the module will capture all packets (use default filter).

Filter Window Toggle button
Brings up the **Filter Design** window for the current statement. The **Filter Design** window is used to edit the statement.

Cut button
Cut the selected State or `ELSE IF` statement. The button does not work if other types of statements are selected.

Add button
Adds a new level if an `ELSE` statement or `ROOT` statement is selected. Adds a new `ELSE IF` statement if a State or an `IF` statement is selected.

Show/Hide Detail button
Shows or hides the details of the current filter. Details are the number of filters used per state and the types of frames being captured for each `IF` or `ELSE IF` statement.

Print button
Prints the current contents of the **Filter States Design** window.

Help button
Displays a help topic on filters

Capture View Toolbar
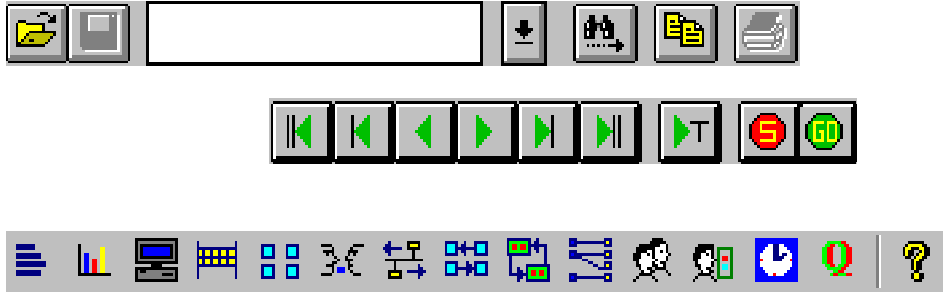
Open File button
Opens a capture file (.CAP). A dialog box will display showing the current directory with all files with extension .CAP.

Save File button
Saves the current contents of this view to a file.
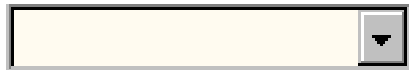
Search Box
Use the box to specify an ASCII text string for which to search. Once the string is entered, press the search button to the right of the search box.

Search button
Start search of the capture file contents for an ASCII text string. Specify the string in the search box to the left. The first instance of the string is found starting from the current position in the capture file.

Copy button
Copies the current contents of the **Summary** pane for pasting into other documents. A window displays with the text converted to ASCII format. Use the window to select the text you want and copy it to the clip board.

Print button
Print the currently selected line in the **Summary** pane.

Stop Load button
Capture files are loaded to Capture View as a background process.

Pressing this button stops the background process. Press the Resume Load button to the right to resume the process.

Resume Load button
Capture files are loaded to Capture View as a background process. Pressing this button resumes the background process.

Go To Trigger button
Pressing this button moves you to the line in the capture file that was set as the trigger position. If no trigger position is set, this button moves you to the first captured frame.

Navigation buttons
Navigation buttons move you through the capture file. There are keys to go to the beginning and the end of the file, page up, page down, previous line, and next line.

Other buttons for views are the same as those in the **Data Views** toolbar.

Frame Size Distribution View button
Selects Frame Size Distribution View for viewing the distribution of frame sizes.

Protocol Distribution View button
Selects Protocol Distribution View for viewing a chart of the distribution of major protocols. Control buttons in this view allow you to customize the way you view the protocol distribution.

Host Table View button
Selects Host Table View for viewing captured information. You can see MAC stations and their traffic in this view.

Network Layer Host Table View button
Selects Network Layer Host Table View for viewing captured information. You can see network (IP/IPX) stations sorted according to the traffic variable you select in this view.

Application Layer Host Table View button
Selects Application Layer Table Host View for viewing captured information. You can see application stations sorted according to their names in this view.

Host Matrix View button
Selects Host Matrix View for viewing captured information. You can see all conversations between MAC stations in this view.

Network Layer Matrix View button
Selects Network Layer Matrix View for viewing captured information. You can see all network conversations for IP and IPX traffic in this view.

Application Layer Matrix View button
Selects Application Layer Matrix View for viewing captured information. You can see all application conversations in this view.

VLAN View button
Brings up VLAN view for viewing network traffic on virtual LANs. Cisco's ISL protocol is the only VLAN recognized.

Address Mapping View button
Brings up Address Mapping View for viewing associations between MAC station names and addresses and network station names and addresses.

Duplicate Address Button
Brings up a table showing all duplicate IP and IPX addresses. The duplicate network and MAC addresses associated each duplicate are displayed.

Expert View Button
Brings up a table showing counts of all expert symptoms detected. All expert views can be accessed after pressing this button..

Application Response Time Button
Brings up a table showing the applications detected and their minimum, maximum, and average response times. The number of connections for each application is also displayed.

 VoIP (Voip software option only)

Brings up a table showing all VoIP calls. Multiple tables and views are available within the VoIP interface.

File Formats

The following file formats are supported in OPV-PE:

.CAP Extension – Capture Files

Capture files contain packets collected from the network. Capture file format is compliant with RFC 1761, referred to as "Snoop" format. However, capture files include extensions that expand the information provided by snoop format.

.NAM Extension – Name Table Files

Name table files contain equivalencies between symbolic names and hexadecimal names. The name table file format is identical to .ini file format. The default hosts.nam file contains names associated with well-known hexadecimal representations. For example, BROADCAST=C000FFFFFFFF.

.CFD Extension – Capture Filters

Capture filter files contain a set of instructions internal to OPV-PE that tells the software to save only a subset of the all the information on the network.

.DFD Extension – Display Filters

Display filters files contain a set of instructions internal to OPV-PE that tells the software to display only a subset of previously captured data. View filters are essentially the same as capture filters, except that they use capture files (.CAP files) as input rather than data being captured from the network.

.TSP Extension – Transmit Specifications

Transmit specifications contain a set of instructions internal to OPV-PE that will generate packets. You can create transmit specifications and generate traffic if you have the Traffic Generator software.

Providing a Name Table to OPV-PE

A default name table file, `hosts.nam`, is included with the software. OPV-PE boots using this default name table. If you wish to change the start up default name table, you must edit the `OPV-PE.ini` file by following these instructions:

1. Locate the `OPV-PE.ini` file in your Windows directory.

2. Open the `OPV-PE.ini` file with your text editor software.

3. Search for this variable, `NameTable=<install-dir>\hosts.nam`.

4. Delete the `hosts.nam` text on that line.

5. Replace text with your default name table file. It should have the `.nam` extension.

6. Save the `OPV-PE.ini` file, exit your editor and start OPV-PE application.

Address and symbolic name associations can be discovered by OPV-PE. This table can be saved as a file with the `.nam` extension and used as the default name table. Refer to Chapter 12 for more information on the name table.

Note

The default name table can always be changed to another within the software. Click on the Name Table button and select **Open**. *Find the name table file you want and click* **OK**.

Establishing Links for GPI-1XX GMM and OPV-LA IMM

Forcing the link is required when the GMM is passively monitoring a 1000 Mbps link, such as when monitoring/analyzing a connection through a tap device. Since the card is not using the transmit port in this configuration, the device has no means of auto-negotiating a connection. The **Fiber Link** → **Force Link** option from the **Module** menu allows you to alert the module that it has a connection and begin listening for data.

The IMM is often connected to a device that cannot auto negotiate the connection, such as when monitoring/analyzing a connection through a tap device. The device will automatically go through a sequence of attempts to disable auto negotiation and establish a link with a device that cannot auto negotiate. However, if a link cannot be automatically established with a device, you can attempt to establish a link by manually disabling auto negotiation mode. The **Fiber Link** option from the **Module** menu allows you to disable auto negotiation and alert the module to begin listening for data. Make sure the No Auto Negotiation item is selected from the menu. Auto negotiation enabled is the default value.

The **Module** menu also has a **Fiber Link** → **Link Status** option which provides information about a 1000 Mbps link. If the carrier wave is present, this option returns a "link OK" message. If there is a problem with the link, a message screen appears with diagnostic information that may help you troubleshoot the link.

The "link OK" message is returned if the device can sense the carrier wave on its receive port. However, if a IMM or GMM has a proper physical connection to a device that cannot auto negotiate the connection, this option will report that the link is OK even though the devices do not recognize each other. The **Link Status** option is of limited use when connecting to devices such as taps where the problem is an auto negotiation failure.

Chapter 4
Configuring OPV-PE

Configuring the Interface

In OPV-PE, you can control the appearance of windows, the primary monitor view, the appearance of tables and charts, and the colors of decode displays. The following sections describe how to set up the interface to best meet your needs.

Customizing Views and Windows

The OPV-PE graphical user interface is extremely flexible. It takes advantage of the features of Windows to allow you to customize your interface.

Multiple windows can be opened within both Summary View and Detail View. These sub-windows can be minimized, maximized, expanded, reduced, and tiled within the area of the Summary or Detail View. You can open as many windows as you have resources in Summary View. You can have all available views of a single resource in Detail View. You can have one view per resource open within Summary View.

Docking Windows

Summary View opens when OPV-PE is started. The **Summary View** window is composed of Summary View area and three docking windows. The docking windows are:

- Alarm Browser

- Resource Browser

- Message View

You can size the docking windows by moving (click the left mouse and hold) the borders separating the windows. You can move the borders all the way to the edge of the **Summary View** window, thus hiding the docking windows.

You can also completely close a docking window. If you close a docking window, use the options from the **View** menu to get the window back.

You can extract any docking window from the **Summary View** window and make it a stand-alone window. If you turn off docking using the right mouse functions, the window will not dock again when it is moved back over the **Summary View** window, allowing you to cascade windows. You can also "float" a docking window within the main window. In effect, you can create your own customized view of all the windows available within the **Summary View** window.

Docking windows are a standard Windows feature. Refer to the Windows documentation for a complete description of docking windows. It is suggested that you do not undock windows.

Capture View Display Options

When using Capture View, you can control the display of data for packet decoding. You can view the time as absolute, as a delta, as elapsed, or any combination of the three. You can show/hide most fields in the decode display. You can also show/hide protocol information about packets and set the starting point for elapsed time

Use the top part of the dialog box to select the columns you want to display in Capture View. Not all columns can display on the screen without having to scroll; limiting the number of columns can make it easier to see the exact information you want. Specific display fields include Absolute Time, Delta Time, Elapsed Time, Frame Size, Status, Network Address, Cumulative Byte Count and Throughput. See Table 4-1 for a description of these fields.

Table 4-1. Configurable Capture View Columns

Capture View Column	Description
Abs Time	The absolute time of arrival for each packet taken from the system clock when the capture was performed. format: hh:mm:ss.mmm.uuu.nnn where ss=seconds, mmm=milliseconds, uuu=microseconds, nnn=nanoseconds
Delta Time	The time between each packet (interpacket gap). format: s.mmm.uuu.nnn where s=seconds, mmm=milliseconds, uuu=microseconds, nnn=nanoseconds
Elapsed Time	The time stamp of each packet measured from a relative starting point. The starting point may be either the module arm time or the arrival time of a specific packet. See below for information on setting the elapsed time starting point.
Size	The frame size of the packet in bytes.
Status	The Status field indicates if the frame has errors. For good frames, the Status field is blank.
Display Network Address	The destination and source IP address.
Cumulative Byte/ Throughput	The Cumulative Byte Count is a sum of all bytes received to this point in time in a capture file. The Throughput is calculated by dividing the cumulative bytes by the elapsed time. The elapsed time is the difference is always measured between the module arm time and the time stamp of the current packet in the capture file.

Use the middle portion of the dialog box to set up the display of the **Summary** column. The **Summary** column will always display. However, this field can just give a very limited synopsis of protocol activity or provide complete details about the protocols used in the packet. Check the **Display Detail Protocol Summary** box to view detail about all the protocols used in the packet. Leaving the **Display Detail Protocol Summary** box unselected gives a synopsis of all protocols in the packet. If you want to display protocol summary details, set the protocols you want to display from the pull-down menu. For example, if you want to display only the Transport layer and below, select Transport Layer. If you are not displaying protocol summary details, the protocol layer you select in the pull-down menu will not affect the display of the **Summary**.

Select the **Display Expert Symptoms** check box if you wish to include expert symptom information in the **Summary** field. Packets that trigger an expert symptom and have expert symptom information will display in reverse video in Capture View.

Use the bottom portion of the dialog box to set the point from which OPV-PE will measure time when calculating and displaying the elapsed time stamp of each packet. Set "time-zero" for capture in the **Elapsed Time Set Mark Option** portion of the **Display Options** dialog box. The default option is Module Arm Time, which starts time zero at the time the module is started. Select **Frame ID nnn's Arrival Time** and set the frame ID number in the box to start time zero when a particular frame arrives. Setting this field only effects the display of the **Elapsed Time** field in the protocol decode.

Setting the Monitoring View for a Module

One monitoring view is available for each module in Summary View. The first tab in the Summary View for a module displays the view selected.

1. In Summary View, choose **Module** from the **Configuration** menu.

2. Choose **Monitor View Preferences**.

3. Click the radio button in the **Monitor View Preferences** tab for the view you want. Only one view is allowed.

4. Click the **OK** button.

Configuring Chart Views

Protocol distribution view and frame size distribution view can be customized using buttons within the chart. The type of information in some chart views can be customized using the procedures below.

Charts graph the "top ten" stations or conversations based on a byte count. The count is the absolute percentage of the number of bytes out for stations, or the absolute number of bytes passed between stations for conversations. The count therefore provides a view of the stations or conversations with the most traffic, which is what users typically want to view. You can, however, create a "top ten" chart for any field that OPV-PE supports. You can also reverse the sort order to create a "bottom ten" chart for any field that OPV-PE supports.

1. In Detail View, make sure the view you want to customize is the currently active window.

2. Choose **Table** from the tab at the bottom of the view.

3. The data view appears as a table. Click on the column you want to use to create a "top ten" list. Note that the information in the table sorts in descending order for the column you selected. If the column you want is not there, see "Customizing Table Views" for information on how to insert a column into the table.

4. Choose **Chart** from the tab at the bottom of the view to return to chart view.

Table Views

The type of information in some table views can be customized. You can add or subtract columns from the table.

1. In Detail View, make sure the view you want to customize is the currently active window. The Table view must be displayed.

2. Choose **View Options…** from the **Monitor Views** or **Capture Views** menu. If the **View Options…** selection is gray, no customization can be performed for this table.

3. Click the radio button for each column you want to display in the table.

4. Click the **OK** button.

View options are not available for all tables.

Protocol Color Coding

OPV-PE provides a real-time protocol decode called Packet Summary View and protocol decodes in Capture View. To use these displays more effectively, you may want to set the colors used for packet display. For example, you might want to display all transport layer packets in red and all others in black if you are looking only for protocol decode information in the transport layer.

To set up or change color coding for protocol decode, do the following:

1. Choose **System Settings…** from the **Configuration** menu. Select the **Protocol Color Coding** tab.

2. Click on a protocol layer.

3. Using the color buttons, set the foreground and background color display for the selected protocol.

4. Repeat as required for other protocol layers.

5. Make sure that the **Use Color Coding** box is checked.

6. Click the **OK** button.

Use the **Default All** button to return all color settings to their default values. Use the **Set Default** button to reset the default to the colors currently displayed.

Module Settings (Properties)

Module settings configure options for the capture, monitor, and transmit functions of devices. To configure modules, select **Module Settings...** from the **Configuration** menu. Tabs appear that apply to the currently active device type; a tab will only appear if this option can be set for the current device type. Hardware devices can have properties set according to Table 4-2 below:

Table 4-2. Hardware Device Properties

Hardware Device	Set Buffer Size	Packet Slice	Capture Buffer	Modes: Full Duplex	Modes: Expert Mode	Modes: Non-WKP	Modes: VoIP Only	MAC Control Frame
IMM	NO	YES	YES	YES*	YES	YES#	YES	YES
OPV-LA	NO	YES	NO	YES*	YES	NO	YES	YES
PMM	NO	YES	YES	YES*	YES	YES#	YES#	NO
DPI-1XX	NO	YES	NO	YES*	YES	NO	NO	NO
GMM	NO	YES	YES	YES*	YES+	NO	NO	YES
GPI-1XX	NO	YES	NO	YES*	YES+	NO	NO	YES
NDIS	YES	YES	YES	NO	YES	YES#	YES#	NO
Fast Ethernet Traffic Analyzer	See note below.							

*IMM, PMM, and GMM support full-duplex, but only PMM has a single-card configuration setting for full-duplex. See the section on full-duplex mode below for an explanation of using full-duplex with analyzer cards.

+Sets values for viewing captured data only. No real-time expert views are supported.

#This option affects the display of tables for local devices only for 10/100 networks.

The Fast Ethernet Traffic Analyzer probe does not have any module settings. The **Module** choice will be grayed out on the **Configuration** menu for Fast Ethernet Traffic Analyzer.

Module settings are described in the subsections below. Default values for Module Settings are shown in Table 4-3:

Table 4-3. Default Module Settings

Module Setting	Default Values
Buffer Size	512K
Packet Slicing Size, Capture	Full packet length
Packet Slicing Size, Monitor	Full packet length (for IMM, PMM), 128 bytes (for standard NDIS modules); no monitor for GMM
Enable Full Buffer Auto Save	Not selected
Modes: Expert Analysis Mode	Selected
Modes: Full Duplex Mode	Not selected (This puts a single PMM card in full-duplex mode)
Modes: Non-WKP Mode	Not selected
MAC Control Frame	Selected (IMM and GMM cards only)

Buffer Size

NDIS cards require that a capture buffer size be set. The buffer size is the amount of system memory that will be used to save captured data. Buffer sizes can be set between 64KB and 16MB.

IMM, PMM, and GMM modules have a hardware buffer and do not require system memory for captured data. The default buffer size is 512KB.

Packet Slice (Slicing Size)

All devices support packet slicing. Packet slicing means that a subset of the entire packet is saved in the capture buffer. You can save the first 32 bytes (Mac layer), the first 64 bytes (Network layer), the first 112 or 128 bytes (Application layer) or the full length of the packet.

Packet slicing can be set separately for monitor and capture except for IMM. For monitor, packet slicing can improve performance when monitoring the entire packet contents is not required. For capture, packet slicing can save space in the capture buffer for more packets when analysis of the entire contents of each packet is not required.

For IMM and PMM modules, the default is no packet slicing (full packet length). For IMM, the slicing size must be 64 bytes or greater and packet slicing of 128 bytes is not supported for 1Gbps Ethernet. For NDIS cards, the default setting is no packet slicing for capture, 128-byte packet slice for monitor. For NDIS modules,

you cannot have both monitor and capture set to full packet size. Packet slicing for monitor mode is not supported for GMM devices.

Capture Buffer

Only local devices support a stop-and-save-to-disk function for the capture buffer. Check the **Enable Full Buffer Auto Save** box to enable the save-to-disk feature. When using the save-to-disk feature, capture is stopped when the buffer is full and the contents are written to disk. Capture is restarted as soon as the data is written to the file. When the capture buffer fills again, the new contents are appended to the file. If you start a new capture, the file is overwritten. If capture is stopped before the capture buffer contents are full, the buffer contents are not automatically written to disk; you must manually save the capture buffer to disk.

Modes

Select the **Modes** tab from the **Configuration → Module → Settings...** to set the modes for a module. Modes cannot be set for GMM devices.

Full-Duplex Mode

⚠ Caution

The setting for full-duplex/half-duplex applies only to single PMM modules. Note that setting a single PMM module to full-duplex is not the way PMM modules are typically used with full-duplex traffic. A more typical configuration is to have two PMMs synchronized, each monitoring receive traffic in one direction of a full-duplex link. The configuration using two modules establishes a passive monitor/capture for full duplex traffic at full line rate. Using a single PMM in full-duplex is more commonly used in a testing environment to measure device performance.

PMMs can be enabled to function in full-duplex mode. If full-duplex is enabled, both the capture and the transmit mode buttons must be set at the same time. The capture buffer memory within the PMM is allocated to both transmit and capture functions, one-half the memory allocated to each. Check or uncheck the box to enable or disable full duplex mode. The tab is context sensitive and is only visible if the device is an PMM. Select the PMM tab from the **Configuration → Module → Settings...** menu to enable full-duplex mode for the PMM. The default is half-duplex mode.

GMM and IMM modules have separate send and receive buffers and ports on the card and are therefore inherently capable of full-duplex. There is no configuration setting for a single card for full-duplex or half-duplex. However, note that full-duplex capture requires two synchronized modules (such as in OPV-LA) connected through a tap device.

Expert Analysis Mode

Expert Views and Alarms can be disabled. When disabled, no Expert Views or Alarms will display in OPV-PE software.

Uncheck the **Enable Expert Analysis Mode** box to disable Expert Views and Alarms. The default is to enable Expert Analysis. If you do not have the Expert Analysis software, you cannot enable Expert Analysis Mode.

Non-Well-Known-Ports Mode

Non-well-known port (non-WKP) numbers in tables can be enabled or disabled for each module when monitoring with local devices. When disabled, most port numbers above 1023 display as TCP Other or UDP Other with no port number provided.

It is recommended that you leave this feature disabled unless you are looking for specific port numbers greater than 1023, since non-WKP numbers can quickly fill Application Layer Tables. OPV-PE always displays the port number if the number is less than or equal to 1023. OPV-PE also displays some ports above 1023 since applications associated with them are widely accepted.

Check the **Monitor TCP/UDP non-well-known-ports individually** box to enable the display of all non-WKP numbers. The default is to not display these port numbers.

With the option enabled all TCP packets with non-WKP numbers (TCP or UDP) will be listed in the Application Tables as in the following example: UDP non-WKP:4620

This feature only affects the tables or charts that display TCP/UDP port numbers. **The display is affected for monitor views only of local NDIS modules.** If you want to display port numbers and name the ports in the display for remote devices, see "Assigning Names to Protocols (Monitor)" on page 20 of this chapter. Also refer to this section for more information on non-WKP numbers.

Monitor VoIP Only Mode

By restricting monitor mode to multimedia tables only, you can improve the rate at which OPV-PE is able to view multimedia protocols without dropping packets. The monitor VoIP only mode is disabled by default; all view tables are built in monitor mode.

Check the **Monitor VoIP Only** box to limit monitor mode to building VoIP tables only. All monitor table buttons are grayed out with the exception of MAC statistics.

This mode can be applied to any local analyzer device. For remote devices, Monitor VoIP Only mode can only be set for OPV-LA devices.

MAC Control Frame

For Gigabit Ethernet a MAC Control Frame is sent to ensure that sending devices do not overflow receive buffers. For IMM or GMM devices, you can select to capture these frames or ignore them. The default is to capture MAC Control Frames. This setting applies only to IMM or GMM devices.

System Settings

System settings establish general timing, file, and port information for the OPV-PE system.

Configuring Ports to Scan

OPV-PE must search the ports on the local system to find an analyzer device installed in the local system. Sometimes this creates a problem with certain devices already on the system. Use this function to restrict the ports which are scanned. The dialog box for configuring ports to scan comes up on OPV-PE start-up. The ports to scan are typically configured at start-up, but can be changed from OPV-PE at any time.

You can use OPV-PE to set the ports on the PC to scan at any time. To set up or change port scanning, do the following

1. Choose **System Settings…** from the **Configuration** menu. Select the **Scanning Ports** tab.

2. A dialog box appears showing the ports within the local system. Check the box of only those ports you want OPV-PE to scan for an analyzer card.

3. Click the **OK** button.

Configuring Remote Communications

The remote server protocol (RSP) is used to control the interface for connecting with remote systems. You configure the options that effect connection time outs, encryption of control packets, and auto-discovery of resources.

To configure remote communications, select **System Settings…** from the **Configuration** menu. Select the **Remote Communications** tab.

Table 4-4. Remote Communications Tab Functions and Default Settings

Tab Selection	Description
Encrypt RSP Packets check box	Select **encryption** if there is a need for security in the network when transferring packets between the remote resource and the local system. The default setting is Not Selected.
No Autodiscovery check box	Select this box to prevent auto-discovery of remote resources. If selected, you will only be able to access remote resources by manual discovery of resources using the **Connect** option from the **Host** menu. This box can be selected when working with only local resources to eliminate viewing all resources in the Resource Browser. The auto-discovery of resources may take some time, especially in a large network. The default setting is Not Selected
RSP Time Out value	Specifies, in seconds, how long the protocol waits before dropping a connection when the remote resource is not responding. The value must be between 1 and 30 seconds. The default setting is 10 seconds.

Setting Update Timers

Timers control how often counters, tables, and displays are updated. There are two types of timers, display timers and polling timers. Remote polling timers control how often data is updated from remote systems. Display timers control how often displays of data are updated in the OPV-PE software. All timer values are in seconds.

For local devices, the MAC Layer counters are updated every second, and other charts and tables for local devices are updated every 10 seconds.

For GMM devices, only the MAC layer counters timer value is used. Other monitor timers are not used by this device.

To configure the timers, select **System Settings…** from the **Configuration** menu. Select the **Timers** tab. The timers are listed and described in Table 4-5, Table 4-6, and Table 4-7.

Table 4-5. Remote Polling Timers

Polling Timers	Description
MAC Layer Counters	Sets the interval for polling devices for MAC layer counters.
Protocol Distribution	Sets the interval for polling devices for the protocol distribution information.
Host Table	Sets the interval for polling devices for MAC layer host table information.
Matrix Views	Sets the interval for polling devices for information on MAC, network, and application layer conversations.
Expert Data	Sets the interval for polling devices for expert data.
Remote Name Table	Sets the polling interval for refreshing the local copy of the name table for a remote resource.

Table 4-6. Strip Chart Display Timers

Display Timers	Description
Strip Chart Display Timer, Local	Sets the time between refreshing counters in strip charts for resources in the local PC. This display timer is available for strip charts only.
Strip Chart Display Timer, Remote	Sets the time between refreshing counters in strip charts for resources in remote hosts. This display timer is available for strip charts only.

The values for polling timers must be between 1 and 214783647 seconds. The values for the display timers must be between 1 and 214783647 seconds. The strip chart display timers must be in multiples of the MAC Layer Counter timer. The default settings, in seconds, are shown in Table 4-7:

Table 4-7. Default Display Timer Settings

Display Timer	Default Value
MAC Layer Counters	3
Protocol Distribution	5
Host Table Views	7
Matrix Views	10
Expert Data View	15
Remote Name Table	300
Strip Chart, Local	1
Strip Chart, Remote	3

Configuring Counter Logging

Counter log files contain snapshots of OPV-PE counter information. All MAC layer statistics can be recorded in the log file.

To configure counter logging, select **Log File Settings…** from the **Configuration** menu.

To enable counter logging, check the **Enable Logging** field. Set the time interval for capturing counter information in the **Time Interval** field. Set the number of rows (line entries) in the log file in the **Log File Maximum Rows** field. For example, setting **Log File Maximum Rows** to 4,000 and **Time Interval** to 5 will record the counter information 4,000 times, once every 5 seconds.

Keep the **Keep History Log** box selected to create history files of counter information. The history file is written when all lines in the log file are full. When a history file is created, the module log file is erased and new counter information is recorded starting with the first line of the file. History files are named by date and time. The format for the name of history files is:

```
mmddhhmm.ss
```

```
mm(month) dd(day) hh(hour) mm(minute) ss(second)
```

The minimum time between creation of unique history files is one second. If you disable the creation of history files and the log file for the module is full, a new log entry causes the module log file to be erased. No history of counters is saved.

The default settings are shown in Table 4-8 below:

Table 4-8. History Log File Settings and Default Values

Log Setting	Default Value
Enable Logging	Not selected
Time Interval	5 seconds
Log File Maximum Rows	4,000
Keep History Log	Selected

Configuring Expert Logging

Expert log files contain entries of OPV-PE expert events. All expert symptoms discovered by OPV-PE are recorded in the log file. Entries in the expert log file are in ASCII text format.

To configure expert logging, select View Options... from the View menu. You must have the Expert View analysis table active to configure the log file.

To enable expert logging, check the **Log Entries to File** box. Specify the name of the log file in the **File Name** field. The default name for the log file uses the module name, for example `192.168.2.95_PMM(1).log.` Log files are given a `.log` extension if no log extension is specified. Leave the **Clean Contents When Rearm** box checked to clear the log file of old entries when a capture is restarted. Select the maximum size of the log file in the **Maximum Log File Size (MB)** field.

History files are created for the expert log when the size of the log file reaches the **Maximum Log File Size (MB)** field. The log file is renamed with a file name extension of .log1 and OPV-PE begins rewriting the .log file. Up to nine history files are saved (`.log1` through `.log9`) before OPV-PE deletes all history files and begins to save history files to `.log1`.

The default settings are as shown in Table 4-9 below:

Table 4-9. Expert Log File Settings and Default Values

Log Setting	Default Value
Log Entries to File	Not selected
File Name	`...\Log\<module-name>.log`
Clean Contents When Rearm	Selected
Maximum Log File Size (MB)	10

Configuring Alarms

Alarms can be configured to generate events such as e-mail messages, pages, or logging messages to a log file. E-mail recipients, pager recipients, and log file names are global parameters that you set. All alarms are automatically sent to one set of e-mail addresses and one log file.

The alarm E-mail feature works only with Microsoft Mail Exchange.

Using E-mail with OPV-PE is turned off by default. If you want to use this feature, you must reset a parameter in the OPV-PE `.ini` file. Set `Enable MAPI=1` to enable the E-mail alarms feature through Microsoft Mail Exchange.

To configure alarm actions, select **Alarms** from the **Configuration** menu and then select either **E-Mail Settings**, **Pager Settings**, or **Log File Settings** from the submenu.

Table 4-10. Alarm Actions

Alarm Action	Setting Description
E-mail Settings	The set of e-mail addresses that will receive mail if an alarm triggers an event with the alarm action set to **e-mail**. When you click on the **Add Recipients** button in the menu you can set up e-mail addresses using Microsoft Mail's address book.
Pager Settings	The pager number that will receive a page if an alarm triggers an event with the alarm action set to **pager**. The other settings for the pager depend on the type of pager. For pager settings, you must set the delay to at least 3 seconds.
Log File Settings	The name of the log file that will have an entry if an alarm triggers an event with the alarm action set to **log**.

Configuring a Multi-Port Tap or Switch

A tap or switch can be attached to the local system or be available as a remote resource on the network. Typically a tap or switch will be used in the wiring closet with a remote analyzer and accessed as a remote resource. However, taps and switches can be attached to the local system and accessed through a COM port on the PC. See "Setting the COM Port for Taps and Switches" for information on configuring these devices to talk to a local PC.

Fluke Networks taps or switches are devices that work in conjunction with a Fluke Networks analyzer to monitor multiple network segments. When connected properly, its icon will be visible in the resource browser. The port of the tap or switch currently being monitored will show under the resource. If you cannot see the tap or switch icon, refer to the analyzer, or tap hardware documentation for more information on connecting these devices to the network.

Although the taps and switches show as a resource to the OPV-PE software, they do not directly perform monitoring and other analysis functions. They act as switching devices for analyzers, so one device can be used to view many different LAN segments, one-at-a-time.

The OPV-PE software can be used to control which LAN segment is selected by the tap or switch. To set the LAN segment:

1. In the resource browser, click on the local or remote resource connected to the switch. The current port being monitored will display under the tap or switch

resource. The example below shows a Switch with the LAN Segment connected to port 5 selected.
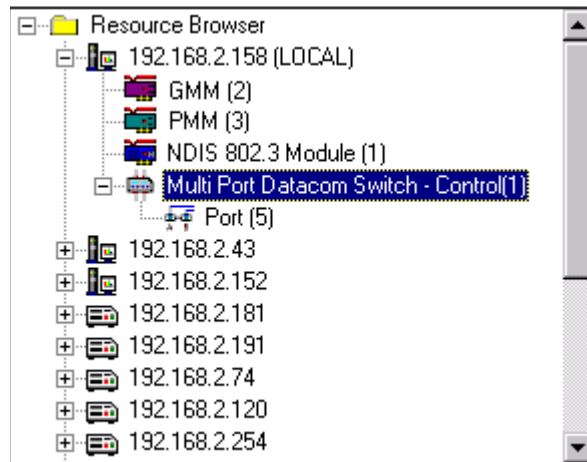
2. Double-click on the tap or switch icon in the resource browser.

3. A list box appears showing the port-pairs on the tap or switch. You must know which LAN segments are connected to the port-pairs on the tap or switch. Use the radio buttons to select the LAN segment you wish to monitor with a Fluke Networks analyzer. Only one LAN segment can be selected.
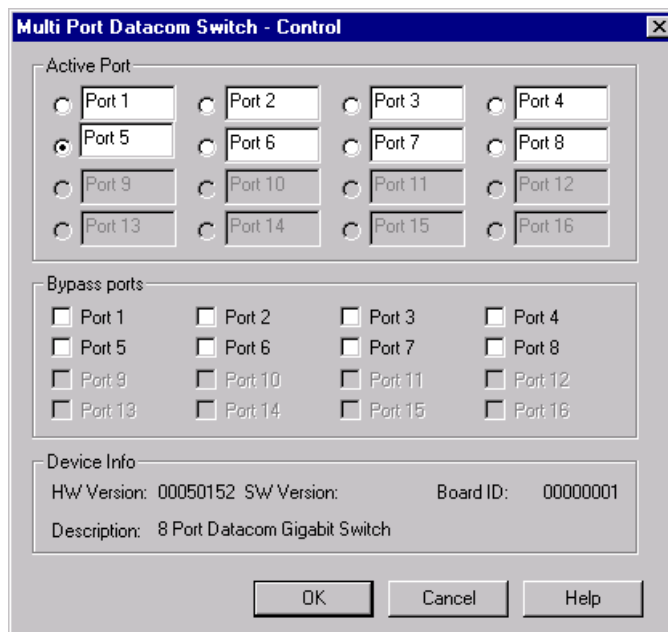
4. Use the **Bypass** check boxes to set any network segments that you want to restrict from being used with an analyzer. Any segment with the **Bypass** box checked cannot be set as the LAN segment.

5. Click the **OK** button.

Information about the exact type of switch or tap is shown at the bottom of the dialog box.

Setting the Local COM Port for Taps and Switches

The tap or switch can be controlled from a PC running OPV-PE software. The tap or switch can be directly connected to a COM port on the PC and controlled as a local resource from OPV-PE. In this configuration, the COM port used to connect the tap or switch to the PC must be configured in OPV-PE software.

To configure the COM port for a local connection to a tap or switch, do the following:

1. Select **System Settings…** from the **Configuration** menu.

2. Select the **Local COM Port for Tap Device** tab to set the port for a multi-port tap. Select the **Local COM Port for Switch Device** tab to set the port for a switch.

3. Set the COM port value to the COM port (COM1 through COM4) where the tap or switch is connected to the PC. Only one port can be selected.

The tap or switch is connected to the PC using a standard 9-pin serial cable. Only one tap or switch device can be connected to the PC.

Settings for Remote Analyzer Devices

You can use OPV-PE to control remote analyzer devices. You must have "super-user" privileges to reset or update these devices.

Resetting a Remote Analyzer Device

A remote analyzer device can be reset using OPV-PE software. To reset a device do the following:

1. Login to OPV-PE with "super-user" privileges.

2. Click on the icon for the remote device in the Resource Browser.

3. Choose **Properties** from the **Host** menu.

4. Click the **Reset DPI/Image Upgrade** button.

5. Check the **Warm Boot** radio button under **Reset Options**. Leave all other fields blank or unmarked.

6. Click the **OK** button.

When you reset the device, you will lose the connection. Use the **Connect** option from the **Remote** menu to reconnect.

Updating a Remote Analyzer Device

You can update the software or change address information for a Fluke Networks analyzer device from OPV-PE.

Before you can reset the device with a new image, you must place the new image on a server that runs TFTP protocol.

Download the new software from Fluke Networks's Web site, `http://www.flukenetworks.com`. Go to the software updates section of the Web site to find the new DPI-1XX image. Place the software on the server that runs the TFTP protocol.

Before you can update device address information automatically, you must have a server that contains the new address information and runs the BOOTP protocol.

Use the following procedure to update a remote analyzer device.

1. Login to the device with "super-user" privileges.

2. Click on the icon for the remote analyzer device in the Resource Browser.

3. Choose **Properties** from the **Host** menu.

4. Set the new IP Address, IP Gateway Address, and Subnet Mask for the device. If no address update is needed, or you are updating the address from a BOOTP server, skip this step.

5. Click the **Reset Device/Image Upgrade** button.

6. Check the **Enable BOOTP** box if you are updating addresses from a BOOTP server.

7. Check the **Image Upgrade (TFTP)** box if you are updating addresses from a TFTP server.

8. Enter the IP address of a server that runs BOOTP and/or TFTP protocols in the **IP Boot Server** field.

9. If you are updating the device image, set the path name to the software image file in the **Boot Image Filename** field.

10. Check the **Warm Boot** radio button under **Reset Options**.

11. Click the **OK** button.

⚠ Caution

You must use the Warm Boot option to load the new image from the network. The Cold Boot option will not update the image.

When you reset the device, you will lose the connection. Use the **Connect** option from the **Remote** menu to reconnect.

When the remote analyzer device is restarted, the new software image is written to non-volatile memory and becomes the new executable image.

Though not a part of the update procedure, you can use the **Cold Boot** option to force the device to run its self-tests. These tests will verify that the unit is operating properly.

Setting the Fast Ethernet Traffic Analyzer Ports for OPV-LA or DPI-1XX

OPV-PE supports the Fast Ethernet Traffic Analyzer RMON/RMON2 probe. If the device is connected to a Fast Ethernet Traffic Analyzer probe, you can set the port-pair mirrored to OPV-LA or DPI-1XX. At least one analyzer port on the OPV-LA or DPI-1XX must be connected to one Tap Port on Fast Ethernet Traffic Analyzer; both analyzer ports may be connected to Fast Ethernet Traffic Analyzer Tap Ports A and B. Setting the port-pair changes the segments connected to Fast Ethernet Traffic Analyzer which are mirrored to OPV-LA or DPI-1XX through its Tap ports. To set or change the Fast Ethernet Traffic Analyzer port-pair, do the following:

1. Login to OPV-PE with "super-user" privileges.

2. Click on the OPV-LA or DPI-1XX icon in the Resource Browser.

3. Click on the Fast Ethernet Traffic Analyzer icon in the Resource Browser. If the remote analyzer device is not connected properly to Fast Ethernet Traffic Analyzer, this icon will not appear.

4. Select the port-pair from the menu. Only those port-pairs present on the Fast Ethernet Traffic Analyzer hardware device will display. Ports are selected in pairs even if only one Fast Ethernet Traffic Analyzer port is connected to a network segment or if only one Tap port is connected to the remote analyzer device.

5. Click the **OK** button.

This procedure accomplishes the same task as pressing the ADVANCE button on the Fast Ethernet Traffic Analyzer device until the desired port-pair is mirrored to

the Tap ports.

Port numbers not physically present on Fast Ethernet Traffic Analyzer will be gray. A selectable port-pair does not indicate that a link has been established from either Fast Ethernet Traffic Analyzer port to a network segment, or whether the port-pair is in full-duplex or half-duplex mode. Refer to your *Fast Ethernet Traffic Analyzer User's Guide* for information on making the proper connections to DPI-1XX and for other information on setting up Fast Ethernet Traffic Analyzer.

Advanced Configuration

`OPV-PE.ini` **File**

OPV-PE uses configuration settings from a `.ini` file called `OPV-PE.ini`. If you want to run the product with different configurations, you can save different sets of configuration information in different `.ini` files. OPV-PE always looks for the file named `OPV-PE.ini` in the Window's system directory and will use that file for its configuration. If no `OPV-PE.ini` file is found in the directory, OPV-PE will build another `OPV-PE.ini` file based on the factory default configuration settings.

Different sets of configuration information can be especially useful for display timers and update timers. The first eight parameters of the `OPV-PE.ini` file are the configuration values for the various display timers.

For information on other `OPV-PE.ini` settings, contact Fluke Networks Customer Support. It is not recommended that you alter the `OPV-PE.ini` file directly.

Customizing Expert Diagnostic Information

The `EXPERTMSG.INI` file contains OPV-PE's diagnostic information. OPV-PE always looks for the file named `EXPERTMSG.INI` in the OPV-PE installation directory and will use that file for its diagnostic information. If no `EXPERT-MSG.INI` file is found in the directory, OPV-PE will not provide diagnostic information.

You can change the diagnostic information if you want. Changing the diagnostic information may be a useful way to customize OPV-PE for your environment. For example, if you have a known problem area to check when certain conditions occur you can include this information directly in the diagnostic information.

Assigning Names to Protocols (Monitor)

OPV-PE assigns names to protocols that have been detected, providing users with an easy way to view what protocols have been discovered on the network. In most cases, protocol names are well known; they are defined by the protocol's creator, or defined by a standards organization. However, you may want explicit information about a protocol that does not have a well known name or is counted in OPV-PE monitor screens as a "TCP OTHER" or "UDP OTHER" protocol.

OPV-PE includes a `MONITOR.INI` file to assign names to protocols. Entries in the `MONITOR.INI` file allow you to:

- Rename the protocols that are currently being detected. For protocols that use TCP or UDP as their transport protocol, the protocol can be assigned a name to override it's default name.

- Extend the list of protocols that are monitored by OPV-PE. You can extend the monitoring of protocols that use TCP or UDP as their transport protocol.

See the section on How OPV-PE Assigns Protocol Names to learn how OPV-PE names protocols by default. Understanding how OPV-PE assigns names to protocols by default is important for understanding how protocol names can be altered and how protocols can be added using `MONITOR.INI`.

The assigning of protocol names does not effect protocol decodes. See Assigning TCP or UDP Ports to Protocol Parsers for information on assigning protocol parsers to specific ports.

The `MONITOR.INI` file is located in your Windows installation directory. Examples of usage are included in the file.

Settings in the `MONITOR.INI` file will override any other configuration settings you have made for the display of protocols.

MONITOR.INI Format

`MONITOR.INI` contains two sections, TCP and UPD. Each section may have zero or more entries beginning with the keyword "mapping". Each "mapping" entry is followed by an equal sign and three variables:

```
mapping= <port num>,<short name>,<long name>
```

`<port num>`	is a two-byte value that appears in a port fields of a TCP or UPD packet header. It identifies the protocol, by port number, to be included as a discrete protocol in OPV-PE's monitor views.
`<short name>`	is an alpha numeric string that is be between 1 and 12 characters This string is used as the name for the protocol in OPV-PE's monitor tables.
`<long name>`	is an alpha numeric string that should be between 1 and 50 characters. This string is used as the name of the protocol where OPV-PE displays a long name.

The structure of the `MONITOR.INI` file is:

```
[TCP]
mapping=<port num>,<short name>,<long name>
    .            .                    .
    .            .                    .
mapping=<port num>,<short name>,<long name>
[UDP]
mapping=<port num>,<short name>,<long name>
    .            .                    .
    .            .                    .
mapping=<port num>,<short name>,<long name>
```

MONITOR.INI Examples

Example 1

Assume that you wish to rename TCP port 80 from HTTP to WWW for World Wide Web. The following entry would be made to the `MONITOR.INI` file in the TCP section:

```
[TCP]
mapping=80,WWW,World Wide Web
```

Example 2

Assume that a company is using a proprietary protocol named "Company X Protocol" that uses UPD port 921. By default this protocol would appear with the generic name "UDP WKP 921" in the monitor tables. Making the following entry to the `MONITOR.INI` file UDP section would give the protocol a name with more meaning:

```
[UDP]
mapping=921,CXP,Company X Protocol
```

Example 3

X Windows could use non-WKP TCP ports in the range 6000 to 6063. However, by default, OPV-PE reports X Windows network traffic with a single entry in the Protocol Distribution table.

For example, if 100 X Windows packets detected on port 6000 and 200 were detected on port 6029, the Protocol Distribution table would report that 300 hundred XWIN packets were detected. If the network manager wanted the Protocol Distribution table to report the number of packet seen on each of the 64 X Window ports, the

MONITOR.INI would need the following 64 entries:

```
[TCP]
mapping=6000,XWIN6000,X Windows on port 6000
mapping=6001,XWIN6001,X Windows on port 6001
    .            .                    .
    .            .                    .
mapping=6063, XWIN6063,X Windows on port 6063
```

Example 4

Assume that a company installed an audio/video application on its network named Video Audio Network Communicator. Assume that the application uses TCP port 2900. By default, packets on this port are attributed to the "TCP OTHERS" entry in the Protocol Distribution table along with other TCP non-WKP packets. To count and display the TCP port 2900 reported individually, the following entry needs to be made to the MONITOR.INI file:

```
[TCP]
mapping=2900,VIDEO,Video Audio Network Communicator
```

How OPV-PE Assigns Protocol Names

OPV-PE explicitly monitors a predefined set of protocols/applications that use TCP or UDP as their transport layer. However, some of the TCP or UCP ports monitored are not given a well-known name. Also, some TCP and UDP ports are not explicitly monitored, and information about these remaining protocols are collected as though they were a single entity, one for TCP and one for UDP.

OPV-PE monitors two port ranges, which are called Well Known Ports (WKP) and non-Well Known Ports (non-WKP). In summary, there are four different ways TCP/ UDP ports are assigned names by OPV-PE. They are:

• WKP that have an assigned, default name (i.e. HTTP, DNS, FTP, …)

• WKP that use a generic name (i.e. TCP WKP 29, UDP PORT 64, …)

• Non-WKP that have been assigned a specific default name (i.e. NFS, LOTUS NOTES, RADIUS, …)

• Non-WKP that have not been assigned a name (TCP OTHER or UDP OTHER)

By changing the MONITOR.INI file, you can change names of generic names of WKPs and assign names to non-WKPs that are not assigned names by default.

Monitoring Well-Known Ports

OPV-PE monitors all protocols that fall in the WKP (Well Known Port) range, ports with a value between 0 and 1023. If OPV-PE detects a TCP or UDP with a port in the WKP range, information will be maintained on that port (total bytes, total packet, conversation, etc.).

Some of the ports have been assigned a name that is typically associated with the port value. For example, TCP port 80 is assigned the name HTTP. This name is used to represent that port when information about the port is displayed in the monitor tables of OPV-PE.

Other WKPs are not assigned a default name. If these ports are detected, their name takes the generic form: "TCP WKP <port num>" or "UDP WKP: <port num>" where <port num> is the WKP value. For example, the TCP port 29 is not assigned a default name so if this port is detected the name used to represent the port would be: "TCP WKP 29".

Monitoring Non Well-Known Ports

OPV-PE also collects information about a subset of ports that fall outside of the WKP range, port numbers greater than 1023. These ports are called non-WKP. Some of these ports are monitored by OPV-PE since applications associated with them are widely accepted. The non-WKP ports that OPV-PE monitors and their associated port values are listed in Table 4-11 and Table 4-12.

Table 4-11. Default Names for Non-WKP TCP Ports

Name	TCP port values
LOTUS NOTES	1352
TNS (Sybase)	1521
RSP	1704
TDS (Oracle)	2048
NFS	2049
CC:MAIL	3264
XWIN	6000-6063

Table 4-12. Default Names for Non-WKP UDP Ports

Name	UDP Port Value
RADIUS	1645
RSP	1704
RADIUS	1812
HSRP	1985
NFS	2049
RTP	5004
RTCP	5005

OPV-PE treats all other non-WKP as a single entity given a single generic name. The name for TCP non-WKP ports is "TCP OTHER". The name for UDP non-WKP ports is "UDP OTHER". For example, if 900 occurrences of the TCP port 11964 was detected and 200 occurrences of the TCP port 10564, there would be a single name to identify these 1100 occurrences of the TCP non-WKPs called "TCP OTHER".

Assigning TCP or UDP Ports to Protocol Parsers

Use the `ANALYSIS.INI` file to assign any built-in OPV-PE parser to a TCP or UDP port. This is useful when a network is running a protocol/application over a TCP or UDP port that is not using the default port. The assignment of a proper parser allows OPV-PE to properly decode and analyze the packets associated with the TCP or UDP port.

The assigning of parsers does not effect how the information is displayed in monitor views. See "Assigning Protocol Names" for information on assigning names for monitor views.

The `ANALYSIS.INI` file is located in your Windows installation directory. Examples of usage are included in the file.

ANALYSIS.INI Format

The `ANALYSIS.INI` file has two sections, TCP and UDP. A section contains one or more entries with the following format:

```
mapping=<port num>,<ip addr>,<parser name>,<name>
```

`<port num>`	is any valid 2 byte value that represents a TCP or UDP port value. It identifies the protocol, by port number, to be parsed in OPV-PE's decode views.
`<ip addr>`	is a valid IP address in dotted decimal notation. This field can have an asterisk (*) to represent all IP addresses.
`<parser name>`	is the name of a valid OPV-PE built-in parser. See Parser Names for a list of parsers.
`<name>`	is a name that will used to identify the mapping.

Example 1

Assume that the network administrator configured Oracle's TNS protocol to use TCP port 1029. This port value is different from the default value for TNS, which is 1521. The entry in the ANALYSIS.INI would be:

```
[TCP]
mapping=1029,*,TNS,Oracle TNS
```

"Oracle TNS" is the string that will be used in OPV-PE's displays to identify this decode.

Example 2

Assume that the network administrator configured Sybase's TDS protocol to use TCP port 11964. This value is different from the value for TDS which is 2048. Furthermore suppose the network administrator only wants to decode TCP port 11964 when associated with IP address 192.168.1.98. The entry in the ANALYSIS.INI file would be:

```
[TCP]
mapping=11964,192.168.1.98,TDS,Sybase TDS
```

Example 3

Assume that two real-time applications have been installed on a network that both use RTP (Real-Time Transport Protocol). Assume that one of the applications uses UDP port 10564 and the other uses 11964. Both of the UDP ports differ from the default port of 5004. The entries in the ANALYSIS.INI file would be:

```
[UDP]
mapping=10564,*,RTP,RTP APPLICATION 1
mapping=11964,*,RTP,RTP APPLICATION 2
```

Parser Names

The tables in Appendix D contain the Parser Names that are built into OPV-PE. Each parser is responsible for decoding a specific protocol. Parser Names are as similar as possible to protocol names. Parser Names must be entered exactly as shown in the tables to correctly reference the built-in parser.

Chapter 5
Resources and Modes

OPV-PE can gather statistical information and view network data from a variety of hardware sources. The types of information you receive from a resource depends on the hardware.

OPV-PE's auto-discovery feature automatically scans the network for available resources, or you can enter the IP address of any host you can reach through a TCP/IP connection. OPV-PE remembers the name of the most recent connection made so you can quickly reconnect to the host.

Resource Browser

The Resource Browser is a single window through which you can access all local and remote resources available in the network. The Resource Browser window works much the same as Microsoft Windows Explorer, allowing you to see hosts and their associated resources in a hierarchical relationship. "Branches" can be expanded or collapsed via point and click, so you can quickly customize your view of available resources.

Remote systems containing resources are listed by IP address unless there is a OPV-PE name table on the system. If an entry exists in the name table for the IP address of a resource, the symbolic name in the name table is used to represent the resource. Resources within remote systems are listed by module type and module number. The module number is assigned by the software from the base address of the module, which is set by jumpers during hardware installation. For NDIS modules, the modules are numbered by the order in which they are discovered within the local or remote host. It is possible to have two different modules with the same name if they are within different hosts.

The Resource Browser opens as a docking window when OPV-PE is started and can be moved to its own window outside the main window.

Double-click on a resource to display a default view of the resource in Summary View. If a remote resource is protected, you are asked for a user name and password. Drag and drop resources onto alarms in the Alarm Browser to activate an alarm for a resource.

Remote vs. Local Resources

Local resources are those within the local PC running OPV-PE. Remote resources are all other resources that can be reached through a TCP/IP connection. When running OPV-PE from the PC, you have complete access and privileges to any resource in the PC. You can access remote resources and establish accounts for your local resources if you are using Remote Control software available from Fluke Networks. Both the local and the remote resource require Remote Control software for remote access to function.

Access to remote resources are controlled from the remote resource. For example, accounts, privileges, and passwords for PMM cards in a DPI-1XX are established at the DPI-1XX. Remote users must have access to a valid account to use the PMMs.

A remote resource can be located in any host which can be accessed via a TCP/IP connection. You'll need to know the IP address of the remote host to log in to the remote resource. If the remote resource can be auto-discovered by OPV-PE, the IP address or the name associated with the IP address of the host will display in the Resource Browser. Typically, resources on the same LAN segment can be auto-discovered.

Naming Remote IP Resources (Aliases)

The Resource Browser initially displays all nodes on a subnet using the IP Address. Users can assign an alias (user defined name) to a node for easy identification. For example, you can assign a name like "Chicago Node One" to the node. In addition, you can add a descriptive comment for any node.

There are two methods for bringing up the **Host Properties** dialog box to create an alias:

- Single-click with the mouse on the node. Select **Properties** from the **Host** menu. This brings up the complete **Host Properties** dialog box.

- Right-click with the mouse on a top-level node (IP Address/Alias Name) and select the **Properties...** option from the popup menu. This brings up the **Host Properties** dialog box for setting the alias.

Within the **Host Properties** dialog box, set the alias name and any optional comment. An example of the **Host Properties** dialog box is shown below. Additional fields may be available in this dialog box depending on the type of node.
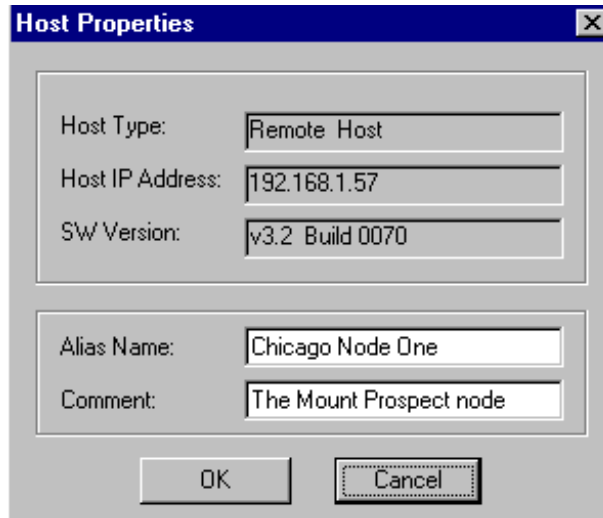
Figure 5-1. Host Properties Dialog Box for Establishing an Alias

All characters are allowed in alias names except $, #, <, and @.

When an alias is established, OPV-PE window title bars change to reflect the new alias name instead of the IP Address. For example, "//192.1.68.2/Module(1)" might display as "//Chicago Node One/Module(1)".

Hovering the mouse over a top-level node which has an alias displays the name with the IP Address in parenthesis along with the optional comment. For example, "Chicago Node One (192.1.68.2). This is Mount Prospect node".

Resource Protection

You are in control of local resources within a PC. Use the functions on the **Host** menu to add and delete users for a resource, change passwords and protections, or view the users currently logged in. There is a guest account for users with no account. The guest user can be given all privileges to effectively disable resource protection.

Note that there is no password protection for starting OPV-PE on the local system. If you can start OPV-PE from a system, you automatically have complete access to all local resources (called super-user privileges).

To access a remote resource, you must have an account and password set up on the remote system containing the resource or use the guest account.

Privileges for remote users can be set to those described in Table 5-1 below:

Table 5-1. Remote User Privileges

Privilege	Description
Monitor Only	Allows a remote user to use the local device to monitor network activity only. You can access real-time monitor views on an armed (started) module, but cannot start/stop a module or define/load a filter.
Capture/Monitor	Allows a remote user to use the local device to monitor activity or capture network data. You can perform all Monitor Only functions plus capture data and perform full seven-layer decode on the packets. You can start/stop a module, define/load a filter, and edit the contents of packets.
Full	Allows a remote user to use the local device to monitor activity, capture network data, or transmit network data. You can perform all Capture/Monitor functions plus all traffic generation capabilities available through OPV-PE.
Super User	Allows a remote user the ability to transmit, capture, or monitor, plus set up, delete, and change accounts for the local PC. You have Full access plus the ability to configure a deployed DPI-1XX, change the access table, and unlock any locked module. Be careful when granting super-user privileges to remote users. This gives remote users complete control of your local resource.

Modes

Modes are applied to resources. Each resource can be in a different mode. There are five modes available with OPV-PE, as shown in Table 5-2 below:

Table 5-2. OPV-PE Resource Modes

Mode	Description	Resource Type
Monitor	Provides real-time views and decodes of packets received by a device. (All except GMM)	All (Limited with GMM)
Capture	Allows packets received by a device to be stored in a buffer for analysis.	All
Capture + Monitor	Provides both real-time monitoring views and the ability to store packets for later analysis.	All. Viewed/captured packets for IMM are identical.
Transmit	Allows the transmission of packets from a device. You must have the Traffic Generator from Fluke Networks to use Transmit mode.	All (Not recommended for NDIS or Portable Analyzer Cards)
Capture + Transmit	Allows simultaneous capture and transmit from the same module.	PMM or GMM only

Both the monitor and capture functions look at the same bit stream being received by a device. The difference between these modes is how the bit stream is stored and viewed. Because each class of device has different capabilities for storing and viewing the bit stream, you must understand the capabilities of the device you are using to completely understand what is possible in each mode.

If you have Traffic Generator, you can use any device in transmit mode. Table 5-3 shows the Bit Stream storage and viewing capabilities of these devices.

Table 5-3. Bit Stream Storage and Viewing from NDIS and Fluke Networks Devices

Device	Bit Stream Storage and Viewing Capabilities
IMM (Integrated Media Module)	IMM is an analyzer card for 10/100/1000 Ethernet networks. IMM supports all counters in OPV-PE and supports all capture functions at full line rate. The IMM also supports monitor and transmit modes for 10/100/1000 Ethernet. Special views are supported for viewing the capture buffer when the device is stopped. IMM supports only one mode at a time, either Capture, Monitor, or Transmit. The default mode for IMM is Capture.
Gigabit Media Module (GMM)	Gigabit Media Module (GMM) is an analyzer card for Gigabit Ethernet networks. GMMs support MAC counters in OPV-PE and supports all capture functions at full line rate. Real-time functions are limited to network statistics and MAC error counters. Special views are supported for viewing the capture buffer when the device is stopped. The default mode for GMMs is Capture + Monitor.
Protocol Media Module (PMM)	Protocol Media Module (PMM) is an analyzer card for 10/100 Ethernet networks. PMMs support all modes and all counters in OPV-PE and support all monitor and capture functions at full line rate. The default mode for PMM is Capture + Monitor.
OPV-LA (10/100/1000 Mbps Network Analysis)	The OPV-LA is a protocol analysis tool that contains its own processor and two IMM modules. The IMM modules in OPV-LA support all counters in OPV-PE. IMM supports all capture and transmit functions at full line rate. The IMM modules are synchronized so you can analyze a full-duplex network segment from a single view. When viewing an OPV-LA resource in the Resource Browser, you will see three "devices": one for the first IMM card, one for the second IMM card, and one for the two cards synchronized as a set. The default mode for modules in OPV-LA is Capture + Monitor. IMM cards in OPV-LA do not support Capture + Transmit mode.
DPI-1XX (10/100 Mbps Network Analysis)	The DPI-1XX is a protocol analysis tool that contains its own processor and two PMMs. The DPI-1XX fully supports all modes and all counters in OPV-PE. The PMMs are synchronized so you can analyze a full-duplex 10/100 network segment from a single view. When viewing a DPI-1XX resource in the Resource Browser, you will see three "devices": one for the first PMM, one for the second PMM, and one for the two cards synchronized as a set. The default mode for modules in a DPI-1XX is Capture + Monitor.
GPI-1XX (1000 Mbps Network Analysis)	The GPI-1XX is a protocol analysis tool that contains its own processor and two GMMs. The GMM modules in GPI-1XX support MAC counters in OPV-PE and support all capture functions. The GMMs are synchronized so you can analyze a full-duplex gigabit network segment from a single view. When viewing a GPI-1XX resource in the Resource Browser, you will see three "devices": one for the first GMM, one for the second GMM, and one for the two cards synchronized as a set. The default mode for modules in a GPI-1XX is Capture + Monitor.

Table 5-3. Bit Stream Storage and Viewing from NDIS and Fluke Networks Devices (continued)

NDIS	OPV-PE NDIS supports up to four Ethernet adapters. The first Ethernet adapter found during system initialization is seen by OPV-PE software as module #1, the second as module #2, and so on.
	Ethernet adapters can be used to capture, transmit, or monitor, but have performance constraints. The effective rate at which an NDIS module can capture or monitor is limited because it must perform these functions in software rather than hardware. An NDIS adapter is often used in Monitor only mode to improve performance, since NDIS adapters cannot capture at full line rate. When using an NDIS adapter, check the **Information** tab to see information about what counters are supported. Each manufacturer supports a different set of counters. The default mode for NDIS adapters is Capture + Monitor.
Fast Ethernet Traffic Analyzer	The Fast Ethernet Traffic Analyzer is a multi-port RMON/RMON2 probe. OPV-PE can display the RMON statistics collected by Fast Ethernet Traffic Analyzer. Icons appear under the Fast Ethernet Traffic Analyzer resource in the Resource Browser to select the port or port-pair to monitor. Monitor port-pairs when connected to full-duplex links. Monitor statistics display as for any other resource. The only mode for Fast Ethernet Traffic Analyzer is Monitor.
	Note
	Fast Ethernet Traffic Analyzer can mirror data from its probe ports to DPI-1XXs equipped with PMMs. You can control the Fast Ethernet Traffic Analyzer ports that are mirrored from OPV-PE through the DPI-1XX device. A special Multi-Port Tap icon appears under the DPI-1XX resource in the Resource Browser to control which ports of Fast Ethernet Traffic Analyzer are mirrored to DPI-1XX. See the chapter "Customizing OPV-PE" for more information on port selection.
Fluke Networks Taps	Taps are fault-tolerant wiring devices that provide connections for DPI-1XX or OPV-LA. The tap shows as a "resource" to the OPV-PE software, but is only used to select a LAN segment for monitoring and LAN analysis functions.
Switches	Switches are wiring devices that provide connections for OPV-LA, DPI-1XX, or GPI-1XX. The switch shows as a "resource" to the OPV-PE software, but is only used to select a LAN segment for monitoring and LAN analysis functions. 4, 6, or 8-port Datacom Switches for 10/100 or Gigabit Ethernet are supported.

See Appendix A for more information on the implementation of OPV-PE and a summary of all hardware differences.

Synchronized Resources

Synchronized resources are multiple hardware devices (two PMM, two GMM, or two IMM) that have been connected so that they use the same clock timer. Synchronized devices display in the Resource Browser as a unique resource. For example, the two IMM modules in a full-duplex OPV-LA are synchronized, so the Resource Browser shows three resources available within the DPI-1XX; the first IMM, the second IMM, and the synchronized configuration of both IMM modules together. Synchronized resources are recognized by the synchronized resource icon in the Resource Browser.

Synchronizing resources allows single actions to start a resource pair. All statistics and all data about stations and conversations will appear as one resource to OPV-PE. This enables you to perform all capture or monitoring functions on a full-duplex network segment. Synchronized resources can also monitor two half-duplex segments. Resources cannot transmit frames when they are synchronized.

Synchronized PMMs within a DPI-1XX are typically used with a Fluke Networks Tap or a Fluke Networks Multi-port Tap to provide a connection to full-duplex network segment(s). The Fluke Networks Multi-port Tap provides a convenient, software-controlled means to switch between segments. Contact customer support for more information on DPI-1XX, Fluke Networks Tap, and Fluke Networks Multi-port Tap products.

Hints and Tips for Resources

The following are a collection of hints and tips you may find useful when using resources or the Resource Browser:

• When launching OPV-PE, be sure to enter the password on the log-in screen so you can see remote devices. If you fail to enter a password, OPV-PE will not allow you to see remote analyzer resources in your network.

• To connect to a remote host, choose **Connect...** from the **Remote** menu and enter the host IP address.

• To set up or change accounts, choose **Access Privileges...** from the **Host** menu.

• To see remote users logged on to your local resources, choose **Current Users...** from the **Host** menu.

• When using PMM or IMM modules, be sure you set the module port and speed before using the resource.

- Use the **Refresh** button in dialog boxes to update the list of user accounts currently established. Remote users with super-user privileges may have created a new account since the dialog box was initially displayed.

- To prevent others from using a local resource, use **Lock** from the **Module** menu.

- Setting the mode to transmit disables monitor and capture. Setting the mode to monitor and/or capture disables transmit.

- Monitor mode can be set in addition to capture if the resource supports monitoring functions. If the resource does not support monitoring functions, the **Monitor** button is disabled.

- Use synchronized PMM, GMM, or IMM modules for full-duplex capture.

- For options to be displayed under the **Host** menu, you must select the local host name in the Resource Browser. Selecting a resource within the local host makes the options in the **Host** menu unavailable.

- Use the **Properties…** option from the **Host** menu to find out information about the host. Information includes host type, IP address, and the OPV-PE software version. The host name must be highlighted in the Resource Browser to get a description.

- If you suspect that a remote resource is not responding, go to Summary View and look at the Resource Browser. If the host for the remote resource is not there, the connection has been lost with the remote host and the resource is not available. Red Xs appearing over a host in the Resource Browser indicate that the host is disconnected.

- To see which capture filter or transmit specification is associated with a particular resource, choose **Active TSP and Capture Filter** from the **Module** menu.

Chapter 6
Views

There are numerous ways to view data from OPV-PE. This section describes the primary windows you use to view data, and the actual data views you can see within each window.

The primary windows for viewing information are shown in Table 6-1.

Table 6-1. OPV-PE's Primary Windows for Viewing Information

Primary GUI Window	Description
Summary View	From Summary View you can see one view of many different resources. Viewing options include configurable charts and tables.
Detail View	From Detail View you can see many different views simultaneously of a single resource.
Capture View	From Capture View you can see many different views of previously captured data. Although the data is "static", the presentation of the data is the same as for viewing real-time data.

The data views that can be seen within each primary window are described independently. Although you may be viewing data for different purposes from each primary view, the way the information is presented in a data view is virtually identical no matter which primary view you are using.

Table 6-2 shows which data views are supported from each primary window.

Table 6-2. Data Views Provided Within Summary, Detail and Capture View

Metric	Summary View (Single View)	Detail View (Multiple Views)	Capture View (Static Data)
MAC Statistics	Y	Y	N
Utilization/Errors Strip Chart	Y	Y	N
Frame Distribution	Y	Y	Y
Protocol Distribution	Y*	Y*	Y
Host Table	Y*	Y*	Y
Network Layer Host Table	Y*	Y	Y
Application Layer Host Table	Y*	Y*	Y
Host Matrix	Y*	Y*	Y
Network Layer Matrix	Y*	Y*	Y
Application Layer Matrix	Y*	Y*	Y
VLANs	Y*	Y*	Y
Address Mapping	Y*	Y*	Y
Duplicate Address (Expert Analysis only)	Y*	Y*	Y
Expert (Expert Analysis only)	Y*	Y*	Y
Application Response Time (Expert Analysis only)	Y*	Y*	Y
Ring Statistics (Token Ring only)	Y	Y	Y
Capture View (protocol decode)	N	Y	Y
VoIP Views (Voice over IP plug-in only)	N	Y	Y
Y = Data View Supported			
N = Data View Not Supported			
Y* = Data View supported, but cannot be displayed in monitor mode when using GMM resources			

This chapter contains information on data views with the exception of Expert Views and VoIP Views. Refer to the Expert chapter for complete information on the VoIP Views. Refer to the Voice over IP chapter for complete information on the VoIP views.

Summary View

Summary View is OPV-PE's global monitoring tool for network data. You can view real-time data from any local resource or any resource you can connect to on the network. You can filter the data before viewing by applying a capture filter.

Each resource is viewed through its own window within Summary View. You can open windows for as many resources as you wish. Furthermore, each resource window can be displayed in six different views.

There are six tabs available for each module window within Summary View:

Table 6-3. Module Window Tabs Within Summary View

Tab	Description/Action
Monitor	Monitoring View. Refer to the list below for the choices. The selected view will show on the tab.
Rx	Receive counters. A list of MAC counters for receive and receive error counters.
Tx	Transmit counters. A list of MAC counters for transmit and transmit error
Alarms	Shows the alarm tables applied to this resource.
Alarm Log	Log of all real-time alarm events that have occurred for this resource.
Description	Provides a brief description of the board, board address, and supported counters.

To change the Summary View for a resource, click the appropriate tab at the bottom of the resource window. Using the tabs, you can get a single monitoring view, see transmit or receive counters, view alarms set and alarms triggered for this resource, or get a description of the resource (counters supported, etc.). The first tab contains the monitoring view which can be configured to display any of the views listed on the following page.

Multiple monitoring views are available from within Summary View. Each view can display as a table or a chart, with the exception of Address Map View or Expert Views. These two views only display as tables. Remember that in Summary View the view you set applies to all resources.

The monitoring views are listed below.

- Utilization/Error
- Frame Size Distribution

- Protocol Distribution

- Host Table

- Network Layer Host Table

- Application Layer Host Table

- Host Matrix

- Network Layer Matrix

- Application Layer Matrix

- VLAN

- Address Map

- Packet Summary

- MAC Statistics

- Ring Statistics

- Expert

- Application Response Time

- Duplicate Address

You can change the monitoring view for Summary View by choosing **Monitor View Preferences** from the **Module** option in the **Configuration** menu. The view you select applies to what you see in the first tab. For each resource you can have only one monitoring view. The monitoring view can be different for each resource.

In Summary View, you get one monitoring view of many different resources. Use Detail View to get many different views of a single resource or to perform detailed analysis functions on captured data. Double-click on the view for the resource or press the 🖼 button to go to Detail View.

Detail View

Detail View is the tool for performing detailed analysis of network data. You can view real-time data from the resource for which you have opened Detail View or you can view and analyze data stored in the capture buffer. You can filter the data before viewing by applying a display filter.

The Detail View allows multiple views for a single resource module and also allows the Capture View to be opened for that same module. By contrast, OPV-PE's Summary View allows one monitoring view for multiple resource modules and the Capture View cannot be opened.

You can have as many windows with data views as are available in Detail View. The initial data view you get of a resource is the view set in the **Configuration** menu for Summary View. Many of the table or chart views within Detail View can be customized.

Files or buffers, such as a capture file or capture buffer, are considered resources just like physical devices that are available from the Resource Browser. If you open a file from Summary View, a **Detail View** window will open for that resource. Viewing static resources such as files or buffers will change the options available from the toolbars and menus and the data views will appear somewhat different. OPV-PE is designed so that you'll only be able to perform the functions that make sense for that resource.

For example, if you open the capture file, it automatically puts you into Capture View. Buttons for capture, transmit, and monitor are grayed out on the **Detail View** toolbar, since these functions make no sense for a file. If you select another view of the information in the file, it will appear in a table with a gray background indicating its a view of a static resource.

Detail View can display multiple views of information. Press the button on the **Data Views** toolbar for the view you wish to be displayed in Detail View. Packet Summary View is available from the **Monitor Views** menu. MAC Statistics and Utilization/Error views show counter information. For these views, the displays depend on the mode of the resource, capture or transmit.

The Data View buttons are as follows:

	Ring Statistics (Token Ring Only)
	MAC Statistics (Rx)
	MAC Statistics (Tx)
	Frame Size Distribution
	Protocol Distribution
	Utilization/Error View (Rx)
	Utilization/Error View (Tx)
	Host Table
	Network Layer Host Table

	Application Layer Host Table
	Host Matrix
	Network Layer Matrix
	Application Layer Matrix
	VLANs
	Address Map
	Duplicate Address (Expert Analysis only)
	Expert (Expert Analysis only)
	Application Response Time (Expert Analysis only)
	VoIP (VoIP only)

Using Capture + Monitor Mode in Detail View

In Detail View you can have both Monitor and Capture views of data. The use of these two modes together allows you to monitor traffic at the same time as you look at the contents of previously captured data. However, some of ways you can look at the capture or monitor data are the same. For example, you can view a host table for the monitor data and also view a host table for the contents of the capture buffer. Because the formatting of the data in both of these views is identical, OPV-PE provides the following visual distinctions to help you distinguish between capture and monitor views:

• For table information of the capture buffer data, all data in the table is grayed.

• For monitor data, the column and row titles are gray, but the data in the table is white.

• The title bar for a monitor view reads "Monitor View" and the title bar for a capture view reads "Capture View."

If you start a resource and then stop it, you can look at the capture buffer contents using the 🔲 button to bring up Capture View. If you restart the resource (start a different capture operation), you will begin refilling the contents of the capture buffer and incrementing counters for monitor views. However, the previous views

that you have of the capture buffer are still open windows within Detail View. In other words, the "view" and decode of previous information is still available, even though the capture buffer itself is refilling with new information. If you do not need this previous view of captured information, it is recommended that you close the **Capture View** window and all associated capture view windows. You can, of course, save this information to a file. Closing unused windows may avoid confusion when looking at similar monitor and capture views. This will also help you distinguish between what is happening real-time and what was saved from the previous capture operation.

Capture View

Capture View is the tool for detailed analysis and editing of packets. You can view the data in the capture buffer or view previously-captured information that has been saved to a file. You can filter the data before viewing by using a display filter. Capture View contains a Packet Editor for editing packets.

Click the 📧 button on the Detail View toolbar to access Capture View. Use the green arrow buttons on the Capture View toolbar to move through the listed items. Capture View also opens automatically when you open a capture file (file with .CAP extension). If opening a large capture file or buffer, a window will display showing the progress of decoding packets.

The initial Capture View display provides a protocol decode of all packets. Other views of captured information are available from the Capture View toolbar. Although similar to the Monitoring View toolbar buttons, the graphs and charts displayed by using the Capture View Toolbar Buttons display detail information about the packets decoded from the capture buffer only. Table data in these other views is grayed to indicate that it is a capture view, not a view of real-time data.

The initial **Capture View** window is divided into three parts or "panes." Capture View shows a synopsis of all captured packets, provides a breakdown of the elements of the packet by protocol, and shows the hex and ASCII values for all characters in the packet. The three panes of the window can be sized any way you like. Click and drag the bars separating the panes to resize them. Use the F11 function key to zoom in on any of the three panes.

Summary Pane

The Summary Pane shows a summary of all packets. Each line in the summary pane is a summary of one packet. Clicking on a packet selects it and displays its detailed protocol breakdown (decode) and its hex values in the remaining two panes of the window.

Detail Pane

The Detail Pane shows the values of the protocol elements associated with each protocol. For example, for the Data Link Control the values for the source address, destination address, and packet length are shown. Single-clicking on a value highlights the value in both the Detail Pane and the Hex Pane.

Hex Pane

The Hex Pane shows the hex and ASCII values for all the bytes in the packet. Single clicking on a value highlights the value in both the Detail Pane and the Hex Pane.

Configuring the Capture View Display

You can customize the display of fields in the Capture View window. Select **Display** from the **Configuration** → **Capture View Options** menu. Choose the items you want displayed from the dialog box. See the "Capture View Display Options" section on page 4-2 for complete information on setting up capture view display options.

A unique color can be used to display packets of each different protocol layer. Set color coding or change color associations from the **Configuration** menu. Choose the **Protocol Color Coding** tab from the **System Settings** menu option. See "Appendix D" for a list of OPV-PE's default protocol color codes.

If you have special decoding or display needs for non-standard protocols, see the "Advanced Configuration" section in Chapter 4 for information on assigning protocol parsers and assigning names to protocols.

Creating Filters from Capture View

From the detail pane of the Capture View window, you can copy the contents of any field to create a Capture or Display filter. Click the right mouse on the field you want to filter on. Selections for copy to a capture or display filter appear. Select the option, and the **Create/Modify Filter** window appears with the field values inserted in the display. See Chapter 7 for more complete information on creating filters.

Exporting and Printing Decodes

You can export packet decode information to another source. You can also print a range of frames in a capture file or in the capture buffer to a text file. Frames can be saved in a variety of formats. See "Export Utilities" in Chapter 12 for more information.

Packet Editor

The Packet Editor can be used to modify the contents of packets when in Capture View. The editor provides two views of packets, detail view and hex view. Edits can be made within either view. Double-click on a packet in the Summary Pane of Capture View to edit a packet.

The editor must be enabled for use. To enable the Packet Editor, check **Enable Packet Edit** from the **Configuration → Capture View Options** menu.

Table 6-4 shows the buttons that are available within the Packet Editor:

Table 6-4. Packet Editor Buttons

Button	Description/Action
Auto CRC	Causes the 4-byte CRC error check value to be automatically calculated and written to the frame. With this option selected, creating frames with a bad CRC is not possible.
Compute CRC	Inserts the correct CRC error check value for the frame. You can use this option to create frames with or without correct CRC error check values.
Set Size	Sets the size of the packet. The current size of the packet is displayed for reference. Packet sizes from 8 to 1518 bytes are allowed.
Decode	Takes the values entered in the **Hex View** window of the Packet Editor, decodes the packet, and displays the resulting decode in the **Decode View** window.
Undo	Undo the last editing action. Only one level of undo is supported.
OK	Save edits.
Cancel	Leave the editor without saving changes.

Editing in Decode View

Editing in decode view allows you to edit packets without remembering offsets. Click on a field. A dialog box pops up showing the current value for the field and asks for a new value. The dialog box for each field is slightly different. Most dialog boxes can display and allow you to enter hexadecimal or decimal values. Some contain a **Use little-endian bit** order check box if bit order swapping is required. Changes made in decode view are automatically reflected in hex view.

Editing in Hex View

Edits are made in hex view by placing the cursor at a location and overwriting the current values. You can also paste (Ctrl + V) the contents of the paste buffer into a location. Values are always overwritten starting at the current cursor location in hex view so offsets remain correct.

Press the **Decode** button to display edits made in hex view in the decode view. Note that changes to the decode view are not automatic. This provides the option of creating error packets that can't be decoded properly.

Data Views

Ring Statistics View (Token Ring Only)

From Detail View, click on the [RS] button to open a window with Ring Statistics View. This view is available only if the Token Ring protocol is used by the resource. Ring Statistics View is not available from Summary View.

Ring Statistics View is available as two different tables. Click on the tabs at the bottom of the window to switch the view. Ring Statistics View is not available as a chart.

The Ring Stations tab shows all ring stations discovered in the local ring. Use this table to determine which stations are in the local ring, determine the ring station order, and discover which stations are Ring Error Monitors, Configuration Report Servers, or Ring Parameter Servers.

The Rings tab shows all rings discovered in the network with the time stamp of the first time that traffic from the ring was encountered on the network. Rings are rediscovered and time stamps changed if the connection is lost and then reestablished between OPV-PE and the local ring.

Rings and ring stations are listed as they are discovered. Click on the Ring Order or the Ring Number columns to sort the rings in ascending or descending order. The tables are updated approximately every 7 seconds.

MAC Statistics View (Rx)

From Detail View, click on the [▦] button to open a window with MAC Statistics View for capture. From Summary View, set the view preferences to **MAC Statistics (Rx)** to see this view in the first tab.

MAC Statistics View for capture shows module activity and counters during capture. It provides a visual reference for what a resource is doing. Counters are incremented as the resource captures packets. This view also provides general information about the resource.

The MAC Statistics View in capture mode is shown in Figure 6-1.
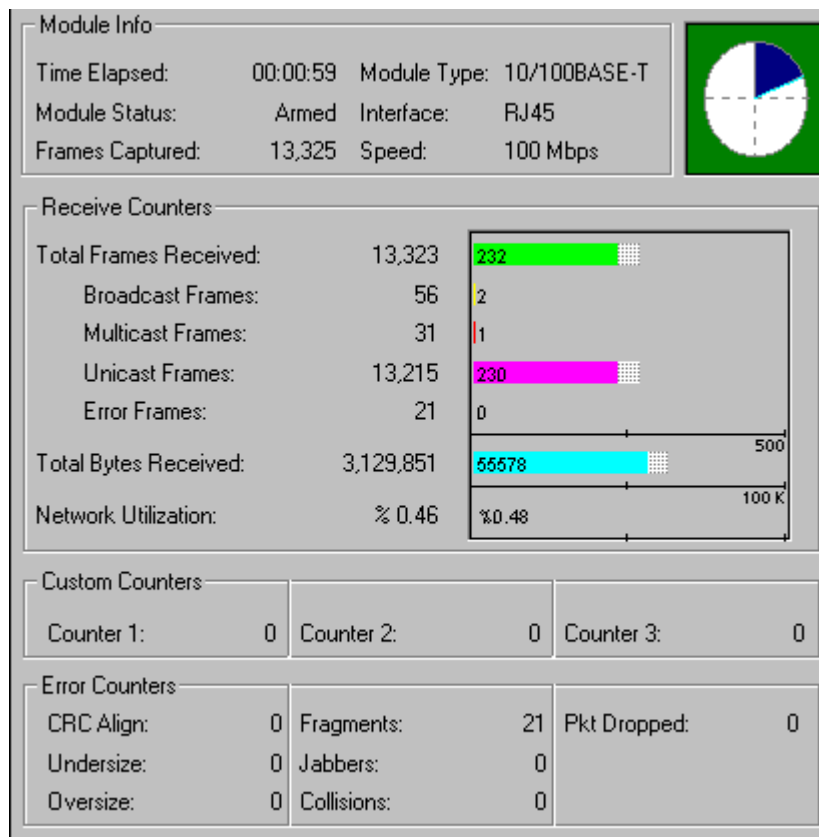
Figure 6-1. MAC Statistics View (Capture)

MAC Statistics View (Tx)

From Detail View, click on the ⊞ button to open a window with MAC Statistics View for transmit. From Summary View, set the view preferences to **MAC Statistics (Tx)** to see this view in the first tab.

MAC Statistics View also shows module activity during transmit. It provides a visual reference for module activity. The module identifier and the current mode are displayed in the window title bar. Counters are incremented as the module performs transmit functions.

The MAC Statistics View in transmit mode is shown in Figure 6-2.
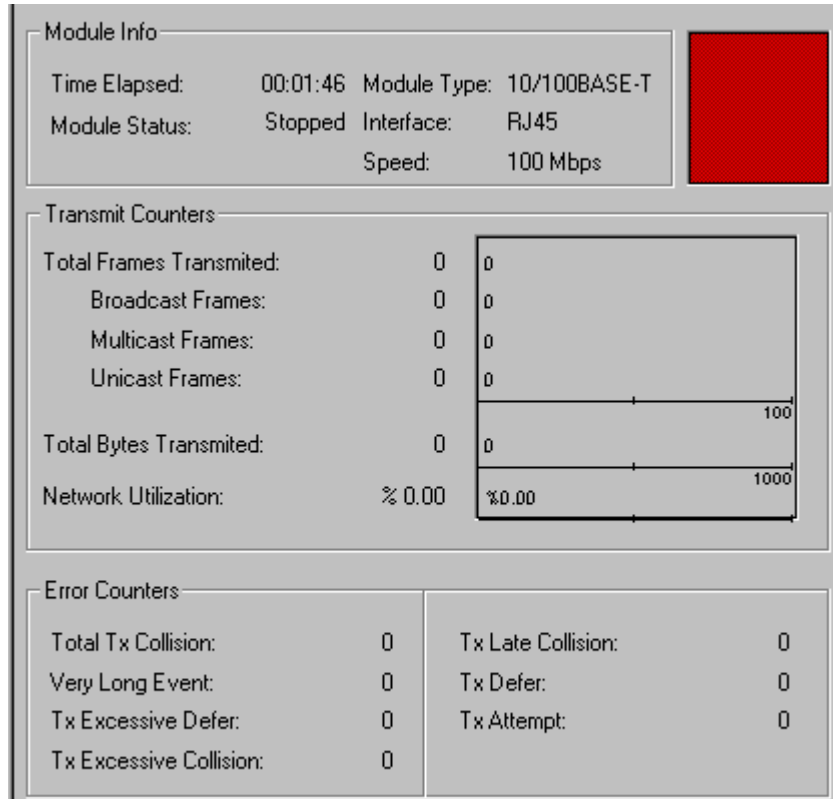
Figure 6-2. MAC Statistics View (Transmit)

Frame Size Distribution View

Frame Size Distribution View is available as a chart or a table. The chart can be toggled between a pie chart and a bar graph.

From Detail View, click on the ≡ button to open a window with Frame Size Distribution View. From Summary View, set the view preferences to **Frame Size Distribution** to see this view in the first tab.

For both the chart and the table, each range of frame sizes is expressed as a percentage of the total number of frames counted.

When using CMM2 or GAM modules, frame sizes of less than 64 bytes are not counted or displayed in Frame Size Distribution view. When using an NDIS module, the byte count in Frame Size Distribution view includes the 4 bytes of the Frame Check Sequence; however, for other views, these 4 bytes are not counted for each packet. Therefore, the total-byte counters in other views will be different than total-byte counters in Frame Size Distribution view.

Table 6-5. Frame Size Distribution View, Frame Size Statistics

Frame Statistic	Description
Frame Size (Bytes)	Size of captured frames, in bytes
No. of Frames	Number of captured frames that are of this frame size
Percentage	Percentage of all captured frames that are of this frame size

Protocol Distribution View

From Detail View, click on the **▉** button to open a window with Protocol Distribution View. From Summary View, set the view preferences to **Protocol Distribution** to see this view in the first tab.

GMM devices do not support this view in monitor mode.

Protocol Distribution View is available as a chart or a table. Protocol Distribution View shows the distribution of major network protocol types.

Chart

Protocol Distribution as a chart can be viewed in many different ways, depending on the buttons selected in the view. There are three types of buttons:

- **Protocol Buttons** select the types of protocol distribution you want to see. There are four protocol buttons that change the protocols you are viewing in the graph.

- **Frame/Byte Buttons** select to view the distribution by byte count or frame count, or can be used to select distribution relative to network capacity. There are three buttons that control how the protocols are counted when displayed in the graph

- **Display Buttons** control the display of information. There are three buttons that control the display only.

The following tables list and describe these buttons.

Table 6-6. Protocol Distribution View, Chart Buttons - Protocols

Chart Button	Description/Action
NET	Shows percentages of all packets by network layer protocol type, such as IP and IPX.
IP	Shows percentages of other protocols used within IP packets only.
IPX	Shows percentages of other protocols used within IPX packets only.
All	Shows percentages of all packets by application.

Table 6-7. Protocol Distribution View, Chart Buttons - Packets

Chart Button	Description/Action
Protocol Buttons	Selects the types of protocol distribution you want to see. There are four protocol buttons that change the protocols you are viewing in the graph:
	NET Shows percentages of all packets by network layer protocol type, such as IP and IPX.
	IP Shows percentages of other protocols used within IP packets only.
	IPX Shows percentages of other protocols used within IPX packets only.
	MoIP Shows percentages of multimedia protocols used.
	All Shows percentages of all packets by application.
Frame/Byte Buttons	Selects to view the distribution by byte count or frame count, or can be used to select distribution relative to network capacity. There are three buttons that control how the protocols are counted when displayed in the graph:
	Frm Counts by frame and displays percentages relative to the total number of frames counted.
	Abs Bts Counts by byte and displays percentages compared to the total network capacity.
	Rel Bts Counts by byte and displays percentages relative to the total number of bytes counted.
Display Buttons	Controls the display of information. There are three buttons that control the display only:
	BAR Display distributions as a bar graph.
	PIE Display distributions as a pie chart.
	‖ Pause the display. When pressed again, counters resume real-time update.

The NET and ALL buttons shows percentage breakdowns for all packets. The IP and IPX buttons show the percentages of only those packets that can be identified as containing IP or IPX information respectively.

Table 6-8. Protocol Distribution View, Graph Type (Chart or Pie) Buttons

Display Button	Description/Action
BAR	Display distributions as a bar graph.
PIE	Display distributions as a pie chart.
‖	Pause the display. When pressed again, counters resume real-time update.

Table

Protocol Distribution View as a table shows frame and byte counts by protocol.

Table 6-9. Protocol Distribution View, Table Column Descriptions

Table Column	Description
Protocol Name	Name of a network protocol (i.e., ARP, IP, IPX, etc.)
Total Frames	Total number of captured frames that are associated with a particular protocol
Rel % Frames	Percentage of all frames captured that are associated with a particular protocol
Total Bytes	Total number of captured bytes that are associated with a particular protocol
Rel % Bytes	Percentage of all bytes captured that are associated with a protocol
Abs % Bytes	Percentage of network capacity (measured in bytes) that are associated with a protocol

Utilization/Error View

Utilization/Error View is a simple strip chart that plots points for network utilization over time.

The scale for network utilization changes on-the-fly when a new peak percentage is reached. The time scale also scales automatically as the resource is monitored over time. The graph has an optional watermark showing the highest utilization point. The errors plotted on the graph are the total number of CRC and Alignment errors.

From Summary View, set the view preferences to **Utilization/Error** to see this view in the first tab. From Detail View, click on the **Capture** button or the **Transmit** button to open a window with the **Utilization** strip chart. From Detail View, the **Utilization/Error** chart is presented with the tables of transmit or receive counters.

Host Table View

From Detail View, click on the button to open a window with Host Table View. From Summary View, set the view preferences to **Host Table** to see this view in the first tab.

Host Table View is available as a chart showing the ten MAC stations with the most traffic or as a table showing all MAC stations. Click on the tab at the bottom of the window to select **Table** or **Chart**.

GMM devices do not support this view in monitor mode.

The station address and name are provided in the table or chart. If a OPV-PE name table exists with an address-to-name entry for this station, the **Station Name** field will be the station name in the name table. If no entry in a OPV-PE name table exists, the name of the **Station Name** field will be the vendor identifier followed by the last 6 bytes of the station address.

Chart

Host Table View as a chart shows only ten MAC stations. The ten stations displayed are those transmitting the largest relative percentage of frames. The chart can be customized to show the "top ten" stations based on a different station information field.

Table

Host Table View as a table shows network activity from the view of MAC stations. The table lists statistics for all stations found. The table can be customized to include other columns of information, or to delete columns you don't want to see. Table columns listed in italics are the default Host Table View columns.

Press the right mouse button on any table entry to create a filter using the selected MAC station. See Chapter 7 for information on filters.

Table 6-10. Host Table View, Table Column Descriptions

Table Column	Description
MAC Station Name	Name of the MAC station
MAC Station Address	MAC station address
Frames In	Number of frames received by the MAC station
Rel % Frames In	Percentage of frames received by this MAC station relative to the total number of frames
Frames Out	Number of frames sent by the MAC station
Rel % Frames Out	Percentage of frames sent by this MAC station relative to the total number of frames
Bytes In	Number of bytes received by the MAC station
Rel % Bytes In	Percentage of bytes received by this MAC station relative to the total number of bytes
Abs % Bytes In	Percentage of bytes received by this MAC station relative to the total network capacity (measured in bytes)
Avg. Size In	Average number of bytes contained within frames received by the MAC station

Table 6-10. Host Table View, Table Column Descriptions (continued)

Bytes Out	Number of bytes sent by the MAC station
Rel % Bytes Out	Percentage of bytes sent by this MAC station relative to the total number of bytes
Abs % Bytes Out	Percentage of bytes sent by this MAC station relative to the total network capacity (measured in bytes)
Errors Out	Number of transmittal errors generated by the MAC station
Broadcast Out	Number of broadcast frames generated by the MAC station
Multicast Out	Number of multicast frames generated by the MAC station

Network Layer Host Table View

From Detail View, click on the 🎛 button to open a window with Network Layer Host Table View. From Summary View, set the view preferences to **Network Layer Host Table** to see this view in the first tab.

GMM devices do not support this view in monitor mode.

Network Layer Host Table View is available as a chart showing the ten network stations with the most traffic or as a table showing all network stations. Click on the tab at the bottom of the window to select **Table** or **Chart**.

The station address and name are provided in the table or chart. The name and address will be the same if OPV-PE does not have a name table with an address-to-name correspondence for this station.

Chart

Network Layer Host Table View as a chart shows only ten network stations. The ten stations displayed are those transmitting the largest relative percentage of frames. The chart can be customized to show the "top ten" stations based on a different station information field.

Table

Network Layer Host Table View as a table shows network activity from the view of network stations. The table lists statistics for all stations found. The table can be customized to include other columns of information. Table columns listed in italics are the default Network Layer Host Table View columns.

Press the right mouse button on any table entry to create a filter using the selected network layer host. See Chapter 7 for information on filters.

Table 6-11 describes the table columns within the Network Layer Host Table View.

Table 6-11. Network Layer Host Table View, Table Column Descriptions

Table Column	Description
Network Station Name	Name of the network station
Network Station Address	Network layer address
VLAN Id	Decimal number of the virtual LAN. Virtual LANs using Cisco's ISL protocols are the only virtual LANs recognized at this time.
Frames In	Number of frames received by the network station
Rel % Frames In	Percentage of frames received by this network station relative to the total number of frames
Frames Out	Number of frames sent by the network station
Rel % Frames Out	Percentage of frames sent by this network station relative to the total number of frames
Bytes In	Number of bytes received by the network station
Rel % Bytes In	Percentage of bytes sent by this network station relative to the total number of bytes
Abs % Bytes In	Percentage of bytes received by this network station relative to the total network capacity (measured in bytes)
Avg. Size In	Average number of bytes contained within frames received by the network station
Bytes Out	Number of bytes sent by the network station
Rel % Bytes Out	Percentage of bytes sent by this network station relative to the total number of bytes
Abs % Bytes Out	Percentage of bytes sent by this network station relative to the total network capacity (measured in bytes)
Avg. Size Out	Average number of bytes in the frames sent by the network station
Non-Unicast Out	Number of non-unicast frames generated by the network station

Application Layer Host Table View

From Detail View, click on the ▦ button to open a window with Application Layer Host Table View. From Summary View, set the view preferences to **Application Layer Host Table** to see this view in the first tab.

GMM devices do not support this view in monitor mode.

Application Layer Host Table View is available as a chart showing the ten network stations with the most traffic or as a table showing all network stations.

The network station address and name are provided in the table or chart. The name and address will be the same if OPV-PE does not have a name table with an address-to-name correspondence for this station.

Chart

Application Layer Host Table View as a chart shows only ten applications over network stations. The ten stations displayed are those transmitting the largest relative percentage of frames. The chart can be customized to show the "top ten" stations based on a different station information field.

Table

Application Layer Host Table View as a table shows network activity from the view of application protocols running on network stations. The table lists all application protocols found on each network station. Each network station may have many application protocols in use. The table lists statistics of all applications within the stations found. The table can be customized to include other columns of information. Table columns listed in italics are the default Application Layer Host Table View columns.

Press the right mouse button on any table entry to create a filter using the selected application layer host. See Chapter 7 for information on filters.

Table 6-12. Application Layer Host Table View, Table Column Descriptions

Table Column	Description
Network Station Name	Name of the network station
Network Station Address	Address of a network station in IP address format
VLAN Id	Decimal number of the virtual LAN. Virtual LANs using Cisco's ISL protocols are the only virtual LANs recognized at this time.
Application	Name of the application protocol
Frames In	Number of frames received by the network station for this application
Rel % Frames In	Percentage of frames received by this network station for this application relative to the total number of frames
Frames Out	Number of frames sent by the network station for this application
Rel % Frames Out	Percentage of frames sent by this network station for this application relative to the total number of frames
Bytes In	Number of bytes received by the network station for this application
Rel % Bytes In	Percentage of bytes received by this network station for this application relative to the total number of bytes

Table 6-12. Application Layer Host Table View, Table Column Descriptions (continued)

Abs % Bytes In	Percentage of bytes relative to the total network capacity (measured in bytes) received by this network station for this application
Avg. Size In	Average number of bytes contained within frames received by the network station for this application
Bytes Out	Number of bytes sent by the network station for this application
Rel % Bytes Out	Percentage of bytes sent by this network station for this application relative to the total number of bytes
Abs % Bytes Out	Percentage of bytes sent by this network station for this application relative to the total network capacity (measured in bytes)
Average Size Out	Average number of bytes contained in frames sent by the network station for this application
Non-Unicast Out	Number of non-unicast frames generated by the network station for this application

Host Matrix View

From Detail View, click on the 🔲 button to open a window with Host Matrix View. From Summary View, set the view preferences to **Host Matrix** to see this view in the first tab.

GMM devices do not support this view in monitor mode.

Host Matrix View is available as a chart showing the ten MAC conversations with the most traffic or as a table showing all MAC conversations. Click on the tab at the bottom of the window to select **Table** or **Chart**.

The station addresses and names are provided in the table or chart. If a OPV-PE name table exists with an address-to-name entry for this station, the **Station Name** field will be the station name in the name table. If no entry in a OPV-PE name table exists, the name of the **Station Name** field will be the vendor name followed by the last 6 bytes of the station address.

Chart

Host Matrix View as a chart shows only ten MAC conversations. The ten conversations displayed are those transmitting the largest relative percentage of frames. The chart can be customized to show the "top ten" conversations based on a different information field.

Table

Host Matrix View as a table shows network activity from the view of MAC station pairs. The table lists statistics for all pairs found. The table can be customized to

include other columns of information. Table columns listed in italics are the default Host Matrix View columns.

Press the right mouse button on any table entry to create a filter using the selected MAC layer conversation. See Chapter 7 for information on filters.

Table 6-13. Host Matrix View, Table Column Descriptions

Table Column	Description
MAC Station Name 1	Name of a MAC station
MAC Station Address 1	MAC station address
MAC Station Name 2	Name of a second MAC station
MAC Station Address 2	Address of a second MAC station
Frames 1—>2	Number of frames sent from MAC Station 1 to MAC Station 2
Frames 2—>1	Number of frames sent from MAC Station 2 to MAC Station 1
Frames 1<—>2	Number of frames sent in either direction between MAC Station 1 and MAC Station 2
Rel % Frames 1<—>2	Percentage of frames sent in either direction between MAC Station 1 and MAC Station 2 relative to the total number of frames
Bytes 1—>2	Number of bytes sent from MAC Station 1 to MAC Station 2
Average size 1—>2	Average size of the frames sent from MAC Station 1 to MAC Station 2
Bytes 2—>1	Number of bytes sent from MAC Station 2 to MAC Station 1
Average Size 2—>1	Average size of the frames sent from MAC Station 2 to MAC Station 1
Bytes 1<—>2	Number of bytes sent in either direction between MAC Station 1 and MAC Station 2
Rel % Bytes 1<—>2	Percentage of bytes sent in either direction between MAC Station 1 and MAC Station 2 relative to the total number of bytes
Abs % Bytes 1<—>2	Percentage of bytes sent in either direction between MAC Station 1 and MAC Station 2relative to the total MAC capacity (measured in bytes)
Average Size 1<—>2	Average size of the frames sent in either direction between MAC Station 2 and MAC Station 1

Network Layer Matrix View

From Detail View, click on the 🖳 button to open a window with Network Layer Matrix View. From Summary View, set the view preferences to **Network Layer Matrix** to see this view in the first tab.

GMM devices do not support this view in monitor mode.

Network Layer Matrix View is available as a chart showing the ten network conversations with the most traffic or as a table showing all network conversations. Click on the tab at the bottom of the window to select **Table** or **Chart**.

The station addresses and names in the conversation are provided in the table or chart. The name and address are the same if OPV-PE does not have a name table with address-to-name correspondences.

Chart

Network Layer Matrix View as a chart shows only ten network conversations. The ten conversations displayed are those transmitting the largest relative percentage of frames. The chart can be customized to show the "top ten" conversations based on a different information field.

Table

Network Layer Matrix View as a table shows network activity from the view of network station pairs. The table lists statistics for all pairs found. The table can be customized to include other columns of information. Table columns listed in italics are the default Network Layer Matrix View columns.

Press the right mouse button on any table entry to create a filter using the selected network layer conversation. See Chapter 7 for information on filters.

Table 6-14. Network Layer Matrix View, Table Column Descriptions

Table Column	Description
Net Station Name 1	Name of a network station
Net Station Address 1	Network layer address of a network station
Net Station Name 2	Network layer address of a second network station
Net Station Address 2	Address of a second network station in IP address format
VLAN Id	Decimal number of the virtual LAN. Virtual LANs using Cisco's ISL protocols are the only virtual LANs recognized at this time.
Frames 1—>2	Number of frames sent from Network Station 1 to Network Station 2
Frames 2—>1	Number of frames sent from Network Station 2 to Network Station 1
Frames 1<—>2	Number of frames sent in either direction between Network Station 1 and Network Station 2
Rel % Frames 1<—>2	Percentage of frames sent in either direction between Network Station 1 and Network Station 2 relative to the total number of frames
Bytes 1—>2	Number of bytes sent from Network Station 1 to Network Station 2

Table 6-14. Network Layer Matrix View, Table Column Descriptions (continued)

Average size 1—>2	Average size of the frames sent from Network Station 1 to Network Station 2
Bytes 2—>1	Number of bytes sent from Network Station 2 to Network Station 1
Average Size 2—>1	Average size of the frames sent from Network Station 2 to Network Station 1
Bytes 1<—>2	Number of bytes sent in either direction between Network Station 1 and Network Station 2
Rel % Bytes 1<—>2	Percentage of bytes sent in either direction between Network Station 1 and Network Station 2 relative to the total number of bytes
Abs % Bytes 1<—>2	Percentage of bytes sent in either direction between Network Station 1 and Network Station 2 relative to the total network capacity (measured in bytes)
Average Size 1<—>2	Average size of the frames sent in either direction between Network Station 2 and Network Station 1

Application Layer Matrix View

From Detail View, click on the ⊞ button to open a window with Application Layer Matrix View. From Summary View, set the view preferences to **Application Layer Matrix** to see this view in the first tab.

GMM devices do not support this view in monitor mode.

Application Layer Matrix View is available as a chart showing the top ten application conversations or as a table showing all application conversations. Click on the tab at the bottom of the window to select **Table** or **Chart**.

The station addresses and names in the conversation are provided in the table or chart. The name and address are the same if OPV-PE does not have a name table with address-to-name correspondences.

Chart

Application Layer Matrix View as a chart shows only ten applications over network conversations. The ten conversations displayed are those transmitting the largest relative percentage of frames. The chart can be customized to show the "top ten" conversations based on a different information field.

Table

Application Layer Matrix View as a table shows network activity from the view of applications over network station pairs. The table lists statistics for applications within all station pairs found. The table can be customized to include other columns

of information.Table columns listed in italics are the Application Layer Matrix View default columns.

Press the right mouse button on any table entry to create a filter using the selected network layer conversation. See Chapter 7 for information on filters.

Table 6-15. Application Layer Matrix View, Table Column Descriptions

Table Column	Description
Net Station Name 1	Name of a network station
Net Station Address 1	Network layer address of a network station
Net Station Name 2	Network layer address of a second network station
Net Station Address 2	Address of a second network station in IP address format
Application	Name of the application running over the network station pair
VLAN Id	Decimal number of the virtual LAN. Virtual LANs using Cisco's ISL protocols are the only virtual LANs recognized at this time. Click on the VLAN ID to see a network station or network conversation view for that VLAN.
Frames 1—>2	Number of frames sent from Network Station 1 to Network Station 2 for this application
Frames 2—>1	Number of frames sent from Network Station 2 to Network Station 1 for this application
Frames 1<—>2	Number of frames sent in either direction between Network Station 1 and Network Station 2 for this application
Rel % Frames 1<—>2	Percentage of frames sent in either direction between Network Station 1 and Network Station 2 for this application relative to the total number of frames
Bytes 1—>2	Number of bytes sent from Network Station 1 to Network Station 2 for this application
Average size 1—>2	Average size of the frames (in bytes) sent from Network Station 1 to Network Station 2 for this application
Bytes 2—>1	Number of bytes sent from Network Station 2 to Network Station 1 for this application
Average Size 2—>1	Average size of the frames (in bytes) sent from Network Station 2 to Network Station 1 for this application
Bytes 1<—>2	Number of bytes sent in either direction between Network Station 1 and Network Station 2 for this application

Table 6-15. Application Layer Matrix View, Table Column Descriptions (continued)

Rel % Bytes 1<—>2	Percentage of bytes sent in either direction between Network Station 1 and Network Station 2 for this application relative to the total number of bytes
Abs % Bytes 1<—>2	Percentage of bytes sent in either direction between Network Station 1 and Network Station 2 for this application relative to the total network capacity (measured in bytes)
Average Size 1<—>2	Average size (in bytes) of the frames sent in either direction between Network Station 1 and Network Station 2 for this application

VLAN View

From Detail View, click on the 🔲 button to open a window with VLAN View. From Summary View, set the view preferences to **VLAN** to see this view in the first tab.

GMM devices do not support this view in monitor mode.

VLAN View is available as a table showing statistics or as a chart showing the ten virtual LANs with the most traffic. Click on the tab at the bottom of the window to select **Table** or **Chart**. The only virtual LAN protocol recognized at this time is Cisco's ISL protocol.

Chart

VLAN View as a chart shows only ten VLANs. The ten VLANs displayed are those transmitting the largest relative percentage of frames. The chart can be customized to show the "top ten" VLANs based on a different information field.

Table

VLAN View as a table shows network activity from the view of virtual LAN traffic. The table lists statistics for all VLANs found. The table can be customized to include other columns of information. You can click on any VLAN ID and see a Network Layer Host Table View or a Network Conversation Matrix View for that VLAN. Table columns listed in italics are the default VLAN View columns.

Table 6-16. VLAN View, Table Column Descriptions

Table Column	Description
VLAN Id	Number (in decimal) of the virtual LAN. Click on the VLAN ID to see network layer and application layer host and matrix tables of that VLAN.
VLAN Type	Indicates the VLAN type, IEEE 802.1Q or Cisco ISL

Table 6-16. VLAN View, Table Column Descriptions (continued)

Frames	Total frames captured that are associated with a VLAN
Rel % Frames	Percentage of all frames captured that are associated with a VLAN
Bytes	Total bytes captured that are associated with a VLAN
Rel % Bytes	Percentage of all bytes captured that are associated with a VLAN
Abs % Bytes	Percentage of the total network capacity in bytes that are associated with a VLAN
Total Bytes	Total bytes captured
Highest Priority Observed	For any VLAN ID (a row in the table), all packets do not necessarily have the same priority number.The highest network priority observed is displayed in this field.

Address Mapping View

From Detail View, click on the ![icon] button to open a window with Address Mapping View. From Summary View, set the view preferences to **Address Map View** to see this view in the first tab.

GMM devices do not support this view in monitor mode.

Address Mapping View is available as a table showing all associations between MAC station names and addresses and network station names and addresses. Address Mapping View is not available as a chart. Use this table if you need to determine what MAC stations are associated with what network stations.

Table 6-17. Address Map View, Table Column Descriptions

Table Column	Description
MAC Station Name	Name of the MAC station
MAC Station Address	MAC station address
Network Station Name	Name of the network station
Network Station Address	Network layer address of the network station

Packet Summary View

Packet Summary View shows a real-time protocol decode. Packets received are decoded and the result of the decode is displayed.

GMM devices do not support this view in monitor mode.

The packets scroll up the screen as they are decoded. A unique color can be used to display packets of each different protocol layer.

From Summary View, set the view preferences to **Packet Summary** to see this view in the first tab. From Detail View, select **Packet Summary** from the **Monitor View** menu to open a window with the Packet Summary View.

Duplicate Address View (Expert Analysis only)

From Detail View, click on the 🔍 button to open a window with Duplicate Address View. You can also see this view from Summary View. To see Duplicate Address View, set the view preferences to Duplicate Address View to this view in the first tab.

GMM devices do not support this view in monitor mode.

Duplicate Address View is available as a table showing all duplicate network addresses. MAC station names and addresses and network station names and addresses. Duplicate Address View is not available as a chart. Use this table if you need to determine what stations may have duplicate addresses.

If you are monitoring a remote device, you must open one of the host tables for that remote device for new duplicate addresses to show in Duplicate Address View.

Table 6-18. Duplicate Address View, Table Column Descriptions

Table Column	Description
Network Station Name	Name of the network station
Network Station Address	Network layer address of the network station (duplicate)
MAC Station Name	Name of the MAC station
MAC Station Address	Address of the MAC station
VLAN ID	Decimal number of the virtual LAN. Virtual LANs using Cisco's ISL protocols are the only virtual LANs recognized at this time. Click on the VLAN ID to see a network station or network conversation view of that VLAN.

Expert View (Expert Analysis only)

From Detail View, click on the 🔲 button to open a window with Expert View. From Summary View, set the view preferences to Expert View to see this view in the first tab.

GMM devices do not support this view in monitor mode.

Multiple tables are available in Expert View. Select a layer on the left and tab on the bottom to create the view you want. Expert View is not available as a chart. Refer to the chapter on the Expert System for complete information on Expert Views.

Application Response Time View (Expert Analysis only)

From Detail View, click on the ⬚ button to open a window with Application Response Time View. From Summary View, set the view preferences to Application Response Time View to see this view in the first tab.

GMM devices do not support this view in monitor mode.

Application Response Time View is available as a table showing connection time and connection number information about application protocols. Application response time view is not available as a chart. Use this table if you want to find out which applications are responding very slowly in the network.

Table 6-19. Application Response Time View, Column Descriptions

Table Column	Description
Server Name	Name or IP address of the transmitting server.
Protocol	Name of the application protocol discovered
Minimum Time	Shortest time taken for the application to make a connection
Maximum Time	Longest time taken for the application to make a connection
Average Time	Average time taken for the application to make a connection
Connections	Number of connections processed for this application

To calculate application response time, OPV-PE causes a stimulus packet to be transmitted so the application layer round trip time can be assessed. However, the packet cannot be sent if the analyzer device used by OPV-PE is connected through a tap device.The application response time will only work if the transmit port of the analyzer is directly connected to a switch port or device.

VoIP View (VoIP software only)

From Detail View, click on the ⬚ button to open a window with VoIP views. Initially, the All Calls table displays. VoIP views are not available from Summary View.

GMM devices do not support this view in monitor mode.

Multiple tables are available in VoIP View. You can view all calls, subsets of calls filtered by protocol or by a QoS metric, single call details, and channel details. Refer to the chapter on VoIP for complete information on VoIP Views.

Hints and Tips for Using Views

- When viewing a table, single click on columns to sort the table data. Click on a column header to list rows in descending order of the values for that column. Click again on a column header and rows will be sorted this time in ascending order. Click on another column header and rows will be sorted by the values in that column.

- To get the "top ten" chart based on a different field, select the Table tab and click on the field to sort the data. Click on the Chart tab to see the new graph.

- View the "bottom ten" for any field by reversing the sort order in a table. Every click on a column header toggles the sort between ascending and descending order for that column. The sort of data in ascending order is not available as a chart.

- A **Pause** button is available on some charts and tables to freeze the display. Click the button again to resume display updating.

- The fields shown in some tables can be customized. Choose **View Options…** from the **View** menu in Detail View to change the columns that display for a table.

- There are many view windows you can open. Keep the number of open windows to a reasonable level to avoid confusion and conserve system resources.

- The Summary View allows only one type of monitoring view per resource. Go to Detail View to see multiple views per resource simultaneously.

- In charts, hold down both the right and left mouse button and move the mouse to rotate the 3D graphic view.

- Double-click with the left mouse button on the view displayed within Summary View to bring up the Detail View for that resource.

- Use **Print** from the **File** menu to print the graph or chart in the currently selected window.

- Cells within a table or an entire table can be exported to an Excel™ spreadsheet. Go to the table view and select the **Export** option from the **File** menu to export the entire table. Information is saved in CSV format which can be opened from Excel.

- Double-click on the MAC Statistics View in Detail View to bring up Capture View.

- Data in a chart will be sorted by the last sorted column in the corresponding table.

- Click the right mouse button on a table entry in Host Table, Network Table, Application Table, Host Matrix, Network Matrix, or Application Matrix view to bring up a menu for creating a filter. You'll get a choice of creating a capture or display filter. When you make a choice from the menu, the **Create/Modify Filter** window opens with the address(es) from the table entry in the address fields for creating a filter.

- From the Detail View pane of the Capture View window, you can copy the contents of any field to create a Capture or Display filter. Select the field with the left mouse and then click the right mouse. Selections for copy to capture or display filter appear. Select the option, and the **Create/Modify Filter** window appears.

- In Capture View, press the F11 key to zoom in on any of the three panes in the window. Press F11 again to restore the view to all three panes.

- To see which capture filter or transmit specification is associated with a particular resource, choose **Active TSP and Capture Filter** from the **Module** menu.

Chapter 7
Capture and Display Filters

For most data analysis operations, you'll want to look at only a subset of all data. Filters allow you to select and count data in just about any way you can imagine.

Capture filters allow you to capture a subset of the network data. Display filters allow you to view a subset of the data you have already captured. They can be used to refine your view of captured information. For example, you might choose to capture all packets sent/received by a specific IP network station. Later, you might decide you want to look at the data for specific types of packets that are flowing through the station. A display filter allows you to view this subset of captured data.

OPV-PE uses a layered approach to developing filters. If you want a simple filter, all filter options can be specified from a single window. However, if you need to create an advanced filter with multiple states and searches to refine exactly what you're looking for, OPV-PE supports a complete filtering language.

Example filters are provided to give you an idea of the types of filters that can be created. This section describes both Capture and Display Filters; the minor differences are noted in the text.

Getting Started with the Filter Interface

For most users, filters can be created and applied from a single window. The overview below describes a simple way to get started with the interface.

1. Select the resource you want to filter from the Resource Browser.

2. Press the **Detail View** ▦ button.

3. Press the **Create/Modify Capture Filter** ▧ button to bring up the **Filter Design** window.

4. Click on a pre-defined filter template from the **Available Filter Templates** box. The data pattern for the filter template you have selected will display in the **Current Filter Template Display** area. Suggestion: Try HTTP to collect HTTP traffic only.

5. Enter an address in the **Add Conversation to Filter Template** area and select the **Apply Conversation to Template** check box. Enter addresses by selecting their corresponding names in the name table.
   Suggestion: Try selecting one MAC station from the name table. You will now capture only HTTP traffic for a single station.

6. Press the **Save Custom Template** button. The newly-created filter template appears in the **Available Filter Templates** box.

7. Press the **Add** button. The filter template appears in the **Template Combination** box.

8. Press the **Load Filter** 🔽 button.

Once you are familiar with the basic steps and can create a subset of data within the capture buffer, you can look at the more complex features of the interface such as display filters, logic combinations, incrementing counters, and multi-state logic.

Creating Filters with Filter Templates

Simple filters can be created using one interactive screen called the **Filter Design** window. The **Filter Design** window is essentially the same for capture or display filters. See one of the filter examples for a picture of this window and information about its parts.

You can define a filter using a single filter template. There are two types of filter templates:

• **Pre-defined Filter Templates**
  A pre-defined filter template looks for a specific data pattern or a collection of data patterns. The filter template is supplied by OPV-PE and cannot be changed.

• **Custom Filter Templates**
  A custom filter template also looks for a specific data pattern or a collection of data patterns. You can base a custom filter template on a pre-defined filter template or directly enter all data patterns. The most common custom template uses a pre-defined template and adds a conversation or port number. You can also directly enter values at packet offsets in hexadecimal, decimal, or ASCII. Once you have created and saved a custom template, you can always access it in the **Available Filter Templates** box.

  • **Add Conversations to Custom Filter Templates**
    A conversation is a data pattern specific to the source and destination addresses, including the protocol type and the direction of traffic. The **Add Conversation to Filter Template** area in the display provides a convenient means of adding addresses to a custom filter template.

- **Add Port Numbers to Custom Filter Templates**
  A port is a data pattern specific to the source and destination port numbers, including the protocol type and the direction of traffic. The **Add Port to Filter Template** area in the display provides a convenient means of adding port numbers to a custom filter template.

There are three key steps to apply a filter template to a hardware resource:

1. After creating custom template, you must save it using the **Save Custom Template** button. This step is not required if you are using a pre-defined template.

2. You must add the template to the **Template Combination** box. Select the template and click on the **Add** button; the name of the template will appear in the **Template Combination** box.

3. You must use the **Load Filter** button so the filter as defined in the **FILTER CREATION** area is loaded to the hardware device.

Each Display or Capture filter applies only to the currently active resource. Once you have created and saved a unique filter template, you can access it from other resources.

A sample **Filter Design** window is shown below.

FILTER CREATION Area
(left side of window)

Template
Combination Box

Add Button (add Filter Template
to Template Combination box)

Template Description
Button

Filter Design
Toolbar
(see below)

Template Combination
Operator Buttons

Delete Custom
Template Button

Available Filter Templates Box

View Filter Button,
Bring Up Filter States
Design Window

Set Filter Actions,
Increment Custom
Counters

Add Port to
Template Area

Clear Template
Button

Packet Type,
Packet Size Filtering

Edit/Create Custom
Filter Template Area

Add Conversation to
Template Area

Bit-Level Filtering

Hex/Dec/ASCII Displays
of Offsets/Lengths

Save Custom
Template Button

Figure 7-1. Filter Design Window

Filter Design Toolbar Buttons (see Chapter 3 for complete descriptions)

Creates a new filter (blank window)   Loads filter to a device

Opens a previously saved filter   Disables filter

Saves a filter to a file   Filter window toggle
(brings up Filter States Design window)

Help button

Creating and Applying a Conversation

The **Add Conversation to Template** area of the **Filter Design** window provides a convenient way to add address byte patterns to a filter. The area consists of a protocol selection, frame type selection, two station addresses, a direction indicator, and an enable/disable check box. Refer to the table below for field definitions that comprise a conversation.

Table 7-1. Defining Conversations

Conversation Element	Description
Protocol	MAC, IP, IPX, or Atalk (AppleTalk)
Frame Type	All, EV2 (Ethernet II), SNAP, 8022 (IEEE 802.2), 8023 (IEEE 802.3), ISL, VLAN Frame type applies to network layer addresses only.
Station Address 1	Complete IP, IPX, MAC, or ATalk station address.
Traffic Direction Indicator	$<->$ Capture/Display all traffic between Station 1 and Station 2 $->$ Capture/Display only the traffic where Station 1 is the Source Address and Station 2 is the Destination Address $<-$ Capture/Display only the traffic where Station 2 is the Source Address and Station 1 is the Destination Address
Station Address 2	Complete IP, IPX, MAC, or ATalk station address.
Apply Conversation to Template check box	Enable (include) or Disable the conversation as part of the filter template.

Protocol and Frame Type

The protocol and the frame type are selected from pull-down boxes. OPV-PE automatically restricts you from entering combinations that make no sense.

OPV-PE will automatically set up the correct protocol and frame type when you select a station address from the name table.

Station Addresses

Station addresses can be entered directly or by clicking on the **Name** 🔲 button after either **Station Address** field. Clicking on either button brings up the current name table to select an address. The **Name Table** window shows all name and address associations, including the protocol and the frame type. The name and address associations displayed are those in the currently active name table. Double-clicking on a name table entry will load that name into the currently-selected **Station Address** field.

There are four station address types:

- MAC address – 12 hexadecimal digits.
  For example, 34FD34AA0001.

- IP dot notation address – 4 decimal numbers in the range of 0 to 255, separated by dots. For example, 12.235.96.2.

- IPX address – 20 hexadecimal digits (without port number) or 22 hexadecimal digits (with port number). For example, 34FD34AA0001000000A1.

- Atalk address - 2 decimal numbers separated by dots. The first can range from 0 to 65534 and the second from 0 to 255. For example 30234.123.

Note:

You will probably want to build a name table with the names and addresses of stations on your network. If you have a name table for your network, be sure to load the name table so names are available in the Name Table window.

If no value is entered for a **Station Address** field, all stations are captured. For example, if you set an address for Station 1, no address for Station 2, and set the direction to `->` all packets having Station 1 as the Source Address are captured, regardless of the Destination Address.

Use wildcards when specifying addresses to capture data on more than one station. An X used as a character for an address string means that any value will be accepted for that position; for example, `343F4AXXXXXX`.

Traffic Direction Indicator

The direction indicator allows you to select a direction between stations. You can filter for packets going from Station 1 to Station 2 (`->`), Station 2 to Station 1 (`<-`), or gather packets in either direction (`<->`).

Apply Conversation to Template Check Box

To apply the conversation to your filter, make sure that the **Apply Conversation to Template** check box is selected. Enabling the conversation will modify the data patterns used in the filter.

A single conversation is defined. If you want to use additional conversations, you can create an advanced filter or use wildcards as described above.

Creating and Applying a Port Number

OPV-PE provides a convenient way to add a port number to a filter. You specify port numbers for the filter by filling out the **Add Port to Template** area of the **Filter Design** window. This area consists of a protocol selection, frame type selection, a port number, a direction indicator, and an **Apply Port to Template** check box. Refer to the table below for field definitions that comprise a port number selection.

Table 7-2. Defining Port Numbers

Conversation Element	Description
Protocol	IP/UDP, IP/TCP
Frame Type	EV2 (Ethernet II), SNAP, ISL, VLAN Frame type applies to network layer addresses only.
Port Number	Decimal UDP or TCP port number.
Traffic Direction Indicator	<-> Capture/Display all traffic where the specified port is the source or the destination -> Capture/Display only the traffic where the specified port is the source <- Capture/Display only the traffic where the specified port is the destination
Apply Port to Template check box	Include or exclude the port specification as part of the filter template.

Selecting Filter Templates

A filter template contains the data patterns for creating the logical conditions that will be used as a test against incoming frames. To select a filter template, click on the template in the **Available Filter Templates** area and press the **Add** button, or double-click on the filter template. The filter template is added to the **Template Combination** box.

Filter templates are always assigned a name and that name is referenced in the template combination. Pre-defined filter templates are provided that can be used without modification, or you can define your own filter templates. See "Standard Filter Templates" in Appendix B for the filter templates supplied with OPV-PE. You cannot alter the pre-defined filter templates.

Most filter templates have a defined offset and pattern within a frame. However, one template has no specific offset and length (MatchAll). Some filter templates have predefined values, such as MAC_DA_Broadcast (FFFFFFFFFFFF).

Multiple Byte Patterns in Filter Templates

Filter templates can be "several templates in one." For example, HTTP, TELNET, and SNMP are provided as single filter templates, but they consist of both source and destination ports. In other words, the template itself contains an OR condition, and will capture a packet whether it appears in the offset for the source port or the offset for the destination port.

An example **Template Description** window is shown below. The HTTP port as the source or destination will be selected by the filter template. Two bit patterns are defined:

First Pattern			Second Pattern	
Offset	Pattern		Offset	Pattern
12	0800		12	0800
23	06		23	06
34	0050		36	0050
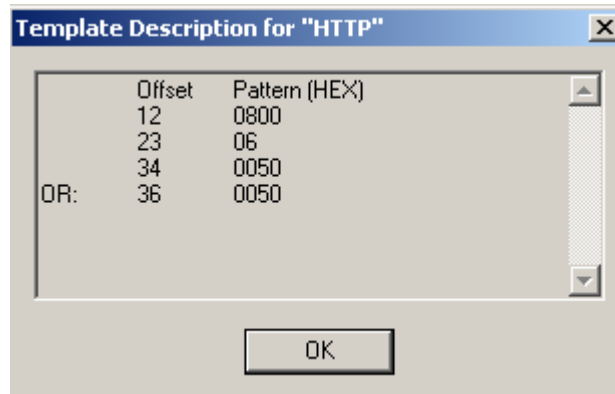
Figure 7-2. Template Description Window Showing a Macro Filter

Creating Custom Filter Templates

Custom filter templates are created from the **Filter Design** window. Custom filter templates display under `Custom_Templates` in the **Available Filter Templates** box of this window. Custom templates allow precise control over the information captured or displayed.

Custom templates are created by modifying a pre-defined template or by directly entering values in the correct offsets in the **Current Filter Template Display** area.

Custom Templates Based on Pre-Defined Templates

Custom filter templates can be created by selecting a pre-defined template and adding conversations or port numbers. For example, assume you want to filter HTTP packets going to or coming from a station. You could select the HTTP filter template and enter the station you want to filter on in the **Add Conversation to Template**

area. You then save the template. When you save a custom template, OPV-PE asks
for a custom template name. OPV-PE will assign a default name such as
`Template1` if no name is provided.

Once you create a filter template, its name will appear in the
`Custom_Templates` section of the **Available Filter Templates** box. Custom tem-
plates can be reused again and again once added to the list of templates. You must
use the **Add** button so the filter template name appears in the **Template Combination**
box for the template to be used in the current filter.

Custom Templates Based on Specification of Bit Patterns

You can create custom templates by entering values in the offsets within the **Current
Filter Template Display** area. The small fields in this area define the data patterns
that comprise a filter template. The offset defines the position within the packet to
start comparing the packet contents with the values in the pattern. If a match occurs,
then this portion of the condition is satisfied. The pattern can be specified as a deci-
mal, hexadecimal, or ASCII value.

Use the **Data Format** pull-down box on the right to specify if the pattern is in deci-
mal, hexadecimal, or ASCII. Use the **Offset Format** pull-down box to specify if the
column and row headers display in decimal or hexadecimal. Note that although you
can display the data in different formats, all formats use a byte boundary. Only byte
quantities can be entered or displayed.

Any specific value you create for filter templates can have "don't care" values. For
example, assume you're only looking for `FF34` in the first two bytes of the MAC
destination address. You could specify the values in your filter as `FF34XXXXXX`,
where X indicates you don't care about the values in the last three offsets. Note that
for IP addresses using decimal values you can only use X characters for complete
sub-addresses. For example, `128.XXX.2.2` is allowed, but `128.12X.2.2` is not
allowed.

The hex or decimal patterns display in black or magenta. The magenta color indi-
cates the bytes are a macro pattern, such as the logical OR of two different patterns,
or a conversation. Displays in magenta within the **Current Filter Template Display**
area do not provide a complete view of the filter template. The **Template Descrip-
tion…** information box provides complete details about any macro pattern. Use the
Template Description… button to see the exact offsets, patterns, and logical opera-
tors you have used to create the filter template. Many ASCII patterns have no corre-
sponding display character.

Use the **Template Description** button to see the exact offsets, patterns, and logical
operators you have used to create the filter template. See Figure 7-2 for an example
of this window.

Entering Values that Cross Byte Boundaries

Port values are generally understood as decimal numbers. For example, an NFS port is known as decimal 2049. Filter patterns are expressed as bytes and begin on byte boundaries. It takes two bytes to express a port number. Therefore, for port numbers you must convert the decimal number to a value that can be entered on a byte boundary. The example below shows how to enter NFS port 2049 in the filter window.

1. Take the port number (2049) and divide by 256. The result is 8 remainder 1. In IP "dot" notation, this could be expressed as "8.1".

2. Set the Data format pull-down box in the filter window to Decimal. Values in the Data pattern area will be entered in decimal.

3. Enter 8 in offset 34 and enter 1 in offset 35. Enter 8 in offset 36 and 1 in offset 37. This sets the filter for both source and destination port.

If a port number is a decimal value less than 256, then the value of the first byte of the port number is zero, and the second byte is the decimal port number. For example, for HTTP port 80, enter zero in offset 34 and 80 in offset 35.

The byte-boundary restriction applies to any other decimal number, such as a number in a data pattern, that you want to filter on. You must first convert it so the value is expressed using byte boundaries.

Bit-Level Filtering

OPV-PE can filter at the bit level. To set a bit pattern, place the cursor within a byte field in the **Edit/Create Custom Filter Template** area. Press the **Set Bit Pattern** button.The **Bit-Level Pattern** dialog box displays. The dialog box gives the number of the offset you are currently changing in its title bar. Enter any values for each bit that you want included in the filter. Leave values that you don't care about marked with an X. An example **Bit-Level Pattern** dialog box is shown below:
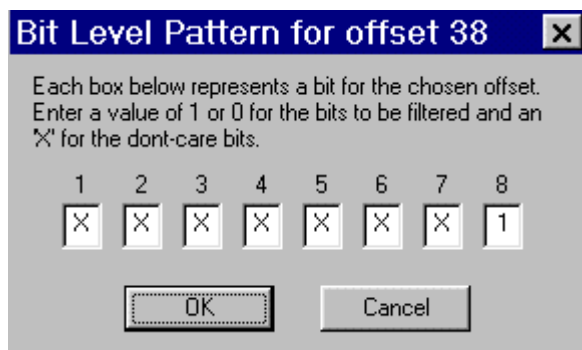
When you view bytes within the **Edit/Create Custom Filter Template** area, those which have bit-level filters applied appear with "BW" in the field. If you place the cursor in the byte field and press the **Set Bit Pattern** button, the **Bit-Level Pattern** dialog box pops up allowing you to view/change the current bit-level filter. A portion of the **Filter Design** window with the bit pattern indicator is shown below:
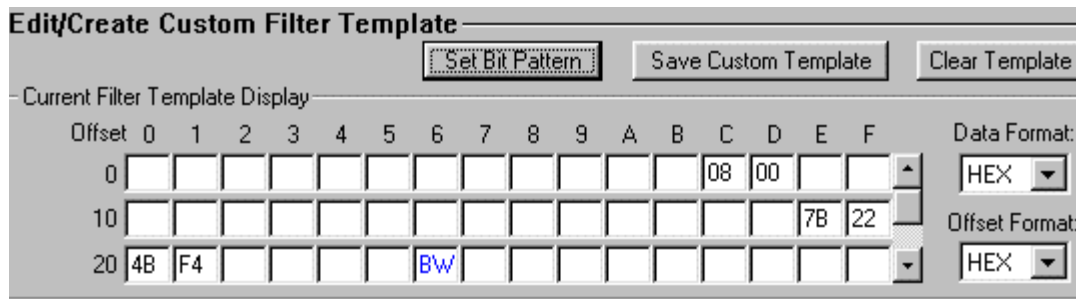
To delete bit-level filtering for a byte, select the "BW" in the byte field and press **Delete**.

If a filter with a bit pattern is loaded to a remote device that is not running OPV-PE Release 4.0 or greater, the bit-level filter is ignored and all values for that byte are treated as "don't care" values.

Filter Creation

The **FILTER CREATION** portion (left side) of the **Filter Design** window is the area that actually specifies what conditions are tested and what actions are taken for this filter statement. See Figure 7-1 for an example of the **FILTER CREATION** area.

- **Create Template Combinations**
  A template combination is built up from various custom or pre-defined filter templates. Logical operators such as AND, OR, and NOT are used to create the logic sequence. Use the operator buttons below the **Template Combination** box to add operators and use the **Add** button to insert filter templates.

- **Set Filter Actions and Custom Counters**
  Press the **Set Filter Actions and Custom Counters** button to set actions and increment counters. The **Filter Actions** dialog box allows you to perform actions that go beyond simple packet capture or display, such as incrementing counters, setting a trigger position, or changing the operational state of the filter. The default setting is to capture the packet (if the filter template conditions are true) and continue.

- **Add Counter Conditions**
  A counter condition is a special condition for accepting/rejecting a packet based on a counter value. Logically, a counter condition functions like a filter template. The settings for counters are test values that can be compared to actual packet counts and thereby determine subsequent actions.

- **Filter Packet Types**
  Four types of frames can be collected and displayed. Refine your selection criteria by selecting only a subset of all frame types. If all boxes are checked, all frame types will pass the filter unless rejected by the other filter criteria you have specified in the **Template Combination** box.

Creating Filter Template Combinations

A template combination provides a way to create a more refined search for specific data. The template combinations are built by selecting a combination of filter templates, operators, and custom counters. An example template combination is shown below:

    MAC_Source_Aaddress AND (SMTP OR FTP)

The **Template Combination** box shows the syntax for the condition. Double-click on filters templates or single-click on operators (buttons) and they appear in the **Template Combination** field.

Filter templates are the primary building blocks of a template combination. A filter template contains the patterns for creating the logical conditions that will be used as a test against incoming frames.

If the operation you try makes no sense in the context of creating a template combination, the operation is not allowed. For example, an OR operator makes no sense after an AND operator. As another example, inserting a filter template immediately after another filter template makes no sense and the operation is not allowed.

The following table describes the buttons that are used as operators to create template combinations.

Table 7-3. Operator Buttons for Template Combinations

Button	Description
AND	Insert logical AND operator. The AND operator has a higher priority than the OR operator (i.e., will be interpreted first).
OR	Insert logical OR operator.
NOT	Insert logical NOT operator.
(	Insert Open Parentheses. Along with the closed parentheses, establishes the ordering and interpretation of the operands. For example, MAC_Source_Address AND SMTP OR FTP is interpreted differently from MAC_Source_Address AND (SMTP OR FTP).
)	Insert Closed Parentheses. Along with the open parentheses, establishes ordering and interpretation of the operands.
Clear All	Clears the entire template combination box.
CE	Clears the Last Entry. Erases only the last operator or template added to the template combination.
Add Counter Condition...	Brings up a dialog box to create a counter condition. You specify a counter name and a value to test against. When you specify the counter condition and click the **OK** button, the counter condition will appear in the **Template Combination** box. See the section on Counter Conditions for more information on using counter conditions.

Filter Actions

The **Filter Actions** dialog box is accessed by pressing the **Set Filter Actions and Custom Counters** button from the **Filter Design** window. Actions do not need to be set for simple filters. The **Filter Actions** dialog box allows you to refine the exact contents of the capture buffer that go beyond the filtering specified in the **Filter Design** window. The default setting is to capture the current packet and continue.

Actions for Capture Filters

Table 7-4 shows actions available for capture filters:

Table 7-4. Capture Filter Actions

Action	Description
Capture	Capture the frame.
Trigger	Capture the frame. Continue capture and fill the buffer to the percentage specified by the user in the **After trigger, continue to capture packets until the buffer is: \<nn\>% full** field.
	For devices other than IMM, mark the frame as a trigger point. In view mode, a trigger frame is numbered as frame-zero and marked with the name TRIGGER.
Increment Custom Counter	Increment the custom counter. For PMM or GMM, any combination of three counters can be incremented. For IMM, any combination of seven counters can be incremented.
Change Filter Operation	Go to a different filter state for processing the next incoming packet. The state can be the current state or any other state defined in the capture filter.

An example **Filter Actions** dialog box for capture filters is shown below:
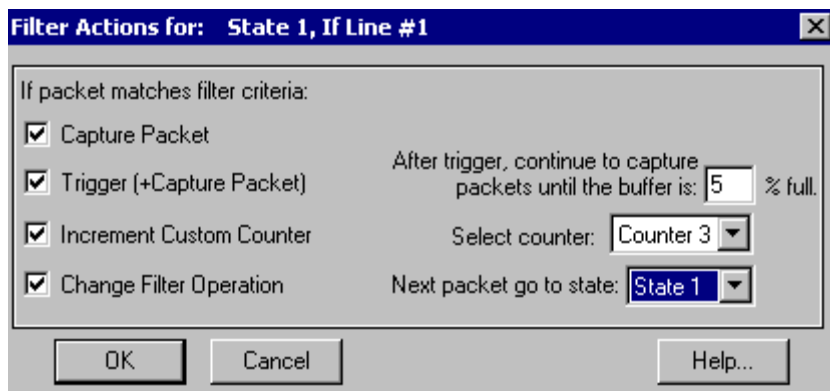
Figure 7-3. Example Filter Actions Dialog Box

The state number and the line number of the statement within the state are given in the title bar of the dialog box.

Actions for Display Filters

Table 7-5 shows actions available for display filters:

Table 7-5. Display Filter Actions

Action	Description
Display Packet	Display the resultant data.
Change Filter Operation	Go to a different filter state for processing the next incoming packet. The state can be the current state or any other state defined in the display filter.

See Multi-State and Multi-Statement Filters for more information on actions in multi-state filters.

Counter Conditions for Filters

Press the **Add Counter Condition…** button to bring up a dialog box to create a counter condition. You specify a counter name and a value to test against. When you specify the counter condition and click the **OK** button, the counter condition appears in the **Template Combination** box. Counter conditions are only available with capture filters.

A counter condition is a special condition for accepting/rejecting a packet based on a counter value. Logically, a counter condition functions like a filter template. The settings for counters are "conditional flags" for subsequent actions. For example, set the counter name to "Counter 1." Set the test value in the >= field to l00. When Counter 1 reaches 100, the filter will carry out the actions that you have chosen for subsequent packets.

You can use a counter just like a filter template. For example, you could create the phrase FTP AND Counter 4 >= 20 in the Template Combination box. This would select FTP packets when Counter 4 reaches a value of 20. For IMM, one of seven custom counters can be used as the test counter. For PMM or GMM, only one counter (Counter 1) can be used as the test counter.

The counter "test values" set in this window are global values. For multi-statement filters, if you set a counter test value in one statement, if you try to change it in another statement you will receive a warning message. See Multi-State Filters for more information on actions in multi-state filters.

Note that if you select the **Add Counter Condition…** box, choose a counter, but leave the "test value" set at 0, the result will be that the filter condition is always true and all actions will be taken immediately.

Global Values that Affect Capture Filter Actions

Table 7-6 describes the options and settings available that have a global setting. If you set the value in one statement, the value will apply to all other statements.

The post trigger buffer position set in the **After trigger, continue to capture packets until the buffer is: <nn>% full** field is a global value. For multi-statement filters, if you attempt to set this value after it has already been set in another statement, you will receive a warning message.

Table 7-6. Capture Filter Global Values

Capture Filter Global	Description
Post Trigger Buffer Position	This defines the percentage of the buffer used to store frames once data capture is triggered. For example, assume the post trigger buffer position is set to 50% for a module with 32MB of memory. After the module is triggered, frames will be captured until 16MB of the module memory is full.
Counter 1 through Counter 7	The value of a custom counter for testing conditions. For example, if the custom counter is set to 10, and the counter is used as part of a condition, the condition will be satisfied when the counter reaches 10. For IMM, seven counters are available. For PMM and GMM, only one counter (Counter 1) is available for a condition counter.

Frame Types

Four types of frames can be collected and displayed. Refine your selection criteria by selecting only a subset of all frame types. If all boxes are checked, all frame types will be subjected to the other filter criteria you have specified in the **Template Combination** box.

The frame type check boxes allow you to select the types of frames you want to capture. For example, if you want to capture only good frames, leave the **Good Frames** box checked and deselect all other frame types. If you want to capture only error frames, leave all frame types selected with the exception of the **Good Frames** box.

For other hardware devices other than IMM, the values that define Undersize and Oversize packets are fixed. Fragments/Undersize packets are those with less than 64 bytes and Jabbers/Oversize are those over 1518 bytes. For IMM, the minimum and maximum packet size can be set as described below.

Frame types are shown in Table 7-7:

Table 7-7. Capture and Display Frame Types/Size

Frame Type/Size	Description
Good Frames	Frames that have no errors.
CRC Error Frames	All frames that contain CRC or Alignment errors (default is packets of 64 to 1518 bytes).
Fragment/Undersize	All fragments and undersized frames (default is packets less than 64 bytes).
Jabber/Oversize	All jabbers and oversize frames (default is packets greater than 1518 bytes).
Minimum Packet Size (IMM only)	Sets the minimum packet size for all filtering activities based on frame size. Packet sizes less than this value are considered Fragments/ Undersize for IMM.
Maximum Packet Size (IMM only)	Sets the maximum packet size for all filtering activities based on frame size. Packet sizes larger than this value are considered Jabbers/Over- size for IMM.

Multi-State and Multi-Statement Filters

To create more complex filters, use OPV-PE's graphical scripting language. You'll find it intuitive and easy to use if you have experience doing simple programming or experience working with "meta-languages." After you become familiar with this graphical scripting language, you'll have a powerful tool for getting exactly the data you want. It is recommended that you first have an understanding of filter templates and creating single filter statements before attempting to create advanced filters.

Click on the **State** 📧 button in the **Filter Design** window to view the **Filter States Design** window for the filter. An example is shown below
:
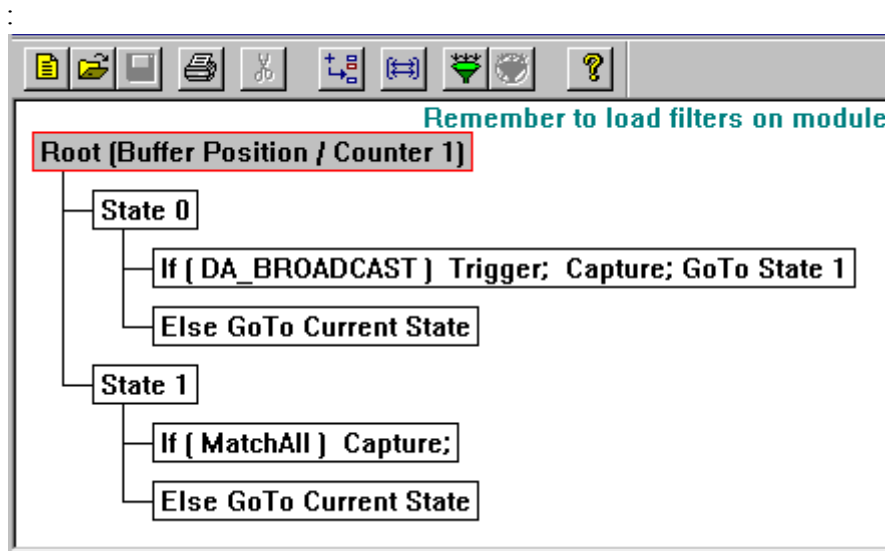
Figure 7-4. Example Filter States Design Window

From the **Filter States Design** window you view the entire structure of the filter. The window shows all the filter statements and the structure of the filter. Each statement is composed of conditions and actions to take if the condition is satisfied. Windows are used to create/modify each statement.

Convenient buttons are available to save, create, open, load, and unload Capture and Display filters. You can also add/delete statements from the toolbar or from the menus. When you add or modify a statement, its associated window is displayed.

All changes and additions to the filter are made from windows. Windows appear when you double-click on the statements shown in the **Filter States Design** window.

Keystrokes and the right mouse button in the **Filter States Design** window are also context sensitive. For example, pressing the **Insert** key when the ROOT statement is selected inserts a new State; pressing the Insert key on a State inserts an IF statement. See Appendix C, "Keyboard Shortcuts" for a list of keystroke actions and their results.

You can write and attach a description to a Capture or Display Filter. You can expand or collapse states of the filter from the menus if you need more room to view other states in the window. Collapsed states (also called branches) are surrounded by dashed lines. The currently selected statement is highlighted with a red border.

Filter Structure

The capture or display filter consists of states, each with a unique label so it can be referenced. Each state contains an IF statement, an ELSE statement, and optional ELSE IF statements. Each IF or ELSE IF statement is comprised of a condition to match against packets and the actions to implement if the condition matches. The ELSE statement is a set of actions to take when the other statements are false. The actions result in the subset of data that is captured or displayed by OPV-PE. The statements and labels have an order, structure, and syntax. You always start and stay in State0 until an action takes you to a different state.

Capture and display filters have the following structure:

```
ROOT statement (The root statement for capture filters con-
tains settings for global variables. The root statement for
display filters contains no variables.)
STATE0 identifier    (Label for GoTo Action to Change the Fil-
ter
                     Operation -- Initial Starting Point)
IF statement (Specify conditions and actions)
ELSE IF statement (optional - same structure as IF statement)
other ELSE IF statements
ELSE statement (if no conditions satisfied, take these
actions)
STATE1 identifier    (Label for GoTo Action to
                     Change the Filter Operation)
IF statement (Specify conditions and actions)
ELSE IF statement (optional - same structure as IF statement)
other ELSE IF statements
ELSE statement (if no conditions satisfied, take these
actions)
.    ...

.    ...

.    ..


STATE3 identifier    (Label for GoTo Action to
                     Change the Filter Operation)
IF statement (Specify conditions and actions)
ELSE IF statement (optional - same structure as IF statement)
other ELSE IF statements
ELSE statement (if no conditions satisfied, take these
actions)
```

Filter States

States are used to group a set of statements. Since statement contain conditions and actions, states are a way to create a set of conditions and actions.

You can specify up to 4 states with most devices, 8 states with PMM. You always start and stay in State0 until an action takes you to a different state. The hardware device stays in a given state until a condition is met which results in an action that changes the filter operation.

When a state change occurs, the next packet is evaluated by the conditions of the new state. **A changed state will apply to the next packet received, not the current packet.**

In most instances, you will only need only one or two states in a filter. Here is an example filter showing three states:

```
STATE0
IF (DA=Santosh) GoTo State1
ELSE IF (DA=Yancy) GoTo State2
ELSE GoTo CurrentState

STATE1
IF (DA_IP_Filter1) Counter1; Capture; GoTo CurrentState
ELSE GoTo State0

STATE2
IF (DA_IP_Filter2) Counter2; Capture; GoTo CurrentState
ELSE GoTo State0
```

Changing States (Changing Filter Operation)

When you select a state other than the current state, a "GoTo" phrase will display as part of the statement in the **Filter States Design** window, showing the next state; for example `GoTo State1`.

To change the state based on the conditions in a statement, double-click on the statement in the **Filter states Design** window. For `IF` or `ELSE IF` statements, this brings up the **Filter Design** window. Use the **Set Filter Actions and Custom Counters** button in the **Filter Design** window to reach the **Filter Actions** dialog box. In the **Filter Actions** dialog box use the **Change Filter Operation** check box to select a state change. The **Next packet go to state:** pull-down box specifies the new state. `CurrentState` means stay in the state number that contains the statement.

Double-click on an `ELSE` statement to bring up a dialog to specify just the actions to take when this statement is reached. The `GoTo` phrase always displays for the `ELSE` statement, even if it's the current state. The default setting for the `ELSE` statement is `GoTo Current State`.

Filter Statements

To create statements, press the ⊞ button from the **Filter States Design** window. Use the window that appears to create a condition and to specify actions to be taken if the condition is satisfied. Once a condition is true, the next condition is not examined. For the next frame you remain in the current state or go to a different state, depending on the GoTo action specified in the statement. If no condition is met, the actions in the ELSE statement are taken.

For IF or ELSE IF statements, the conditions of the statement are created using the **Filter Design** window. If you are adding a statement, you cannot load the filter until you return to the **Filter States Design** window. The **Load Filter** ⏚ and **Unload Filter** ⏚ buttons on the **Filter Design** toolbar are disabled.

The window for the ELSE statement specifies the actions when no conditions for previous statements are satisfied. You can only specify actions and the next state to execute.

Table Table 7-8 shows a synopsis of the logic sequence for statements:

Table 7-8. Logic Sequence for Capture and Display Filter Statements

Logic Sequence	Description
IF statement	IF (these conditions are satisfied) THEN (take these actions, go to State n)
ELSE IF statement	ELSE IF (these conditions are satisfied) THEN (take these actions, go to State n)
ELSE IF statement	ELSE IF (these conditions are satisfied) THEN (take these actions, go to State n) The ELSE IF statement can appear multiple times.
ELSE statement	ELSE (take these actions, go to State n)

Capture and Display Filter Differences

Display and capture filters are activated in different ways. Also, some options for capture filters are not used in display filters. Some options available in capture filters make no sense for display and are therefore not supported:

• Display filters do not use custom counters.

• The action "display" is available for display filters. The actions "capture" and "trigger" and "increment customer counter" are available with capture filters.

• Display filters do not have global settings. Global settings for the capture filter include the test value you can set for each custom counter when they are used as counter conditions and a buffer trigger position.

Activating Display Filters

Activate (load) a display filter by pressing the **Load Filter** button on the **Filter Design** or **Filter States Design** toolbar. Deactivate (unload) a display filter by pressing the **Unload Filter** button on the **Filter Design** or **Filter States Design** toolbar or the **Unload Display Filter** button on the Detail View toolbar.

You can keep the display filter ON at all times; if you make changes, the next time you view data in Capture View the new filter will be used immediately. If you already have a Capture View window open for the capture file, select the **Refresh...** option from the **File** menu in Capture View to refresh the view using the new filter.

You can also create and immediately activate a display filter from VoIP tables using the right mouse button.

Activating Capture Filters

The capture filter must be loaded to the hardware module. It is not active until you press the **Load Filter** button on the **Filter Design** or **Filter States Design** toolbar. It remains active for that module until you unload the filter. Unload a capture filter by pressing the press the **Unload Filter** button on the **Filter Design** or **Filter States Design** toolbar. Since capture filters are associated with a hardware module, different capture filters can be loaded to different modules.

For IMM devices, you can load a filter while capture is in progress. For other devices, you must stop the device before loading the filter.

You can load a filter from Summary View (main window) using the button.

You can also create and immediately activate a capture filter for the current resource from VoIP tables using the right mouse button.

Filter Examples

Filter examples are supplied with OPV-PE. To see examples, open a capture filter file (.CFD extension) or a display filter file (.DFD extension) from the **Filter** window. From the **Module** menu, select **Filter Description** to access a description of any filter. To find more examples, look in the ...\examples\filter directory.

Filter Example, Capture Conversation

The **Filter Design** window in Figure 7-5 shows a template that captures all packets going to and coming from two IP stations. The conversation is specified by entering the two IP addresses, using the <-> indicator to capture packets in both directions. The **Apply Conversation to Template** check box is selected to apply the conversation to the filter template. The filter template is named **Station_7and_8_Conversation.**

Note that the filter template must be applied to the filter by pressing the **Add** button. Filter templates must appear in the **Template Combination** box before they can be loaded to the hardware device.

.
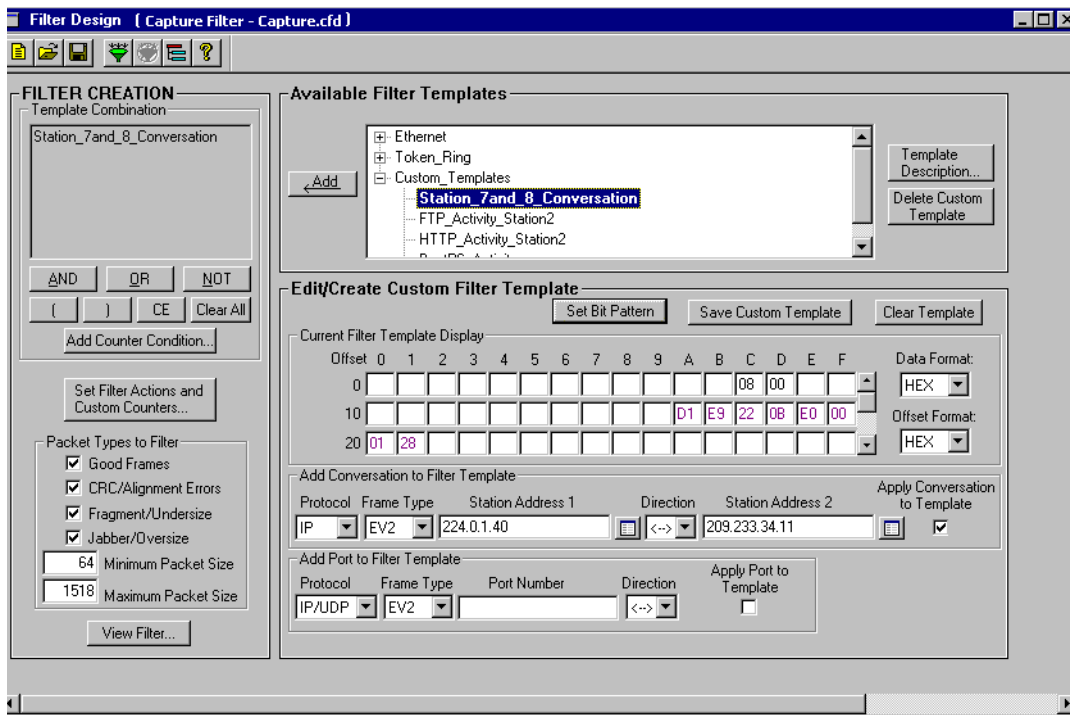
Figure 7-5. Filter Design Window, Conversation Example

The steps used to create the filter template and load it to a resource are shown below:

1. Press the **Clear Template** button.

2. Press the **Name** 🔲 button for **Station Address 1**. Select the address from the name table and click **OK**.

3. Press the **Name** 🔲 button for **Station Address 2**. Select the address from the name table and click **OK**.

4. Pull down the **Direction** box and set the indicator to bi-directional (<->).

5. Be sure the **Apply Conversation to Template** check box is selected in the **Add Conversation to Filter Template** area.

6. Press the **Save Custom Template** button.

7. Enter the name of the new filter template in the **Add to Available Filter Templates** dialog box. The name in the example is **Station_7and_8_Conversation**. The new filter template name appears in the `Custom_Templates` section of the **Available Filter Templates** box.

8. Press the **Add** button to apply the filter template. The filter template appears in the **Template Combination** box.

9. Press the **Load Filter** 🔽 button to load the filter to the resource.

10. You are now ready to start capture. The capture buffer will contain only the packets that match the filter criteria. The filter criteria includes the templates shown in the **Template Combination** box and the packet types selected in the lower portion of the **FILTER CREATION** box.

Filter Example, Template Combination

The **Filter Design** window in Figure 7-6 shows the capture filter with a logical combination built in the **Template Combination** box. This filter collects all traffic to and from a single station that make use of the HTTP or FTP protocols. The two templates are combined with an OR statement to collect both types of protocols. The two templates are named HTTP_Activity_Station2 for the user-defined HTTP template and FTP_Activity_Station2 for the user-defined FTP template.

The conversation is specified without a second station and uses the -> indicator. Traffic is captured in the sending direction for a single station, regardless of the other station in the conversation. In the example, the station address has been defined as part of each custom filter template.
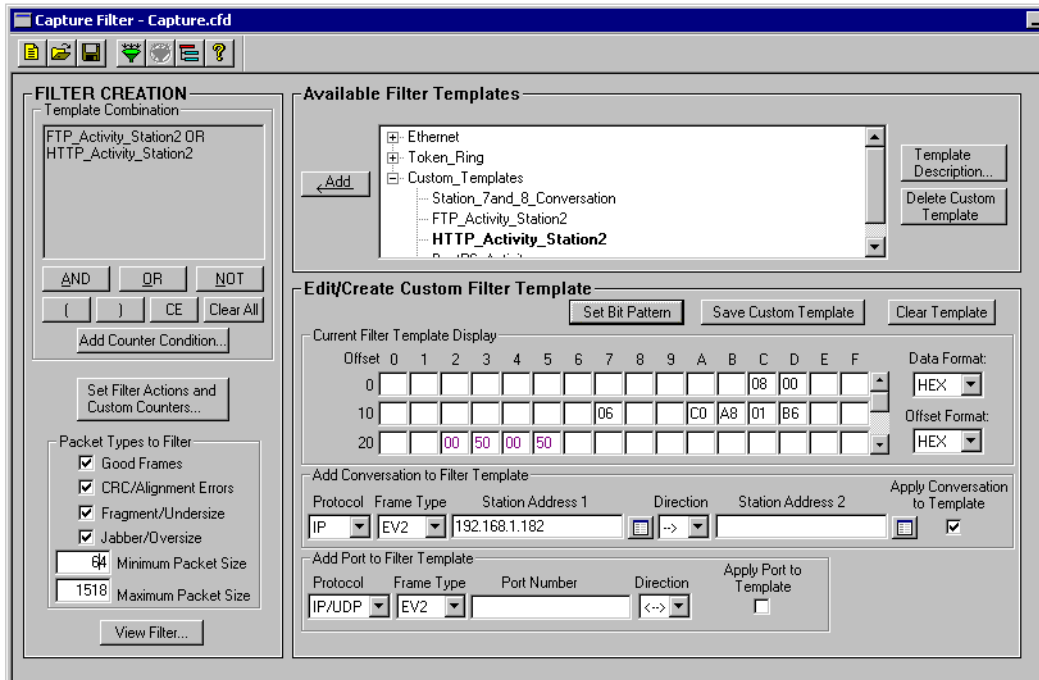
Figure 7-6. Filter Design Window, Template Combination Example

The following steps describe how to create two filter templates, logically combine them using an OR operator, and load the resulting Template Combination to a resource:

1. Select the **HTTP** pre-defined filter template from the **Available Filter Templates** box.

2. Press the **Name** ▤ button for **Station Address 1**. Select the address from the name table and click **OK**.

3. Pull down the **Direction** box and set the indicator to source address (`->`).

4. Be sure the **Apply Conversation to Template** check box is selected in the **Add Conversation to Filter Template** area.

5. Press the **Save Custom Template** button.

6. Enter the name (**HTTP_Activity_Station2**) of the new filter template in the **Add to Available Filter Templates** dialog box. The new filter template name will appear in the `Custom_Templates` available for other filtering operations.

7. Using the **FTP** pre-defined filter template as the starting point, repeat steps 1 through 6 to create a similar custom template for FTP.

8. Highlight the **HTTP_Activity_Station2** template in the `Custom_Templates` section of the **Available Filter Templates** box. Press the **Add** button to apply the filter template. The filter template appears in the **Template Combination** box.

9. Press the **OR** operator button. The operator is appended to the filter template in the **Template Combination** box.

10. Highlight the **FTP_Activity_Station2** template in the `Custom_Templates` section of the **Available Filter Templates** browser. Press the **Add** button to apply the filter template. The filter template appears in the **Template Combination** box. You now have two filter templates in the **Template Combination** box connected by an **OR** operator.

11. Press the Load Filter ▼ button to load the filter to the resource.

12. You are now ready to start capture. The capture buffer will contain only the packets sent from Station2 that have an FTP or HTTP port number.

Filter Example, Capture TCP Port Traffic

The **Filter Design** window in Figure 7-7 shows the capture filter for a specific TCP Port. This filter collects all TCP/IP traffic that uses the BootPS port number.
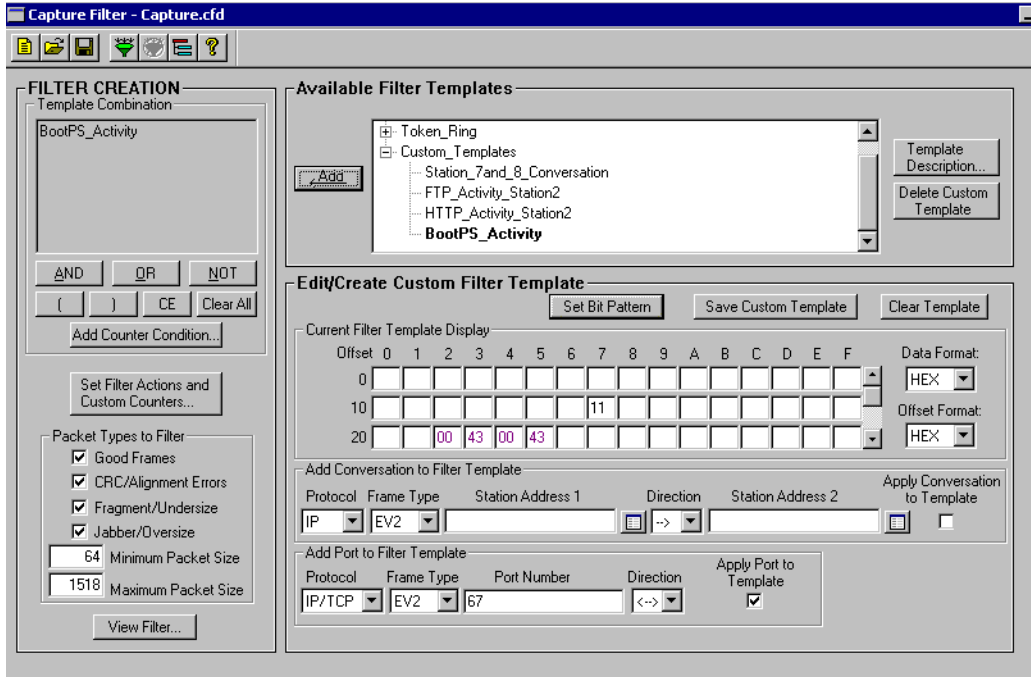
Figure 7-7. Filter Design Window, Capture TCP Port Example

The following steps describe how to create the BootPS filter template and load in to a resource.

1. Press the **Clear Template** button.

2. In the **Apply Port to Template** area, enter the **Protocol** and **Frame Type.** For the BootPS port, use the IP/TCP protocol. In the example, the frame type is set to EV2.

3. Enter the port number in decimal in the **Apply Port to Template** area. The decimal port number for BootPS is 67.

4. Pull down the **Direction** box and set the indicator to bi-directional (<->).

5. Be sure the **Apply Port to Template** check box is selected in the **Add Port to Filter Template** area. Be sure the **Apply Conversation to Template** check box is NOT selected in the **Add Conversation to Filter Template** area. No specific stations are associated with the new filter template.

6. Press the **Save Custom Template** button.

7. Enter the name of the new filter template in the **Add to Available Filter Templates** dialog box. The name in the example is **BootPS_Activity**. The new filter template name appears in the Custom_Templates section of the filter browser.

8. Press the **Add** button to apply the filter template. The filter template appears in the **Template Combination** box.

9. Press the **Load Filter** ⬇ button to load the filter to the resource.

10. You are now ready to start capture. The capture buffer will contain only the packets that contain either a source or destination BootPS port number.

Filter Example, Advanced Filter

The **Filter States Design** window below shows the capture filter Example.CFD. The **Filter States Design** window shows the structure of the filter. In the example, the filter has multiple states and statements. From the **Filter States Design** window, shown in Figure 7-8, double-click on a statement to bring up its **Filter Design** window to see the details of how the statement is constructed.
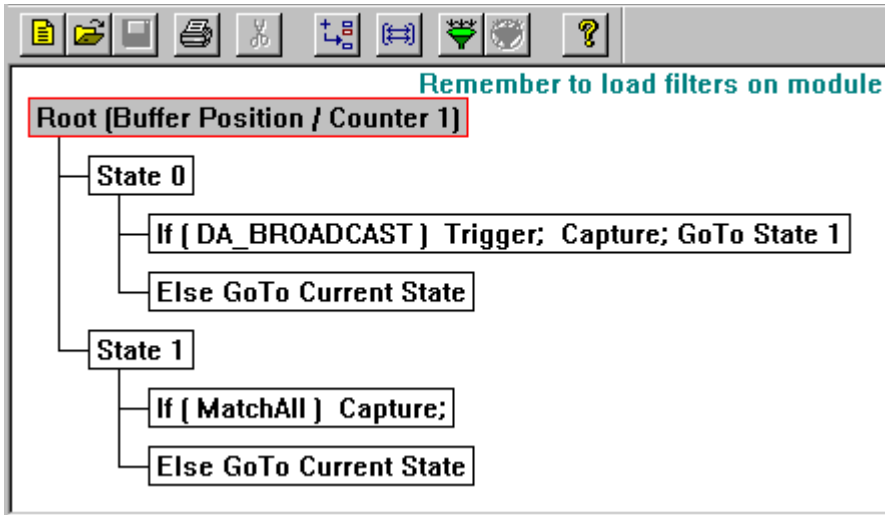
Figure 7-8. Advanced Filter, Filter States Design Window

Packets are tested first by the IF statement in State0. If the packet matches the broadcast mask (FFFFFFFFFFFF in the first six bytes), the packet is captured, the buffer is triggered, and the next packet is filtered by State1. If the packet does not contain the Broadcast address, the packet is not captured and the next packet is filtered.

State1 is executed after the first broadcast packet is encountered. The IF statement in State1 indicates that all packets should be captured. The flow for testing packets remains in State1 until the capture process is manually stopped or the buffer is filled to the percentage entered by the user.

Rules of the Capture or Display Filter

- There must be at least one IF and one ELSE statement per state. ELSE IF statements are optional.

- The Post Trigger Buffer Position must be greater than zero and less than 100.

- There is always one and only one ROOT statement; you can't delete the ROOT statement.

- In the capture filter, setting trigger will always set capture.

- For devices other than IMM, Custom Counter 1 is the only counter that can be used as a counter condition in a filter template. For IMM, all 7 custom counters can be used as a counter condition.

- The maximum number of states allowed is four for IMM or GMM. The maximum number of states for PMM is eight.

- The number of filters allowed depends on the analyzer-card hardware. A maximum of 16 total hardware filters are allowed for IMM modules, which can be distributed across its four allowed states. A maximum of 8 hardware filters per state are allowed for PMM modules, and 4 per state for GMM modules. Depending on the number of states, the micro filters, and the logic combinations used, it is possible to exceed the maximum number of hardware filters. Contact Fluke Networks customer support if you are experiencing problems with writing complex filters that exceed the maximum number of hardware filters.

Hints and Tips for Using Filters

- Remember to load the Capture filter on the module before you start capture.

- If you want to look at captured data in many different ways, use display filters rather than capture filters. Capture large blocks of unfiltered data and look at different subsets of the data by using a variety of display filters.

- Use the **Template Description** button to find out the exact mask and logical operations in a filter template.

- Use conversations for capturing or displaying station-to-station or router-to-router activity.

- Always attach a description to a filter you are saving with the **Description** menu.

- To see which capture filter is associated with the current resource, choose **Active TSP and Capture Filter** from the **Module** menu. The capture filter name is also displayed in the status bar in Detail view.

- In the **Filter Design** window, make sure that the templates you want in the filter are displayed in the **Template Combination** box. If a template is not displayed in the **Template Combination** box, it is not part of the filter to be applied.

- Be sure to click the **Apply Conversation to Template** check box to include a conversation as part of your filter.

- AND operations narrow the search results and are typically used between templates that define masks for different offsets and lengths. Using AND operations between filter templates that define masks for the same offsets and lengths will result in a pattern-conflict warning message.

- OR operations expand the search results and are useful between filter templates that define masks for the same offsets and lengths.

- To edit a statement in the **Filter States Design** window, double-click on the statement.

- Use the right mouse button to learn about the options available for any statement in a filter. You can immediately see what options are possible depending on what type of statement is selected.

- Use the [t_] button to add states or statements to the **Filter States Design** window.

- From the Detail View pane of the Capture View window, you can copy the contents of any field to create a Capture or Display filter. Select the field with the left mouse and then click the right mouse button. Selections for copy to capture or display filter appear. Select the option, and the **Filter Design** window appears.

- Click the right mouse button on a table entry in Host Table, Network Table, Application Table, Host Matrix, Network Matrix, or Application Matrix view to bring up a menu for creating a filter. You'll get a choice of creating a capture or display filter. When you make a choice from the menu, the **Filter Design** window opens with the address(es) from the table entry in the address fields for creating a filter.

- You must use the **Add** button for a template to be used in the current filter. Make sure all templates display in the **Template Combination** box that you want to use in the filter.

Filtering Tips Unique to IMM/OPV-LA Devices

- When applying a filter to the data buffer of a IMM or OPV-LA device, you do not need to stop the device before applying the filter.

- Filters applied to IMM/OPV-LA data buffers affect monitor and capture simultaneously.

- In the **Filter States Design** window for IMM devices, when the **Show/Hide Detail** button is pressed, a line of information appears on the top of the page. This information can help you determine how many hardware filters are used in the filter. If you are running into the upper limit of hardware filters or would like more information on how hardware filters are calculated, contact customer support for information.

Chapter 8
Traffic Generator

The Traffic Generator software option allows you to generate packets and send them onto a network. This can be used to force the network to respond to known or suspected problem conditions or loads. Transmitted data can answer "What If?" questions about the network or particular network resources.

To transmit data, you first set up a Transmit Specification. After the Transmit Specification is loaded to a module, click on the **Start** button to begin transmit. You can also transmit a previously-captured data file (capture file).

You can transmit the contents of a capture file. Data previously collected in the capture file can be loaded to a module and sent to the network.

Using OPV-LA, you can transmit packets to simulate high traffic conditions and see how the network performs. OPV-PE can also transmit a variety of user-defined packet contents to see their effect on the network.

With multiple modules, transmitted data can be captured by another analyzer card. You can use the capture and view features in the OPV-PE software to analyze the results, all from the same PC.

Although you can transmit using NDIS modules, these devices are not always accurate transmit devices. The actual rate of transmission for an NDIS module is not predictable.

Transmit Specifications

An example **Transmit Specification** dialog box is shown in Figure 8-1 on page 8-2. For additional views of this dialog box, see the Transmit Specification examples at the end of this chapter. To bring up the **Transmit Specification** dialog box, press the 〔▦〕 button from the **Detail View** toolbar.

8-1

Transmit Specification Dialog Box

Transmit Specifications are defined in a dialog box. The **Transmit Specification** dialog box contains:

- A **Defined Streams** list box (top) for viewing defined streams.

- Radio buttons and fields for defining a stream (middle)

- Buttons for adding, modifying, or deleting streams, editing data

- Transmission status information

- Buttons for loading the module, opening/saving the specifications, and adding streams using templates and Magic Packets™
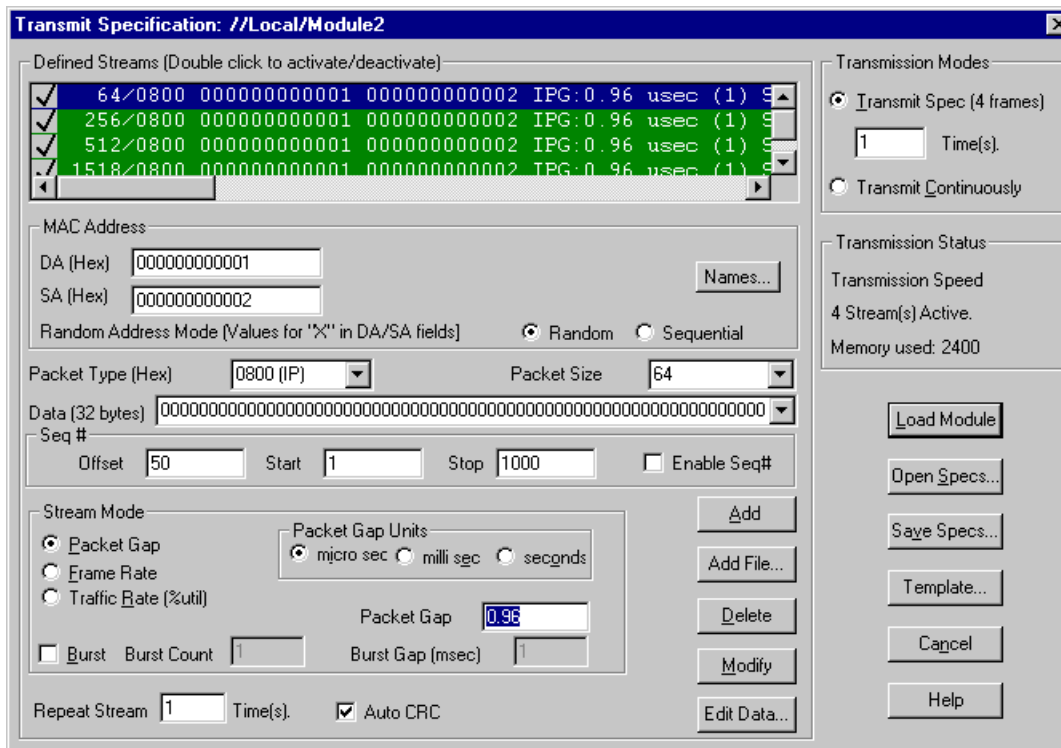
Figure 8-1. Transmit Specification Dialog Box

Defined Streams List Box

A defined stream is a specification for transmitting frames from a module. Multiple streams can be defined for a Transmit Specification. Define a stream using the options available from the dialog box and click on the **Add** button. You can also add a capture file as a defined stream using the **Add File…** button. The added stream appears in the **Defined Streams** list box. Streams are transmitted by the module in the order in which they are defined.

A defined stream may be activated or deactivated by double-clicking on the stream. An activated stream has a check mark next to it in the **Defined Streams** list box and is highlighted with the Windows highlight color; a deactivated stream has no check mark and displays in the Windows inactive color. Only activated streams are loaded to the module when you click on the **Load Module** button. Before loading a module, make sure you have activated the streams you want.

Figure 8-1 on page 8-2 shows a synopsis of all streams defined for the Transmit Specification. In the example, three streams are defined and only two are activated. The stream highlighted in the highlight color set for Windows is the currently selected stream. Streams highlighted in the inactive color set for Windows are inactive. The settings for the currently selected stream show in the fields of the dialog box below the **Defined Streams** list box.

If you modify the values in the current stream and click on **Add**, a new stream is added as the stream after the currently selected stream in the **Defined Streams** list box. If you modify the values in the current stream and click on **Modify**, the definition of the current stream is changed.

Radio Buttons and Fields for Defining a Stream

Specify the contents and the size of the stream using the **DA**, **SA**, **Packet Type**, **Packet Size**, and **Data** fields. DA and SA values can be retrieved from the currently active name table using the **Names…** button. Random or sequential address generation is supported by selecting the appropriate radio buttons and using X values in the **DA** or **SA** field.

Sequence numbers (Start Seq# and Stop Seq#) are used to number the packets; packet numbering may be useful at the receiving end. When viewing packets at the receiving end, the default location for the two-byte sequence number is 32H and 33H. This value can be set in the **Seq# Offset** field.

Set the stream mode using the radio buttons and the **Burst** check box. The stream mode defines the rate at which packets are transmitted from a module and whether bursts of packets with a different rate will be transmitted within the stream.

Set the **Repeat Streams** field to repeat the stream more than one time. This setting specifies the number of times to repeat one complete stream – not how many times to repeat transmission of the entire specification, nor the number of bursts within the stream. The **Auto CRC** check box specifies if a valid CRC will be automatically generated for the stream.

Stream Buttons

The **Add**, **Add File...**, **Modify**, **Delete**, and **Edit Data...** buttons perform functions for a single stream.

Table 8-1. Single-Stream Function Buttons

Stream Button	Stream Function
Add	Adds a new stream after the currently selected stream in the **Defined Streams** window. The values displayed in the fields of the **Transmit Specification** window are used as the values for the new stream.
Add File…	Adds a new stream defined by capture file (`.CAP file`) in the **Defined Streams** window. A dialog box appears asking for the name of the capture file. The first packet in the capture file is the defined stream. All subsequent packets in the capture file are ignored.
Modify	Changes the definition of the current stream. The values displayed in the fields of the **Transmit Specification** window overwrite the values of the currently selected stream.
Delete	Deletes the currently selected stream.
Edit Data…	Brings up the packet editor. You can use the packet editor to modify the currently selected stream.

Transmission Mode and Status Controls

The **Transmission Mode** radio buttons control how many times all streams are transmitted once they are loaded to the module. You can transmit the entire specification n times or continuously. The transmission mode is not part of the Transmit Specification when saving to a file and must be set each time you load the Transmit Specification.

The **Transmission Status** section provides information about the number of activated streams, speed of transmission, and the amount of module memory used by active streams.

Transmit Specification Control Buttons

The **Load Module**, **Open Specs**, and **Save Specs** buttons perform functions on a complete Transmit Specification. Be sure to use the **Load Module** button to load the

specification to the module before you begin transmission. The **Template** button allows you to use predefined data as a starting point for new stream. It also lets you create Magic Packets™.

Transmit Specification control buttons are described in Table 8-2:

Table 8-2. Transmit Specification Control Buttons

Control Button	Transmit Specification Function
Load Module	Loads the current resource with the currently defined Transmit Specification. Be sure to use the **Load Module** button to load the specification to the resource before you begin transmission.
Open Specs...	Opens a previously saved Transmit Specification. A dialog box appears to specify the name and location of the Transmit Specification.
Save Specs…	Saves the currently defined Transmit Specification to a file. A dialog box appears to specify the name and location of the Transmit Specification.
Template…	Shows menus that list the currently defined templates for packets. Selecting a template places the values of the template in the fields of the **Transmit Specification** dialog box. You can then change the values of the fields in the **Transmit Specification** dialog box or use the **Edit Data…** button to create exactly the packet you wish.
Cancel	Exit the **Transmit Specification** dialog box. Make sure you have added/modified all streams, saved new Transmit Specifications, and loaded the resource before pressing Cancel.

Repeating Frames

There are three ways to repeat frames when transmitting:

Table 8-3. Methods to Repeat Frames

Repeat Frames Method	Transmission Function
Check the Bursts box	Repeats frames of a stream with a specific timing set between the frames. The special timing is set in the **Burst Gap** field, the number of repetitions in the **Burst Count** field.
Repeat Streams	Repeats the stream n times. The gap between frames is set by the Stream Mode as a packet gap, frame rate, or traffic rate.
Set the Transmission Mode	You can set the module to loop through the entire Transmit Specification n number of times. Streams are repeated in the specification from first to last until you stop the module or all streams are transmitted n times.

⚠ **Caution**

Repeating frames using the transmission mode feature is a function implemented in software for PMMs or NDIS modules; there is a time gap of about 50ms between each transmission of the entire specification. Use *Repeat Frames 'n' Times* or *Bursts* where timing issues are critical when sending frames for these devices.

Ways of repeating frames can be used together. For example, assume the following two streams are defined:

```
Stream 1; packet gap=100msec, burst count=4, burst
gap=4msec,
repeat frame 2 times
Stream 2; packet gap=200msec, no burst

The example results in the following:

Transmit Stream 1
Wait 100msec
Transmit Stream 1
Wait 100msec
Transmit Stream 1
Wait 100msec
Transmit Stream 1
Wait 104msec
Transmit Stream 1
Wait 100msec
Transmit Stream 1
Wait 100msec
Transmit Stream 1
Wait 100msec
Transmit Stream 1
Wait 104msec
Transmit Stream 2
Wait 200msec
```

If the transmission mode is set to continuous, the entire sequence above is repeated until the module is stopped.

The **Repeat Stream** field sets how many times to repeat the current stream. For example, if the **Repeat Stream** field is set to a value of 8, the current stream would be sent 8 times before the next stream in the Transmit Specification is sent.

Stream Modes

An interpacket gap for a frame can be set in three different ways; Packet Gap, Frame Rate and Traffic Rate. The stream mode defines the rate at which packets are transmitted from a module. The modes are as shown in Table 8-4 below:

Table 8-4. Stream Modes

Stream Mode	Rate Setting
Packet Gap	The rate is set as an interval of time between packets. The interval can be set in seconds, milliseconds, or microseconds.
Frame Rate	The rate is set in number of frames per second.
Traffic Rate	The rate is set as a percentage of the maximum speed (10Mbps or 100Mbps) for the module.

Use Protocol Media Modules, if you want to transmit at faster than line rate, set the gap to 0.88 microseconds for 100Mbps or 3.2 microseconds for 10Mbps.

Bursts

Bursts cause a stream to be transmitted again and again. Check the **Bursts** box to send a burst of packets with the stream. Set **Burst Count** to the number of times to send the frame. An interval (packet gap) can be set between bursts in the **Burst Gap** field.

The following example shows how bursts and burst timing work. Assume three streams are defined as follows:

```
Stream 1; Packet Gap=100msec., No burst
Stream 2; Packet Gap=20msec, Burst Count=3, Burst
Gap=4msec
Stream 3; Packet Gap=5msec., No burst
```

The example results in the following:

```
Transmit Stream 1
Wait 100msec
Transmit Stream 2
Wait 20msec
Transmit Stream 2
Wait 20msec
Transmit Stream 2
Wait 24msec
Transmit Stream 3
Wait 5msec
```

Transmission Mode

You can either transmit the specification continuously or transmit it n times.

Select **Transmit Continuously** to transmit activated streams in a loop until the module is stopped.

Select **Transmit Spec (N frames)** to transmit activated streams a specific number of times. The number of streams does not necessarily equate to the number of frames transmitted.

⚠ Caution

The transmission mode should always be set prior to loading the module. The transmission mode is not saved as part of the Transmit Specification. Unless you set the transmission mode, you may inadvertently flood the network with packets.

The **Transmission Status** area of the dialog box provides status information about the transmission. The fields indicate the speed of the currently active module, the number of streams that are active, and the total memory in the buffer required to transmit the specification. The total memory increments as you add/change streams, giving you an instant reflection of how much data you are transmitting. A warning message is shown if you exceed the transmit buffer size.

Specifying Transmit Data

Data fields for the Transmit Specification can be modified in two ways: by using the Packet Editor or by changing the data fields shown in the **Transmit Specification** dialog box. If you are inserting a new stream, you can use a template as the starting point for packet data. The insertion of a new packet into the **Defined Streams** list box will appear below the currently highlighted packet stream.

Packet Editor

The packet editor can be used to modify the contents of a stream data. The editor provides two views of packets, a decoded view and a hex view. Edits can be made within either view. Select the **Edit Data** button to bring up the editor.

Table 8-5 shows the buttons that are available from within the packet editor:

Table 8-5. Packet Editor Buttons

Packet Editor Button	Editing Function
Compute CRC	Inserts the correct CRC error check value for the frame. You can use this option to create frames with or without correct CRC error check values.
Decode	Takes the values entered in the **Hex View** window of the packet editor, decodes the packet, and displays the resulting decode in the **Decode View** window.
Undo	Undo the last editing action. Only one level of undo is supported.
OK	Save edits.
Cancel	Leave the editor without saving changes.

Editing in Decode View

Editing in decode view allows you to edit packets without remembering offsets. Click on a field and a dialog box pops up which shows the current value for the field and asks for a new value. The dialog boxes for each field is slightly different. Most dialog boxes display and allow you enter values in hexadecimal or decimal. Some contain a **Use little-endian bit** order check box if bit order swapping is required. Changes made in decode view are automatically reflected in hex view.

Editing in Hex View

Edits are made in hex view by placing the cursor at a location and overwriting the current values. You can also paste (Ctrl + V) the contents of the paste buffer into a location. Values are always overwritten starting at the current cursor location in hex view so offsets remain correct.

Press the **Decode** button to display edits made in hex view in the decode view. Note that changes to the decode view are not automatic. This provides the option of creating error packets that can't be decoded properly.

Note
NDIS modules cannot transmit without a valid CRC.

Changing Fields Directly in the Dialog Box

The values of various fields in the currently selected stream are shown in the Transmit Specification fields below the **Defined Stream** list box. You can change the stream data by editing these fields directly.

DA and SA Fields

The **DA** and **SA** fields define the MAC layer destination address and MAC layer source address for the stream. Note that the MAC address values appear in the stream synopsis in the **Defined Streams** list box.

Use an X in any offset of the **DA** or **SA** fields to indicate "wild card" addresses. OPV-PE will generate packets with different values in that offset. For example, set the **DA** field to 432FFFFFXX. When transmitting packets, values will be generated either sequentially or randomly and sent for the last 2 positions of the DA.

The values for the wild cards can be random or sequential, as defined by the **Random Access Mode** buttons below the **DA** and **SA** fields.

Click on the **Names** button to see the currently active name table. You can set the DA or SA from the name table and they will appear in the **DA** or **SA** fields in the **Transmit Specification** window. The name appears to the right of the DA or SA address if the name table contains a symbolic name for the address.

Packet Type

Sets the packet type for the current stream. Use the pull-down box to see available options. In the example stream, the packet is an IP packet. This field can also be used to enter the packet length for IEEE802.2 or SNAP frames.

Packet Size

Sets the packet size. Use the pull-down box to view common sizes. The size must be from 8 to 15,000 bytes.

Data Field

Specifies the data to be sent as part of the packet. Use the pull-down box to see commonly used values. Any hexadecimal value can be entered in the **Data** field and sent with the packet. Up to the first 32 bytes of data can be specified in this field. The entire data within the packet can be edited using the Packet Editor.

Sequence Numbers

Sets a starting number and ending number for packets transmitted, and also sets the offset within the frame where the sequence number will be stored. You cannot store the sequence number in the first 12 offsets of the frame. Also, you should take care not to store the sequence number in any part of the packet that contains other information that will used by the network or by the receiving station.

Auto CRC Check Box

Setting the check box also affects the contents of the stream. If checked, a correct CRC value is automatically generated for the packet. If unchecked, bad CRC packets can be generated using PMMs. NDIS modules cannot generate bad CRC packets.

Using Templates

If you are inserting a new stream, you can use a template as the starting point for packet data. To select a template, click on the **Template…** button at the bottom of the **Transmit Specification** dialog box. Nested menus to select a template will display.

Templates insert the required values for commonly known packet types in the data for the stream. For example, if you select the template for IPX, the value $0x8137$ is inserted in the **Packet Type** field.

You can create and insert you own templates into the menus. You can also insert Magic Packets™ using the **Template...** menu.

Creating Templates

To create your own template:

1. Click on the ⬚ button and open a capture file or use packets within the capture buffer that are displayed in Capture View.

2. Find the packet you want to add as a transmit template. You must make this packet the first packet in the capture file or capture buffer. Either delete all packets that come before the packet you want, or filter out all other packets using a display filter.

3. Select the first line (first packet) of the capture file.

4. If desired, edit this line using the packet editor. The values you enter in this first packet define the new template.

5. Save the new capture file (the template). Make sure you give a name you will recognize later. Place it in the `..\Template` directory or one of its subdirectories.

6. You must restart OPV-PE to view the new packet template in the template menus.

Templates display in the Template menu when using the **Insert Packet** option of the **Edit** menu. The exact placement of the new template on the menu depends on the directory location within the `..\Template` directory.

Transmitting Capture Files

You can transmit the contents of a capture file as one of the streams in the Transmit Specification. Place a capture file as a stream into the **Defined Streams** list box using the **Add File…** button.

The entire contents of the capture file is transmitted with timestamps intact. As with any other stream, you can repeat transmission by using the **Repeat Stream** field. All other fields do not apply when the stream is defined by a capture file.

Transmit Specification Examples

Transmit Specification examples are supplied with OPV-PE. Open a transmit specification file (\transmit subdirectory, .TSP extension) from the **Transmit Specification** dialog box to see examples.

Two Transmit Specification examples are shown in the following sections.

• The Packet Gaps example shows a specification made up of several streams with different packet sizes that use packet gaps.

• The Bursts example shows a stream that uses bursts.

To find examples, look in the ..\examples\transmit directory.

Transmit Specification Example, Packet Gaps

A Transmit Specification example in its dialog box is shown in Figure 8-2. The dialog box only shows the values for the currently highlighted stream. The current stream appears highlighted within the Defined Streams window. Multiple streams are defined in the specification. All activated streams (indicated by the check mark in the Defined Streams window) will be transmitted.

Figure 8-2. Transmit Specification Dialog Box, Packet Gaps

Transmit Specification Example, Bursts

A **Transmit Specification** dialog box is shown in Figure 8-3. The dialog box only shows values for one stream, the stream that contains a burst. Multiple streams are defined in the specification. Since a burst of 100 is specified, 101 frames will be transmitted even though there are only two "streams" defined.
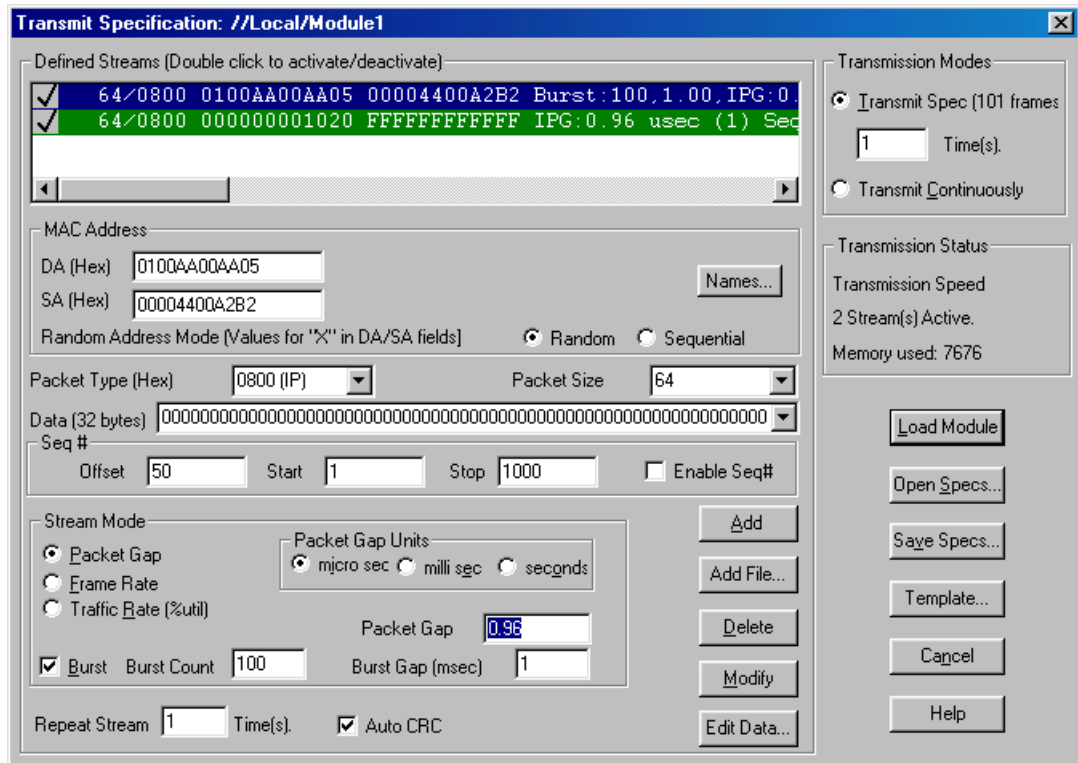
Figure 8-3. Transmit Specification Dialog Box, Bursts

Hints and Tips for a Transmit Specification

- Take care with what you transmit. OPV-PE can transmit packets at more than 100% of network bandwidth. It is possible to flood the network and cripple performance.

- Make sure to activate streams before loading the specification to the module.

- Always set the transmission mode before loading the specification to a module. Unless you do, you may inadvertently flood the network with packets. The transmission mode is not saved as part of the specification, so it should be checked before each module load.

- Transmitted packets can be sent to another module. Use sequence numbers to aid in analyzing the packets at the receiving end.

- Using bursts is the easiest way to simulate high traffic conditions.

- Always save your defined specification. The Transmit Specification can only be saved using the dialog box.

- An NDIS module cannot transmit bad physical layer error packets, such as bad CRC packets, runt packets, oversized packets, packets with less than minimum packet size, and so on. Use PMMs or GMMs to generate these error packets.

- To see which transmit specification is associated with a particular resource, choose **Active TSP and Capture Filter** from the **Module** menu.

- You can add your own transmit templates. Open a capture file and find the packet you want to add as a transmit template. Make this packet the first packet in the capture file, edit the packet if necessary, and save the new capture file. Make sure you give a name you will recognize later. Place it in the **..\Fluke Net-works\Template** directory or one of its subdirectories.

Chapter 9
Alarms

OPV-PE's alarms facility enables you to create alarms to automatically monitor network resources. Access to OPV-PE's alarms facility is through the **Resource Browser** docking window located in OPV-PE's main window. The **Resource Browser** window features a hierarchical directory comprising all hardware devices and hosts discovered.

Right-click on a resource to bring up its alarms. A unique set of alarms exist for each analyzer device on the network.

Alarms are created using an Alarm Editor. The **Alarm Editor** window contains tabs that group all possible alarms. Each alarm within the alarm table contains default threshold values, notification settings, a sampling interval value and an **Enable/ Disable** click box.

Starting a resource automatically activates the alarms associated with that resource. You must have Monitor mode set for a resource to have alarms trigger and have alarm actions occur.

Actions resulting from alarms are varied and flexible because they are assigned to each individual alarm. Whenever an alarm threshold is exceeded, an audible beep sounds on the host and an alarm message appears in the **Message** window. Individual alarms can also be configured to log alarms to a log file, contact individuals by e-mail, dial pager numbers, restart the resource, auto save data, stop the resource and save data, execute a program, or send an SNMP trap message to a management station.

⚠ Note

Alarms only apply to OPV-PE 4.1 or later versions. You cannot create alarms if the remote software (OPV-LA image file or OPV-PE) is less than version 4.1. You cannot generate alarms for Explorer 10/100 or Explorer Gigabit hardware analyzers.

Current Module Alarms

When you right-click on an analyzer device in the Resource Browser, a menu appears. Select **Alarms...** and the **Current Module Alarms** dialog box appears with a list of alarms set up for the resource. If you have no alarms set for the resource, no alarms will display. Alarms apply to each analyzer card. If the host contains two analyzer cards, a separate **Current Module Alarms** dialog box appears for each card.

Alarm Group	Variable	Sample Type	Rising Value	Falling Value	Codec Type	Severity	Actions	Interval
MAC	Oversize Frames	Delta	100		N/A	Warning	Message	5
APP	POP Response ...	Absolute	60		N/A	Critical	Message	5
Network	RARP Octets	Delta	32000		N/A	Major	Message	5
Token Ri...	4096-8191 Byte...	Delta	32000		N/A	Critical	Message	5
Expert	Network Layer - ...	Delta	5		N/A	Warning	Message	5
MQOS	RTCP Packet D...	Absolute	5		PCMA	Minor	Message	5

New Alarm   Modify Alarm   Delete Alarm

OK

Figure 9-1. Current Module Alarms

From the **Current Module Alarms** dialog box you can add, modify, or delete alarms for the resource.

Press **New Alarm** to enable new alarms for a resource. The Alarm Editor dialog box appears. Multiple alarms of any type may be added. See the following section for more information on the Alarm Editor.

ALARM EDITOR

MAC | Application Response | Network | Token Ring | MQOS | Expert |

Variable	Sample Type	Rising Value	Falling Value	Severity	Actions	Interval	Enabled
64 Bytes Frames	Delta			Normal	Message		☐
65-127 Bytes Frames	Delta			Normal	Message		☐
128-255 Bytes Frames	Delta			Normal	Message		☐
256-511 Bytes Frames	Delta			Normal	Message		☐
512-1023 Bytes Frame	Delta			Normal	Message		☐
1024-1518 Bytes Fram	Delta			Normal	Message		☐
Oversize Frames	Delta	100		Normal	Message	5	☐
Frames	Delta	50000		Normal	Message	5	☐
Broadcast Frames	Delta	5000		Normal	Message	5	☐
Multicast Frames	Delta	5000		Normal	Message	5	☐
Unicast Frames	Delta	5000		Normal	Message	5	☐

OK   Cancel   Help

Figure 9-2. Alarm Editor

Highlight one or more alarms in the Current Module Alarm window. Press **Modify Alarm** to modify the highlighted alarms. From the **Modify Alarms** dialog box, change the characteristics for current alarms. The alarm variable name or alarm group name cannot be changed. Use the **New Alarm** option to add an alarm with a different variable.

MODIFY ALARMS

Alarm Group	Variable	Sample Type	Rising Value	Falling Value	Codec Type	Severity	Actions	Interval
Token Ring	4096-8191 Bytes Fram	Delta	32000		Not Applicable	Critical	Message	5
Expert	Network Layer - ICMP	Delta	5		Not Applicable	Warning	Message	5
MQOS	RTCP Packet Dropped	Absolute	5		PCMA	Minor	Message	5

OK   Cancel
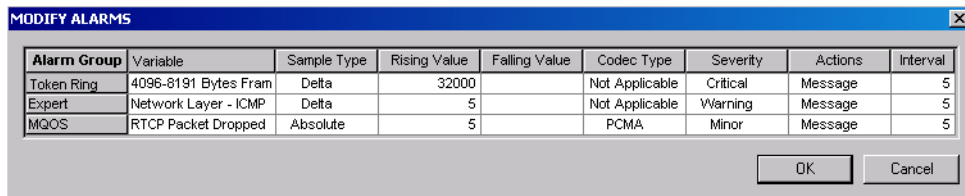
Figure 9-3. Modify Alarms

To delete one or more alarms, select the alarm(s) and press **Delete Alarm** in the **Current Module Alarms** dialog box. The alarms are deleted only for the current resource.

Alarm Editor

There are six alarm groups that appear on the tabs in the Alarm Editor. The Expert tab and Application Response tab are only available if you have the Expert Analysis. The VoIP tab only appears if you have the VoIP software plug-in.

Table 9-1 lists the alarm groups in the Alarm Editor.

Table 9-1. Alarm Editor

Alarm Editor	Description
VoIP	Allows you to modify and enable any of the 7 VoIP alarms. Alarms test for call jitter times, call setup times, dropped packets, and R-factors in VoIP calls. You can set alarms to test against specific codecs.
Expert	Allows you to modify and enable any of the 35 Expert alarms. Alarms test for discrete conditions at different protocol layers, such as NFS retransmissions at the application layer, overload utilization percentages at the MAC layer, or TCP/IP SYN packets at the transport layer. See the chapter on the Expert System for a description of the expert alarms.
Application Response	Allows you to modify and enable any of 8 application response time alarms. Alarms test for application response times related to application protocols such as SMTP, HTTP, or NFS.
MAC (Ethernet MAC Layer)	Allows you to modify and enable any of 21 MAC layer alarms. Alarms test for conditions related to Ethernet conditions such as utilization rate, packet size, errors, and frame types.
Token Ring Alarm	Allows you to modify and enable any of 29 Token Ring alarms. Alarms test for conditions related to Token Ring conditions such as utilization rate, packet size, errors, and frame types.
Network	Allows you to modify and enable any of the 65 Network alarms. Alarms test for conditions related to Network Layer conditions, such as IP/IPX/ARP packet or octet counts.

Click on the appropriate tab to display the alarm table you want. Each alarm can be used with the default values provided by OPV-PE, or you can modify them with the Alarms Editor to precisely meet your resource monitoring needs.

The complete selection of alarms for that type is shown in each tab in the alarm editor. Each line in the table is called an alarm or alarm row. You can add as many alarms as you want in the table.

If a threshold is exceeded for any enabled alarm, an alarm event occurs. The event is reported according to the value configured in the **Action** field for the alarm row.

VoIP Alarms

For VoIP alarms, alarms can be created from the VoIP Views interface as well as by double-clicking on the host.

The **Codecs** field within the alarm editor allows you select a specific codec or to ignore the type of codec used. For example, to trigger the alarm only when a G.711 codec is used, set the **Codecs** field to **G.711**. To trigger the alarm without looking at the codec type, set the **Codecs** field to **All Codecs**.

VoIP uses a simple threshold value to trigger the alarm. When the threshold value is crossed, the alarm is triggered and the alarm action is taken. Most alarms trigger when the current value exceeds a threshold, such as for call jitter. However, the R-factor alarms trigger when the current value goes below the threshold value. The lower the R-factor, the lower the call quality, so alarms trigger when the R-factor drops below a threshold.

The alarm conditions are checked for each call; if threshold values are reached, alarms will trigger only once per call.

Expert Alarms

During transmit or receive, expert symptoms are logged as they occur. You can test for certain thresholds for these conditions by setting alarms using the Expert tab of the Alarm Editor. See the chapter on the Expert system for more information about the expert alarms listed below.

Expert Alarms are only available if you are using Expert Analysis.
Table 9-2 lists all Expert Alarms.

Table 9-2. Expert Alarms, Listed by Protocol Layer

Application Layer	Network Layer
ICMP All Errors	HSRP Coup/Resign
ICMP Destination Unreachable	Duplicate Network Address
ICMP Redirect	Unstable MST
Excessive BOOTP	SAP Broadcasts
Excessive ARP	OSPF Broadcasts
NFS Retransmissions	RIP Broadcasts
	Total Router Broadcasts
Transport Layer	ISL Illegal VLAN ID
TCP/IP SYN Attack	ISL BPDU/CDP Packets
TCP/IP RST Packets	IP Time to Live Expiring
TCP/IP Retransmissions	Illegal Network Source Address
TCP/IP Zero Window	
Data Link Layer, Ethernet	**Data Link Layer, TOKEN RING**
Overload Utilization Percentage	Overload Utilization Percentage
Overload Frame Rate	Overload Frame Rate
Illegal MAC Source Address	Illegal MAC Source Address
Total MAC Stations	Total MAC Stations
New MAC Stations	New MAC Stations
Excessive Broadcasts	Excessive Broadcasts
Excessive Multicasts	Excessive Multicasts
Excessive Collisions	

Using Alarms with Different Devices

Alarms can be used with the following hardware analyzer devices or adapters. For analyzer cards or adapters, the hardware device must reside in a host that is running a version of OPV-PE 4.1.

The software image for OPV-LA analyzers must be at version 4.1.

Table 9-3 shows the alarms that can be used with each Fluke Networks analyzer device.

Table 9-3. Alarms and Hardware Devices

	Ethernet	Token Ring	Network	Application Response	Expert	VoIP
Local NDIS Module	YES	YES	YES	YES	YES	YES
Remote NDIS Module	YES	YES	YES	YES	YES	YES
OPV-LA System	YES	N/A	YES	YES	YES	YES
Fast Ethernet Traffic Analyzer	YES	N/A	YES	NO	NO	NO

GPI-1XX and DPI-1XX analyzer devices are not supported for alarms in OPV-PE version 4.1.

Thresholds and Alarms

Alarm thresholds are set by specifying the values in the **Sample Type**, **Rising Value**, **Falling Value**, and **Interval** fields for each alarm row in the alarm table. The numbers or percentages set for rising and falling values are referred to as thresholds. The key to creating a meaningful alarm is to specify these values so you get alerted to the exact network conditions you want to analyze.

The sample type can be set to either **Delta** or **Absolute**. The setting for the **Sample Type** field determines how OPV-PE will use the threshold values set in the **Rising Value** and **Falling Value** fields.

An absolute sample means that if the **Rising Value** is exceeded an alarm event occurs. If a value is specified for the **Falling Value**, an alarm event occurs when the value drops below the threshold.

A delta sample type means that if a difference between samples increases (rising) or decreases (falling) over time is more than the specified threshold, an alarm event occurs. The **Interval** field sets the time period between samples. Samples are actually taken at least twice as often as the interval. This allows the detection of threshold crossings that span the sample boundary. For example, if the delta sample is taken twice per interval, the sum of the latest two samples are compared to the threshold.

For most cases, the default **Sample Type** of delta is more useful. One exception is the MAC Layer Alarm for Utilization. Because utilization is expressed in the **Rising Value** field as a percentage, the absolute sample type is more useful to catch utilization that exceeds a certain percentage from a baseline of zero network traffic.

VoIP alarms do not use the **Sample Type**, **Rising Value**, **Falling Value**, and **Interval** fields. A simple threshold value is used to trigger the alarm when the threshold is exceeded.

Alarm Actions

Each line in an alarm table has a unique set of actions associated with it that will occur if the alarm is triggered.

By default, two actions always occur when an alarm is triggered – an audible alarm and a message in the **Message** window. You can set one additional action to occur when you set the action to a type other than **Message**. For example, setting the alarm action to **E-mail** results in an audible alarm, a message, and an e-mail message when the alarm is triggered.

You can have one of nine actions associated with the alarm. Possible actions appear in a menu when you select the **Actions** field. Not all actions are available for all device types. Use the scroll bar to see all available actions. Table 9-4 describes alarm actions and which host types are supported.

Table 9-4. Alarm Actions

Alarm Action	Description	Support by Host Type
Message	records the message in the Message window in the OPV-PE main window and sounds the audible alarm. No other actions occur if this setting is selected. This is the default value for alarm actions.	OPV-PE, OPV-LA
E-mail	sends the message to pre-configured e-mail addresses. Your e-mail application does not need to be running for alarms to generate e-mail messages.	OPV-PE, OPV-LA
Pager	sends alarms to pre-configured pager numbers.	OPV-PE only
Log	records alarms in a pre-configured log file and saves the buffer to disk.	OPV-PE, OPV-LA
Stop&Save	stops the module when the alarm occurs. If the host is a PC running OPV-PE, the buffer is saved to disk. The name auto-matically assigned to this file is based on the date and time of the alarm event.	OPV-PE
Stop&Report	stops the module when the alarm occurs. OPV-LA only reports that the analyzer has stopped by sending a message.	OPV-LA
Restart	resets all counters and begins capture from the point where the alarm occurred. All counters are set to zero and the resource begins capture. This allows you to collect data and count it after a particular event has occurred.	OPV-PE, OPV-LA
Auto Save	automatically saves data in the capture buffer at the time the event occurs.	OPV-PE

<div align="center">**Table 9-4. Alarm Actions (continued)**</div>

SNMP Trap	sends an SNMP trap to a specified management station(s). The trap destinations are configured as part of the host configuration for devices containing analyzer cards. The SNMP service must be installed and started for the trap to be sent. The OPV-PE MIB or OPV-LA MIB for the host will be available for the SNMP management station.	OPV-PE, OPV-LA
Execute	starts an executable file. OPV-PE does not allow selection of a non-executable file. Executable files with extensions of .exe, .bat, or .cmd are allowed. When the Execute action is selected, a dialog box appears to specify the executable file. Only one file can be selected with each alarm condition.	Local OPV-PE only

You can select but not configure the E-mail, Log File, Pager, or SNMP Trap action on a remote host running OPV-PE. If the settings that support these actions have not been configured correctly at the remote host, the alarm action does not occur when the alarm is triggered.

Setting an absolute value as the threshold for an alarm will trigger an action only once.

Log File Settings

There is one log file per host. All alarms on the local host go in one log file in OPV-PE. To set the name of this file, select **Host → Alarm Setting → Log File Settings**.

For the OPV-LA, log information is stored at the OPV-LA until requested by the user. OPV-LA hosts can store about 500 alarm messages. If more than 500 alarms occur, the OPV-LA writes over the log message with the earliest timestamp. When you want to view the file, go to **Host → Alarm Setting → Log File Settings.** Enter a file name, press **Get Alarm Log File**. The log information will be transferred to the named file in the `...\OPV-PE\Log` directory on the local host. Note that the dialog box for the log file name does not accept a complete path name for the OPV-LA log file.

E-Mail Settings

Microsoft Exchange or message utilities must be installed and enabled before E-mail and pager actions can occur.

When sending E-mail, multiple addresses can be configured from the **Host → Alarm Setting → E-mail Settings...** menu. Setting the addresses for alarm actions is a global setting for the host. All alarms reported by OPV-PE will go to the same set of E-mail addresses. For example, you cannot send some alarms to one set of e-mail addresses and some alarms to another set of e-mail addresses.

E-mail settings for OPV-PE hosts and OPV-LA hosts are slightly different. For analyzer devices in OPV-PE hosts, you set the list e-mail recipients for alarms from the **Host → Alarm Setting → E-mail Settings...** menu. All other e-mail configuration is performed from the local e-mail utility. For OPV-LA, e-mail is completely configured from the **Host → Alarm Setting → E-mail Settings...** menu. You set the sender address, SMTP domain, and the SMTP mail server address as well as the list of e-mail recipients for alarms. An example dialog box for setting up e-mail for OPV-LA hosts is shown below.
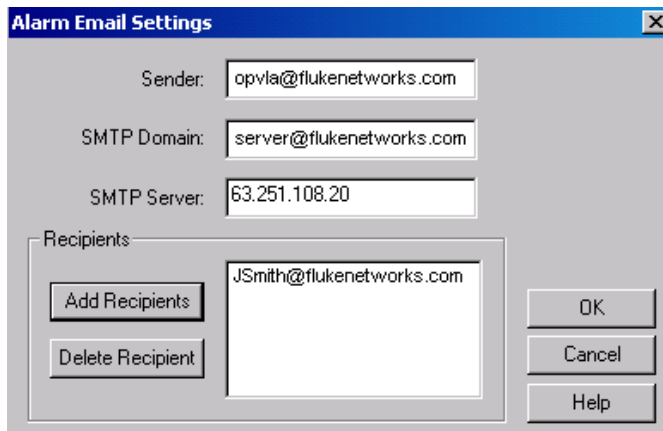
Figure 9-4. E-Mail Settings for OPV-LA

Pager Settings

The host must have a modem to use a pager. You must set an appropriate delay time when making a call to a pager.

When making a call to a pager, a single number can be configured from the **Host → Alarm Setting → Pager Settings...** menu. Setting the pager number for alarm actions is a global setting for the host. All alarms reported for analyzer devices in the host will go to the same pager number. public

SNMP Trap Settings

SNMP traps containing alarms can be sent to specified management stations as one of the alarm actions. Each host has its own list of management stations to receive traps. A set of management stations identified by their IP addresses is called a community.
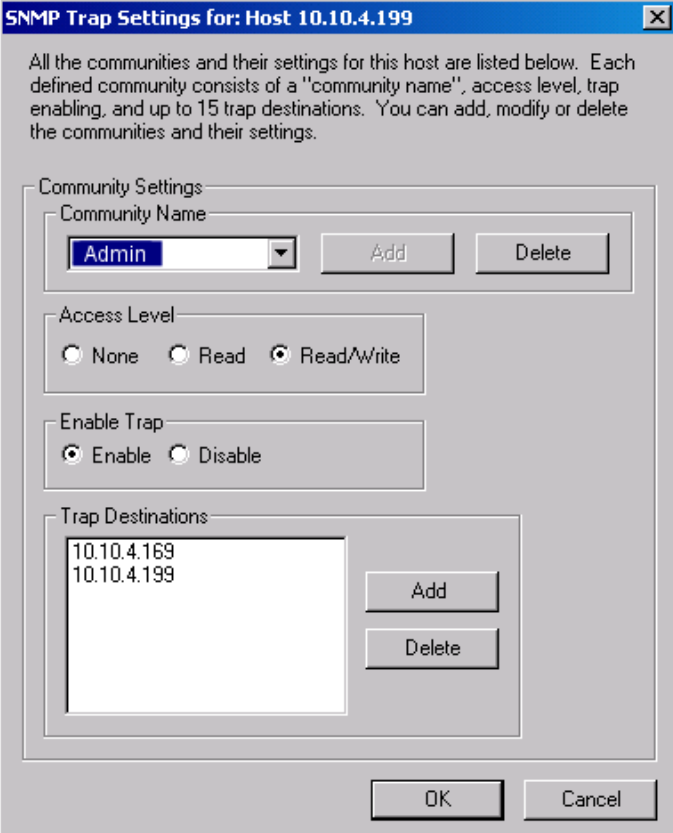
Any alarm, when triggered, is sent to all IP addresses specified in all communities configured for the host.

Trap Settings for OPV-LA

The stations to receive traps for a remote OPV-LA can be established from the local host running OPV-PE.

To set up trap destinations for a remote OPV-LA device, select the OPV-LA device in the Resource Browser and from the menu bar select **Host → Alarms Settings → SNMP Trap settings**. The SNMP Traps dialog box appears. Use the **Community Settings** area to add or delete communities. List all IP addresses for the community in the **Trap Destinations** area.

The community does not require read or write privileges to receive SNMP traps containing alarms. You can disable any community from receiving traps by setting the **Disable** radio button. When you click the **Disable** button for a community, all IP addresses set as Trap Destinations for the community are deleted. Figure 9-5 shows an example SNMP Trap Settings dialog box for a OPV-LA host.

Figure 9-5. SNMP Trap Settings for OPV-LA

Multiple IP addresses may be set for each trap. A maximum of 15 trap destinations can be assigned to each community. All alarms will be sent to all specified trap destinations.

The traps and MIB variables defined for OPV-LA are defined in SNMPv2. Refer to the *OPV-LA User's Guide* for more information on SNMP management capabilities for OPV-LA and MIB information.

Trap Settings for OPV-PE Hosts

PCs running OPV-PE 4.1 that contain Fluke Networks analyzer cards or NDIS cards can function as hosts for sending SNMP Traps. When an alarm occurs and the **Actions** type is **SNMP Trap**, an SNMP Trap is sent to all the Trap Destinations configured for the local host.

For OPV-PE to send SNMP traps, the SNMP service must be installed, configured, and started on the OPV-PE host. The SNMP service must be installed, configured, and started locally. OPV-PE cannot perform SNMP Trap Setting for a remote OPV-PE host, only set alarms and alarm actions. Refer to Microsoft Windows documentation for information about how to install, run, and configure SNMP trap destinations on your Windows system.

OPV-PE has six different traps, one for each of the alarm groups. The number of alarm variable is the same except for VoIP alarms, which contain some additional information. Each trap contains all the information (Severity, Threshold, etc.) as specified in the alarm interface for each alarm.

Communities do not require read or read/write privileges to receive traps.

OPV-PE does not provide the full functionality of an SNMP extension agent. The OPV-PE extension agent is only for sending traps. MIB variables are defined only to be sent along with the trap. Although MIB variables are defined as read-only, the SNMP management station cannot do a GET operation on those variables.

The traps and MIB variables defined for OPV-PE are defined in SNMPv1. Refer to the `OPV-PEalarms.mib` file in your OPV-PE directory for complete MIB details.

Viewing the Alarm List and the Alarm Log

There are several ways to access the list of alarms or a log of alarm events. From Detail View, click on the [icon] button to open a window from which you can see the **Alarms List** and **Alarm Log** tab. From Summary View, click on the **Alarms** or **Alarm Log** tab for the resource.

Click on the **Alarms List** tab to view all alarms set for this resource. This is same view as the alarms listed in the Current Module Alarms dialog box. The alarm group name is listed for the alarm.

Click on the **Alarm Log** tab to see a list of the alarms that have triggered for this resource. Alarms are numbered consecutively as they occur over time.

Hints and Tips for Alarms

- Click, hold, and drag a column border to resize columns in the alarm table.

- To set more than one alarm of the same type, click on the type you want to duplicate and press the **Insert** key. A new alarm row appears below the current row. Fill out the settings in the new row.

- To set one alarm that has multiple actions, click on the alarm type you want to duplicate and press the **Insert** key. Change the **Actions** field of the new row to the additional action you want. For example, you could have one alarm of type Packets with the action set to E-mail and one alarm of type Packets with the alarm type set to Pager. Note that if the alarm rows are identical except for the action, you will get two messages in the message window for the alarm, since a message is always posted when any alarm is triggered.

- You can copy values in one alarm row to another. Click on the Alarm Type in the alarm row you want to copy. The row highlights; press Crtl + C to copy. Click on the Alarm Type in the alarm row where you want to place the copied values and press Crtl + V.

Alarm Examples

The following are six examples for alarms and alarm groupings. Each provides a picture of the **Current Module Alarms** dialog box and a description of what will occur when for the alarms are triggered.

Alarm Example, Utilization

Alarm Group	Variable	Sample Type	Rising Value	Falling Value	Codec Type	Severity	Actions	Interval
MAC	Utilization %	Absolute	50		N/A	Normal	Message	5

New Alarm   Modify Alarm   Delete Alarm

OK

Figure 9-6. Alarm Example, Utilization

This simple example shows an alarm group consisting of one MAC Layer alarm for Utilization. This alarm samples network traffic at five-second intervals. When the absolute, rising value of 50 (percent utilization) is exceeded, OPV-PE issues an audible alarm and displays a message in OPV-PE's message window.

Alarm Example, MAC Errors

Alarm Group	Variable	Sample Type	Rising Value	Falling Value	Codec Type	Severity	Actions	Interval
MAC	Oversize Frames	Delta	100		N/A	Normal	Message	5
MAC	Errors	Delta	250		N/A	Normal	E-Mail	5
MAC	Errors	Delta	50		N/A	Normal	Message	5
MAC	CRC/Alignment	Delta	100		N/A	Normal	Message	5
MAC	Fragments	Delta	100		N/A	Normal	Message	5

[New Alarm]   [Modify Alarm]   [Delete Alarm]

[OK]

Figure 9-7. Alarm Example, MAC Errors

This example shows an alarm group consisting of five MAC Layer alarms: Errors (two alarms), Oversize Frames, CRC/Alignment, and Fragments. Each of these alarm counters are checked at five-second intervals. When an alarm threshold for any of these five alarms is exceeded, OPV-PE issues an audible alarm and displays a message in OPV-PE's message window.

Assume that overall error rate is of particular interest in this example. The Severity setting instructs OPV-PE to include a Warning message with all alarm messages when the error rate is greater than 250. The Actions setting instructs OPV-PE to send an e-mail message whenever the rising value (threshold) for the overall error rate exceeds 250.

Alarm Example, Frame Size

MAC	256-511 Byte Fr...	Delta	100		N/A	Normal	Log File	5
MAC	512-1023 Byte F...	Delta	100		N/A	Normal	Log File	5
MAC	1024-1518 Byte ...	Delta	100		N/A	Normal	Log File	5
MAC	Oversize Frames	Delta	100		N/A	Warning	Log File	5

New Alarm | Modify Alarm | Delete Alarm

OK

Figure 9-8. Alarm Example, Frame Size

This example shows an alarm group consisting of four MAC Layer alarms:
Oversize Frames, 256-511 Byte Frames, 512-1028 Byte Frames, and 1024-1518
Byte Frames. Each of these alarms samples network traffic at five-second intervals.
When an alarm threshold for any of these four alarms is exceeded, OPV-PE issues
an audible alarm and displays a message in OPV-PE's **Message** window. In
addition, the alarms will be logged to the Log file specified. For Oversize Frames,
the notification is a warning message.

Alarm Example, VoIP Calls

Alarm Group	Variable	Sample Type	Rising Value	Falling Value	Codec Type	Severity	Actions	Interval
🔴 MQOS	Setup Time	N/A	200	N/A	N/A	Normal	Message	N/A
🔴 MQOS	Jitter	N/A	500	N/A	All Codecs	Critical	Stop&S...	N/A
🔴 MQOS	Jitter	N/A	200	N/A	All Codecs	Warning	E-Mail	N/A
🔴 MQOS	User R Factor	N/A	50	N/A	All Codecs	Warning	Message	N/A

New Alarm   Modify Alarm   Delete Alarm

OK

Figure 9-9. Alarm Example, Call Jitter and Call Setup Time

This example shows an alarm group consisting of four alarms: Call Setup Time, Call Jitter, severe Call Jitter, and User R-factor. When an alarm threshold for any of these four alarms is exceeded, OPV-PE issues an audible alarm and displays a message in OPV-PE's **Message** window.

The Severity setting instructs OPV-PE to include Warning message when the call jitter exceeds 200ms. A Critical message is included with all alarm messages when the call jitter exceeds 500ms, plus instructions to OPV-PE to stop and save frame contents to a capture file. For the R-factor alarm, the alarm triggers when the User R-factor value drops below the threshold value.

Two alarms are set for the jitter alarm variable. You can use the same variable to create multiple alarms. Each alarm is defined by a single row in the table.

Alarm Example, Token Ring

Alarm Group	Variable	Sample Type	Rising Value	Falling Value	Codec Type	Severity	Actions	Interval
Token Ri...	Frames	Delta	50000		N/A	Normal	Message	5
Token Ri...	Errors	Delta	400		N/A	Critical	E-Mail	5
Token Ri...	Utilization %	Absolute	10		N/A	Normal	Message	5
Token Ri...	Line Errors	Delta	100		N/A	Warning	Message	5

New Alarm   Modify Alarm   Delete Alarm

OK

Figure 9-10. Alarm Example, Token Ring

This example shows alarms consisting of four MAC Layer alarms for Token Ring: Frames, Total Errors, Utilization, and Line Errors. All of these alarm counters are checked at five-second intervals. When an alarm threshold for any of these four alarms is exceeded, OPV-PE issues an audible alarm and displays a message in OPV-PE's message window.

Assume that overall error rate is of particular interest in this example. The Severity setting instructs OPV-PE to include a Critical message with all alarm messages when the error rate is greater than 400. A Warning message is included when line error rate exceeds 100. The Actions setting instructs OPV-PE to send an e-mail message whenever the rising value for the overall error rate exceeds the threshold.

Alarm Example, Expert and Application Response

Alarm Group	Variable	Sample Type	Rising Value	Falling Value	Codec Type	Severity	Actions	Interval
APP	HTTP Respons...	Absolute	100		N/A	Warning	Message	5
APP	DNS Response ...	Absolute	100		N/A	Warning	Message	5
APP	FTP Response ...	Absolute	60		N/A	Warning	Message	5
Expert	Transport Layer ...	Delta	100		N/A	Warning	Message	5

New Alarm Modify Alarm Delete Alarm

OK

Figure 9-11. Alarm Example, Expert and Application Response

This example shows alarms consisting of three Application Response and one Expert alarm. All of these alarm counters are checked at five-second intervals. When an alarm threshold for any of these four alarms is exceeded, OPV-PE issues an audible alarm and displays a warning message in OPV-PE's message window.

Two different alarm groups are represented, Expert and Application Response.

Chapter 10
Expert Features

Automatic diagnostic analysis, expert data views, application response times, and expert alarms are referred to collectively as OPV-PE Expert Features.

OPV-PE observes the traffic on network segments, learns their unique characteristics, and constructs a database of network entities from the traffic it sees. OPV-PE uses protocol decoding to learn about the connections, network stations, routing nodes, and subnetworks related to the frames in the buffer or capture file. From this information, OPV-PE can detect potential problems on the network.

Problems detected by OPV-PE are categorized as being either symptoms or analyses. When OPV-PE detects an abnormal or unusual network event, it logs a symptom. A symptom indicates that a threshold has been exceeded and may indicate a problem on your network.

Several symptoms analyzed together, high rates of recurrence of specific symptoms, or single instances of particular network events causes OPV-PE to conclude that the network has a problem. These are logged as analyses.

In addition to reporting significant problems, OPV-PE provides helpful diagnostic information related to the symptom or analyses.

No configuration is required to begin using the expert logic; however, some of the default thresholds for expert events may be changed. Configuration settings are organized as a tree structure within a single window to allow for efficient and easy configuration changes.

In monitor mode, the expert system does not work with remote DPI-1XX analyzers, GMM analyzer cards, or remote analyzer cards or NDIS cards running in systems with OPV-PE 3.2 or lower. Expert features will work on captures obtained from these devices.

Expert System Views

The expert views present expert information on capture files, a capture buffer, or in monitoring mode. The following Expert views are available from the **Data Views** or **Capture View** toolbar:

Expert View

Expert views are available from the Data Views or Capture View toolbars, if supported by the current resource. The Expert system presents a matrix of different views showing network symptoms, analyses, and entities by protocol layer. Also, an Expert Diagnostic Message showing the definition, possible causes, and suggested actions can be obtained for any symptom or analyses.

Application Response Time View

The Application Response Time view depicts performance information for specific applications. For each supported application the Application Response Time View will present the Application, Minimum Response Time (Min Time), Maximum Response Time (Max Time), Average Response Times (Avg Time), and the Number of Connections (Connections) processed to derive these times.

Duplicate Network Address View

The Duplicate Network Address view depicts each duplicate network (IP/IPX) address detected and its associated MAC layer bindings.

See Chapter 6, "Views" for more information on Expert Views.

Getting Started with Expert View

When OPV-PE finds an event that could indicate a network problem, the event is logged in appropriate tables, and the appropriate counters are incremented in the overview tables.

When you press the ![button] button to start Expert View, overview tables of symptoms are displayed. An example of the symptom overview tables is shown in Figure 10-1. You can access different expert views by clicking one of the layer buttons to the left of the tables, or by selecting one of the tabs at the bottom. One side of the matrix selects an overview or a breakdown by protocol layer. The tabs at the bottom form the other axis, allowing views of symptoms, analyses, or network entities.
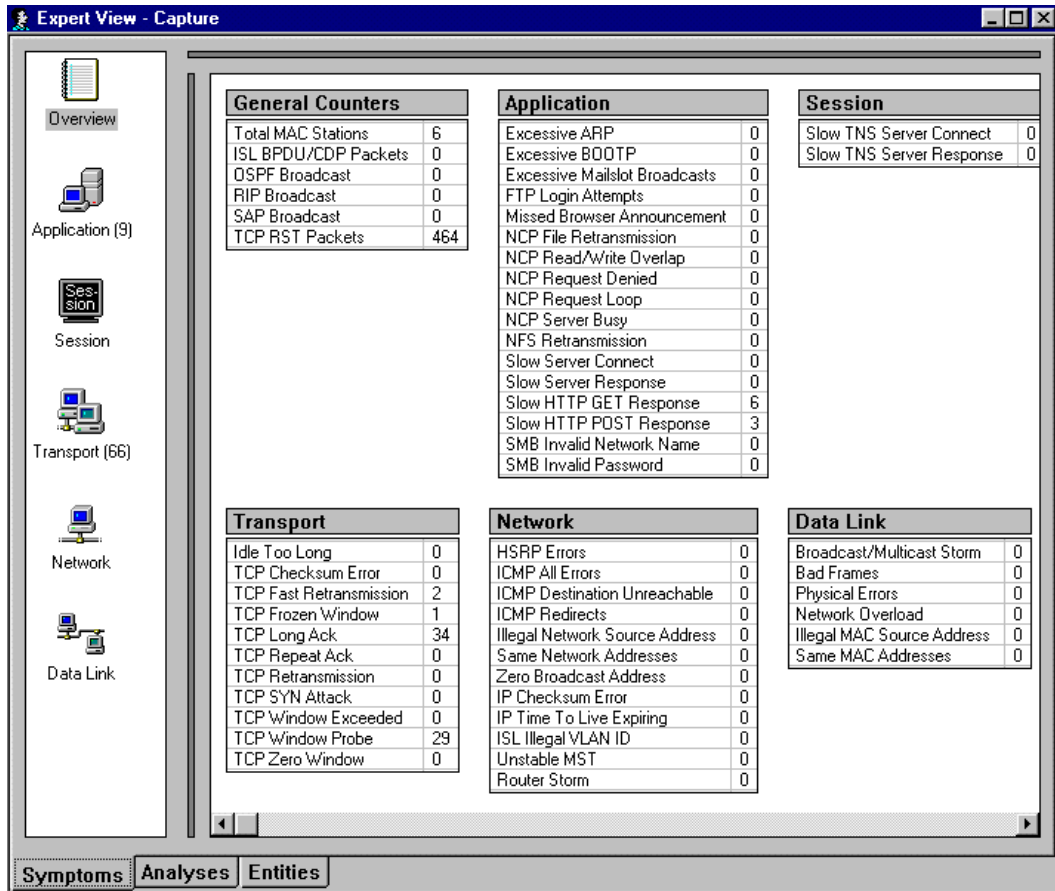
Figure 10-1. Expert Overview Example

Expert Overview Details

Click on any counter in the display to view a table listing only the events for the selected symptom. The display has a summary area showing all symptoms and a detail area for the current selected symptom.

The summary area contains a table showing frame ID (Capture View only), source address, destination address, VLAN ID, timestamp and other information for each event. Each table entry shows a summary in the **Expert Summary** field that provides more information about the symptom. The Expert Overview Detail table contains the last 2,000 symptoms for each protocol layer.

An example of the overview detail tables, after clicking on the TCP Retransmissions counter, is shown in Figure 10-2. The summary area (top) lists all occurrences of the selected symptom. The detail area (bottom left) shows an object tree view of the symptom selected in the summary area. This provides information about the stations and ports that are associated with the selected symptom. The vital statistics for the symptom selected in the summary area is shown in the detail area to the right. The first table shows other symptoms discovered for this conversation. Detailed statistics for each entity in the conversation and statistics for the conversation itself are also included.

The summary and detail areas are separated by large gray bars (one vertical and one horizontal) which can be used to size each area as needed.

Click on a column header to sort the symptoms in the summary area by the values in the column. Clicking a column header a second time changes the sort order from descending to ascending.

Expert Symptom	Timestamp	Expert Summary
TCP/IP Fast Retransmission	Fri May 05 09:29:50	In 0 ms (< 100 ms) betw...
TCP/IP Fast Retransmission	Fri May 05 09:29:51	In 0 ms (< 100 ms) betw...

Overview

Application (9)

Session

Transport (64)

Network

Data Link

TCP/IP Fast Retransmissio...
└─ TCP: 1551 <-> 80
   ├─ 161.231.16.2
   │ └─ 080020:A32A5
   └─ 161.231.16.14
      └─ 006097:9FA68

Symptoms	
TCP/IP Fast Retransmission	2
TCP/IP Long Ack	3
TCP/IP Window Probe	26

Host 1: 161.231.16.2	
Packets In	3861
Packets Out	4379
Octets In	49658
Octets Out	27419
Non Unicast Packets Out	0
Associated MAC Address	08002

Host 2: 161.231.16.14	
Packets In	280
Packets Out	232
Octets In	20386
Octets Out	26118
Non Unicast Packets Out	0
Associated MAC Address	00609

Symptoms | **Analyses** | **Entities**

Figure 10-2. Expert Overview Detail Table Example

Expert Layers

OPV-PE categorizes network problems according to the network "layer" at which they occur. During capture or monitor, OPV-PE decodes frames. The decode information embedded in each frame is used to categorize the problem.

Layers are selected from the panel on the left of the Expert window. A display of symptoms can be refined by pressing one of the layer icons in the display.

The categories used by the Expert system are shown below. The categories correspond roughly to the OSI protocol layer model for communications.

Layer	Description
Application	OPV-PE checks for application problems. These are generally servers running protocols with a client-server relationship, such as HTTP or FTP.
Session	OPV-PE checks for problems related to administration and security.
Transport	OPV-PE checks for problems related to the efficiency of end-to-end communications and error recovery. This layer essentially logs connection-related problems.
Network	OPV-PE checks for network addressing and routing problems. It also interprets traffic between subnets.
Data Link	OPV-PE logs symptoms/problems with the actual transfer of data across the network. For example, it keeps track of the number of broadcast frames and the number of bytes transmitted during a predefined interval to detect network overload. Physical errors such as CRC errors and frames that are too short are also detected. The software does not perform diagnoses on the physical characteristics of the network such as electrical voltage and current.

Figure 10-3 shows an example Expert Application Layer window for symptoms. The summary area (top) lists all symptoms for the selected layer. The detail area (bottom left) shows an object tree view of the symptom selected in the summary area. This provides information about the stations, ports, and their relationships that are associated with the selected symptom. The vital statistics for the symptom selected in the summary area are shown in the detail area to the right. The first table shows other symptoms discovered for this conversation. Detailed statistics for each entity in the conversation and statistics for the conversation itself are also included.

The summary and detail areas are separated by large gray bars (one vertical and one horizontal) which can be used to size each area as needed.
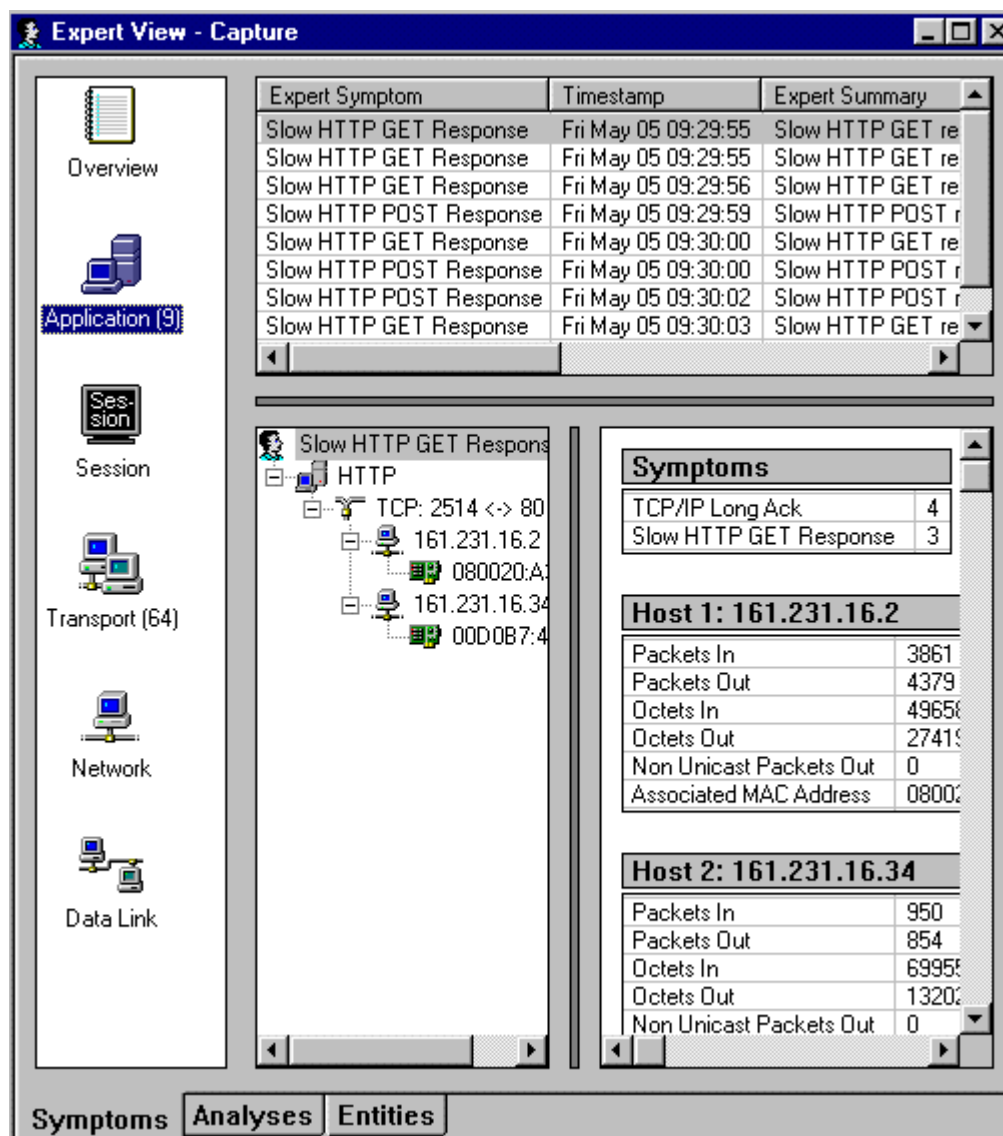
Figure 10-3. Expert Application Layer Example

The interface provides a matrix of expert information views. For each layer, the symptoms, analyses, and objects can be displayed by selecting a tab at the bottom of the window.

Click on a column header to sort the symptoms in the summary area by the values in the column. Clicking a column header a second time changes the sort order from descending to ascending. Double-click the network address in Station 1 in the Application/Session Layer to jump to the first connection to that server in the Transport Layer. Double-click the network address in Station 2 in the Application/ Session Layer to jump to the first connection from the client to that server in the Transport Layer.

Table 10-1 is a list of the general categories of symptoms and analyses discovered by OPV-PE's expert logic broken down by layer.

Table 10-1. Expert Symptoms and Analyses by Layer

Layer	Expert Symptoms	Expert Analyses
Application	Excessive Mailslot Broadcasts FTP Login Attempts Missed Browser Announcement NCP File Retransmission NCP Read/Write Overlap NCP Request Denied NCP Request Loop NCP Server Busy NFS Retransmission Slow HTTP GET Response Slow HTTP POST Response Slow Server Connect Slow Server Response SMB Invalid Network Name SMB Invalid Password	No Server Response No HTTP POST Response NCP Too Many Retransmissions NCP Too Many Requests Denied NCP Too Many Request Loops
Session	TNS Slow Server Connect TNS Slow Server Response	No WINS Response
Transport	Idle Too Long TCP Checksum Errors TCP Fast Retransmission TCP Frozen Window TCP Long Ack TCP Repeat Ack TCP Retransmission TCP SYN Attack TCP Window Exceeded TCP Window Probe TCP Zero Window	Non-Responsive Station Too Many Retransmissions
Network	HSRP Errors All ICMP Errors Illegal Network Source Address IP Checksum Errors IP Time To Live Expiring ISL Illegal VLAN ID Router Storm Same Network Addresses Unstable MST Zero Broadcast Address	Duplicate Network Address
Data Link	Bad Frames Broadcast/Multicast Storms Excessive ARP Excessive BOOTP Illegal MAC Source Address Network Overload Physical Errors Same MAC Addresses	None

Expert Symptoms, Analyses, and Network Entities

When you capture or monitor packets on a network segment, OPV-PE immediately begins constructing a database of network entities from the traffic it sees. OPV-PE uses protocol decoding to learn all about the connections, network stations, routing nodes, and subnetworks related to the frames in the capture buffer. From this information, OPV-PE can detect potential problems on the network. These problems are categorized as symptoms or analyses. Alarms can be set to automatically alert you as these potential problems are discovered.

When viewing expert symptoms or analyses in the Summary area, double-click on a Frame ID to jump to that frame in Capture View. Capture View shows the frame decode. Double-click on an address to jump to a table highlighting an entry describing the associated entity.

Symptoms

When the Expert detects an abnormal or unusual network event, it logs a symptom. A symptom indicates that a threshold has been exceeded and may indicate a problem on your network. Counters for symptoms can be used to trigger alarms.

Press the **Symptoms** tab on the Expert window to view network events that may result in network problems. See Figure 10-1 and Figure 10-3 for examples of displays of symptoms.

Tables in the Detail Area for Symptoms

The first list displays which types of symptoms and how many of them are found in the connections between the two network stations.

The second list displays the network traffic of the first network station. It shows how many packets and bytes of data are sent and received by the station. It shows how many broadcast packets the station sent and the MAC addresses associated to the station.

The third list displays the network traffic of the second network station, if present.

The fourth list displays the network traffic between the two network stations. It shows how many packets and bytes of data are sent from the first to the second and the second to the first.

Analyses

High rates of recurrence of specific symptoms or single instances of particular network events cause the software to assert that the network has a real problem. These are logged as analyses. Analyses should be investigated immediately. Counters for analyses can be used to trigger alarms.

Press the **Analyses** tab on the Expert window to view the diagnoses derived from the current packet analysis. Analyses display exactly like symptoms. See Figure 10-1 and Figure 10-3 for examples.

Tables in the Detail Area for Analyses

The first list displays which types of diagnoses and how many of them are found in the connections between the two network stations.

The second list displays the network traffic of the first network station. It shows how many packets and bytes of data are sent and received by the station. It shows how many broadcast packets the station sent and the MAC addresses associated with the station.

The third list displays the network traffic of the second network station, if present.

The fourth list displays the network traffic between the two network stations. It shows how many packets and bytes of data are sent from the first to the second and the second to the first.

Entities

OPV-PE extracts information from the data stream to form its network entity database. Entities can be DLC stations (physical and logical link layers), network stations (network layer), connections (transport layer), sessions (session layer), applications (presentation, and application layers), a subnetwork, a router, or other useful data entities.

Press the **Entities** tab on the Expert View window to view network objects discovered from the current packet analysis.The example below shows the entities discovered for the Transport Layer. The detail area shows details for both the conversation and the individual stations in the conversation.
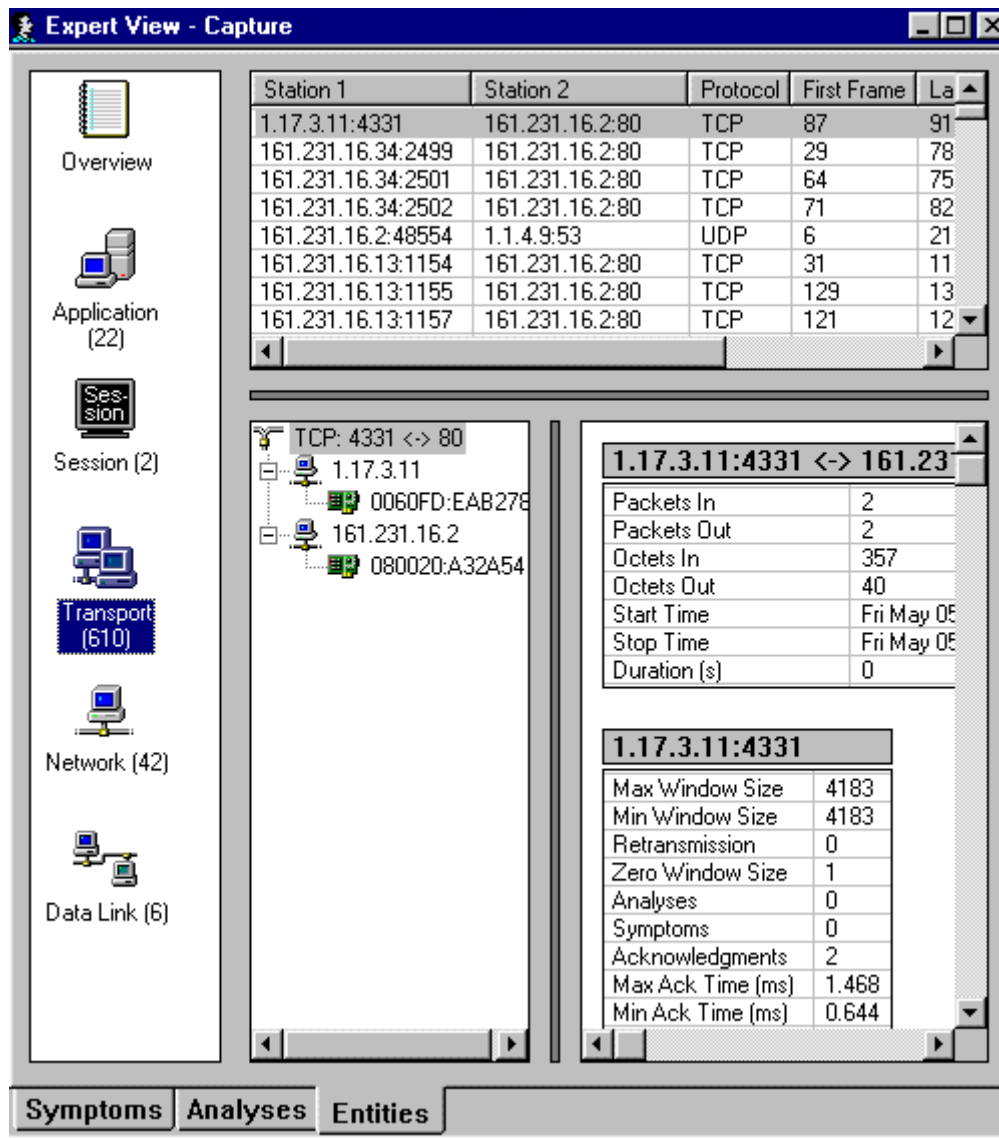
Figure 10-4. Entities for the Transport Layer Example

Application/Session Lists for Entities

The list displays the number of packets and bytes of application data that are sent and received by the server. The times when the first and last packets seen by this server are noted, and the duration is the difference between the times. The maximum and minimum response times of this server are shown. The average response time is the total response time divided by the number of responses.

Transport Lists for Entities

The first list displays the network traffic between the connection. It shows the number of packets and bytes of TCP data sent and received by the first station. The times when the first and last packet seen in this connection are noted, and the duration is the difference between the times.

The second list displays statistics for the first station. It shows the maximum and minimum window sizes, number of retransmissions, and the number of zero window size events that occurred in this TCP connection. The number of diagnoses and symptoms found are also shown. The maximum and minimum acknowledge times are displayed if they are present. The average acknowledge time is the total acknowledge time divided by the number of acknowledgments.

The third list displays the same statistics described above for the other station in the conversation.

Network Lists for Entities

The first list displays the network traffic of the network station. It shows how many packets and bytes of data are sent and received by the station. It also shows how many broadcast packets the station sent and the MAC addresses associated with the station.

The second list displays the protocols this station used, the number of packets and bytes of data of that protocol sent and received by the station, and the first and last frames in which the protocol occurred.

The third list displays the network traffic between this station and other network stations. It shows how many packets and bytes of data are passed between the two stations, how many packets and bytes of data are used on a certain protocol, and the first and last frames used.

Data Link Lists for Entities

The first list displays the network traffic of the physical station. It shows how many packets and bytes of data are sent and received by the station. It shows the network addresses associated to the station.

The second list displays the protocols this station used, the number of packets and bytes of data of that protocol sent and received by the station, and the first and last frames in which the protocol occurred.

The third list displays the network traffic between this station and other physical stations. It shows how many packets and bytes of data are passed between the two stations, and how many packets and bytes of data are used on a certain protocol, and the first and last frames used.

Expert Diagnostic Messages

From any summary table you can double-click on any symptom or analysis to display an Expert Diagnostic Message. Contents of the **Expert Diagnosis** window include:

- A summary of the symptom or analyses, including addresses and frame IDs

- A description of the Expert symptom or analyses

- Possible causes

- Recommended actions

Figure 10-5 shows an example of the **Expert Diagnosis** window.
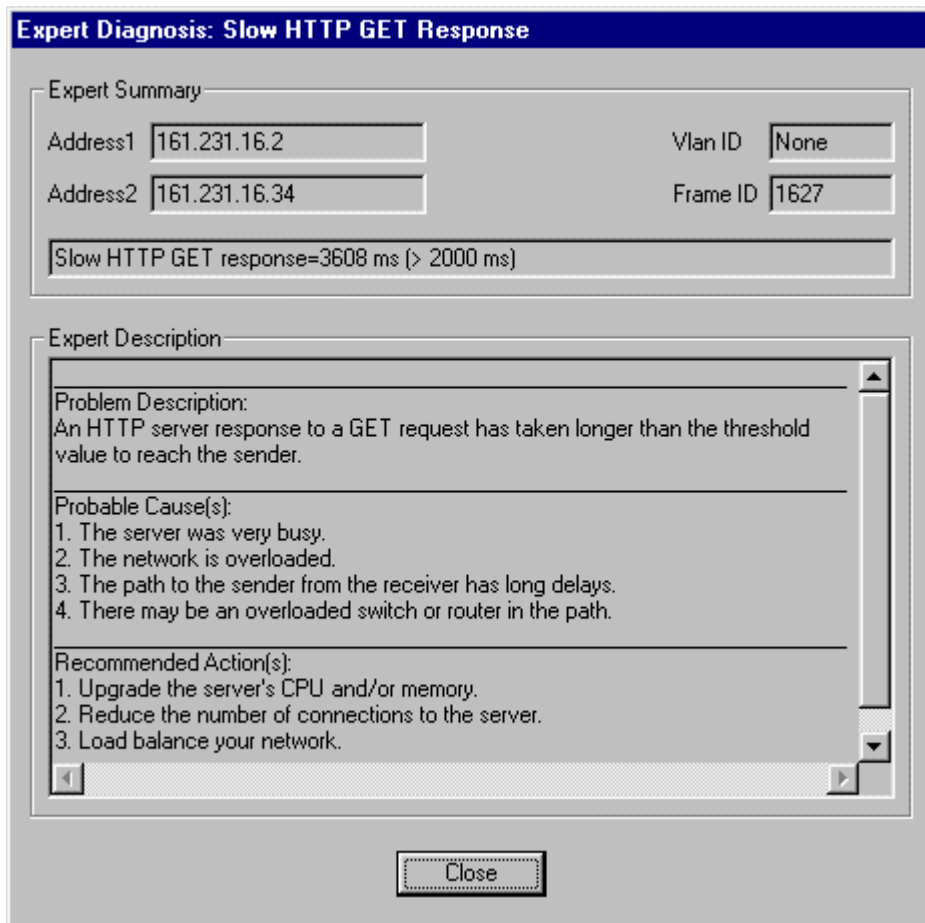
Figure 10-5. Expert Diagnosis Example

Working with the Expert System

Configuring the Expert System

Use the Expert Configurations dialog box to change expert settings. With the Expert View visible, select **Expert Settings** from the **Configuration** menu to view configuration options. An example Expert Configurations dialog box is shown below.
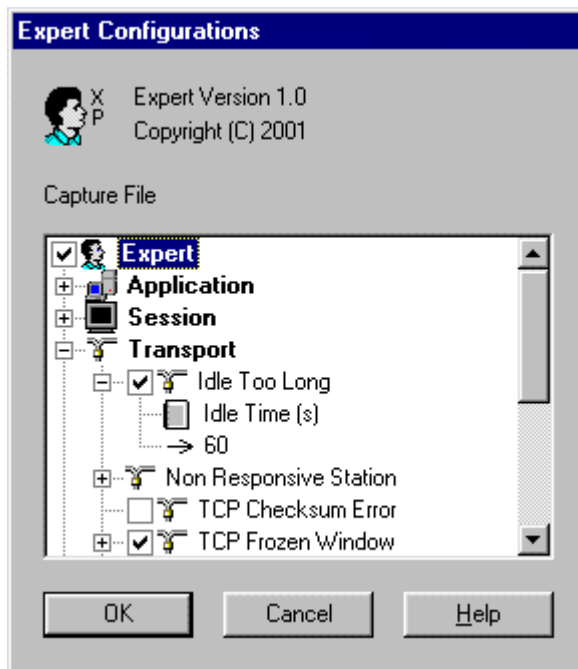
Figure 10-6. Expert Configuration Example

Settings are organized in a tree structure, with different network layers as the main branches in the tree. Symptoms are displayed as items under the layers. There is a checkbox in front of each item that can be enabled/disabled. Disabling an entire branch in the tree, such as Data Link, disables all expert symptoms that can be disabled for that layer. Transport or application symptoms cannot be disabled completely, so there is no checkbox by these items. The entire expert system can be disabled by removing the top level check next to **Expert**.

If the symptom has a threshold value, two items are displayed under it. The first shows what the threshold value means, the second is an edit control showing the current threshold value. The value is always a number. In the example above, the Idle Too Long symptom is expanded. The display shows the meaning (Idle Time, in seconds) and the current threshold (60) for triggering this event.

The tree can be expanded or collapsed by clicking on the plus or minus icon, double-clicking on the item, or using direction keys. The checkbox can be checked or unchecked by clicking on the checkbox or by selecting the symptom and pressing the **Space** bar. The edit control is activated by selecting the value and clicking on it or pressing the **Space** bar.

When a setting is changed, the number is checked against minimum and maximum values. Clicking anywhere inside the dialog box besides the edit control or pressing **Return** key closes the edit control and enters the new configuration value. Pressing the **Escape** key restores the original value.

Module Settings for the Expert System

Turning the expert system on or off can be controlled on a per-device basis. Select **Module → Settings...** from the **Configuration** menu. From the **Modes** tab, turn on/off the expert system using the check box.

Setting Expert Alarms

Expert Alarms allows you to set thresholds related to Expert Symptoms. Alarms can be configured to perform an action such as a page or e-mail, as with all other OPV-PE alarms. Alarms test for thresholds at different protocol layers, such as the number of NFS retransmissions at the application layer or a specific overload utilization percentage at the MAC layer.

Some network problems are not single events, but are indicated by certain thresholds or counters being exceeded. To catch these type of problems, use Expert Alarms. Many event counters within the Expert Alarm Table that can be used to flag network conditions that are not single events, such as excessive multicast broadcasts.

Customizing Expert Diagnostic Information

OPV-PE provides diagnostic information that is general to all networks. However, you can customize the diagnostic information to suit your environment.

As you use any diagnostic system you may find that certain error events occur regularly and or that events have a unique meaning in your environment. Custom solutions may apply to fixing the problems that are indicated by expert symptoms. By customizing the diagnostic information, you build an "information base" that applies to your particular environment. When the same problems occur, the custom information displays as well as standard information, providing the diagnostician with the benefit of previous experience related to your particular network.

The `ExpertMsg.INI` file contains OPV-PE's diagnostic information. This file can be changed using a text editor, thus giving you a way to add information. Rules for adding information to `ExpertMsg.INI` are included at the beginning of the file. Either possible causes or recommended actions can be added, or any other special technical note.

OPV-PE always looks for the file named `ExpertMsg.INI` in the OPV-PE installation directory and will use that file for its diagnostic information. If no `ExpertMsg.INI` file is found in the directory, OPV-PE will not provide diagnostic information.

Exporting Expert Data

You can export expert data to a comma delimited .csv file. With an Expert window active, select **Export...** from the **File** menu. The symptom list in the top panel is exported by default. From the Overeiw tab, all counters are exported.

If you want to export the Detail data in the bottom right panel of an Expert display, click on any field in any table in this panel and select **Export...** from the **File** menu. . Data for all tables in this panel are exported.

Printing Expert Data

You can print expert data. With an Expert window active, select **Print** from the **File** menu or press the print button on the Detail View toolbar. The symptom list in the top panel is printed by default. From the Overeiw tab, all counters are printed.

If you want to print the Detail data in the bottom right panel of an Expert display, click on any field in any table in this panel and select **Print** from the **File** menu. Data for all tables in this panel are printed.

Working with Timestamps

The number of symptoms reported may be different between monitor and capture. The capture feature performs at full line rate and captures all packets whereas the monitor may or may not include all packets.

Timestamps, when viewing expert tables, contain the time and date when the information was captured. Frames are processed for inclusion in the expert table in batches of 100, so it is possible for two frames to have exactly the same timestamp in expert tables. The order in which symptoms or analyses are displayed is always the same order in which they were encountered in the capture file or buffer. The timestamps for analyzer devices increment from the time the device was last started.

If OPV-PE detects two symptoms in the same packet, OPV-PE will display the symptom that it determines to be the most hazardous to network function.

Working with Analyzer Devices

For OPV-LA or NDIS resources, expert views present expert information on capture files, capture buffers, or in real-time monitor mode. For GPI-1XX or DPI-1XX resources, expert views are available for capture files or capture buffers; no real-time expert views are supported.

An analyzer card with a hardware capture buffer is typically used for expert analysis. Use of an NDIS card severely limits the number of packets that can be analyzed and the effectiveness of network diagnostics.

Application Response Time

The response time for various applications is measured in milliseconds (ms). A threshold can be set in the Application Response Time Alarms for all supported applications. Supported applications are:

- DNS

- FTP

- Gopher

- HTTP

- NFS

- NNTP

- POP

- SMTP

- TELNET

From Detail View, press the Application Response Time button to see application response times. See Chapter 6 on Views for more information on the Application Response Time table.

To calculate application response time, OPV-PE causes a stimulus packet to be transmitted so the application layer round trip time can be assessed. However, the packet cannot be sent if the analyzer device used by OPV-PE is connected through a tap device.The application response time will only work if the transmit port of the analyzer is directly connected to a switch port or device.

Application Layer

Excessive Mailslot Broadcasts

Counter

Excessive Mailslot Broadcasts is a counter of Mailslot Broadcasts packets per second that exceed a threshold. A count of all Excessive Mailslot Broadcasts events displays in the **Overview** counters of Expert View.

Expert Analysis

Excessive Mailslot Broadcasts events are automatically logged as expert symptoms. The **Symptom Summary** field provides the number of mailslot broadcasts measured in packets per second for the network segment. For example:

```
Rate of change of SMB Mailslot Broadcasts=40
```

The threshold value for this symptom can be changed. The default threshold value is 6 mailslot broadcasts per second.

Diagnostic Details

_____

Problem Description:

The expert threshold for SMB Mailslot broadcasts has been exceeded for this segment, resulting in an Excessive Mailslot Broadcast symptom.

_____

Probable Cause(s):

1. Buggy software that puts too many broadcast messages onto the network.

_____

Recommended Action(s):

1. Re-evaluate/investigate the software in question.

FTP Login Attempts

Counter

FTP Login Attempts is a counter of FTP login attempts that exceed a threshold. A count of all FTP Login Attempt events displays in the **Overview** counters of Expert View.

Expert Symptom

FTP Login Attempt events are automatically logged as expert symptoms. The **Symptom Summary** field provides the number of login attempts. For example:

```
Login attempts=4 (> 3)
```

The threshold value for this symptom can be changed. The default threshold value is greater than 3 login attempts.

Diagnostic Details

_____

Problem Description:

The expert threshold for the number of FTP login attempts has been exceeded.

_____

Probable Cause(s):

1. The client software specified an invalid user name or password.

_____

Recommended Action(s):

1. Make sure that the user name and/or password is valid.

Missed Browser Announcement

Counter

Missed Browser Announcement is a counter of events where the time elapsed since the last browser announcement exceeds a threshold. A count of all Missed Browser Announcement events displays in the **Overview** counters of Expert View.

Expert Symptom

Missed Browser Announcement events are automatically logged as expert symptoms. The **Symptom Summary** field provides the time elapsed since the last browser announcement compared to a threshold value. For example:

```
Time passed since last announcement=4000 ms (> 3000 ms)
```

The threshold value for this symptom can be changed. The default threshold value is multiplier of 2. The time interval to use is read from the announcement packet. For example, assume that the time-out value read from an SMB packet is 480,000 ms. If the multiplier value is set to 2, then the symptom displays when there is no browser announcement for 960,000 ms (2 X 480,000 ms).

Diagnostic Details

_____

Problem Description:

No Browser announcement has been sent within the stated interval multiplied by the threshold value.

_____

Probable Cause(s):

1. The network is overloaded so that the packets are lost.
2. The station has been shutdown.

_____

Recommended Action(s):

1. Load balance your network.

NCP File Retransmission

Counter

NCP File Retransmission is a counter of all times where a portion of a file is retransmitted. A count of all NCP File Retransmission events displays in the **Overview** counters of Expert View.

Expert Symptom

NCP File Retransmission events are automatically logged as expert symptoms. The **Symptom Summary** field provides the two addresses between which the retransmission occurred. For example:

```
Between [00000010.0207012303E3] and [302A9950.000000000001]
```

Diagnostic Details

_____
Problem Description:

A part of a file has been retransmitted.

_____
Probable Cause(s):

1. There may be a problem with the NCP client application.
_____
Recommended Action(s):

1. Upgrade the NCP client application.

NCP Read/Write Overlap

Counter

NCP Read/Write Overlap is a counter of all times where a portion of a file overlaps the transmission of other parts of the file. A count of all NCP Read/Write Overlap events displays in the **Overview** counters of Expert View.

Expert Symptom

NCP Read/Write Overlap events are automatically logged as expert symptoms. The **Symptom Summary** field provides the two addresses between which the overlap occurred. For example:

```
Between [00000010.0207012303E3] and [302A9950.000000000001]
```

Diagnostic Details

_____

Problem Description:

A part of a transmitted file overlaps with the other parts.

_____

Probable Cause(s):

1. There may be a problem with the NCP client application.

_____

Recommended Action(s):

1. Upgrade the NCP client application.

NCP Request Denied

Counter

> NCP Request Denied is a counter of all times where the number of request denied replies exceed a threshold within an interval. A count of all NCP Request Denied events displays in the **Overview** counters of Expert View.

Expert Symptom

> NCP Request Denied events are automatically logged as expert symptoms. The **Symptom Summary** field provides the number of requests denied within the 100 ms interval. For example:

```
Requests denied within 100 ms=5
```

> The number of request denied replies to look for can be changed. The default is 2 requests. The interval can be changed by setting the NCP Request Loop time value, which specifies the interval of time to look for repeating requests. The default is 100 ms.

Diagnostic Details

_____

Problem Description:

The expert threshold for the number of request denied replies within the request loop time has been exceeded.

_____

Probable Cause(s):

1. There may be a problem with the configuration of the application.
2. There may be a problem with the NCP client application.

_____

Recommended Action(s):

1. Upgrade the NCP client application.
2. Reconfigure the application.

NCP Request Loop

Counter

> NCP Request Loop is a counter of all times where the same request occurs within an interval. A count of all NCP Request Loop events displays in the **Overview** counters of Expert View.

Expert Symptom

> NCP Request Loop events are automatically logged as expert symptoms. The **Symptom Summary** field provides the following information:

```
Loops on same request in 100 ms
```

> The interval of time to look for repeating requests can be changed. The default is 100 ms.

Diagnostic Details

_____

Problem Description:

The same request has been sent repeatedly within the threshold value.

_____

Probable Cause(s):

1. Some reply packets may have been lost.
2. There may be a problem with the NCP client application.

_____

Recommended Action(s):

1. Upgrade the NCP client application.

NCP Server Busy

Counter

NCP Server Busy is a counter of all NCP Server Busy responses that exceed a threshold for a single station. A count of all NCP Server Busy displays in the **Overview** counters of Expert View.

Expert Symptom

NCP Server Busy events are automatically logged as expert symptoms. The **Symptom Summary** field provides the number of busy responses measured in packets per second. For example:

```
Rate of change of NCP Server Busy=[5]
```

The threshold value for this symptom can be changed. The default value is 10 packets per second.

Diagnostic Details

_____
Problem Description:

The expert threshold for the number of NCP Server Busy responses has been exceeded for this station.

_____
Probable Cause(s):

1. The server was very busy.

_____
Recommended Action(s):

1. Reduce the number of connections to the server.

NCP Too Many File Retransmissions

Counter

NCP Too Many File Retransmissions is a counter of events where the ratio of file retransmissions to file requests exceeds a threshold value for a single station. A count of all NCP Too Many File Retransmission events displays in the **Overview** counters of Expert View.

Expert Analysis

NCP Too Many File Retransmissions events are automatically logged as expert analyses. The **Symptom Summary** field provides the file retransmission ratio, showing the total number of retransmissions divided by the total number of file requests. For example:

```
File retransmission ratio is (8 / 28) = 28%
```

The threshold value for this symptom can be changed. The default value is a 20% retransmission ratio.

Diagnostic Details

_____

Problem Description:

The expert threshold for the ratio of file retransmissions over file requests sent has been exceeded.

_____

Probable Cause(s):

1. The server was very busy.
2. There may be a problem with the NCP server application.

_____

Recommended Action(s):

1. Upgrade the NCP server application.

NCP Too Many Requests Denied

Counter

NCP Too Many Requests Denied is a counter of events where the ratio of file requests denied to file requests exceeds a threshold value for a single station. A count of all NCP Too Many Requests Denied events displays in the **Overview** counters of Expert View.

Expert Analysis

NCP Too Many Requests Denied events are automatically logged as expert analyses. The **Symptom Summary** field provides the file requests denied ratio, showing the total number of requests denied divided by the total number of file requests. For example:

```
Requests denied ratio is (8 / 28) = 28%
```

The threshold value for this symptom can be changed. The default value is a 20% requests denied ratio.

Diagnostic Details

_____

Problem Description:

The expert threshold for the ratio of requests denied over requests sent has been exceeded.

_____

Probable Cause(s):

1. There may be a problem with the configuration of the application.
2. There may be a problem with the NCP client application.

_____

Recommended Action(s):

1. Upgrade the NCP client application.
2. Reconfigure the application.

NCP Too Many Request Loops

Counter

NCP Too Many Request Loops is a counter of events where the ratio of file request loops to file requests exceeds a threshold value for a single station. A count of all NCP Too Many Request Loops events displays in the **Overview** counters of Expert View.

Expert Analysis

NCP Too Many Request Loops events are automatically logged as expert analyses. The **Symptom Summary** field provides the request loops ratio, showing the total number of request loops divided by the total number of requests. For example:

```
Requests loops ratio is (8 / 28) = 28%
```

The threshold value for this symptom can be changed. The default value is a 20% request loops ratio.

Diagnostic Details

_____

Problem Description:

The expert threshold for the ratio of request loops over requests sent has been exceeded

_____

Probable Cause(s):

1. Some reply packets may have been lost.
2. There may be a problem with the NCP client application.

_____

Recommended Action(s):

1. Upgrade the NCP client application.

NFS Retransmissions

Counter

NFS Retransmissions is a counter of all NFS Retransmissions over a period of time per segment. A count of all NFS Retransmissions displays in the **Overview** counters of Expert View. A threshold for this counter can be set in Expert Alarms.

Expert Symptom

NFS Retransmission events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the addresses of the client and server involved. For example:

```
Client [206.250.228.69] retransmitting to Server
[206.250.228.14]
```

Diagnostic Details

_____
Problem Description:
There is a retransmission of an NFS request packet. The RPC identifier for this connection has been reused.

_____
Probable Cause(s):
1. An NFS data may be transmitted over several fragmented IP packets. If any of the IP fragments is missing, it will result in a retransmission.
2. The network is overloaded.
3. The path to the receiving station has long delays.
4. There may be an overloaded switch or router.

_____
Recommended Action(s):
1. Check if there are any missing IP fragments.
2. If you see repeated delays and too many retransmissions, your router or switch may need upgrading.

No HTTP POST Response

Counter

No HTTP POST Response is a counter of all POST requests to an HTTP server that never receive a response or exceed a time out value. A count of all No HTTP POST Responses displays in the **Overview** counters of Expert View.

Expert Analysis

No HTTP POST Response events are automatically logged as expert analyses. For example:

```
HTTP POST request not responded
```

Diagnostic Details

_____

Problem Description:

There is no HTTP server response to a POST request, resulting in a connection reset.

_____

Probable Cause(s):

1. The server was very busy.
2. There may be a problem with the HTTP server application.

_____

Recommended Action(s):

1. Upgrade the HTTP server application.

No Server Response

Counter

No Server Response is a counter of responses to server requests that never happen or exceed a time out value. A count of all No Server Responses displays in the **Overview** counters of Expert View.

Expert Analysis

No Server Response events are automatically logged as expert analyses. The **Symptom Summary** field provides information about the type of server involved. For example:

```
SMTP server not responded
```

This analysis applies to text-based application protocol servers such as FTP, SMTP, NNTP, and POP3.

Diagnostic Details

_____

Problem Description:

There is no server ready message for the server.

_____

Probable Cause(s):

1. The server was very busy.
2. There may be a problem with the server application.

_____

Recommended Action(s):

1. Upgrade the server application.

Slow HTTP GET Response

Counter

Slow HTTP GET Response is a counter of all Slow HTTP GET Responses that exceed a threshold. A count of all Slow HTTP GET Responses displays in the **Overview** counters of Expert View. A threshold for this counter can be set in Expert Alarms.

Expert Symptom

Slow HTTP GET Response events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the time required for the response and the threshold value. For example:

```
Slow HTTP GET response=3608 ms (> 2000 ms)
```

The threshold value for this symptom can be changed. The default value is 2000 milliseconds.

Diagnostic Details

_____
Problem Description:

An HTTP server response to a GET request has taken longer than the threshold value to reach the sender.

_____
Probable Cause(s):

1. The server was very busy.
2. The server is overloaded.
3. The path to the sender from the receiver has long delays.
4. There may be an overloaded switch or router in the path.

_____
Recommended Action(s):

1. Upgrade the server's CPU and /or memory.
2. Reduce the number of connections to the server.
3. Load balance your network.

Slow HTTP POST Response

Counter

Slow HTTP POST Response is a counter of all HTTP POST responses that exceed a threshold. A count of all Slow HTTP POST Responses displays in the **Overview** counters of Expert View. A threshold for this counter can be set in Expert Alarms.

Expert Symptom

Slow HTTP POST Response events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the time required for the response and the threshold value. For example:

```
Slow HTTP POST response=2918 ms (> 2000 ms)
```

The threshold value for this symptom can be changed. The default value is 2000 milliseconds.

Diagnostic Details

_____

Problem Description:

An HTTP server response to a POST request has taken longer than the threshold value to reach the sender.

_____

Probable Cause(s):

1. The server was very busy.
2. The server is overloaded.
3. The path to the sender from the receiver has long delays.
4. There may be an overloaded switch or router in the path.

_____

Recommended Action(s):

1. Upgrade the server's CPU and /or memory.
2. Reduce the number of connections to the server.
3. Load balance your network.

Slow Server Connect

Counter

Slow Server Connect is a counter of all server connect responses that exceed a threshold. A count of all Slow Server Connects displays in the **Overview** counters of Expert View.

Expert Symptom

Slow Server Connect events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the type of application server, the time taken for the server to connect, and the threshold value. For example:

```
Slow FTP server connect=298 ms (> 200 ms)
```

The threshold value for this symptom can be changed. The default value is 200 milliseconds.

This symptom applies to text-based application protocol servers such as FTP, SMTP, NNTP, and POP3. These servers send a ready message when a client first logs in. If the response time is too long (exceeds the threshold), the symptom is recorded. For slow responses other than the ready message, see the Slow Server Response symptom.

Diagnostic Details

_____

Problem Description:

The first server ready message has taken longer than the threshold value to reach the sender.

_____

Probable Cause(s):

1. The server was very busy.
2. The server is overloaded.
3. The path to the sender from the receiver has long delays.
4. There may be an overloaded switch or router in the path.

_____

Recommended Action(s):

1. Upgrade the server's CPU and /or memory.
2. Reduce the number of connections to the server.
3. Load balance your network.

Slow Server Response

Counter

Slow Server Response is a counter of server responses that exceed a threshold. A count of all Slow Server Responses displays in the **Overview** counters of Expert View.

Expert Symptom

Slow Server Response events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the type of application server, the time taken for the server to respond, and the threshold value. For example:

```
Slow SMTP server response=1258 ms (> 1000 ms)
```

The threshold value for this symptom can be changed. The default value is 200 milliseconds.

This symptom applies to text-based application protocol servers such as FTP, SMTP, NNTP, and POP3. The symptom is recorded whenever the server response exceeds the threshold for a client request. For slow responses to initial log on (server ready message), see the Slow Connect Response symptom.

Diagnostic Details

_____

Problem Description:

A response from the server has taken longer than the threshold value to reach the sender.

_____

Probable Cause(s):

1. The server was very busy.
2. The server is overloaded.
3. The path to the sender from the receiver has long delays.
4. There may be an overloaded switch or router in the path.

_____

Recommended Action(s):

1. Upgrade the server's CPU and /or memory.
2. Reduce the number of connections to the server.
3. Load balance your network.

SMB Invalid Network Name

Counter

SMB Invalid Network Name is a counter of SMB sessions that could not be established because of invalid network names. A count of all SMB Invalid Network Name displays in the **Overview** counters of Expert View.

Expert Analysis

SMB Invalid Network Name events are automatically logged as expert symptoms. The **Symptom Summary** field provides the following information:

```
Invalid network name in tree connect
```

Diagnostic Details

_____

Problem Description:

An SMB session could not be established because the requesting station had specified a network resource name that does not exist on the target station.

_____

Probable Cause(s):

1. The client software specified a network resource name that does not exist on the server.

_____

Recommended Action(s):

1. Make sure that the name is valid.

SMB Invalid Password

Counter

> SMB Invalid Password is a counter of SMB sessions that could not be established because of an invalid password. A count of all SMB Invalid Password displays in the **Overview** counters of Expert View.

Expert Analysis

> SMB Invalid Password events are automatically logged as expert symptoms. The **Symptom Summary** field provides the following information:

```
Invalid password
```

Diagnostic Details

_____

Problem Description:

An SMB session could not be established because the password was invalid.

_____

Probable Cause(s):

1. The client software specified an invalid user name or password.

_____

Recommended Action(s):

1. Make sure that the user name and/or password is valid.

Session Layer

No WINS Response

Counter

No WINS Response is a counter of responses to WINS server requests that never happen or exceed a time out value. A count of all No WINS Responses displays in the **Overview** counters of Expert View.

Expert Analysis

No WINS Response events are automatically logged as expert analyses. The **Symptom Summary** field provides the following information:

```
WINS request not responded within 1000 ms
```

The time out value for this symptom can be changed. The default value is 1000 ms.

Diagnostic Details

_____

Problem Description:

There is no response from the WINS server.

_____

Probable Cause(s):

1. The UDP packets have been lost.
2. The WINS server is disconnected.
3. The WINS client is misconfigured.

_____

Recommended Action(s):

1. Check the WINS server is up and running.
2. Reconfigure the WINS client.

TNS Slow Server Connect

Counter

TNS Slow Server Connect is a counter of all TNS server connect responses that exceed a threshold. A count of all TNS Slow Server Connects displays in the **Overview** counters of Expert View.

Expert Symptom

TNS Slow Server Connect events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the time elapsed for the server connect and the threshold value. For example:

```
Slow TNS server connect=298 ms (> 200 ms)
```

The threshold value for this symptom can be changed. The default value is 100 milliseconds.

This symptom applies to TNS servers only. If the response time is too long (exceeds the threshold), the symptom is recorded. For slow responses other than the ready message, see the TNS Slow Server Response symptom.

Diagnostic Details

_____

Problem Description:

The TNS server has taken longer than the threshold value to accept/refuse a connection.

_____

Probable Cause(s):
1. The server was very busy.
2. The network is overloaded.
3. The path to the sender from the receiver has long delays.
4. There may be an overloaded switch or router in the path.

_____

Recommended Action(s):
1. Upgrade the server's CPU and/or memory.
2. Reduce the number of connections to the server.
3. Load balance your network.

TNS Slow Server Response

Counter

TNS Slow Server Response is a counter of TNS server responses that exceed a threshold. A count of all TNS Slow Server Responses displays in the **Overview** counters of Expert View.

Expert Symptom

TNS Slow Server Response events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the time elapsed for the server to respond and the threshold value. For example:

```
Slow TNS server response=238 ms (> 200 ms)
```

The threshold value for this symptom can be changed. The default value is 50 milliseconds.

This symptom applies only to TNS servers. The symptom is recorded whenever the server response exceeds the threshold for a client request. For slow responses to initial log on, see the TNS Slow Connect Response symptom.

Diagnostic Details

_____
Problem Description:

A response from the TNS server has taken longer than the threshold value to reach the sender.

_____
Probable Cause(s):
1. The server was very busy.
2. The network is overloaded.
3. The path to the sender from the receiver has long delays.
4. There may be an overloaded switch or router in the path.

_____
Recommended Action(s):
1. Upgrade the server's CPU and/or memory.
2. Reduce the number of connections to the server.
3. Load balance your network.

Transport Layer

Idle Too Long

Counter

The Idle Too Long counter increments when a connection is idle for greater than a threshold value, measured in seconds. A count of all Idle Too Long events displays in the **Overview** counters of Expert View.

Expert Symptom

Idle Too Long events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the duration of the idle connection. For example:

```
Connection has been idle for 61 s
Connection was idle for 128 s
```

An idle connection is defined as no packet activity for the connection.

The threshold for this symptom can be changed. The default threshold is an idle connection for 60 seconds.

Diagnostic Details

_____

Problem Description:

The connection has been idle for longer than the threshold value.

_____

Probable Cause(s):

1. One of the hosts may be disconnected.
2. The application on the connection is not running correctly.

_____

Recommended Action(s):

1. Check the hosts are up and running.
2. Check the application on the hosts is running correctly.

Non Responsive Station

Counter

Non Responsive Station is a counter of all non-responsive stations over a period of time per segment. A non-responsive station is defined as successive TCP/IP retransmissions over the same connection that are greater than a threshold value. A count of all non-responsive stations displays in the **Overview** counters of Expert View. A threshold for the number of Non Responsive Station events can be set in Expert Alarms.

Expert Analysis

Non Responsive Station events are automatically logged as expert analyses. The **Symptom Summary** field provides the IP address of the non-responsive station. For example:

```
Station [206.250.228.11] not responding
```

The threshold value for the number of retransmissions can be changed. The default threshold is 3 successive retransmissions.

Diagnostic Details

_____

Problem Description:

The threshold set for consecutive retransmissions has been exceeded.
This resulted in a Non Responsive Station symptom.

_____

Probable Cause(s):

1. An ACK sent by the receiver was lost.
2. The network is overloaded.
3. The path to the receiving station has long delays.
4. There may be a problem with the receiver's TCP/IP stack.
5. There may be an overloaded switch or router.

_____

Recommended Action(s):

1. Load balance your network.
2. If you see repeated delays and too many retransmissions, your router or switch may need upgrading.

TCP Checksum Errors

Counter

TCP Checksum Errors is a counter of all incorrect TCP checksums over a period of time per segment. A count of all TCP Checksum Errors events displays in the Overview counters of Expert View.

Expert Symptom

TCP Checksum Errors events are automatically logged as expert symptoms. The **Symptom Summary** field provides the IP source and destination address for the checksum error. For example:

```
SA=[206.250.228.69] DA=[206.250.228.11]
```

Diagnostic Details

_____

Problem Description:

A TCP/IP packet has a checksum value that is in error.
The packet may be discarded.

_____

Probable Cause(s):

1. The station that sent this packet may have a faulty network stack.
2. The router that forwarded this packet may have a faulty stack.

_____

Recommended Action(s):

1. Identify the station that sent this packet (Source Addresses).
2. Verify the transport layer stack for this station.
3. The station may need to be reset.

TCP Fast Retransmission

Counter

TCP Fast Retransmission is a counter of all TCP retransmissions that are less than a threshold value. A count of all TCP Fast Retransmissions displays in the **Overview** counters of Expert View. A threshold for this counter can be set in Expert Alarms.

Expert Symptom

TCP Fast Retransmission events are automatically logged as expert symptoms. The **Symptom Summary** field provides the IP addresses of the client and server involved. For example:

```
In 5 ms (< 100 ms) between [206.250.228.69]/[TCP/IP
WKP:1988] and [206.250.228.11]/[SMTP]
```

Diagnostic Details

_____

Problem Description:

A TCP/IP packet has been retransmitted. There was no ACK form the receiver, causing the sender to retransmit the packet. And the time from the last transmission is less than the threshold value.

_____

Probable Cause(s):

1. An ACK sent by the receiver was lost.
2. The network is overloaded.
3. The path to the receiving station has long delays.
4. There may be a problem with the receiver's TCP/IP stack.
5. There may be a problem with the sender's TCP/IP stack.
6. There may be an overloaded switch or router.

_____

Recommended Action(s):

1. Load balance your network.
2. If you see repeated delays and too many retransmissions, your router or switch may need upgrading.

TCP Frozen Window

Counter

> The TCP Frozen Window counter increments when the TCP window is frozen for greater than a threshold value, measured in seconds. A count of all TCP Window Frozen events displays in the **Overview** counters of Expert View. A threshold for this counter can be set in Expert Alarms.

Expert Symptom

> TCP Frozen Window events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the frozen window size, duration, and the well-known ports (WKP) involved, including the port number and the IP address. For example:

```
Frozen at 29909 for [19 ms] between [206.250.228.69]/[TCP
WKP:1988] and [206.250.228.11]/[SMTP]
```

> A frozen window event is defined as the TCP window size remaining the same for all packets over a threshold interval for one connection in one direction. If only one packet is detected over the threshold interval, it is logged as a TCP frozen window event. Events of this type can indicate when a problem with the TCP/IP connection or excessive network traffic.

> The threshold for this symptom can be changed. The default threshold is a frozen window of 5 seconds.

Diagnostic Details

_____

Problem Description:

A TCP/IP packet has the window size stuck for longer than the threshold interval. If the window size is less than the maximum, the flow of data is restricted. The sender will not exceed the receiver's window size.

_____

Probable Cause(s):

1. The receiver is overloaded.
2. The receiver has run out of buffer space.
3. There may be a problem with the receiver's TCP/IP stack.
4. There may too many connections to the receiver resulting in reduced buffer space.

_____

Recommended Action(s):

1. Upgrade the receiver's CPU and/or Memory.
2. Reduce the number of connections to the receiver.
3. Increase the network bandwidth.

TCP Long Ack

Counter

The TCP Long Ack counter increments when the TCP acknowledgment for a connection is not seen for greater than a threshold value, measured in milliseconds. A count of all TCP Long Ack events displays in the **Overview** counters of Expert View. A threshold for this counter can be set in Expert Alarms.

Expert Symptom

TCP Long Acks are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the acknowledgment time and the well-known ports (WKP) involved, including the port number and the IP address. For example:

```
Ack Time=[300 ms] between [206.250.228.69]/[TCP/IP
WKP:1988] and [206.250.228.11]/[SMTP]
```

The time required to acknowledge a TCP/IP packet is calculated for every packet. When a value exceeds a threshold value, the event is logged as an Expert Symptom.

The threshold for this symptom can be changed. The default threshold is no acknowledgment for 200 milliseconds.

Diagnostic Details

_____

Problem Description:

A TCP/IP ACK (Acknowledgment) has taken longer than threshold value to reach the sender.

_____

Probable Cause(s):

1. The receiver which generated the ACK was very busy.
2. The network is overloaded.
3. The path to the sender from the receiver has long delays.
4. There may be a problem with the receiver's TCP/IP stack.
5. There may be an overloaded switch or router in the path.

_____

Recommended Action(s):

1. Load balance your network.
2. If you see repeated delays and long acknowledgments, your receiver may need upgrading.

TCP Repeat Ack

Counter

The TCP Repeat Ack counter increments when the TCP acknowledgment number is less than the immediately preceding acknowledgement. A count of all TCP Repeat Ack events displays in the **Overview** counters of Expert View.

Expert Symptom

TCP Repeat Acks are automatically logged as expert symptoms. The **Symptom Summary** field indicates that the acknowledgement numbers are out of sequence. For example:

```
Acknowledgement number is less than the one before
```

Diagnostic Details

_____

Problem Description:

A TCP/IP acknowledgement number is less than the one before.

_____

Probable Cause(s):

1. The network is overloaded.
2. There may be a problem with the sender's TCP/IP stack.

_____

Recommended Action(s):

1. Update the sender's TCP/IP stack.

TCP Retransmissions

Counter

TCP Retransmissions is a counter of all TCP Retransmissions over a period of time per segment. This variable counts the number of retransmitted packets to measure excessive retransmission in TCP/IP. A count of all TCP Retransmissions displays in the **Overview** counters of Expert View. A threshold for this counter can be set in Expert Alarms.

Retransmissions are determined by sweeping the capture data periodically to catch connections that retransmitted within an interval.

Expert Symptom

TCP Retransmissions are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the well-known ports (WKP) involved, including the port number and the IP address. For example:

```
Between [206.250.228.69]/[TCP/IP WKP:1988] and
[206.250.228.11]/[TCP/IP WKP:197]
```

Diagnostic Details

_____

Problem Description:

A TCP/IP packet has been retransmitted. There was no ACK from the receiver, causing the sender to retransmit the packet.

_____

Probable Cause(s):

1. An ACK sent by the receiver was lost.
2. The network is overloaded.
3. The path to the receiving station has long delays.
4. There may be a problem with the receiver's TCP/IP stack.
5. There may be an overloaded switch or router.

_____

Recommended Action(s):

1. Load balance your network.
2. If you see repeated delays and too many retransmissions, your router or switch may need upgrading.

TCP RST Packets

Counter

TCP RST Packets is a counter of all TCP RST Packets over a period of time per segment. This variable counts the number of RST responses to monitor resets in TCP/IP. A count of all TCP RST packets displays in the **Overview** counters of Expert View. A threshold for this counter can be set in Expert Alarms.

TCP SYN Attack

Counter

The TCP SYN Attack counter increments when a change in the number of SYN requests per second exceeds a threshold. A count of all TCP SYN Attack events displays in the **Overview** counters of Expert View. A threshold for this counter can be set in Expert Alarms.

Expert Symptom

TCP SYN Attack events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the rate of change for SYN requests. For example:

```
Rate of change of TCP SYN's=150
```

The threshold value for the delta of SYN requests per second can be changed. The default is 100 SYN requests per second.

Diagnostic Details

_____

Problem Description:

The threshold for the number of SYN connections on the segment has been exceeded. There may be a SYN attack.

_____

Probable Cause(s):

1. An intruder is trying to break into your network.
2. The network is heavily overloaded.
3. Your Web server is under attack.
4. There may be a problem with the receiver's TCP/IP stack.
5. There may be an overloaded switch or router.

_____

Recommended Action(s):

1. Load balance your network.
2. If you see all the SYNs going to the same station, you may be under attack.
3. If you see too many SYN requests coming from unknown IP addresses, you need to use a firewall or some other means of authentication.

TCP Window Exceeded

Count

> TCP Window Exceeded is a counter of all events where the data length of a TCP packet exceeds the current window size. A count of all TCP Window Exceeded events displays in the **Overview** counters of Expert View.

Expert Symptom

> TCP Window Exceeded events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the length of the data length TCP packet and the current TCP window size on the receiving end. For example:

```
Data length of 128 bytes exceeds last window size of 0
```

Diagnostic Details

_____
Problem Description:

The TCP packet data size exceeds the TCP window of the receiving end.

_____
Probable Cause(s):

1. The network is overloaded so that the new window size is not acknowledged promptly.
2. There may be a problem with the sender's TCP/IP stack.

_____
Recommended Action(s):

1. Ignore this message if the connection was just reset.
2. Upgrade the sender's TCP/IP stack.

TCP Window Probe

Counter

TCP Window Probe is a counter of all TCP Window Probe events over a period of time per segment. A count of all TCP Window Probe events displays in the **Overview** counters of Expert View. A threshold for this counter can be set in Expert Alarms.

Expert Symptom

TCP Window Probe events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the well-known ports (WKP) involved, including the port number and the IP address. For example:

```
Between [206.250.228.69]/[TCP/IP WKP:1988] and
[206.250.228.11]/[SMTP]
```

The TCP window size is examined for every packet to check for one-byte data packets. If a TCP/IP packet with one byte of data is encountered, the event is logged. One-byte data packets are sent periodically by the sender to see if the receiver's window has reopened to allow the sender to resume transmitting.

Diagnostic Details

_____
Problem Description:

A TCP/IP packet with one byte of data has been sent to check whether the receiver's window has been reopened.

_____
Probable Cause(s):
1. The receiver is overloaded.
2. The receiver has run out of buffer space.
3. The non-responsive receiver intends the sender to close the connection.
4. There may be a problem with the receiver's TCP/IP stack.
5. There are too many connections to the receiver resulting in reduced buffer space.
_____
Recommended Action(s):
1. Upgrade the receiver's CPU and/or Memory.
2. Reduce the number of connections to the receiver.
3. Increase the network bandwidth.

TCP Zero Window

Counter

TCP Zero Window is a counter of all TCP Zero Window events over a period of time per segment. A count of all TCP Zero Window events displays in the **Overview** counters of Expert View. A threshold for this counter can be set in Expert Alarms.

Expert Symptom

TCP Zero Window events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the time, location, and the well-known ports (WKP) involved, including the port number and the IP address. For example:

```
Stuck at 0 for [14 ms] between [206.250.228.69]/[TCP/IP
WKP:1988] and [206.250.228.11]/[SMTP]
```

The TCP window size is examined for every packet to check against a window size of zero. If the window size remains zero for a threshold interval for one connection in one direction, the event is logged. Events of this type indicate when a receiver's buffer is full which can indicate problems with the network.

Expert Diagnosis

_____

Problem Description:

A TCP/IP packet indicates zero window size for longer than the threshold interval. The receiver is shutting down communication and will accept no more data from the other end.

_____

Probable Cause(s):

1. The receiver is overloaded.
2. The receiver has run out of buffer space.
3. The non-responsive receiver intends the sender to close the connection.
4. There may be a problem with the receiver's TCP/IP stack.
5. There are too many connections to the receiver resulting in reduced buffer space.

_____

Recommended Action(s):

1. Upgrade the receiver's CPU and/or Memory.
2. Reduce the number of connections to the receiver.
3. Increase the bandwidth of your network.

Too Many Retransmissions

Counter

Too Many Retransmissions is a counter of events where the ratio of retransmissions to packets sent exceeds a threshold value for a single station. A count of all Too Many Retransmissions events displays in the **Overview** counters of Expert View.

Expert Analysis

Too Many Retransmissions events are automatically logged as expert analyses. The **Symptom Summary** field provides the retransmission ratio, showing the total number of retransmissions divided by the total number of packets sent. For example:

```
Retransmission ratio is (49 / 50) = 98%
```

The threshold value for this analysis can be changed. The default value is a 20% retransmission ratio.

Diagnostic Details

_____

Problem Description:

The expert threshold for the ratio of retransmissions over packets sent has been exceeded.

_____

Probable Cause(s):

1. The network is overloaded.
2. The path to the receiving station has long delays.
3. There may be a problem with the receiver's TCP/IP stack.
4. There may be an overloaded switch or router.

_____

Recommended Action(s):

1. Load balance your network.
2. If you see repeated delays and too many retransmissions, your router or switch may need upgrading.

Network Layer

Duplicate Network Address

A separate table showing duplicate network addresses is available. Press the button on the Data View or Capture View toolbar to see this table.

Counter

Duplicate Network Address is a counter of all duplicate network addresses over a period of time per segment. A count of all duplicate network addresses displays in the **Overview** counters of Expert View. A threshold for this counter can be set in Expert Alarms for all duplicate network addresses.

IP address 0.0.0.0 is not counted as a duplicate address.

Expert Symptom

Duplicate network addresses are automatically logged as either "Duplicate IP Address" or "Duplicate IPX Address" expert symptoms. The **Symptom Summary** field provides information about the duplicate IP or IPX address. For example:

Addr=[206.250.228.67]

Diagnostic Details

_____

Problem Description:

This network address has multiple MAC station address associations.
This is a serious problem if the associated MAC stations are not routers.

_____

Probable Cause(s):

1. An existing network address has been assigned to a new machine without verification.
2. An old (discarded) machine using this address has been re-introduced into the network.

_____

Recommended Action(s):

1. Change the network address of one or more hosts so that there are no duplicates.

HSRP Coup

Counter

> HSRP Coup events are counted in the HSRP Errors counter, which displays in the Overview counters of Expert View. A Coup message indicates that the router wishes to become active. A threshold can be set in Expert Alarms for HSRP Coup/ Resign packets, which includes both Resign and Coup HSRP messages.

Expert Symptom

> HSRP Coup events are automatically logged as expert symptoms. The Symptom Summary field provides the IP address of the router trying to become active. For example:

    SA=[206.250.226.11] DA=[206.250.228.69]

Diagnostic Details

_____

Problem Description:

A Router has generated an HSRP Coup message.

_____

Probable Cause(s):

1. A stand-by router has assumed the function of the active router.

_____

Recommended Action(s):

1. Make sure that the router coming up is a stand-by router.
2. Make sure there was a router Resign message (by the Master router) before the coup.

HSRP Errors

Counter

Some Hot Standby Routing Protocol (HSRP) packets are counted in the HSRP
Errors counter, which displays in the Overview counters of Expert View. Both
Coup and Resign packets are counted. Coup/Resign packets in the HSRP are used
to activate/deactivate routers. A threshold can be set in Expert Alarms for HSRP
Coup/Resign packets, which includes both Resign and Coup HSRP messages.

HSRP Resign

Counter

> HSRP Resign events are counted in the HSRP Errors counter, which displays in the Overview counters of Expert View. A Resign message indicates that the router is requesting to become inactive. A threshold can be set in Expert Alarms for HSRP Coup/Resign packets, which includes both Resign and Coup HSRP messages.

Expert Symptom

> HSRP Resign events are automatically logged as expert symptoms. The Symptom Summary field provides the IP address of the router trying to become inactive. For example:

```
SA=[206.250.226.11] DA=[206.250.228.69]
```

Diagnostic Details

_____

Problem Description:

A router has generated an HSRP Resign message.

_____

Probable Cause(s):

1. The stand-by router is returning routing functions to the active router.

_____

Recommended Action(s):

1. Make sure the router is going back to stand by mode.
2. Make sure you get a Coup message or Hello message from new router that has taken over.

ICMP All Errors

Counter

ICMP All Errors is a counter of all ICMP symptoms. A count of all ICMP symptoms displays in the **Overview** counters of Expert View. This counter can also be set in Expert Alarms to set a threshold for all ICMP errors.

The following types of ICMP errors are counted:

- **Destination Unreachable**
  Network Unreachable, Host Unreachable, Protocol Unreachable, Port Unreachable, Fragmentation Needed [D/F Set], Source Route Failed, Destination Network Unknown, Destination Host Unknown, Destination Network Access Denied, Destination Host Access Denied, Network Unreachable for TOS, Host Unreachable for TOS, Destination Unreachable (catches all other Destination Unreachable Errors)

- **Source Quench**

- **Redirect**
  Network Redirect, Host Redirect, Network Redirect for TOS, Host Redirect for TOS, ICMP Redirect (catches all other Redirect errors)

- **Time Exceeded**
  ICMP Time Exceeded, Time To Live Exceeded, Fragment Reassembly Time Exceeded

- **Parameter Problem**
  Bad IP Header, Required IP Option Missing, ICMP Parameter Problem (catches all other Parameter errors)

ICMP Bad IP Header

Counter

>ICMP Bad IP Header events are counted in the ICMP All Errors counter. A count of all ICMP errors displays in the **Overview** counters of Expert View. A threshold can be set in Expert Alarms for all ICMP errors.

Expert Symptom

>ICMP Bad IP Header events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the IP addresses involved. Examples are:

```
Sent by Destination Host [206.250.228.69] to
[206.250.228.11]. Bad Octet at 14. SA=[206.250.228.11]
DA=[206.250.228.69]
```
```
Sent by Gateway [206.250.228.61] to [206.250.228.11] when
forwarding to Destination [206.250.228.69]. Bad Octet at
14. SA=[206.250.228.11] DA=[206.250.228.69]
```

Diagnostic Details

_____

Problem Description:

An ICMP Parameter Problem (IP header is bad) message has been sent.

_____

Probable Cause(s):

1. A host/router may send this message if the IP header parameters have problems that prevent it from processing the packet.
2. A host/router may have a bad network stack or a bad interface card.
3. There may be incorrect arguments in IP options.

_____

Recommended Action(s):

1. Check the **ICMP Pointer** field to see the octet in the IP header where the error was detected.
2. Verify that the source that sent this IP header has a good network interface card.
3. Verify that the network stack on the source that sent the bad IP header parameters is working properly.

ICMP Destination Host Access Denied

Counter

ICMP Destination Host Access Denied events are counted in the ICMP All Errors and the ICMP Destination Unreachable counters. A count of all destination unreachable ICMP symptoms and a count of all ICMP errors displays in the **Overview** counters of Expert View. A threshold can be set in Expert Alarms for all destination unreachable ICMP errors or for all ICMP errors.

Expert Symptom

ICMP Destination Host Access Denied events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the IP addresses involved. For example:

```
[206.250.228.69] cannot be reached by [206.250.228.11].
SA=[206.250.228.11] DA=[206.250.228.69]
```

Diagnostic Details

_____

Problem Description:

An ICMP Destination Host Administratively Prohibited message has been sent.

_____

Probable Cause(s):

1. If a router has a routing table problem, it may send this message.
2. A host may send this message if the destination host does not have proper access.
3. The source may have an incorrectly configured subnet mask.

_____

Recommended Action(s):

1. Check the routing tables of the router that this message was generated from.
2. Check the netmask configuration of the source and/or the router.
3. Ignore this message if the host is truly prohibited (no action required).

ICMP Destination Host Unknown

Counter

ICMP Destination Host Unknown events are counted in the ICMP All Errors and the ICMP Destination Unreachable counters. A count of all destination unreachable ICMP symptoms and a count of all ICMP errors displays in the **Overview** counters of Expert View. A threshold can be set in Expert Alarms for all destination unreachable ICMP errors or for all ICMP errors.

Expert Symptom

ICMP Destination Host Unknown events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the IP addresses involved. For example:

```
[206.250.228.69] cannot be reached by [206.250.228.11].
SA=[206.250.228.11] DA=[206.250.228.69]
```

Diagnostic Details

_____

Problem Description:

An ICMP Destination Host Unknown message has been sent.

_____

Probable Cause(s):

1. If a router has a routing table problem, it may send this message.
2. A router may send this message if it does not know the destination host.
3. The source may have an incorrectly configured subnet mask.

_____

Recommended Action(s):

1. Check the routing tables of the router that this message was generated from.
2. Check the netmask configuration of the source and/or the router.
3. Ignore this message if the host is truly unknown (no action required).

ICMP Destination Network Access Denied

Counter

ICMP Destination Network Access Denied events are counted in the ICMP All Errors and the ICMP Destination Unreachable counters. A count of all destination unreachable ICMP symptoms and a count of all ICMP errors displays in the **Overview** counters of Expert View. A threshold can be set in Expert Alarms for all destination unreachable ICMP errors or for all ICMP errors.

Expert Symptom

ICMP Destination Network Access Denied events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the IP addresses involved. For example:

```
[206.250.228.69] cannot be reached by [206.250.228.11].
SA=[206.250.228.11] DA=[206.250.228.69]
```

Diagnostic Details

_____

Problem Description:

An ICMP Destination Network Administratively Prohibited message has been sent.

_____

Probable Cause(s):

1. If a router has a routing table problem, it may send this message.
2. A host may send this message if the network does not have proper access.
3. The source may have an incorrectly configured subnet mask.

_____

Recommended Action(s):

1. Check the routing tables of the router that this message was generated from.
2. Check the netmask configuration of the source and/or the router.
3. Ignore this message if the network is truly prohibited (no action required).

ICMP Destination Network Unknown

Counter

> ICMP Destination Network Unknown events are counted in the ICMP All Errors and the ICMP Destination Unreachable counters. A count of all destination unreachable ICMP symptoms and a count of all ICMP errors displays in the **Overview** counters of Expert View. A threshold can be set in Expert Alarms for all destination unreachable ICMP errors or for all ICMP errors.

Expert Symptom

> ICMP Destination Network Unknown events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the IP addresses involved. For example:

```
[206.250.228.69] cannot be reached by [206.250.228.11].
SA=[206.250.228.11] DA=[206.250.228.69]
```

Diagnostic Details

_____

Problem Description:

An ICMP Destination Network Unknown message has been sent.

_____

Probable Cause(s):

1. If a router has a routing table problem, it may send this message.
2. A router may send this message if it does not know the destination network.
3. The source may have an incorrectly configured subnet mask.

_____

Recommended Action(s):

1. Check the routing tables of the router that this message was generated from.
2. Check the netmask configuration of the source and/or the router.
3. Ignore this message if the network is truly unknown (no action required).

ICMP Destination Unreachable

ICMP Destination Unreachable is a counter of all ICMP destination unreachable errors over a period of time per segment. A count of all destination unreachable ICMP symptoms displays in the **Overview** counters of Expert View. A threshold for this counter can be set in Expert Alarms for all destination unreachable ICMP errors.

The following types of destination unreachable ICMP errors are counted:

Network Unreachable, Host Unreachable, Protocol Unreachable, Port Unreachable, Fragmentation Needed [D/F Set], Source Route Failed, Destination Network Unknown, Destination Host Unknown, Destination Network Access Denied, Destination Host Access Denied, Network Unreachable for TOS, Host Unreachable for TOS, Destination Unreachable (catches all other Destination Unreachable Errors)

Expert Symptom

ICMP Destination Unreachable is also an expert symptom, and has its own Diagnostic Details. However, this expert symptom reflects only those destination unreachable conditions which cannot be assigned to one of the other destination unreachable symptoms defined above.

ICMP Destination Unreachable events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the IP addresses involved. For example:

```
[206.250.228.69] cannot be reached by [206.250.228.11].
SA=[206.250.228.11] DA=[206.250.228.69]
```

Diagnostic Details

_____

Problem Description:

An ICMP Destination Unreachable message has been sent.

_____

Probable Cause(s):

1. If a router has a routing table problem, it may send this message.
2. A host may send this message if a destination is unreachable.
3. If the packet needs to be fragmented and the "don't fragment" flag is set the host/router will send this message.
4. The source may have an incorrectly configured subnet mask.

_____

Recommended Action(s):

1. Check the routing tables of the router that this message was generated from.
2. Check the netmask configuration of the source.
3. Ignore this message if the destination is truly unreachable (no action required).

ICMP Fragment Reassembly Time Exceeded

Counter

ICMP Fragment Reassembly Time Exceeded events are counted in the All ICMP Errors counter. A count of all ICMP errors displays in the **Overview** counters of Expert View. A threshold can be set in Expert Alarms for all ICMP errors.

Expert Symptom

ICMP Fragment Reassembly Time Exceeded events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the IP addresses involved. For example:

```
Sent by Destination Host [206.250.228.69] to
[206.250.228.11]. SA=[206.250.228.11] DA=[206.250.228.69]
```

Diagnostic Details

_____

Problem Description:

An ICMP Fragment Reassembly Time Exceeded message has been sent.

_____

Probable Cause(s):

1. A host may send this message if it cannot reassemble the fragments (due to missing fragments) on time.
2. There may be a lot of missing IP fragments (possibly due to NFS traffic or network overload).
3. The routing tables may be incorrect on the source.

_____

Recommended Action(s):

1. Check the routing tables of the source.
2. Check the netmask configuration of the source.
3. Check for missing IP fragments.
4. May need to upgrade the host that sent this message.

ICMP Fragmentation Needed [D/F set]

Counter

> ICMP Fragmentation Needed [D/F set] events are counted in the ICMP All Errors and the ICMP Destination Unreachable counters. A count of all destination unreachable ICMP symptoms and a count of all ICMP errors displays in the **Overview** counters of Expert View. A threshold can be set in Expert Alarms for all destination unreachable ICMP errors or for all ICMP errors.

Expert Symptom

> ICMP Fragmentation Needed [D/F] set events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the IP addresses involved. For example:

```
MTU of next Hop=2 to reach [206.250.228.69]. Cannot be
reached by [206.250.228.11] as D/F Set.
SA=[206.250.228.11] DA=[206.250.228.69]
```

Diagnostic Details

_____
Problem Description:
An ICMP Destination (Fragmentation needed, but, D/F set) Unreachable
message has been sent.

_____
Probable Cause(s):
1. If a router has a routing table problem, it may send this message.
2. If the packet needs to be fragmented and the "don't fragment" flag is set the host/router will send this message.
3. The source may have an incorrectly configured subnet mask.

_____
Recommended Action(s):
1. Check the routing tables of the router that this message was generated from.
2. Check the netmask configuration of the source.
3. Ignore this message if the D/F is meant to be set (no action required).

ICMP Host Redirect

Counter

ICMP Host Redirect events are counted in the ICMP Redirect Errors counter and the ICMP All Errors counter. A count of ICMP redirect errors and a count of all ICMP errors displays in the **Overview** counters of Expert View. A threshold can be set in Expert Alarms for all ICMP redirect errors or for all ICMP errors.

Expert Symptom

ICMP Host Redirect events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the IP addresses involved. For example:

```
Use Gateway [206.250.54.61] to reach [206.250.228.69] from
[206.250.228.11].  SA=[206.250.228.11] DA=[206.250.228.69]
```

Diagnostic Details

_____
Problem Description:

An ICMP Host Redirect message has been sent.

_____
Probable Cause(s):

1. If a router has a routing table problem, it may send this message.
2. A router may send this message if according to its (proper) routing tables it finds a shorter path via a different router.
3. The source may have an incorrectly configured subnet mask.
4. The host (source) may have an old routing table.

_____
Recommended Action(s):

1. Check the routing tables of the router that this message was generated from.
2. Check the netmask configuration of the source.
3. Ignore this message if the redirect message is valid (no action required).

ICMP Host Redirect for TOS

Counter

ICMP Host Redirect for TOS events are counted in the ICMP Redirect Errors counter and the ICMP All Errors counter. A count of ICMP redirect errors and a count of all ICMP errors displays in the **Overview** counters of Expert View. A threshold can be set in Expert Alarms for all ICMP redirect errors or for all ICMP errors.

Expert Symptom

ICMP Host Redirect for TOS events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the IP addresses involved. For example:

```
Use Gateway [206.250.54.61] to reach [206.250.228.69] and
TOS 22 from [206.250.228.11].  SA=[206.250.228.11]
DA=[206.250.228.69]
```

Diagnostic Details

_____

Problem Description:

An ICMP Redirect for TOS and Host message has been sent.

_____

Probable Cause(s):

1. If a router has a routing table problem, it may send this message.
2. A router may send this message if according to its (proper) routing tables it finds a shorter path via a different router.
3. The source may have an incorrectly configured subnet mask.
4. The host (source) may have an old routing table.

_____

Recommended Action(s):

1. Check the routing tables of the router that this message was generated from.
2. Check the netmask configuration of the source.
3. Ignore this message if the redirect message is valid (no action required).

ICMP Host Unreachable

Counter

ICMP Host Unreachable events are counted in the ICMP All Errors and the ICMP Destination Unreachable counters. A count of all destination unreachable ICMP symptoms and a count of all ICMP errors displays in the **Overview** counters of Expert View. A threshold can be set in Expert Alarms for all destination unreachable ICMP errors or for all ICMP errors.

Expert Symptom

ICMP Host Unreachable events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the IP addresses involved. For example:

```
[206.250.228.69] cannot be reached by [206.250.228.11].
SA=[206.250.228.11] DA=[206.250.228.69]
```

Diagnostic Details

_____

Problem Description:

An ICMP Destination Host Unreachable message has been sent.

_____

Probable Cause(s):

1. If a router has a routing table problem, it may send this message.
2. A host may send this message if a destination host is unreachable.
3. The source may have an incorrectly configured subnet mask.

_____

Recommended Action(s):

1. Check the routing tables of the router that this message was generated from.
2. Check the netmask configuration of the source.
3. Ignore this message if the host is truly unreachable (no action required).

ICMP Host Unreachable for TOS

Counter

>ICMP Host Unreachable for TOS events are counted in the ICMP All Errors and the ICMP Destination Unreachable counters. A count of all destination unreachable ICMP symptoms and a count of all ICMP errors displays in the **Overview** counters of Expert View. A threshold can be set in Expert Alarms for all destination unreachable ICMP errors or for all ICMP errors.

Expert Symptom

>ICMP Host Unreachable for TOS events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the IP addresses involved. For example:

```
TOS=22 service on [206.250.228.69] unavailable for
[206.250.228.11].  SA=[206.250.228.11] DA=[206.250.228.69]
```

Diagnostic Details

_____
Problem Description:
An ICMP Destination Host is Unreachable for TOS message has been sent.

_____
Probable Cause(s):
1. If a router has a routing table problem, it may send this message.
2. A host may send this message if a destination host is unreachable for the type of service requested.
3. The source may have an incorrectly configured subnet mask.

_____
Recommended Action(s):
1. Check the routing tables of the router that this message was generated from.
2. Check the netmask configuration of the source.
3. Ignore this message if the host is truly unreachable for TOS (no action required).

ICMP Inconsistent Subnet Mask

Counter

ICMP Inconsistent Subnet Mask events are counted in the ICMP All Errors counter. A count of all destination unreachable ICMP symptoms and a count of all ICMP errors displays in the **Overview** counters of Expert View. A threshold can be set in Expert Alarms for all ICMP errors.

Expert Symptom

IMCP Inconsistent Subnet Mask events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the IP addresses involved. For example:

```
Addr=[206.250.228.69].  Subnet mask=[255.255.255.240]
```

Diagnostic Details

_____

Problem Description:

The subnet mask reply does not match the one used by the two stations.

_____

Probable Cause(s):

1. There may be a problem with the stations' configuration.

_____

Recommended Action(s):

1. Reconfigure the stations.

ICMP Network Redirect

Counter

ICMP Network Redirect events are counted in the ICMP Redirect Errors counter and the ICMP All Errors counter. A count of ICMP redirect errors and a count of all ICMP errors displays in the **Overview** counters of Expert View. A threshold can be set in Expert Alarms for all ICMP redirect errors or for all ICMP errors.

Expert Symptom

ICMP Network Redirect events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the IP addresses involved. For example:

```
Use Gateway [206.250.54.61] to reach [206.250.228.69] from
[206.250.228.11].  SA=[206.250.228.11] DA=[206.250.228.69]
```

Diagnostic Details

_____

Problem Description:

An ICMP Network Redirect message has been sent.

_____

Probable Cause(s):

1. If a router has a routing table problem, it may send this message.
2. A router may send this message if according to its (proper) routing tables it finds a shorter path via a different router.
3. The source may have an incorrectly configured subnet mask.
4. The host (source) may have an old routing table.

_____

Recommended Action(s):

1. Check the routing tables of the router that this message was generated from.
2. Check the netmask configuration of the source.
3. Ignore this message if the redirect message is valid (no action required).

ICMP Network Redirect for TOS

Counter

> ICMP Network Redirect for TOS events are counted in the ICMP Redirect Errors counter and the ICMP All Errors counter. A count of ICMP redirect errors and a count of all ICMP errors displays in the **Overview** counters of Expert View. A threshold can be set in Expert Alarms for all ICMP redirect errors or for all ICMP errors.

Expert Symptom

> ICMP Network Redirect for TOS events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the IP addresses involved. For example:

```
Use Gateway [206.250.54.61] to reach [206.250.228.69] and
TOS 22 from [206.250.228.11].  SA=[206.250.228.11]
DA=[206.250.228.69]
```

Diagnostic Details

_____

Problem Description:

An ICMP Redirect for TOS and Network message has been sent.

_____

Probable Cause(s):

1. If a router has a routing table problem, it may send this message.
2. A router may send this message if according to its (proper) routing tables it finds a shorter path via a different router.
3. The source may have an incorrectly configured subnet mask.
4. The host (source) may have an old routing table.

_____

Recommended Action(s):

1. Check the routing tables of the router that this message was generated from.
2. Check the netmask configuration of the source.
3. Ignore this message if the redirect message is valid (no action required).

ICMP Network Unreachable

Counter

ICMP Network Unreachable events are counted in the ICMP All Errors and the ICMP Destination Unreachable counters. A count of all destination unreachable ICMP symptoms and a count of all ICMP errors displays in the **Overview** counters of Expert View. A threshold can be set in Expert Alarms for all destination unreachable ICMP errors or for all ICMP errors.

Expert Symptom

ICMP Network Unreachable events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the IP addresses involved. For example:

```
[206.250.228.69] cannot be reached by [206.250.228.11].
SA=[206.250.228.11] DA=[206.250.228.69]
```

Diagnostic Details

_____
Problem Description:
An ICMP Destination Network Unreachable message has been sent.

_____
Probable Cause(s):
1. If a router has a routing table problem, it may send this message.
2. A host may send this message if a network is unreachable.
3. The source may have an incorrectly configured subnet mask.

_____
Recommended Action(s):
1. Check the routing tables of the router that this message was generated from.
2. Check the netmask configuration of the source.
3. Ignore this message if the network is truly unreachable (no action required).

ICMP Parameter Problem

Counter

ICMP Parameter Problem events are counted in the ICMP All Errors counter. A count of all ICMP errors displays in the **Overview** counters of Expert View. A threshold can be set in Expert Alarms for all ICMP errors.

Expert Symptom

ICMP Parameter Problem events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the IP addresses involved. For example:

```
Bad IP Header sent from [206.250.228.11] to
[206.250.228.69].  SA=[206.250.228.11] DA=[206.250.228.69]
```

This Expert Symptom will be used to identify a parameter problem only if the problem cannot be identified as a Bad IP Header or as a Missing IP Option.

Diagnostic Details

_____

Problem Description:

An ICMP Parameter Problem message has been sent.

_____

Probable Cause(s):

1. A host/router may send this message if the IP header parameters have problems that prevent processing of the packet.
2. A host/router may have a bad network stack or a bad interface card.
3. There may be incorrect arguments in IP options.

_____

Recommended Action(s):

1. Check the **ICMP Pointer** field to see the octet in the IP header where the error was detected.
2. Verify that the source that sent this IP header has a good network interface card.
3. Verify that the network stack on the source that sent the bad IP header parameters is working properly.

ICMP Port Unreachable

Counter

ICMP Port Unreachable events are counted in the ICMP All Errors and the ICMP Destination Unreachable counters. A count of all destination unreachable ICMP symptoms and a count of all ICMP errors displays in the **Overview** counters of Expert View. A threshold can be set in Expert Alarms for all destination unreachable ICMP errors or for all ICMP errors.

Expert Symptom

ICMP Port Unreachable events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the IP addresses involved. For example:

```
Port=22 on [206.250.228.69] cannot be reached by
[206.250.228.11].  SA=[206.250.228.11] DA=[206.250.228.69]
```

Diagnostic Details

_____

Problem Description:

An ICMP Destination Port Unreachable message has been sent.

_____

Probable Cause(s):

1. If a router has a routing table problem, it may send this message.
2. A host may send this message if a port is unreachable.
3. The source may have an incorrectly configured subnet mask.

_____

Recommended Action(s):

1. Check the routing tables of the router that this message was generated from.
2. Check the netmask configuration of the source.
3. Ignore this message if the port is truly unreachable (no action required)
   Ex: SNMP port connection requests.

ICMP Protocol Unreachable

Counter

ICMP Protocol Unreachable events are counted in the ICMP All Errors and the ICMP Destination Unreachable counters. A count of all destination unreachable ICMP symptoms and a count of all ICMP errors displays in the **Overview** counters of Expert View. A threshold can be set in Expert Alarms for all destination unreachable ICMP errors or for all ICMP errors.

Expert Symptom

ICMP Protocol Unreachable events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the IP addresses involved. For example:

```
Protocol=IP on [206.250.228.69] cannot be reached by
[206.250.228.11].  SA=[206.250.228.11] DA=[206.250.228.69]
```

Diagnostic Details

_____

Problem Description:

An ICMP Destination Protocol Unreachable message has been sent.

_____

Probable Cause(s):

1. If a router has a routing table problem, it may send this message.
2. A host may send this message if a protocol is unreachable.
3. The source may have an incorrectly configured subnet mask.

_____

Recommended Actions:

1. Check the routing tables of the router that this message was generated from.
2. Check the netmask configuration of the source.
3. Ignore this message if the protocol is truly unreachable (no action required).

ICMP Redirect

Counter

ICMP Redirect is a counter of all ICMP redirect errors over a period of time per segment. A count of all redirect ICMP symptoms displays in the **Overview** counters of Expert View. A threshold for this counter can be set in Expert Alarms.

The following types of ICMP redirect errors are counted:

Network Redirect, Host Redirect, Network Redirect for TOS, Host Redirect for TOS, ICMP Redirect (catches all other Redirect errors).

Expert Symptom

ICMP Redirect is also an expert symptom, and has its own Diagnostic Details. However, this expert symptom reflects only those redirect conditions which cannot be assigned to one of the other redirect symptoms defined above.

ICMP Redirect events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the IP addresses involved. For example:

```
Use Gateway [206.250.54.61] to reach [206.250.228.69] from
[206.250.228.11].  SA=[206.250.228.11] DA=[206.250.228.69]
```

Diagnostic Details

_____

Problem Description:

An ICMP Redirect message has been sent.

_____

Probable Cause(s):

1. If a router has a routing table problem, it may send this message.
2. A router may send this message if according to its (proper) routing tables it finds a shorter path via a different router.
3. The source may have an incorrectly configured subnet mask.
4. The host (source) may have an old routing table.

_____

Recommended Action(s):

1. Check the routing tables of the router that this message was generated from.
2. Check the netmask configuration of the source.
3. Ignore this message if the redirect message is valid (no action required).

ICMP Required IP Option Missing

Counter

> ICMP Required IP Option Missing events are counted in the ICMP All Errors
> counter. A count of all ICMP errors displays in the **Overview** counters of Expert
> View. A threshold can be set in Expert Alarms for all ICMP errors.

Expert Symptom

> ICMP Required IP Option Missing events are automatically logged as expert
> symptoms. The **Symptom Summary** field provides information about the IP
> addresses involved. For example:

```
Bad IP Header sent from [206.250.228.11] to
[206.250.228.69].  SA=[206.250.228.11] DA=[206.250.228.69]
```

Diagnostic Details

_____

Problem Description:

An ICMP Parameter Problem (IP Options required, but, missing) message has been sent.

_____

Probable Cause(s):

1. A host/router may send this message if the IP header parameters have
   problems that prevent processing of the packet.
2. A host/router may have a bad network stack or a bad interface card.
3. There may be incorrect arguments in IP options.

_____

Recommended Action(s):

1. Check the **ICMP Pointer** field to see the octet in the IP header where the error
   was detected.
2. Verify that the source that sent this IP header has a good network interface card.
3. Verify that the network stack on the source that sent the bad IP header
   parameters is working properly.

ICMP Source Quench

Counter

ICMP Source Quench events are counted in the ICMP All Errors counter. A count of all ICMP errors displays in the **Overview** counters of Expert View. A threshold can be set in Expert Alarms for all ICMP errors.

Expert Symptom

ICMP Source Quench events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the IP addresses involved. Examples are:

```
Sent by Destination Host [206.250.228.69] to
[206.250.228.11].  SA=[206.250.228.11] DA=[206.250.228.69]
```

```
Sent by Gateway Host [206.250.228.61] to [206.250.228.11]
when forwarding to Destination [206.250.228.69].
SA=[206.250.228.11] DA=[206.250.228.69]
```

Diagnostic Details

_____
Problem Description:

An ICMP Source Quench message has been sent.

_____
Probable Cause(s):
1. If a router has a buffer space problem, it may send this message.
2. A host may send this message if it can't keep up with processing of packets and is reaching its limits.
3. The network may be overloaded.

_____
Recommended Action(s):
1. Check the routing table buffer statistics and upgrade the router if problem persists.
2. If the message is from a host, you may need to upgrade its resources.
3. Increase the bandwidth of your network to reduce network overload.
4. If the message is infrequent, ignore it. The problem will rectify itself.

ICMP Source Route Failed

Counter

ICMP Source Route Failed events are counted in the ICMP All Errors and the
ICMP Destination Unreachable counters. A count of all destination unreachable
ICMP symptoms and a count of all ICMP errors displays in the **Overview** counters
of Expert View. A threshold can be set in Expert Alarms for all destination
unreachable ICMP errors or for all ICMP errors.

Expert Symptom

ICMP Source Route Failed events are automatically logged as expert symptoms.
The **Symptom Summary** field provides information about the IP addresses involved.
For example:

```
[206.250.228.69] cannot be reached by [206.250.228.11].
SA=[206.250.228.11] DA=[206.250.228.69]
```

Diagnostic Details

_____

Problem Description:

An ICMP Destination Unreachable (Source Route Failed) message has been sent.

_____

Probable Cause(s):

1. If a router has a routing table problem, it may send this message.
2. A router may send this message if it cannot route the packet.
3. The source may have an incorrectly configured subnet mask.

_____

Recommended Action(s):

1. Check the routing tables of the router that this message was generated from.
2. Check the netmask configuration of the source.

ICMP Time Exceeded

Counter

> ICMP Time Exceeded events are counted in the ICMP All Errors counter. A count of all ICMP errors displays in the **Overview** counters of Expert View. A threshold can be set in Expert Alarms for all ICMP errors.

Expert Symptom

> ICMP Time Exceeded events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the IP addresses involved. For example:

```
Sent by Gateway [206.250.228.61] to [206.250.228.11] when
forwarding to Destination [206.250.228.69].
SA=[206.250.228.11] DA=[206.250.228.69]
```

Diagnostic Details

_____

Problem Description:

An ICMP Time Exceeded message has been sent.

_____

Probable Cause(s):

1. A router may send this message if it encounters an IP packet with a TTL value of `0`.
2. The source may have an incorrectly configured subnet mask, causing longer hops.
3. The routing tables may be incorrect on the source.
4. A host may send this message if it cannot reassemble the fragments (due to missing fragments) on time.

_____

Recommended Action(s):

1. Check the routing tables of the source.
2. Check the netmask configuration of the source.
3. Check for missing IP fragments.
4. May need to upgrade your router or host.

ICMP Time to Live Exceeded

Counter

ICMP Time to Live Exceeded events are counted in the ICMP All Errors counter. A count of all ICMP errors displays in the **Overview** counters of Expert View. A threshold can be set in Expert Alarms for all ICMP errors.

Expert Symptom

ICMP Time to Live Exceeded events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the IP addresses involved. For example:

```
Sent by Gateway [206.250.228.61] to [206.250.228.11] when
forwarding to Destination [206.250.228.69].
SA=[206.250.228.11] DA=[206.250.228.69]
```

Diagnostic Details

_____

Problem Description:

An ICMP Time To Live Exceeded message has been sent.

_____

Probable Cause(s):

1. A router may send this message if it encounters an IP packet with a TTL value of 0.
2. The source may have an incorrectly configured subnet mask, causing longer hops.
3. The routing tables may be incorrect on the source.

_____

Recommended Action(s):

1. Check the routing tables of the source.
2. Check the netmask configuration of the source.

Illegal Network Source Address

Counter

Illegal Network Source Address is a counter of all illegal network source addresses over a period of time per segment. A count of all illegal MAC source addresses displays in the **Overview** counters of Expert View. A threshold for this counter can be set in Expert Alarms.

Expert Symptom

Illegal network source addresses are automatically logged as expert symptoms. The **Symptom Summary** field provides the illegal address encountered. For example:

```
Addr=[255.255.255.255]
```

This symptom can help catch malfunctioning routers or bad addresses generated due to collisions.

Diagnostic Details

_____

Problem Description:

A broadcast network address has appeared as a source address.
This is a problem associated with a bad host.

_____

Probable Cause(s):

1. Someone is transmitting illegal frames using a traffic generator.
2. There may be a faulty adapter card/host.

_____

Recommended Action(s):

1. Filter on the MAC address to determine the faulty card and replace it.

IP Checksum Errors

Counter

IP Checksum Errors is a counter of all incorrect IP checksums over a period of time per segment. A count of all IP Checksum Errors events displays in the Overview counters of Expert View.

Expert Symptom

IP Checksum Errors events are automatically logged as expert symptoms. The **Symptom Summary** field provides the IP source and destination address for the checksum error. For example:

```
SA=[206.250.228.69] DA=[206.250.228.11]
```

Diagnostic Details

_____
Problem Description:

An IP packet has a checksum value that is in error. The packet may be discarded.

_____
Probable Cause(s):

1. The station that sent this packet may have a faulty network stack.
2. The router that forwarded this packet may have a faulty stack.

_____
Recommended Action(s):

1. Identify the station that sent this packet (Source Addresses).
2. Verify the network layer stack for this station.
3. The station may need to be reset.

IP Time to Live Expiring

Counter

IP Time to Live Expiring is a counter of all expiring connections over a period of time per segment. A count of all IP Time to Live Expiring events displays in the Overview counters of Expert View. A threshold for this counter can be set in Expert Alarms to generate an alarm based on a specific number of expiring connections.

Expert Symptom

IP Time to Live Expiring events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the "time-to-live" (TTL) and the source and destination addresses. For example:

```
TTL=1 SA=[206.250.228.69] and DA=[206.250.228.11]
```

Diagnostic Details

_____

Problem Description:

An IP packet has a time to live value that is going to expire.
The packet may be discarded.

_____

Probable Cause(s):

1. The network is overloaded.
2. Router tables may be misconfigured.

_____

Recommended Action(s):

1. Increase the network bandwidth.
2. Check your router configuration.

ISL BPDU/CDP Packets

Counter

ISL BPDU/CDP Packets is a counter of all Bridge Protocol Data Unit (BPDU) or Cisco Discovery Protocol (CDP) packets in an ISL frame over a period of time per segment. A count of BPDU/CDP packets displays in the **Overview** counters of Expert View.

ISL Illegal VLAN ID

Counter

ISL Illegal VLAN ID is a counter of all ISL illegal VLAN IDs over a period of time per segment. A count of all ISL Illegal VLAN ID displays in the **Overview** counters of Expert View. A threshold for this counter can be set in Expert Alarms.

Expert Symptom

ISL Illegal VLAN IDs are automatically logged as expert symptoms. The **Symptom Summary** field provides the number of the illegal VLAN ID. For example:

VLAN ID=[1036]

Diagnostic Details

_____

Problem Description:

The VLAN ID in the ISL protocol is illegal. The allowable range is from 1 to 1024.

_____

Probable Cause(s):

1. An error made in the VLAN configuration for the Switch may have introduced an illegal VLAN ID.
2. A faulty Switch.

_____

Recommended Action(s):

1. Reconfigure the VLAN configuration on the switch to use valid ID's.
2. Replace the faulty Switch.

OSPF Broadcasts

Counter

OSPF Broadcasts is a counter of all OSPF broadcasts over a period of time per segment. A count of all OSPF broadcasts displays in the **Overview** counters of Expert View. A threshold for this counter can be set in Expert Alarms.

If OSPF broadcasts fall below a certain threshold, this may indicate that an OSPF router is not functioning properly.

RIP Broadcasts

Counter

RIP Broadcasts is a counter of all RIP broadcasts over a period of time per segment. A count of all RIP broadcasts displays in the **Overview** counters of Expert View. A threshold for this counter can be set in Expert Alarms.

If RIP broadcasts fall below a certain threshold, this may indicate that a RIP router is not functioning properly.

Router Storm

Counter

Router Storm is a counter of all events where the router broadcasts exceed a threshold for a single router. A count of all Router Storm events displays in the **Overview** counters of Expert View.

Expert Symptom

Router Storm events are automatically logged as expert symptoms. The **Symptom Summary** field provides the number of router broadcasts measured in packets per second. For example:

```
Rate of change of Router Broadcasts=[5]
```

The threshold value for this symptom can be changed.

Diagnostic Details

_____
Problem Description:
The expert threshold for the number of router broadcast messages has been exceeded for this router.

_____
Probable Cause(s):
1. There may be a problem with the router's configuration.

_____
Recommended Action(s):
1. Reconfigure the router.

Same Network Addresses

Counter

> Same Network Addresses is a counter of all events where the same source and destination network addresses are seen in the same packet. A count of all Same Network Address events displays in the **Overview** counters of Expert View.

Expert Symptom

> Same Network Address events are automatically logged as expert symptoms. The **Symptom Summary** field provides the network address. For example:

> `Addr=[255.23.252.6]`

Diagnostic Details

_____

Problem Description:

A packet with the source and destination network addresses has been received.

_____

Probable Cause(s):

1. A protocol analyzer has been transmitting error packets.

_____

Recommended Action(s):

1. Find out the source device and fix the problem.

SAP Broadcasts

Counter

SAP Broadcasts is a counter of all SAP broadcasts over a period of time per segment. A count of all SAP broadcasts displays in the **Overview** counters of Expert View. A threshold for this counter can be set in Expert Alarms.

If SAP broadcasts fall below a certain threshold, this may indicate that a SAP router is not functioning properly.

Total Router Broadcasts

Counter

Total Router Broadcasts is a counter of all total router broadcasts over a period of time per segment. A threshold for this counter can be set in Expert Alarms for total router broadcasts.

If total router broadcasts go above a certain threshold, this may indicate that a router in the network is generating excessive broadcast messages.

Unstable MST

Counter

The Unstable MST counter increments when a change in the number of MST topology changes per second exceeds a threshold. The default threshold is a delta of 5 topology changes per second; however, this value can be changed from the Expert Thresholds tab in the **Configuration** → **Module** → **Settings...** menu. A count of all Unstable MST events displays in the Overview counters of Expert View. A threshold for this counter can be set in Expert Alarms.

MST topology changes are topology changes required to support IEEE 802.1d (Minimum Spanning Tree). Excessive topology changes infer that the Minimum Spanning Tree (MST) is unstable.

Expert Symptom

Unstable MST events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the rate of change for the MST topology. For example:

```
Rate of change of Topology=10
```

Diagnostic Details

_____

Problem Description:

The threshold for the number of IEEE 802.1D packets with topology change bit has been exceeded for this segment. The Spanning tree may be unstable.

_____

Probable Cause(s):

1. There may be too many configuration changes for the bridge/switch.
2. There may be a temporary loss of connectivity.

_____

Recommended Action(s):

1. Identify the device causing this message and fix it.

Zero Broadcast Address

Counter

Zero Broadcast Address is a counter of all events where the destination network addresses is all zeros. A count of all Zero Broadcast Address events displays in the **Overview** counters of Expert View.

Expert Symptom

Zero Broadcast Address events are automatically logged as expert symptoms. The **Symptom Summary** field provides an indication that a zero network address has been discovered. For example:

```
Addr=[0.0.0.0]
```

Diagnostic Details

_____

Problem Description:

A packet with a zero network address in its destination has been received.

_____

Probable Cause(s):

1. A protocol analyzer has been transmitting error packets.

_____

Recommended Action(s):

1. Find out the source device and fix the problem.

MAC Layer

Bad Frames

Counter

Bad Frames is a counter of all bad frames over a period of time per segment. A count of all bad frames displays in the **Overview** counters of Expert View.

The Bad Frames counter is a total count of several MAC layer symptoms. The bad frames counter includes the following MAC layer events:

- CRC Frames -- Frames from 64 to 1518 bytes with a CRC error.

- Fragment Frames -- Frames less than 64 bytes with a CRC error.

- Jabber Frames -- Frames greater than 1518 bytes with a CRC error.

- Oversize Frames -- Frames greater than 1518 bytes without a CRC error.

- Runt Frames -- Frames less than 64 bytes without a CRC error.

Broadcast/Multicast Storms

Counter

> The Broadcast/Multicast Storms counter increments when a change in the number of total Broadcast/Multicast packets per second exceeds a threshold. Broadcast/Multicast Storms can be used to monitor extreme peaks in the number of broadcast and/or multicast messages. A count of all instances where the threshold is reached displays in the Overview counters of Expert View.

Expert Symptom

> Broadcast/Multicast Storm events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the rate of change for broadcast and multicast packets. For example:

```
Rate of change of Bcast/Mcast Packets=500
```

> The threshold value for this symptom can be changed. The default threshold is a delta of 400 broadcast/multicast events per second.

Diagnostic Details

_____

Problem Description:

The broadcast storm expert threshold has been exceeded for this segment, resulting in a MAC Broadcast Storm symptom.

_____

Probable Cause(s):

1. The network is overloaded.
2. Variations in application traffic patterns.
3. Heavy Internet usage.
4. Too many broadcast/multicast packets from the switch/bridge.

_____

Recommended Action(s):

1. Load balance your network.
2. If you see repeated storms, your router or switch may needed upgrading or reconfiguring.

CRC Frame counter

Counter

The CRC Frame counter increments when a frame has a CRC error and is greater than 63 bytes in length. A count of all CRC Frames is included in the Bad Frames counter. The CRC Frame counter is used for Expert Alarms.

Expert Symptom

CRC Frame events are automatically logged as expert symptoms. The **Symptom Summary** field contains the following information:

```
CRC error with more than 63 bytes
```

Diagnostic Details

_____
Problem Description:

A packet with more than 63 bytes of data and a CRC error has been received.

_____
Probable Cause(s):
1. The network is overloaded, resulting in too many collisions.
2. A faulty hub/switch/router device.
3. An end station may have a faulty network interface card.
4. A protocol analyzer has been transmitting error packets.

_____
Recommended Action(s):
1. Find out the source device and fix the problem.

Excessive ARP

Counter

The Excessive ARP counter increments when a change in the number of ARP requests per second exceeds a threshold. A count of all Excessive ARP events displays in the **Overview** counters of Expert View. A threshold for this counter can be set in Expert Alarms.

Expert Symptom

Excessive ARP events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the rate of change for ARP requests. For example:

```
Rate of change of ARP Requests=20
```

This threshold value for this symptom can be changed. The default threshold is a

delta of 10 ARP requests per second.

Diagnostic Details

_____

Problem Description:

The expert threshold for ARP Broadcasts has been exceeded for this segment, resulting in an Excessive ARP symptom.

_____

Probable Cause(s):

1. The network is overloaded.
2. Variations in application traffic patterns.
3. Heavy Internet usage.
4. Too many new TCP/IP connections.

_____

Recommended Action(s):

1. Load balance your network.
2. If you see repeated overloads and too many retransmissions, your router or switch may need upgrading.
   Your network may have just come up after a power down;
   if so, ignore this problem.
3. If there is a high level of Internet usage, then ignore this message.

Excessive BOOTP

Counter

The Excessive BOOTP counter increments when a change in the number of BOOTP/DHCP requests per second exceeds a threshold. A count of all Excessive BOOTP events displays in the **Overview** counters of Expert View. A threshold for this counter can be set in Expert Alarms.

Expert Symptom

Excessive BOOTP events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the rate of change for BOOTP/DHCP requests. For example:

```
Rate of change of Bootp/Dhcp Requests=25
```

The threshold value for this symptom can be changed. The default threshold is a delta of 10 BOOTP/DHCP requests per second.

Diagnostic Details

_____

Problem Description:

The expert threshold for the number of BOOTP/DHCP requests has been exceeded for this segment.

_____

Probable Cause(s):

1. The network has many devices that are being reset.
2. The DHCP server has many requests from floating clients.

_____

Recommended Action(s):

1. Load balance your network. Add more DHCP servers.
2. Your network may have just come up after a power down. If so, ignore this problem.

Excessive Broadcasts

Counter

Excessive Broadcasts is a counter that can be used to monitor fluctuations in the number of broadcast messages over a period of time per segment. A delta threshold for this counter can be set in Expert Alarms to establish what is considered excessive broadcasts. An alarm event can also be generated based on an absolute number of broadcasts over time.

The default is 400 broadcast packets per second on a 100MB network.

Excessive Collisions

Counter

Excessive Collisions is a counter that can be used to monitor fluctuations in the number of collisions or the absolute number of collisions over a period of time per segment. A delta threshold for this counter can be set in Expert Alarms to establish what is considered excessive collisions. An alarm event can also be generated based on an absolute number of collisions over time.

The Excessive Collision counter is incremented by counting runt packets and by counting packets with CRC errors. The Excessive Collisions counter only applies to Ethernet networks.

Excessive Multicasts

Counter

Excessive Multicasts is a counter that can be used to monitor fluctuations in the number of multicast messages over a period of time per segment. A delta threshold for this counter can be set in Expert Alarms to establish what is considered excessive multicasts. An alarm event can also be generated based on an absolute number of multicasts over time.

The default is 400 multicast packets per second on a 100MB network.

Fragment Frame

Counter

The Fragment Frame counter increments when a frame has a CRC error and is less than 64 bytes in length. The Fragment Frame counter is used for Expert Alarms. A count of all Fragment Frames is included in the Bad Frames counter that displays in the Overview counters of Expert View.

Expert Symptom

Fragment Frame events are automatically logged as expert symptoms. The **Symptom Summary** field contains the following information:

```
CRC error with less than 64 bytes
```

Diagnostic Details

_____

Problem Description:

A packet with less than 64 bytes of data and a CRC error has been received.

_____

Probable Cause(s):

1. The network is overloaded, resulting in too many collisions.
2. A faulty hub/switch/router device.
3. An end station may have a faulty network interface card.
4. A protocol analyzer has been transmitting error packets.

_____

Recommended Action(s):

1. Find out the source device and fix the problem.

Illegal MAC Source Address

Counter

Illegal MAC Source Address is a counter of all illegal MAC station source addresses over a period of time per segment. A count of all illegal MAC source addresses displays in the **Overview** counters of Expert View. A threshold for this counter can be set in Expert Alarms.

Expert Symptom

Illegal MAC source addresses are automatically logged as expert symptoms. The **Symptom Summary** field provides the illegal address encountered. For example:

`Addr=[FFFFFF:FFFFFF]`

This symptom can help catch malfunctioning NICs or bad addresses generated due to collisions. Illegal MAC source addresses may be discovered on Ethernet or Token Ring networks.

Diagnostic Details

_____

Problem Description:

A broadcast Ethernet (or Token Ring) address has appeared as a source address. This is a problem associated with a bad adapter card.

_____

Probable Cause(s):

1. Someone is transmitting illegal frames using a traffic generator.
2. There may be a faulty adapter card.

_____

Recommended Action(s):

1. Filter on the Network address to determine which host has the faulty card and replace it.

Jabber Frame

Counter

The Jabber Frame counter increments when a frame has a CRC error and is greater than 1518 bytes in length. A count of all Jabber Frames is included in the Bad Frames counter that displays in the Overview counters of Expert View. The Jabber counter is used for Expert Alarms.

Expert Symptom

Jabber Frame events are automatically logged as expert symptoms. The **Symptom Summary** field contains the following information:

```
CRC error with more than 1518 bytes
```

Diagnostic Details

_____

Problem Description:

A packet with more than 1518 bytes of data and a CRC error has been received.

_____

Probable Cause(s):

1. The network is overloaded, resulting in too many collisions.
2. A faulty hub/switch/router device.
3. An end station may have a faulty network interface card.
4. A protocol analyzer has been transmitting error packets.

_____

Recommended Action(s):

1. Find out the source device and fix the problem.

Network Overload

Counter

Network Overload is a counter of instances where a threshold for the percentage change in network utilization is exceeded. Network utilization is compared to the utilization for the previous time segment. The default threshold is a 40% change in network utilization. A count of all instances where the threshold is reached displays in the Overview counters of Expert View.

Expert Symptom

Network Overload events are automatically logged as expert symptoms. The Symptom Summary field provides information about the change in utilization. For example:

```
Utilization=42%
```

Diagnostic Details

_____

Problem Description:

The expert utilization threshold has been exceeded for this segment, resulting in a LAN Overload symptom.

_____

Probable Cause(s):

1. The network is overloaded.
2. Variations in application traffic patterns.
3. Heavy Internet usage.
4. Too many broadcast/multicast packets.

_____

Recommended Action(s):

1. Load balance your network.
2. If you see repeated overloads and too many retransmissions, your router or switch may needed upgrading.

New MAC Stations

Counter

New MAC Stations is a counter of all the new MAC stations over a period of time per segment. A threshold for this counter can be set in Expert Alarms. The threshold for new MAC stations is typically set to `1` as an absolute value.

The new MAC station counter detects new MAC stations (nodes) on a LAN segment. After a segment is stabilized with a specific number of stations, this counter can indicate possible intruder stations.

Oversized Frame

Counter

The Oversize Frame counter increments when a frame has a CRC error and is greater than 1518 bytes in length. A count of all Oversize Frames is included in the Bad Frames counter that displays in the Overview counters of Expert View. The Oversize Frame counter is used for Expert Alarms.

Expert Symptom

Oversized Frame events are automatically logged as expert symptoms. The **Symptom Summary** field contains the following information:

```
Oversized frame has more than 1518 bytes
```

Diagnostic Details

_____

Problem Description:

A packet with more than 1518 bytes of data has been received.

_____

Probable Cause(s):

1. A faulty hub/switch/router device.
2. An end station may have a faulty network interface card.
3. A protocol analyzer has been transmitting error packets.

_____

Recommended Action(s):

1. Find out the source device and fix the problem.

Overload Frame Rate

Counter

Overload Frame Rate counts frames over a one-second time period. A threshold for the number of frames per second can be set in Expert Alarms.

Overload Frame Rate can help catch network overloads.

Values for the threshold can range from 1 to 148,800 frames/sec for a 100 MB network. The default is 37,200 frames/sec.

Overload Utilization Percentage

Counter

Overload Utilization Percentage counts bits over time and compares this value to the maximum utilization possible (bandwidth). A threshold for this percentage value can be set in Expert Alarms.

Overload utilization percentage can help catch network overloads.

The default for a 100MB network is 25% of maximum utilization.

Physical Errors

Counter

The Physical Errors counter increments when a change in the number of total MAC physical errors per second exceeds a threshold. Physical errors include CRC/ alignment errors, dropped events, collisions, jabbers, oversize packets, undersize packets, and fragments. A count of all instances where the threshold is reached displays in the Overview counters of Expert View.

Expert Symptom

Physical Error events are automatically logged as expert symptoms. The **Symptom Summary** field provides information about the rate of change for total MAC physical errors. For example:

```
Rate of change of Errors=450
```

The threshold value for this symptom can be changed. The default threshold is a delta of 400 physical error packets per second.

Diagnostic Details

_____

Problem Description:

The error threshold has been exceeded for this segment, resulting in a MAC Physical Errors symptom.

_____

Probable Cause(s):

1. The network is overloaded.
2. A faulty hub/switch/router device.
3. A hub may have been incorrectly used.
   Ex:, an uplink port may have been used as a data port.
4. An end station may have a faulty network interface card.

_____

Recommended Action(s):

1. Restart the capture after setting up a filter to capture error packets only.
2. Based on the capture, isolate the device that is in error and fix the problem.

Runt Frame

Counter

The Runt Frame counter increments when a frame is less than 64 bytes in length. The Runt Frame counter is used for Expert Alarms. A count of all Runt Frames is included in the Bad Frames counter that displays in the Overview counters of Expert View.

Expert Symptom

Runt Frame events are automatically logged as expert symptoms. The **Symptom Summary** field contains the following information:

```
Runt frame has less than 64 bytes
```

Diagnostic Details

_____

Problem Description:

A packet with less than 64 bytes of data has been received.

_____

Probable Cause(s):

1. A faulty hub/switch/router device.
2. An end station may have a faulty network interface card.
3. A protocol analyzer has been transmitting error packets.

_____

Recommended Action(s):

1. Find out the source device and fix the problem.

Same MAC Addresses

Counter

Same MAC Addresses is a counter of all events where the same source and destination network addresses are seen in the same packet. A count of all Same MAC Address events displays in the **Overview** counters of Expert View.

Expert Symptom

Same MAC Address events are automatically logged as expert symptoms. The **Symptom Summary** field provides the MAC address. For example:

```
Addr=[00800F:13A65B]
```

Diagnostic Details

_____

Problem Description:

A packet with the source and destination MAC addresses has been received.

_____

Probable Cause(s):

1. A protocol analyzer has been transmitting error packets.

_____

Recommended Action(s):

1. Find out the source device and fix the problem.

Total MAC Stations

Counter

Total MAC Stations is a counter of all the MAC stations over a period of time per segment. A count of all MAC stations displays in the **Overview** counters of Expert View. A threshold for this counter can be set in Expert Alarms. The MAC station counter helps detect excessive MAC stations (nodes) on a LAN segment. This helps indicate possible intruder stations as well as help the network manager limit and control the number of stations allowed on a segment.

Hints and Tips for Expert Features

- Double-click any symptom in a table to view Diagnostic information.

- When looking at Expert View in Monitor only mode, Frame IDs are displayed for information only and you cannot examine a frame related to a symptom. If you need to look at specific frames related to Expert Symptoms, look at the frame information in the capture buffer or in a capture file.

- Expert Views can be disabled on a per module basis. Select **Module** → **Settings…** from the **Configuration** menu and choose the **Modes** Tab. Remove the check from the **Expert Views** box.

- Click, hold, and drag a column border to resize columns in any Expert View Table. Increasing the size of the **Symptom** column gives you a view of the complete name of the symptom.

- Click, hold, and drag a column border to remove columns in any Expert View Table. Double-click on the same column border to bring back the display of a column.

- Duplicate addresses appear both in the Duplicate Network Address Table and as a symptom in Expert View.

- Thresholds can be set for Expert Symptoms. Select **Expert Settings…** from the **Configuration** menu and find the symptom you want to change. Some threshold values for symptoms cannot be changed.

- Expert Symptoms can be selectively disabled. Select **Expert Settings…** from the **Configuration** menu and find the symptom you want to disable from the tree structure. Remove the check from the symptom. Some symptoms cannot be disabled.

- Expert Symptoms can be displayed in the Summary field of Capture View. From the Configuration menu, select **Capture View Options** → **Display** and select the **Display Expert Symptom** check box. Packets that trigger an expert symptom and have expert symptom information will display in reverse video.

Summary of Expert Counters and Symptoms

Table 10-2 on the following page provides a summary of expert features by symptom/counter/application name. The meanings of the column headings are listed below.

Expert Symptom	Logged as an Expert Event and appears in the expert tables.
Expert Analysis	Logged as an Expert Event and appears in the expert tables.
Counter in Expert View	Has an associated counter that displays in the **Overview** page of Expert View. The counter will display in the Symptoms tab if it is a symptom, and in the Analyses tab if it is an analysis.
Expert Alarm	Has an alarm you can set in the Expert Alarm editor.
Application Response Time Alarm	Has an alarm you can set in the **Application Response Time** Alarm editor.
Expert Threshold	A threshold can be set in the **Expert Configuration** dialog box.

Table 10-2. Summary of Expert Features

Counter, Symptom, or Application	Expert Symptom	Expert Analyses	Counter in Expert View	Expert Alarm	Application Response Time Alarm	Expert Threshold
Application Response Time					X (by application)	
Bad Frames			X			
Broadcast/Multicast Storm	X		X			X
CRC Frames	X		z	X		
DNS Response Time					X	
Duplicate Network Address (also displays as a separate view)		X	X	X		
Excessive ARP	X		X	X		X
Excessive BOOTP	X		X	X		X
Excessive Broadcasts				X		
Excessive Collisions				X		
Excessive Multicasts				X		
Excessive Mailslot Broadcasts	X		X			X
Fragment Frames	X		z	X		
FTP Login Attempts	X		X			X
FTP Response Time					X	
Gopher Response Time					X	
HSRP Coup	X		z	z		
HSRP Errors			X	X		
HSRP Resign	X		z	z		

X = present
z = does not exist as a unique counter, but is counted in other categories

Table 10-2. Summary of Expert Features (continued)

Counter, Symptom, or Application	Expert Symptom	Expert Analyses	Counter in Expert View	Expert Alarm	Application Response Time Alarm	Expert Threshold
HTTP Response Time					X	
ICMP All Errors			X	X		
ICMP Bad IP Header	X		z	z		
ICMP Destination Host Access Denied	X		z	z		
ICMP Destination Host Unknown	X		z	z		
ICMP Destination Network Access Denied	X		z	z		
ICMP Destination Network Unknown	X		z	z		
ICMP Destination Unreachable	X		X	X		
ICMP Fragment Reassembly Time Exceeded	X		z	z		
ICMP Fragmenta-tion Needed [D/F set]	X		z	z		
ICMP Host Redirect	X		z	z		
ICMP Host Redirect for TOS	X		z	z		
ICMP Host Unreachable	X		z	z		
ICMP Host Unreachable for TOS	X		z	z		
ICMP Inconsistent Subnet Mask	X		z	z		

X = present
z = does not exist as a unique counter, but is counted in other categories

Table 10-2. Summary of Expert Features (continued)

Counter, Symptom, or Application	Expert Symptom	Expert Analysis	Counter in Expert View	Expert Alarm	Application Response Time Alarm	Expert Threshold
ICMP Network Redirect	X		z	z		
ICMP Network Redirect for TOS	X		z	z		
ICMP Network Unreachable for TOS	X		z	z		
ICMP Parameter Problem	X		z	z		
ICMP Port Unreachable	X		z	z		
ICMP Protocol Unreachable	X		z	z		
ICMP Redirect	X		X	X		
ICMP Required IP Option Missing	X		z	z		
ICMP Source Quench	X		z	z		
ICMP Source Route Failed	X		z	z		
ICMP Time Exceeded	X		z	z		
ICMP Time to Live Exceeded	X		z	z		
Idle Too Long	X		X			X
Illegal MAC Source Address (Ethernet or Token Ring)	X		X	X		
Illegal Network Source Address	X		X	X		
IP Checksum Errors	X		X			

X = present
z = does not exist as a unique counter, but is counted in other categories

Table 10-2. Summary of Expert Features (continued)

Counter, Symptom, Analyses, or Application	Expert Symptom	Expert Analysis	Counter in Expert View	Expert Alarm	Application Response Time Alarm	Expert Threshold
IP Time to Live Expiring	X		X	X		
ISL BPDU/CDP Packets	X		X			
ISL Illegal VLAN ID	X		X	X		
Jabber Frames	X		z	X		
Missed Browser Announcement	X		X			X
NCP File Retransmission	X		X			
NCP Read/Write Overlap	X		X			
NCP Request Denied	X		X			X
NCP Request Loop	X		X			X
NCP Server Busy	X		X			X
NCP Too Many File Retransmissions		X	X			X
NCP Too Many Requests Denied		X	X			X
NCP Too Many Request Loops		X	X			X
New MAC Stations				X		
Network Overload	X		X			X
NFS Response Time					X	
NFS Retransmis-sions	X		X	X		
NNTP Response Time					X	

X = present
z = does not exist as a unique counter, but is counted in other categories

Table 10-2. Summary of Expert Features (continued)

Counter, Symptom, or Application	Expert Symptom	Expert Analysis	Counter in Expert View	Expert Alarm	Application Response Time Alarm	Expert Threshold
No HTTP POST Response		X	X			
No Server Response		X	X			
No WINS Response		X	X			X
Non Responsive Stations		X	X			X
OSPF Broadcasts			X	X		
Overload Frame Rate				X		
Overload Utilization Percentage				X		
Oversize Frames	X		z	X		
Physical Errors	X		X			X
POP Response Time					X	
RIP Broadcasts			X	X		
Router Storm	X		X			X
Runt Frames	X		z	X		
Same MAC Addresses	X		X			
Same Network Addresses	X		X			
SAP Broadcasts			X	X		
Slow HTTP GET Response	X		X			X
Slow HTTP POST Response	X		X			X
Slow Server Connect	X		X			X

X = present
z = does not exist as a unique counter, but is counted in other categories

Table 10-2. Summary of Expert Features (continued)

Counter, Symptom, or Application	Expert Symptom	Expert Analysis	Counter in Expert View	Expert Alarm	Application Response Time Alarm	Expert Threshold
Slow Server Response	X		X			X
SMB Invalid Network Name	X		X			
SMB Invalid Password	X		X			
SMTP Response Time					X	
TCP Checksum Errors	X		X			
TCP Fast Retrans-missions	X		X			X
TCP Long Ack	X		X			X
TCP Repeat Ack	X		X			
TCP Retransmissions	X		X	X		
TCP RST Packets			X	X		
TCP SYN Attack	X		X	X		X
TCP Frozen Window	X		X			X
TCP Window Exceeded	X		X			
TCP Window Probe	X		X			
TCP Zero Window	X		X	X		
TELNET Response Time					X	
TNS Slow Server Connect	X		X			X

X = present
z = does not exist as a unique counter, but is counted in other categories

Table 10-2. Summary of Expert Features (continued)

Counter, Symptom, or Application	Expert Symptom	Expert Analysis	Counter in Expert View	Expert Alarm	Application Response Time Alarm	Expert Threshold
TNS Slow Server Response	X		X			X
Too Many Retransmissions		X	X			X
Total MAC Stations			X	X		
Total Router Broadcasts				X		
Unstable MST	X		X	X		X
Zero Broadcast Address	X		X			

X = present
z = does not exist as a unique counter, but is counted in other categories

Chapter 11
Voice over IP

Voice over IP is a software plug-in to OPV-PE that analyzes multimedia traffic over Ethernet-based networks. Voice over IP validates Quality of Service (QoS) parameters presented by PSTN/IP Gateways, IP switches, and IPBXs. Voice over IP provides a rich set of reported and calculated data to validate IP networks that carry the multimedia data.

The transmission of voice and video over traditional "data-only" networks is one of the most active areas in today's telecommunications industry. Voice over IP (VoIP) refers to the transmission of voice that has been compressed and transmitted over an IP (Internet Protocol) network. H.323, SIP, SDP, MGCP, and SCCP are key industry standards that enable VoIP communication. These standards address call control, multimedia management, bandwidth management, and interfaces between LANs and other networks.

Given the rapid acceptance of IP as the de facto protocol, QoS has become one of the biggest challenges for network administrators, especially for voice and video applications that require real-time performance. Policy-based systems, gateways, switches, and routers are often configured with a myriad of vendor and protocol combinations to work in unison to provide priority for the real-time demands of multimedia traffic.

Voice over IP provides full protocol decodes and important QoS metrics in an easy-to-access graphical interface. Given the non-deterministic nature of IP, the measurement of the actual call traffic is an essential tool to ensuring network QoS. Voice over IP provides a distributed solution to measure the QoS of all the existing calls without having to generate a specific "test call". Measuring real calls eliminates the need to add test traffic to the network, doesn't limit the solution to spot checks, and enables the solving of "real-world" call problems in a deployed environment.

Full decode of multimedia protocols by Voice over IP provides users with the ability to look at any captured packet and understand its contents. Voice over IP validates that the network is performing as it has been configured and helps you troubleshoot problems. Voice over IP provides graphic summaries of Call Jitter, Dropped Packets, and Call Set-up Time to view network performance at-a-glance. Point-and-click on graphs to see call tables. Click on any call to get complete call details.

Voice over IP features are only available from OPV-PE menus and toolbars when you have the Voice over IP plug-in module.

Protocols Supported by Voice over IP

Voice over IP recognizes and decodes all major VoIP protocols. Support includes the following:

- **H.323 (ITU)**
  The H.323 suite of protocol specifications created by ITU, including Q.931, RAS, H.245, and T.120.

- **SIP (IETF)**
  The suite of protocols created by IETF, including SIP, SDP, and others.

- **SCCP (Cisco)**
  Skinny Client Control Protocol (SCCP). SCCP is the proprietary signalling and communications protocol in Cisco's AVVID (Architecture for Voice, Video and Integrated Data).

Voice over IP also recognizes and decodes all major Codec protocols used for VoIP. Refer to Table 1-5 for a list of all protocols supported. Check the Fluke Networks web site for updates on additional protocol support by Voice over IP.

Using Voice over IP with Analyzer Hardware

Voice over IP works with the complete range of analyzer devices and analyzer cards available from Fluke Networks, as well as NDIS-compatible NIC cards. However, it is highly recommended that Voice over IP be used with the OPV-LA generation of Fluke Networks analyzers. These hardware tools provide the hardware buffer sizes, processor speeds, and connectivity demanded by real-world network QoS applications.

VoIP User Interface Overview

The OPV-PE VoIP interface can be used with capture files, a capture buffer, or in real-time monitoring mode. To view VoIP graphs and tables, click on the VoIP button on the Detail View toolbar or select VoIP View from the Monitor or Capture menus.

The VoIP view consists of tabs for viewing graphs of VoIP call data and configuring the interface. Upon startup, the interface displays the Jitter tab, showing a percentage breakdown of calls based on Call Jitter values that are greater than a threshold value. Using the mouse, you can find more detailed information about VoIP calls and VoIP call data. The figure on the next page shows the flow of the interface from the highest level view to the most detailed view. The VoIP views can also be accessed by pressing the VoIP ⬢ button on the Detail View toolbar or by pressing **Control + Q**.

Voice over IP Monitor and Capture views are nearly identical; however, some displays and fields only apply to one or the other. The **Utilization** tab only displays in Monitor mode. Alarms can only be configured when in Monitor mode.

Monitor View

Capture View

VoIP

Select VoIP from
Capture or
Monitor View

VoIP

Select Range in Graph to
View Associated Calls

Summary Range Graphs

| All Calls | User R-factor | Network R-factor | Jitter | RTCP Jitter | Dropped Packets | RTCP Dropped... | Setup Time | Utilization | Configuration |

Select Tab to View a Range Breakdown Graph

Set Max Calls

Set Alarms (Monitor)

Set Refresh Options

Alarm Log (Monitor)

Call Summary Range Table

Single Row	Summarizes a Call....	
Single Row	Summarizes a Call....	

Utilization

Utilization Tab only
appears in Monitor Mode

View All Calls

Select Single Call to See Call Details

All Calls Table

Call Detail

Call Fields....   Call Fields....

Call Fields....   Call Fields....

Call Fields....   Call Fields....

Single Call Display Filter   View Channel Details

Buttons to Filter All Calls by
Protocol or Call Status

Channel View Table

Figure 11-1. Voice over IP Interface Overview

- **Summary Range Graphs**
  The Summary Range graphs provide a percentage breakdown of calls by key QoS metrics. Breakdowns are provided for Call Jitter, RTCP Jitter, Dropped Packets, RTCP Dropped Packets, Call Setup Time, Network R-factor, and User R-factor. Up to five ranges are allowed. The timing or packet-count ranges for each category can be configured by the user.

- **All Calls Table**
  The All Calls table provides a summary table of all calls discovered. You can display only the calls that use a specific protocol. You can also display completed calls only or incomplete calls only.

- **Call Tables for a Specific Range**
  Selecting any range in any of the Summary Range graphs brings up a Call Table that displays all the calls that fall within that range.

- **Call Details for a Single Call**
  Selecting any call in a call table brings up an information box with the complete details for the call.

- **Channel Details for a Single Call**
  Click on View Channel Details of the Single Call Detail View to display channel information for the selected call. The Channel Table provides detailed channel information in tabular format.

OPV-PE and RTCP Jitter Values

VoIP provides two different measurements (views) of call jitter and dropped packets, one calculated by OPV-PE and one extracted from RTCP packets. RTCP (Real-Time Control Protocol) is a control protocol for the RTP (Real-Time Transport Protocol). RTP supports the transport of real-time data such as video and audio streams. RTCP packets are sent by participants in an RTP session to convey information on the quality of data delivery and session membership.

OPV-PE uses the formula specified in RFC 1889 for RTCP to calculate jitter, and the RTCP jitter OPV-PE reads from RTCP packets should use the same formula. However, the values extracted from RTCP packets by OPV-PE and the values calculated by OPV-PE do not exactly match, and may differ greatly in some cases. It depends primarily on the point in the network where OPV-PE is gathering jitter information. If OPV-PE is viewing network traffic close to one end point, then the jitter values for the far end point may nearly match the RTCP-reported jitter. However, if OPV-PE is viewing network traffic towards the mid-point between the end points, then the RTCP and OPV-PE jitter may differ substantially.

Also, the jitter calculation for OPV-PE only measures network jitter. The application itself may implement a jitter buffer, which could make for further differences between the reported RTCP jitter and the jitter measured by OPV-PE.

The difference between the RTCP jitter and OPV-PE-calculated jitter may provide some clues as to what is happening with calls where high jitter rates are disrupting network QoS.

Configuring VoIP

Logic internal to OPV-PE decodes the VoIP frames and organizes call information into easy-to-read graphs and tables. Configuration is not required to use the VoIP logic; however, the displays can be customized to view exactly the call information you want to see.

VoIP is primarily configured from the **Configuration** tab. However, there is some configuration for VoIP that is done on a per-module basis. Module configuration sets up the monitoring of Voice over IP only, effectively increasing Voice over IP monitor performance. See the following subsection on performance optimization for a description.

The VoIP **Configuration** tab in Monitor mode shown below. Different options will be enabled/disabled in Monitor mode.

Figure 11-2. VoIP Configuration

The configuration performed from the **Configuration** tab is described below:

- **Refresh Options (VoIP Window Management)**
  By default, Voice over IP tables are refreshed when you re-open any window containing a table. However, there may be instances where you want to compare data in the same table at different times. For this purpose, Voice over IP provides an option to create a new window each time you view the data.

  To create new windows, click on the radio button on the right. To refresh table views when windows are selected, select the radio button on the left. This option applies to call summary tables, the call detail window showing a single call, and channel tables.

- **Set Maximum Number of Completed Calls**
  The **Maximum Number of Completed Calls** section allows you to set the maximum number of completed calls that will be captured. When the number of completed calls reaches this number, the next completed call causes the earliest completed call to be deleted from all tables. Setting this value low reduces the system memory used for call analysis. A higher setting allows you to keep more call detail records.

  The minimum number of calls is 2,000. The default value is 2,000 calls.

- **VoIP Alarms (Monitor Only)**
  The **VoIP Alarms...** alarm button on the **Configuration** tab applies to real-time functions and can only be set in monitor mode. The button brings up the **Current Module Alarms** dialog box for setting or viewing VoIP alarms. Refer to Chapter 9 on Alarms for complete information on setting Voice over IP alarms.

- **Alarm Log (Monitor Only)**
  Press the **Alarm Log** button to view the log of all alarms.

VoIP Performance Optimization

Real-time monitoring of calls is supported, but the utilization of the network will greatly affect the calls that you see in the Voice over IP tables. The monitor function can record all calls at 10 Mbps. For 100 or 1000 Mbps networks, high network usage will result in missed packets and therefore missed calls. Note that all traffic is captured in capture mode, regardless of the network utilization.

You can increase the monitoring performance of VoIP by disabling the monitoring of other statistics for a specific module.

To enable this feature from Summary View, select **Configuration** → **Module** → **Settings...**. Select the **Modes** tab and enable the check box for **Monitor** Voice over IP **Only**. The VoIP performance option can also be set in Detail View for a specific module. Select **Configuration** → **Settings...** and select the **Modes** tab.

Call Filtering with VoIP

VoIP has a feature for quickly creating a filter from tables. Click the right mouse button on any call in the table to see the filter options supported for this type of call. This feature only works in capture mode after the analyzer is stopped.

For calls in Range Summary tables and the All Calls table, the menu has a **Single Call Display Filter** option. You can create and apply a display for the selected call without having to go to the filter window. This saves several steps in the filter creation process. You can also create a single call display filter from the Call Details window by clicking on **Single Call Display Filter**.

Return to Capture View to see the subset of packets created by applying the display filter.
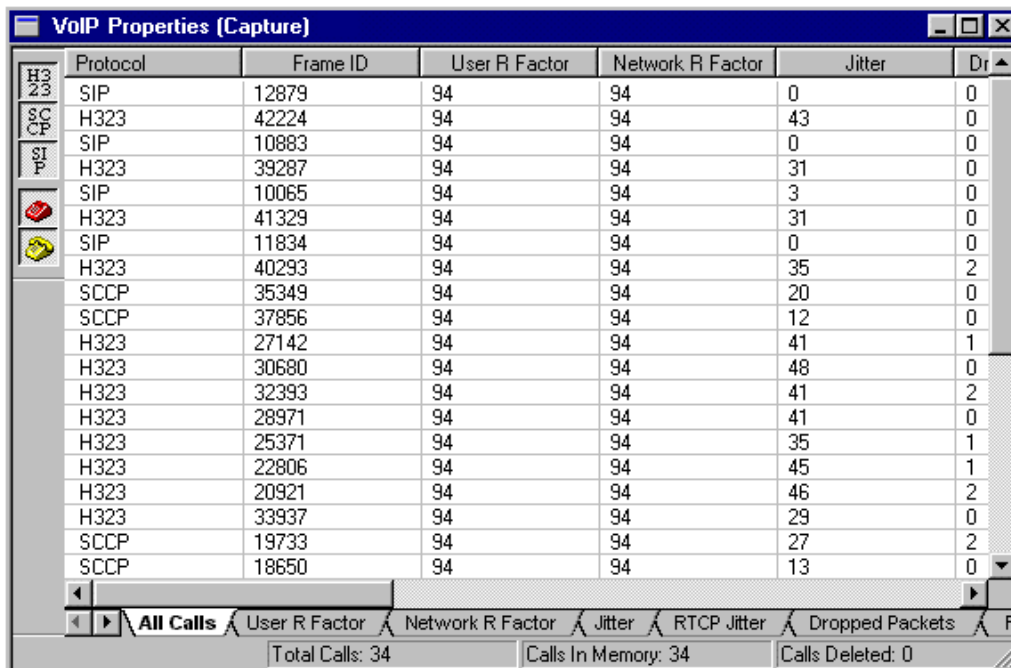
The filter created through this process will filter all the internet traffic to and from the source and destination IP addresses for the selected call. The filter will collect all RAS, Q.931, and H.245 call set-up packets for this call. If the call includes a gatekeeper, these packets will be included as well.

See "Filtering on Single Channels" on page 28. for information on filtering channels within calls.

All Calls Table

The All Calls table provides a summary table of all calls discovered. An example of the All Calls table is shown below.

The buttons to the left of the table allow you to filter the call data. You can display only the calls that use a specific protocol. You can also display completed calls only or incomplete calls only.

Protocol	Frame ID	User R Factor	Network R Factor	Jitter	Dr
SIP	12879	94	94	0	0
H323	42224	94	94	43	0
SIP	10883	94	94	0	0
H323	39287	94	94	31	0
SIP	10065	94	94	3	0
H323	41329	94	94	31	0
SIP	11834	94	94	0	0
H323	40293	94	94	35	2
SCCP	35349	94	94	20	0
SCCP	37856	94	94	12	0
H323	27142	94	94	41	1
H323	30680	94	94	48	0
H323	32393	94	94	41	2
H323	28971	94	94	41	0
H323	25371	94	94	35	1
H323	22806	94	94	45	1
H323	20921	94	94	46	2
H323	33937	94	94	29	0
SCCP	19733	94	94	27	2
SCCP	18650	94	94	13	0

All Calls / User R Factor / Network R Factor / Jitter / RTCP Jitter / Dropped Packets / R

Total Calls: 34   Calls In Memory: 34   Calls Deleted: 0

Figure 11-3. VoIP All Calls Table

Field Descriptions for All Calls Table

The following table provides brief descriptions of all fields in the **All Calls** table.

Table 11-1. All Calls Table Field Descriptions

Table Column	Description
Protocol	H.323, SCCP, or SIP.
Frame ID	Frame ID of the first frame from which the conversation was detected. This field is useful when doing post capture analysis. If there is a need for in-depth analysis of a specific call, the first frame associated with the call can be quickly determined.
User R Factor	Voice quality measure expressed as a numeric value between 0 and 94. The value is calculated by OPV-PE. OPV-PE uses a formula that includes packet loss, jitter, transmission delay, and recency to determine the User R-factor.
Network R Factor	Voice quality measure expressed as a numeric value between 0 and 94. The value is calculated by OPV-PE. OPV-PE uses a formula that includes packet loss, jitter, and transmission delay to determine the Network R-factor.
Jitter	Maximum jitter, measured in milliseconds, for all channels within a call. The value is calculated by OPV-PE. OPV-PE uses the formula described in RFC 1889 to calculate jitter.
Dropped Packets	Maximum number of dropped packets for all channels within a single call. The value is calculated by OPV-PE.
RTCP Jitter	Maximum jitter, measured in milliseconds, for all channels within a call. This is the jitter value reported in RTCP packets.
RTCP Dropped Packets	Maximum number of dropped packets for all channels within a single call. This is the number of dropped packets reported in RTCP packets.
Status	Status of the call. The Status is either "Active" or "Complete".
Source Address	The IP source address of the initiator of the call.
Destination Address	The IP destination address of the receiver of the call.
Start Time	Time at which the call was started.
Stop Time	Time at which the call was complete.
Call Setup TIme	Time that was taken for the call to be setup (the time taken from the start of the call until the phone rings).
Total Call Time	Duration of the call from Start Time to Stop Time.

Call Range Graphs and Summaries

Each tab in the interface except the utilization and configuration tabs brings up a range breakdown of calls using the selected metric.

Call Jitter, Call RTCP Jitter, Call Setup Time

Figure 11-4 shows an example of the **Call Jitter** tab in the VoIP View window. Double-click on a section of the bar or pie graph to see a table of calls for the selected jitter range.

Click on the "pencil" button to change the ranges for jitter in the graph. A **Range Editor** dialog box appears which allows you to modify ranges for this chart type.

Call RTCP Jitter and Call Setup Time displays and configuration are identical to Call Jitter.
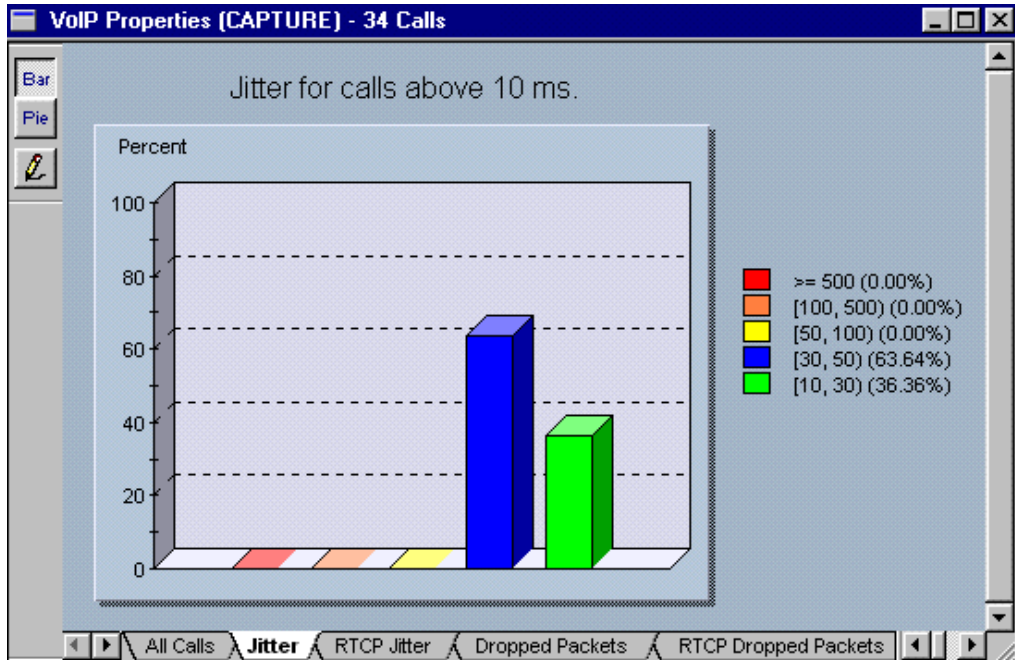
Figure 11-4. VoIP Jitter Graph Example

The title of the graph indicates the minimum value for the selected metric. All calls that meet this minimum value are included in the graphic breakdown. Calls that do not meet this minimum are not included. In the example on the next page, all calls that have a Jitter value greater than 10ms are included. Note that this means the total number of calls in a capture will not necessarily match the total number of calls in the graphic breakdown.

Ranges for the graph can be changed. An example configuration screen for setting Call Jitter ranges is shown below. All values are in milliseconds.

Figure 11-5. VoIP Configuration, Call Jitter Ranges

The default ranges for Call Jitter, Call RTCP Jitter, and Call Setup Time are shown in the table below.

Table 11-2. Defaults for Call Jitter and Call Setup Time Ranges (in milliseconds)

Range	Call Jitter	Call RTCP Jitter	Call Setup Time
Range 1	500 and up	500 and up	1000 and up
Range 2	100 - <500	100 - <500	500 - <1000
Range 3	50 - <100	50 - <100	300 - <500
Range 4	30 - <50	30 - <50	200 - <300
Range 5	10 - <30	10 - <30	150 - <200

Dropped Packets, RTCP Dropped Packets

Figure 11-6 shows an example of the **Dropped Packets** tab in the **VoIP Properties** window. Click on a section of the bar or pie graph to see a table of calls for the selected dropped packets range. Click on the "pencil" button to change the ranges for dropped packets in the graph.

RTCP Dropped Packets displays and configuration are identical to those for Dropped Packets.
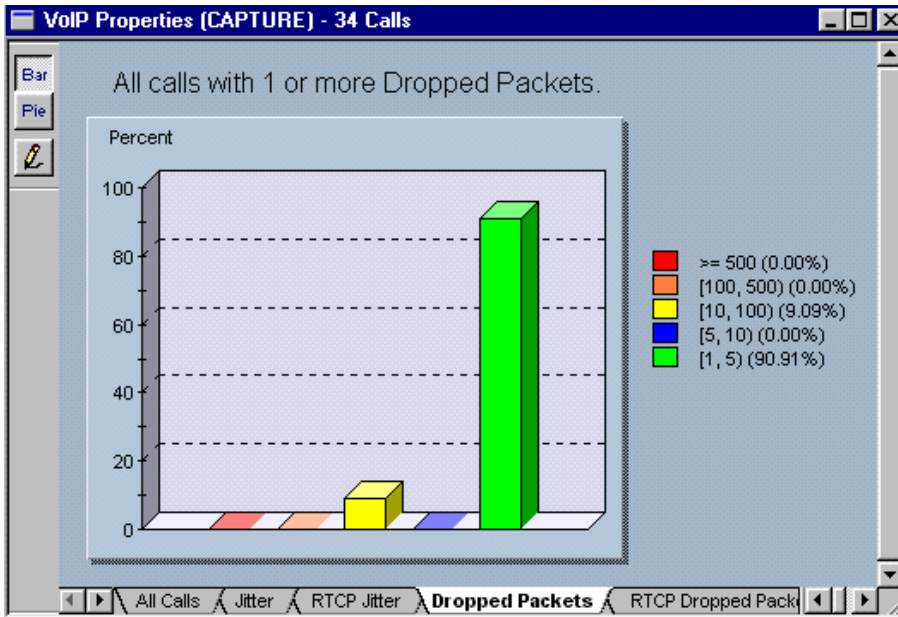
Figure 11-6. VoIP Packets Dropped Graph Example

The title of the graph indicates the minimum value for the selected metric. All calls that meet this minimum value are included in the graphic breakdown. Calls that do not meet this minimum are not included. In the example on the next page, all calls that have one or more dropped packets are included. Note that this means the total number of calls in a capture will not necessarily match the total number of calls in the graphic breakdown.

An example configuration screen for setting Dropped Packet ranges is shown below.

Dropped Packets Threshold Range Editor

Range 1	500	>= AND <	MAXIMUM	☑ Enabled
Range 2	100	>= AND <	500	☑ Enabled
Range 3	10	>= AND <	100	☑ Enabled
Range 4	5	>= AND <	10	☑ Enabled
Range 5	1	>= AND <	5	☑ Enabled

Restore Defaults   OK   Cancel

Figure 11-7. VoIP Configuration, Packets Dropped

The default ranges for Packets Dropped, and RTCP Packets Dropped are shown in the table below.

Table 11-3. Defaults for Packets Dropped Ranges

Range	Dropped Packets	RTCP Dropped Packets
Range 1	500 and up	500 and up
Range 2	100 - 499	100 - 499
Range 3	10 - 99	10 - 99
Range 4	5 - 9	5 - 9
Range 5	1 - 4	1 - 4

Field Descriptions for Call Range Summaries

The following tables provide brief descriptions of all table columns for call range summaries. Only the metric of interest will be displayed in the table. For example, if you are looking at calls in a specific range for Call Jitter, RTCP Jitter and other metrics will not be displayed.

Table 11-4. Call Range Summary Field Descriptions

Table Column	Description
Protocol	H.323, SCCP, or SIP.
Frame ID	Frame ID of the first frame from which the conversation was detected. This field is useful when doing post-capture analysis. If there is a need for in-depth analysis of a specific call the first frame associated with a call can be quickly determined.
User R Factor *	Voice quality measure expressed as a numeric value between 0 and 94. The value is calculated by OPV-PE. OPV-PE uses a formula that includes packet loss, jitter, transmission delay, and recency to determine the User R-factor.
Network R Factor *	Voice quality measure expressed as a numeric value between 0 and 94. The value is calculated by OPV-PE. OPV-PE uses a formula that includes packet loss, jitter, and transmission delay to determine the Network R-factor.
Jitter *	Maximum jitter, measured in milliseconds, for all channels within a call. The value is calculated by OPV-PE. OPV-PE uses the formula described in RFC 1889 to calculate jitter.
Dropped Packets *	Maximum number of dropped packets for all channels within a single call. The value is calculated by OPV-PE.
RTCP Jitter *	Maximum jitter, measured in milliseconds, for all channels within a call. This is the jitter value reported in RTCP packets.
RTCP Dropped Packets *	Maximum number of dropped packets for all channels within a single call. This is the number of dropped packets reported in RTCP packets.
Status	Status of the call. The Status is either "Active" or "Complete".
Source Address	The IP source address of the initiator of the call.
Destination Address	The IP destination address of the receiver of the call.
Start Time	Time at which the call was started.
Stop Time	Time at which the call was completed.
Call Setup TIme*	Time that was taken for the call to be setup (the time taken from the start of the call until the phone rings).
Total Call Time	Duration of the call from Start Time to Stop Time.

* Only one of these fields will appear in the Call Range Summary Table.

VQMon Metrics

There are a variety of objective factors that contribute to call quality. Some of these factors, such as packet loss or packet delay variation (jitter), are reported in other VoIP graph summaries. However, these individual measurements do not tell a complete story and do not attempt to quantify user perceptions of voice quality. The VQmon metrics in VoIP, called R-factors, use a formula to take into account both user perceptions and the cumulative effect of equipment impairments to arrive at a numeric expression of voice quality.

VoIP calculates two equipment impairment values to report as voice-quality metrics: the Network R-factor and the User R-factor. The Network R-factor is generated based on the physical equipment impairments. The User R-factor adds perceptual effects to the equipment impairment, such as recency and delay. The user R-factor attempts to add the "perceived" annoyance that a user may experience during a call based on a perceptual effect called recency. Recency is an auditory phenomenon where distracting events that have occurred more recently appear to have a greater impact on perceived quality. The User R-factor has been found to match well with users' purely subjective ratings of voice quality.

These metrics are calculated by a formula that balances all equipment impairments and perception factors. Each metric is reported as a single number on a per-call basis, typically in the range of 15 to 94. Lower numbers indicate greater equipment impairment or perceived poor voice quality. In VoIP, calls are broken down into a set of ranges for the Network R-factor and User R-factor values calculated for each call. The actual R-factor numbers associated with a single call can be viewed in the Channel Details Table for the call.

It takes some experience to map the exact meaning of the R-factor metrics to your particular network. In general, the R-factors should map well to a sliding scale of how voice quality is perceived. At the extremes, calls with values greater than 80 will have few quality problems and those with values less than 50 will have significant problems. The Network R-factor can be compared to the User R-factor to help determine which factors predominate in any voice quality degradation -- equipment impairments such as packet loss, or, more subjective factors such as recency and delay. Table 11-5 shows ranges of voice quality for the R-factors. The R-factor is also converted to a Mean Opinion Score (MOS), which corresponds to purely subjective rating by users of speech quality on a numeric scale of 1 to 5.

Table 11-5. Voice Quality, R-factors, and MOS Range

Desirability Scale	R-factor Range	MOS Range
Desirable	94 - 80	4.4 - 4.0
Acceptable	80 - 70	4.0 - 3.6
Reach Connection	70 - 50	3.6 - 2.6
Not Recommended	50 - 0	2.6 - 1

If you would like more detailed information about how R-factors are calculated, please call Fluke Networks customer support. The R-factors used in VoIP extend the ITU standard E Model for estimating transmission quality.

A sample display of call breakdown by Network R-factor is shown below. User R-factor display is identical to Network R-factor.
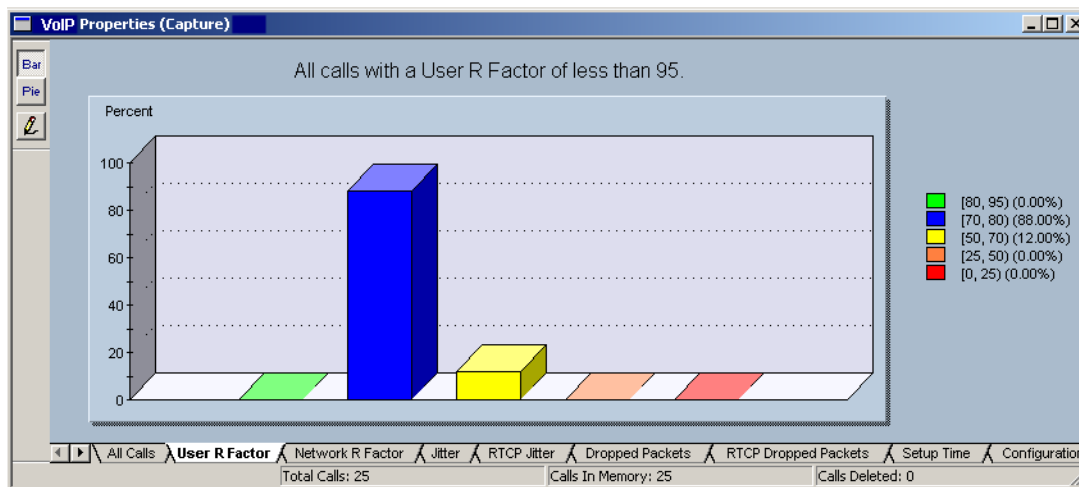
Figure 11-8. VoIP R-factor Example

The title of the graph indicates the maximum value (80) for the selected metric. All calls that meet this minimum value are included in the graphic breakdown. Calls that do not meet this minimum are not included. In the example on the next page, all calls that have an R-factor of less than 80 are included. Note that this means the total number of calls in a capture will not necessarily match the total number of calls in the graphic breakdown.

Ranges for the graph can be changed. An example configuration screen for setting R-factor ranges is shown below.

Figure 11-9. VoIP Configuration, R-factor Ranges

The default ranges for Network R-factor and User R-factor are shown in the table below.

Table 11-6. Ranges for R-factors

Range	Network R-factor	User R-factor
Range 5	<25	<25
Range 4	<50 -25	<50 -25
Range 3	<70 - 50	<70 - 50
Range 2	<80 - 70	<80 - 70
Range 1	94 - 80	94 - 80

Utilization Graph

When selected in Monitor mode, Voice over IP displays the **Utilization** tab. The utilization graphs provides a view of total bandwidth utilization and Voice over IP bandwidth utilization over time. The utilization for VoIP services is compared to total utilization and total bandwidth. An example utilization graph is shown below.
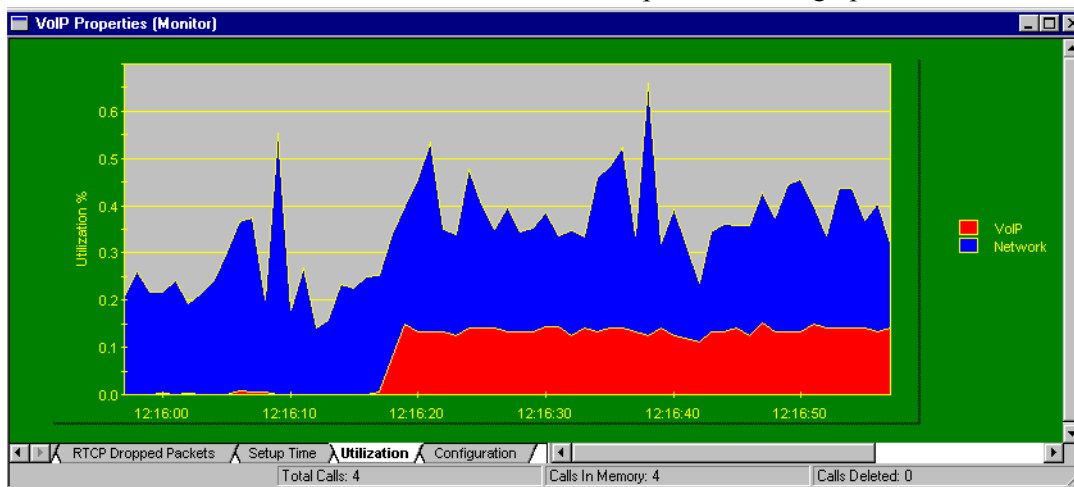
Figure 11-10. VoIP Utilization Graph Example

The utilization is calculated after OPV-PE has decoded packets.

Field Descriptions for Call Details

To view all details for any call, double-click on any call summary (row) in a call summary table. The **Call Detail** window appears showing all call fields for the selected call. An example **Call Detail** window for an H.323 call is shown below:
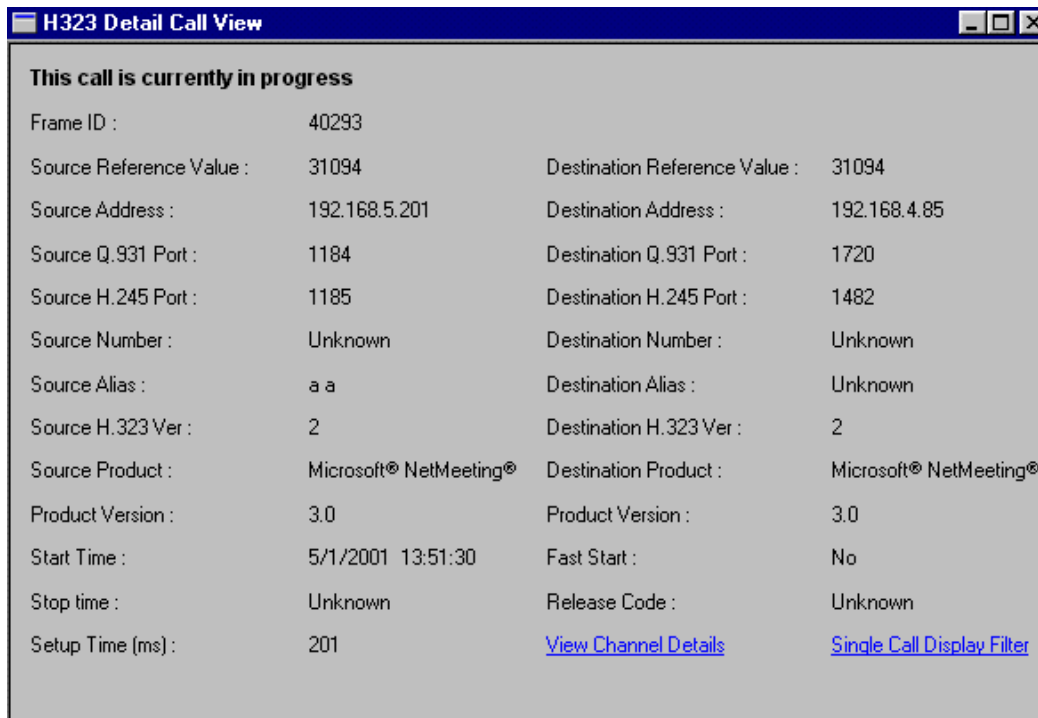
Figure 11-11. Example Call Details Window (H.323)

Click on **View Channel Details** to view channels for this call. Click on **Single Call Display Filter** to filter out all packets except the packets of this call.

The following tables provide brief descriptions of all fields in the **Call Detail** window for SCCP, H.323, or SIP calls.

Table 11-7. SCCP Call Field Descriptions

Table Column	Description
FID	Frame ID of the first frame from which the conversation was detected. This field is useful when doing post capture analysis. If there is a need for in-depth analysis of a specific call, the first frame associated with the call can be quickly determined.
Caller Name	Caller's name.
Caller Port	TCP port of the end point initiating the call.
Caller Address	IP Address of the end point initiating the call.
Caller Number	Phone number of the calling party.
Start Time	Time at which the call was started.
Stop Time	Time at which the call was completed.
Setup Time (ms)	Time that was taken for the call to be setup (the time taken from the start of the call until the phone rings).
Callee Name	Name of the receiver of the call.
Callee Port	TCP port of the end point receiving the call.
Callee Address	IP Address of the end point receiving the call.
Callee Number	Phone number of the called party.
SCCP Version	SCCP protocol Version used in this call.
Call Status	Status of the call. An active call has the status of "Setting up" or "set up complete". A completed call has the status of "Set up failed", "Aborted", or "Complete".

Table 11-8. H.323 Call Field Descriptions

Field Name	Description
Frame ID	Frame ID of the first frame from which the conversation was detected. This field is useful when doing post capture analysis. If there is a need for in-depth analysis of a specific call, the first frame associated with call can be quickly determined.
Source Reference Value	The Call Reference Value for the conversation used by H.225.0 on the source side.
Source Address	The IP address of the initiator of the call.
Source Q.931 Port	The Q.931 TCP port of the initiator of the call.
Source H.245 Port	The H.245 TCP port of the initiator of the call.
Source Number	Phone number of the initiator of the call.
Source Alias	An alias of the initiator of the call.
Source H.323 Ver	The version of H.323 being used by the initiator of the call.
Source Product	The product being used by the initiator of the call.
Product Version	The product version being used by the initiator of the call.
Start Time	Time at which the call was started.
Stop Time	Time at which the call was completed.
Setup Time (ms)	Time that was taken for the call to be setup (the time taken from the start of the call until the phone rings).
Destination Reference Value	The Call Reference Value for the conversation used by H.225.0 on the destination side.
Destination Address	The IP address of the receiver of the call.
Destination Q.931 Port	The Q.931 TCP port of the receiver of the call. This port has a default value of 1720.
Destination H.245 Port	The H.245 TCP port of the receiver of the call
Destination Number	Phone number of the receiver of the call.
Destination Alias	An alias of the receiver of the call.
Destination H.323 Ver	The version of H.323 being used by the receiver of the call.
Destination Product	The product being used by the receiver of the call.
Product Version	The product version being used by the receiver of the call.
Fast Start	Indicates whether or not Fast Start was used during call setup.
Release Code	Code indicating the status of the call when it was completed.

Table 11-9. SIP Call Field Descriptions
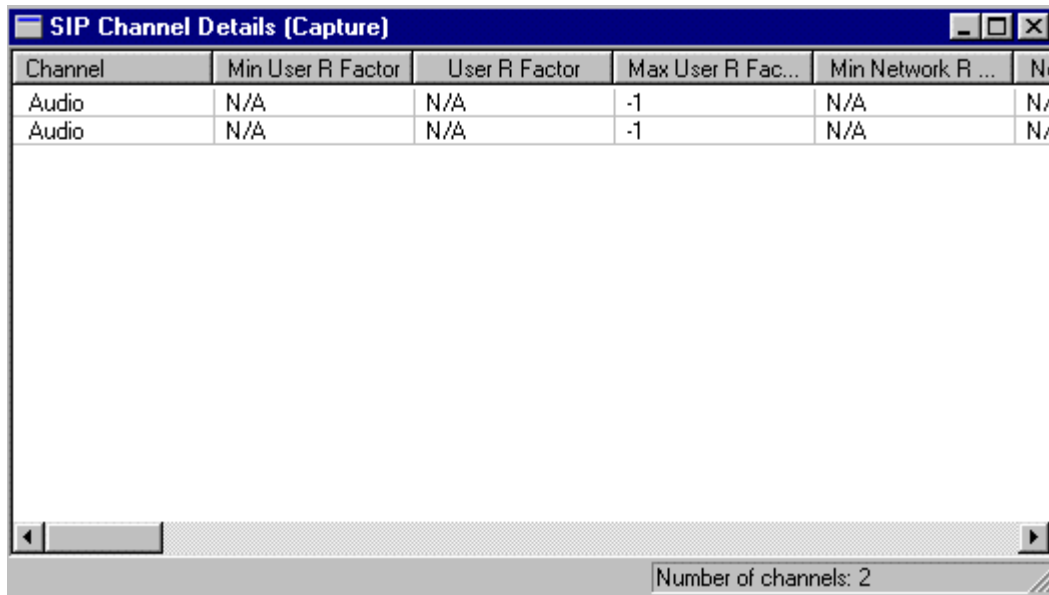
Field Name	Description
FID	Frame ID of the first frame from which the conversation was detected. The the frame ID of the first INVITE message.
Caller	SIP URL or other URI of the caller. The addr-spec in the "From" parameter.
Caller Name	Display name of the caller. The display name in the "From" parameter, if it exists.
Caller Tag	The tag of "From", if it exists.
Caller Address	The IP address of the initiator of the call.
Start Time	Time at which the call was started, i.e. the time of the first INVITE message of the call.
Stop Time	Time at which the call was complete.
Setup Time (ms)	Time that was taken for the call to be setup. This is the duration from "INVITE" to the 180 or 183 (ringing) response if available, or to the 200 response otherwise. If none of these responses are received, the field value is set to "Unknown".
Call-ID	Globally unique ID to identify a SIP call.
Callee	SIP URL or other URI of the callee. The addr-spec in the "To" parameter.
Callee Name	Display name of the callee. The display name in the "To" parameter, if it exists.
Callee Tag	The tag of "To", if it exists.
Callee Address	The IP address of the receiver of the call.
SIP Version	The version of SIP being used.
Response Code	The response code number from the callee.
Call Status	Status of the call. An active call has the status of "Setting up" or "Set up complete", and a complete call has the status of "Set up failed", "Aborted", "Complete".

Channel Table Details

You can look at channel information for any call. Single-click on the **View Channel Details** link in the **Single Call Detail View** box to display channel information. A table appears showing all channels within the call.

If you have reached channel view from the graphic summaries, the channel that has the highest value for the metric associated with the graph is highlighted for easy identification. For example, if you select a jitter range and select a call within that range, the channel that has the highest jitter value for that call will be highlighted. R-factors are included for the audio channels of the call.

Figure 11-12 shows an example channel table for a call.

SIP Channel Details (Capture)					
Channel	Min User R Factor	User R Factor	Max User R Fac...	Min Network R ...	N
Audio	N/A	N/A	-1	N/A	N/
Audio	N/A	N/A	-1	N/A	N/

Number of channels: 2

Figure 11-12. Channel Table Example

Table 11-10 and Table 11-11 describe the columns in the table for each protocol. H.323 and SIP channel tables are the same.

Table 11-10. H.323 or SIP Channel Table Column Descriptions

Table Column	Description
Channel	Channel type, Audio, Video, or Data.
Min User R Factor	The lowest User R-factor calculated during a sampling interval for a call.
User R Factor	Voice quality measure expressed as a numeric value between 0 and 94. The value is calculated by OPV-PE. OPV-PE uses a formula that includes packet loss, jitter, transmission delay, and recency to determine the User R-factor.
Max User R Factor	The highest User R-factor calculated during a sampling interval for a call.
Min Network R Factor	The lowest Network R-factor calculated during a sampling interval for a call.
Network R Factor	Voice quality measure expressed as a numeric value between 0 and 94. The value is calculated by OPV-PE. OPV-PE uses a formula that includes packet loss, jitter, and transmission delay to determine the Network R-factor.
Max Network R Factor	The highest Network R-factor calculated during a sampling interval for a call.
Estimated MOS	A conversion of the combined R-factors to a Mean Opinion Score. The MOS maps to a purely subjective evaluation of call quality where users rate speech samples on a scale of 1 to 5.
Dst Addr	The destination IP address.
Dst Port	The destination UDP port.
Src Addr	The source IP address.
Src Port	The source UDP port.
Sync Source	Synchronization source. Internal number identifying the source.
Packet Count	Packet Count. The value is calculated by OPV-PE.
Byte Count	Byte Count. The value is calculated by OPV-PE.
Dropped Packets	Packets Dropped. The value is calculated by OPV-PE.
Codec	Codec/Decoder type. (DataType in H.245)
Jitter (ms)	Jitter in milliseconds. The value is calculated by OPV-PE. OPV-PE uses the formula described in RFC 1889 to calculate jitter.
Min Jitter (ms)	Minimum Jitter in milliseconds. The value is calculated by OPV-PE. OPV-PE uses the formula described in RFC 1889 to calculate jitter.

Table 11-10. H.323 or SIP Channel Table Column Descriptions (continued)

Max Jitter (ms)	Maximum Jitter in milliseconds. The value is calculated by OPV-PE. OPV-PE uses the formula described in RFC 1889 to calculate jitter.
Low Seq Num	Lowest Sequence Number. Lowest RTP sequence number seen.
High Seq Num	Highest Sequence Number. Highest RTP sequence number seen.
RTCP Packet Count	Real-time Transport Control Protocol (RTCP) Packet Count.
RTCP Byte Count	RTCP Byte Count.
RTCP RTP Packet Count	RTCP reported RTP Packet Count.
RTCP RTP Byte Count	RTCP reported RTP Byte Count.
RTCP Jitter (ms)	RTCP reported jitter. Average reported RTCP interarrival jitter.
RTCP Min Jitter (ms)	RTCP reported minimum jitter. Minimum reported interarrival jitter.
RTCP Max Jitter (ms)	RTCP reported maximum jitter. Maximum reported interarrival jitter.
RTCP High Seq Num	High Sequence Number reported by RTCP.
RTCP Sender Report Count	Number of RTCP Sender Reports seen.
RTCP Receiver Report Count	Number of RTCP Receiver Reports seen.
RTCP Source Description Count	Number of RTCP Source Descriptions seen.
RTCP Goodbye Count	Number of RTCP Goodbyes seen.
RTCP Application-Defined Count	Number of RTCP Application Definitions seen.
RTCP Unknown Report Count	Count of all other RTCP reports seen.
RTCP CName	Canonical Name. (RTCP Source Description, CNAME field)
RTCP Name	User's Name. (RTCP Source Description, NAME field)
RTCP Email	User's electronic mail address. (RTCP Source Description, EMAIL field)
RTCP Phone	User's phone number. (RTCP Source Description, PHONE field)
RTCP Location	User's geographic location. (RTCP Source Description, LOCATION field)
RTCP Tool	Name of application or tool. (RTCP Source Description, TOOL field)
RTCP Note	Notice about the source. (RTCP Source Description, NOTE field)

Table 11-11. SCCP Channel Table Column Descriptions

Table Column	Description
Channel	Channel type, Audio, Video, or Data.
Min User R Factor	The lowest User R-factor calculated during a sampling interval for a call.
User R Factor	Voice quality measure expressed as a numeric value between 0 and 94. The value is calculated by OPV-PE. OPV-PE uses a formula that includes packet loss, jitter, transmission delay, and recency to determine the User R-factor.
Max User R Factor	The highest User R-factor calculated during a sampling interval for a call.
Min Network R Factor	The lowest Network R-factor calculated during a sampling interval for a call.
Network R Factor	Voice quality measure expressed as a numeric value between 0 and 94. The value is calculated by OPV-PE. OPV-PE uses a formula that includes packet loss, jitter, and transmission delay to determine the Network R-factor.
Max Network R Factor	The highest Network R-factor calculated during a sampling interval for a call.
Estimated MOS	A conversion of the combined R-factors to a Mean Opinion Score. The MOS maps to a purely subjective evaluation of call quality where users rate speech samples on a scale of 1 to 5.
Src Addr	IP address of the caller
Src Port	UDP port of the caller
Dst Addr	IP address of the callee
Dst Port	UDP port of the callee
Sync Source	Synchronization Source. Internal number identifying the source.
Packet Count	Packet Count. The value is calculated by OPV-PE.
Byte Count	Byte Count. The value is calculated by OPV-PE.
Dropped Packets	Packets Dropped. The value is calculated by OPV-PE.
Codec	Codec/Decoder type. (DataType in H.245)
Jitter (ms)	Jitter in milliseconds. The value is calculated by OPV-PE. OPV-PE uses the formula described in RFC 1889 to calculate jitter.
Min Jitter (ms)	Minimum Jitter in milliseconds. The value is calculated by OPV-PE. OPV-PE uses the formula described in RFC 1889 to calculate jitter.
Max Jitter (ms)	Maximum Jitter in milliseconds. The value is calculated by OPV-PE. OPV-PE uses the formula described in RFC 1889 to calculate jitter.

Table 11-11. SCCP Channel Table Column Descriptions (continued)

Low Seq Num	Lowest Sequence Number. Lowest RTP sequence number seen.
High Seq Num	Highest Sequence Number. Highest RTP sequence number seen.

Filtering on Single Channels

You can filter on channels within a single call. For the Channel View table, the filter menu available with the right-mouse click depends on the channel you select. For Audio or Video channels, the menu has three filter options, **Quick RTCP and RTP Channel Display Filter**, **Quick RTP Channel Display Filter**, and **Quick RTCP Channel Display Filter**. You can create a display filter for the selected RTCP/RTP channel without having to first go to the filter window. For a data channel there is one filter option, **Quick Data Channel Display Filter**.

Call Playback

To get a subjective measure of call quality, you can listen to calls that contain RTP packets encapsulating PCMU or PCMA voice data (G.711 codec). The PCMU/PCMA data is converted to wave file format and automatically played.

To playback a call from VoIP, perform these steps:

1. Double click on a completed or active phone call which has RTP packets containing PCMU or PCMA data.

2. Select **View Channel Details** from the **Call Detail View** window.

3. The Channel Table appears. Right click on an audio channel and select **Playback PCMU/PCMA Data**.

4. The **Save As** window prompts for the name of the file. The audio data is saved in a wave file format (.wav). After saving the file, the audio data is played.

5. A small dialog box appears while the audio data is playing. Press the **Cancel** button to stop playback.

Once the wave file is saved, it can be played from other media players.

Note that you will only hear one side of a complete audio communication. The complete conversation is composed of two channels and you are only listening to one of the channels.

Customizing VoIP Table Displays

You can customize the display of table information for Voice over IP to include or exclude Voice over IP fields from the All Calls, Summary Range, or Channel table displays.

To change the view options, the table type you want to change must be in the foreground. For example, to change the fields that display in the All Calls table, the All Calls table must display in the foreground.

To set the columns for a table display, select **View Options** from the **Views** menu. The dialog box contains all possible display fields with a check box. Exclude fields from the table display by removing the check from the check box next to the field. The default is to display all fields.

Customizing All Calls or Range Summary Tables

Select **Voice over IP Views** for the **Monitor Views** or **Capture Views** menu. With either the All Calls table or one of the Range Summary Tables displayed, select **View Options...** from the **View** menu. Check the boxes for all fields you want to include in the table display.

The table modifications remain until the table window is closed. When the window is closed and reopened, the default fields in the table are restored.

An example table options dialog box is shown below.
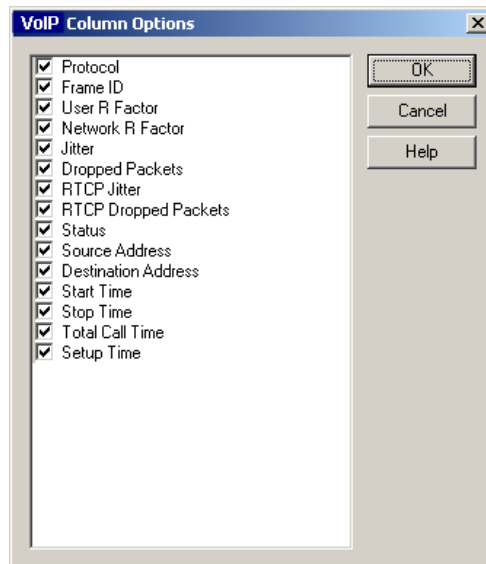
Figure 11-13. VoIP View Options Example

Customizing Channel Tables

The channel table is different for each call type, H.323, SIP, or SCCP. The channel table fields for each call type can be customized.

Select **Voice over IP Views** for the **Monitor Views** or **Capture Views** menu. Select a single call, and from the Call Detail window select **View Channel Details** to bring up the Channel table. Select **View Options...** from the **View** menu. Check the boxes for all fields you want to include in the table display.

The table modifications remain until the window is closed. When the window is closed and reopened, the default fields in the table are restored.

An example dialog box for configuring SCCP channel table options is shown below.
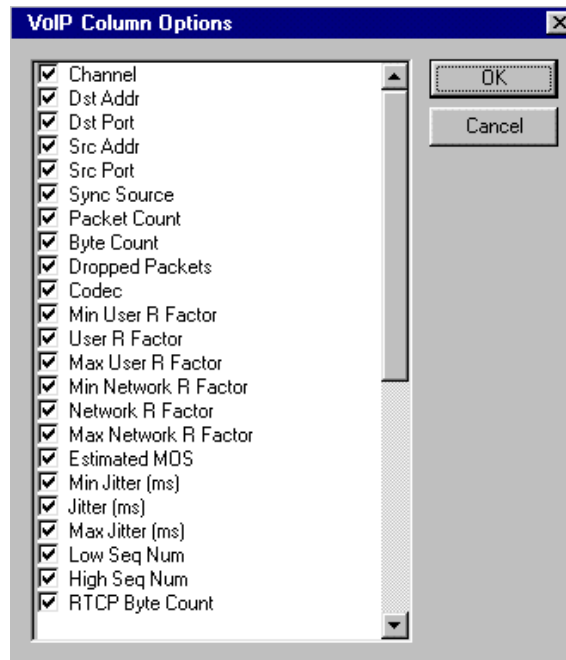
Figure 11-14. VoIP Channel Table View Options, SCCP Example

Exporting VoIP Data

You can export VoIP tables to CSV format. VoIP data in `.csv` format can be imported to many spreadsheet and database applications like Microsoft Excel or to your own application, allowing you to display or report data. CSV is a comma-delimited text format used by many applications to import/export text data.

The order of the fields in the exported files is essential to proper interpretation of the data. This section includes a table showing which VoIP fields are exported and in what order.

Exporting All VoIP Data to CSV Format

Perform these steps to export all VoIP table data.

1. Make sure that one of the Voice over IP views is open and is the currently selected view.

2. Choose **Export VoIP Data...** from the **File** menu.

3. Enter the file name in the **Save As...** dialog box. All call data will automatically be saved in CSV format and the file is given an extension of .csv.

4. Click the **Save** button.

The VoIP export information is arranged by protocol, H.323, SCCP, and SIP. When viewed in a spread sheet application, a single row has the complete information for a single call, including all call detail fields and all channel fields for all channels within the call.

Call detail fields are listed first, followed by all possible channels within the call. If a channel is not used for a call, the fields for that channel will be blank in the CSV export file.

Exporting a Single VoIP Table to CSV Format

Perform these steps to export the current VoIP table to CSV format.

1. Select the view you want to export. If you already have the desired view open, click the window to make it the currently selected view.The table can be a range summary table, the detail view fields for a single call, the channel table for a selected call, or the all calls table.

2. Choose **Export...** from the **File** menu.

3. Enter the file name in the **Save As...** dialog box. The data will automatically be saved in CSV format. The file is given an extension of .csv.

4. Click the **Save** button.

Only the VoIP information displayed in the current table is exported. For example, when exporting the All Calls table, only the fields within the All Calls table are exported. For the All Calls table, you can use the buttons to select a subset of calls before exporting.

Chapter 12
Counters

OPV-PE provides sophisticated counters to enable you to precisely monitor network activity. OPV-PE features three types of counters at the MAC layer: Packet Counters, Custom Counters, and Error Counters. When the **MAC Statistics** window is in Capture mode, you can use all three types of counters. When the **MAC Statistics** window is in Transmit mode, custom counters are not relevant and do not appear in the **MAC Statistics** window.

OPV-PE provides three types of MAC layer counters:

Table 12-1. MAC Layer Counter Types

Counter Type	Description
Packet Counters	Count the number and type of packets and bytes captured or transmitted by the OPV-PE.
Custom Counters	User-defined counters that you can use to control data capture activities while the OPV-PE is in capture mode.
Error Counters	Count the number of errors that occur while the OPV-PE is monitoring/capturing or transmitting data.

Counters of VoIP events are provided with the VoIP software option.

Log files contain snapshots of OPV-PE counter information. All byte, frame, and error counter values are recorded in the log file. Refer to the section on Logging for more information.

Packet Counters

Packet counters count the number of packets/bytes received or transmitted. Packet counters are viewed from the **MAC Statistics** window.

The following packet counters are supported:

- Total Frames

- Broadcast Frames

- Multicast Frames

- Unicast Frames

- Error Frames

- Total Bytes Received

- A breakdown of the total number of error frames is provided by the error counters.

Custom Counters

Custom counters are user-defined counters established in capture filters. When a certain condition in the filter is satisfied, counter 1, 2, or 3 can be incremented as a result of one of the actions taken by the capture filter. Custom counters are available in capture mode only.

Custom counters are incremented in the MAC Statistics view as packets are captured. By setting counters, you can visually see in the MAC Statistics view how many frames of a certain type have been captured.

Error Counters

During receive, error events are counted as they occur. The MAC statistics view and the table associated with the Utilization/Errors chart displays the receive error counters.

Table 12-2 contains an alphabetical list, with descriptions, of OPV-PE's Ethernet error counters.

Table 12-2. Alphabetical List and Descriptions of Ethernet Error Counters

Counter Type	Description
Collision Indication	This counter is the sum of CRC/Align and Fragments error counters, as these conditions are usually caused by collisions. See the CRC/Align and Fragments counters described below.
CRC/Align	A counter that shows the total number of packets received that had a length between 64 and 1518 octets, inclusive, but had either a bad FCS with an integral number of octets (FCS/CRC Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Fragments	A counter showing the total number of packets received that were less than 64 octets and had either an FCS/CRC error or an Alignment Error.
Jabbers	A counter that shows the total number of packets that were received that were longer than 1518 octets and had either an FCS/CRC error or an Alignment Error.
Oversize	A counter showing the total number of packets received that were longer than the 1518 octets and were otherwise well formed (good FCS).
undersize	A counter showing the total number of packets received that were shorter than 64 octets and were otherwise well formed (good FCS).
Total Tx Collision	A counter showing the total number of collisions that have occurred when attempting to transmit.
Tx Attempt	A counter of the number of transmission attempts that have failed.
Tx Defer	A counter that shows the number of times the transmitter had transmit data available and was ready to transmit but had to defer transmission due to sensing other traffic.
Tx Excessive Collision	A counter that shows the number of times packets collided 16 times without successful transmission.
Tx Excessive Defer	A counter that shows the number of times the transmitter had to defer for greater than 3,036 byte times.
Tx Late Collision	A counter that shows the number of collisions that occur greater than 512 bit times after a transmission has started.
Undersize	A counter showing the total number of packets received that were less than 64 octets in length and were otherwise well-formed (good FCS).
Very Long Event	A counter that shows the number of times the transmitter is active for greater than a maximum event length. The maximum event length is 4ms to 7ms for 10Mbps network speeds and 0.4 to 0.75ms for 100Mbps network speeds.

Table 12-3 contains an alphabetical list, with descriptions, of OPV-PE's Token Ring error counters.

Table 12-3. Alphabetical List and Descriptions of Token Ring Error Counters

Token Ring Counter	Description
Abort Delimiter	A counter that records events where a reporting Ring Station encounters recoverable internal errors, forcing it to transmit an Abort Delimiter frame.
AC Error	A counter that records events where the reporting Ring Station's nearest active upstream neighbor could not set the address recognized bits or frame copied bits in the newly transmitted frame after copying the bits on the last frame received.
Burst Error	A counter that records events where the reporting Ring Station encounters signal transition or signal error on the Token Ring physical medium
Frame Copy	A counter that records when a reporting Ring Station copies a frame containing the Ring Station's own (duplicate) address.
Frequency	A counter that records events where the reporting Ring Station attempts to receive a frame containing an improper ring-clock frequency.
Internal Error	A counter that records events where the reporting Ring Station encounters a recoverable internal error.
Line Error	A counter that records events where the reporting Ring Station's checksum process detects an error in a received data frame or token that the Ring Station transmitted.
Lost Frame	A counter that records events where a reporting Ring Station generates a frame to a specific address and does not receive the returned frame.
Token Error	A counter that records events where the Token Ring Active Monitor does not detect a ring token.

Expert Counters

Expert counters count the number of Expert events discovered by the Expert Analysis logic. Some counters are used in the Expert Alarm editor and some display in the Overview Table of Expert View. See the *Expert Systems* chapter for more information on expert counters.

The following table contains an alphabetical list, with descriptions, of OPV-PE's expert counters.

Table 12-4. Alphabetical List and Descriptions of Expert Counters

Counter Type	Description
Bad Frames	The number of bad frames including CRC frames, jabber frames, runt frames, oversize frames, and fragment frames.
Broadcast/Multicast Storms	The number of Broadcast/Multicast Storm events. The event occurs when a change in the number of total Broadcast/Multicast packets per second exceeds a threshold.
Duplicate Network Address	The number of duplicate network addresses over a period of time per segment.
Excessive ARP	The number of Excessive ARP events. The event occurs when a change in the number of ARP requests per second exceeds a threshold.
Excessive BOOTP	The number of Excessive BOOTP events. The event occurs when a change in the number of BOOTP/DHCP requests per second exceeds a threshold over a period of time per segment.
Excessive Broadcasts	The number of broadcast messages over a period of time per segment.
Excessive Collisions	The absolute number of collisions over a period of time per segment.
Excessive Mailslot Broadcasts	The number of mailslot broadcast events over a period of time per segment.
Excessive Multicasts	The number of multicast messages over a period of time per segment.
HSRP Errors	The number of HSRP Coup and Resign messages over a period of time per segment.
ICMP All Errors	The number of ICMP symptoms. This includes all destination unreachable errors, redirect errors, source quench, time-out errors, and parameter problems.

Table 12-4. Alphabetical List and Descriptions of Expert Counters (continued)

Counter Type	Description
ICMP Destination Unreachable	The number of ICMP destination unreachable errors over a period of time per segment. Unreachable errors include Network Unreachable, Host Unreachable, Protocol Unreachable, Port Unreachable, Fragmentation Needed [D/F Set], Source Route Failed, Destination Network Unknown, Destination Host Unknown, Destination Network Access Denied, Destination Host Access Denied, Network Unreachable for TOS, and Host Unreachable for TOS.
ICMP Redirect	The number of ICMP redirect errors over a period of time per segment. Redirect errors include Network Redirect, Host Redirect, Network Redirect for TOS, and Host Redirect for TOS.
Illegal MAC Station Address	The number of illegal MAC station source addresses over a period of time per segment.
Illegal Network Source Address	The number of illegal network source addresses over a period of time per segment.
IP Checksum Errors	The number of incorrect IP checksums over a period of time per segment
IP Time to Live Expiring	The number of expiring connections over a period of time per segment.
ISL BPDU/CDP Packets	The number of Bridge Protocol Data Unit (BPDU) or Cisco Discovery Protocol (CDP) packets over a period of time per segment.
ISL Illegal VLAN ID	The number of ISL illegal VLAN IDs over a period of time per segment.
NCP Server Busy	The number of NCP Server Busy events a period of time per segment.
Network Overload	The number of instances where a threshold for the percentage change in network utilization is exceeded.
New MAC Stations	The number of the new MAC stations over a period of time per segment.
NFS Retransmissions	The number of NFS Retransmissions over a period of time per segment.
Non Responsive Stations	The number of Non Responsive Station events. A non-responsive station is defined as successive TCP/IP retransmissions over the same connection that are greater than a threshold value.
OSPF Broadcasts	The number of OSPF broadcasts over a period of time per segment.
Overload Frame Rate	The number of frames over a one-second time period.

Table 12-4. Alphabetical List and Descriptions of Expert Counters (continued)

Counter Type	Description
Overload Utilization Percentage	Counts bits over time and compares this value to the maximum utilization possible (bandwidth).
No HTTP POST Response	The number of no HTTP POST responses over a period of time per segment.
No Server Response	The number of no server responses over a period of time per segment.
Physical Errors	The number of Physical Error events. The event occurs when a change in the number of total MAC physical errors per second exceeds a threshold.
RIP Broadcasts	The number of RIP broadcasts over a period of time per segment.
Router Storm	The number of router storm events over a period of time per segment.
Same MAC Addresses	The number of same network addresses over a period of time per segment.
Same Network Addresses	The number of same MAC addresses over a period of time per segment.
SAP Broadcasts	The number of SAP broadcasts over a period of time per segment.
Slow HTTP GET Response	The number of slow HTTP GET responses over a period of time per segment.
Slow HTTP POST Response	The number of slow HTTP POST responses over a period of time per segment.
Slow Server Connect	The number of slow server responses over a period of time per segment.
Slow Server Response	The number of slow server responses over a period of time per segment.
SMB Invalid Network Name	The number of SMB invalid network names over a period of time per segment.
TCP Checksum Errors	The number of incorrect TCP checksums over a period of time per segment. This counter is turned OFF by default and must be turned ON by the user.
TCP/IP Frozen Window	The number of TCP/IP Frozen Window events over a period of time per segment.
TCP/IP Long Acks	The number of TCP/IP Long Ack events over a period of time per segment.

Table 12-4. Alphabetical List and Descriptions of Expert Counters (continued)

Counter Type	Description
TCP/IP Repeat Ack	The number of TCP/IP Repeat Ack events over a period of time per segment.
TCP/IP Retransmissions	The number of TCP/IP Retransmissions over a period of time per segment.
TCP/IP RST Packets	The number of TCP/IP RST Packets over a period of time per segment.
TCP/IP SYN Attack	The number of TCP/IP SYN Attack events. The event occurs when a change in the number of SYN requests per second exceeds a threshold.
TCP/IP Window Probe	The number of TCP/IP Window Probe events over a period of time per segment.
TCP/IP Zero Window	The number of TCP/IP Zero Window events over a period of time per segment.
Total MAC Stations	The number of the new MAC stations over a period of time per segment.
Total Router Broadcasts	The number of total router broadcasts over a period of time per segment.
Unstable MST	The number of excessive MST topology events. The event occurs when a change in the number of MST topology changes per second exceeds a threshold.

VoIP Counters

VoIP counters count the number of packet events discovered in the data stream.

The following table contains an alphabetical list, with descriptions, of the counters used in VoIP Views.

Table 12-5. Alphabetical List and Descriptions of VoIP Counters

Counter Type	Description
Byte Count	Count of all bytes associated with a VoIP channel.
Packet Count	Count of all packets associated with a VoIP channel.
Packets Dropped	Count of all packets dropped associated with a VoIP channel.

Counter Log File Overview

Counter log files contain snapshots of OPV-PE counter information. All byte, frame, and error counter values are recorded in the log file. The time interval for capturing snapshots, the number of snapshots in the log file, and the creation of history files are set in the **System Settings** option of the **Configuration** menu.

For OPV-PE, log files are maintained by module. A log file and a set of history files are created in a unique directory for each Protocol Media Module and each Ethernet Adapter. The directory for the module log is named `...\log\local\module_n`. The module log file is named `module_n.csv` where `n` is the number of the module. The log directory structure starts from the installation directory for OPV-PE.

For OPV-PE in NDIS mode, log files are maintained by the Ethernet adapter (NDIS) running the OPV-PE software. The directory for the NDIS log is named `...\log\local\NDIS_n` and the NDIS log file is named `NDIS_n.csv` where `n` is the number of the adapter the NDIS driver detected.

The log files are text files in CSV format, a format easily imported into spreadsheet applications such as Microsoft Excel. Each line entry in the log file will create a separate row in the spreadsheet. Column titles for all counters are provided in the CSV text file. A template file for viewing counter information as graphs is provided. The template file works with Microsoft Excel™ Version 5.0 or greater.

See "Configuring Counter Logging" in the "Customizing OPV-PE" chapter.

Log Directory Structure

The following is the directory structure for log files. The root directory is the installation directory for OPV-PE.

```
(root)\log\local\module_1 (directory for module 1)
   module_1.csv (log file for module 1)
   \history (history directory for module 1)
      mmddhhmm.ss (first history file for module 1)
      mmddhhmm.ss (second history file for module 1)
      mmddhhmm.ss (third history file for module 1)
(root)\log\local\module_2 (directory for module 1)
   module_2.csv (log file for module 2)
   \history (history directory for module 2)
      mmddhhmm.ss (first history file for module 2)
      mmddhhmm.ss (second history file for module 2)
      mmddhhmm.ss (third history file for module 2)
(root)\log\local\module_n (directory for module n)
   module_n.csv (log file for module n)
   \history (history directory for module n)
      mmddhhmm.ss (first history file for module n)
      mmddhhmm.ss (second history file for module n)
      mmddhhmm.ss (third history file for module n)
(root)\log\local\NDIS_1 (directory for Ethernet Adaptor 1)
   NDIS_1.csv (log file for NDIS adapter)
   \history (history directory for NDIS adapter)
      mmddhhmm.ss (first history file)
      mmddhhmm.ss (second history file)
      mmddhhmm.ss (third history file)
(root)\log\local\NDIS_n (directory for Ethernet Adaptor 'n')
   NDIS_n.csv (log file for NDIS adapter)
   \history (history directory for NDIS adapter)
      mmddhhmm.ss (first history file)
      mmddhhmm.ss (second history file)
      mmddhhmm.ss (third history file)
```

Chapter 13
Utilities

OPV-PE includes the following utilities to enhance your ability to manage your Ethernet, Token Ring, or Fast Ethernet network:

Table 13-1. Ethernet and Fast Ethernet Network Management Utilities

Utility	Description
Name Table Utility	Provides associations between symbolic names and network addresses.
NIS-to-Name-Table Utility	Converts an NIS name table on a UNIX system to OPV-PE format.
Sniffer Translator Utility	Enables OPV-PE and Sniffer systems to exchange captured data.
Get Version Information Utility	Provides information about Protocol Media Modules installed in your PC.
Identify-a-Module Utility	Verifies that the correct module is connected to the correct network or network segment.
Split Capture File	Allows the splitting of extremely large capture files into two files.
Logging Utilities	Provides logging of counter, expert, and alarm information.
Export Utilities	Provides various means to export OPV-PE data to different formats.

Name Table Utility

A name table provides associations between easy-to-remember symbolic names (`Mickey`) and hard-to-remember network addresses (`0x78AB00004235`).

OPV-PE and Fluke Networks analyzer devices learn names automatically by viewing the network portion of DNS, SAP, and NetBIOS packets. A default name table is supplied by OPV-PE containing well-known name-to-address associations. You can change the default name table. A conversion utility (**NIS-to-Name-Table** utility) is available to convert existing name tables into the name table format used by OPV-PE.

Figure 13-1 on page 13-3 shows the Name Table dialog box. The name table contains three columns: Protocol, Name, Address. The 1st column contains the name of the Protocol that the address is associated with. The 2nd contains a name in the form of a character string that represents the address. The 3rd column contains the numeric address. Names can be associated with MAC, IP, IPX, or SNA addresses in a name table.

Name table data is presented as a table which can be sorted by clicking the column headers. Click and drag on column dividers to size columns.

The **Name Table** dialog box initially displays the default name table. You can manually add, modify, or delete name table entries. You can also change the active name table so that OPV-PE will use a different name table file. You can create many name tables, but only one table is active at a time.

You can also let OPV-PE learn names and addresses automatically from the network for MAC, IP, IPX, or SNA protocols. You can have OPV-PE record all new addresses in the name table, or only those that have a corresponding symbolic name. OPV-PE can capture name-address associations in real-time monitoring mode as well as capture mode. New names are added to the name table in monitor mode as they are discovered in the data stream. You must save any changes to the currently active name table in a name table file or changes will be lost when you exit OPV-PE.
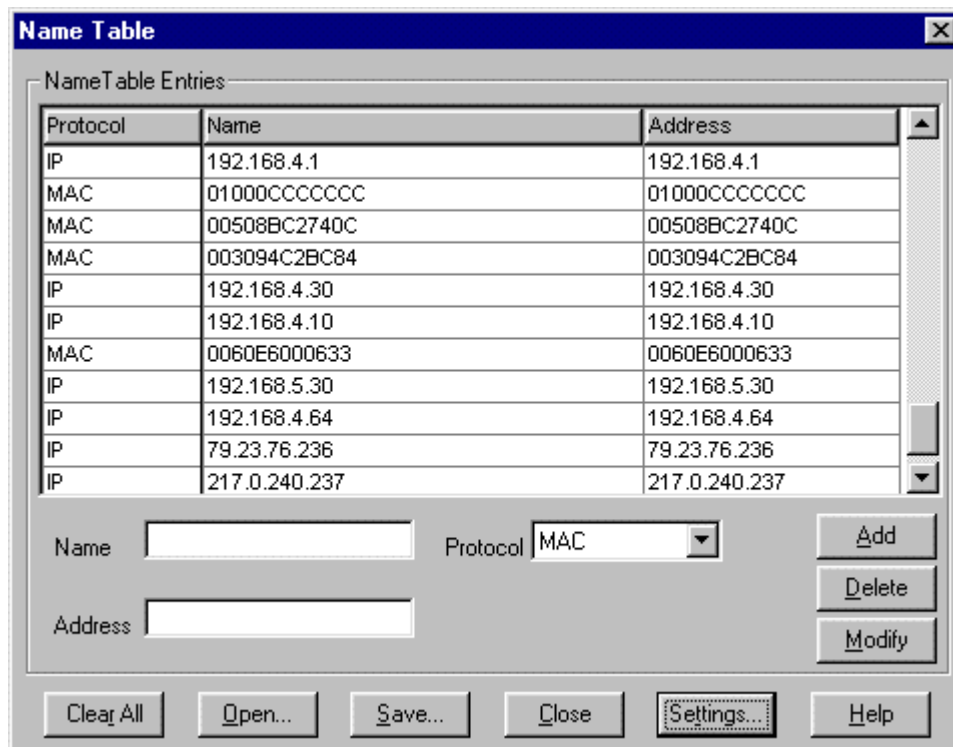
Figure 13-1. Example Name Table Dialog Box

There are several options you can set for the display and recording of name table entries. Options are set by pressing the **Settings…** button to bring up the **Name Table Settings** dialog box

To learn all addresses, select the **Learn Addresses** check box in the **Name Table Settings** dialog box. OPV-PE will enter all new addresses. If no symbolic name is associated with an address, the address is repeated in the name column for that entry in the name table.

To learn only addresses that have corresponding symbolic names, make sure the **Learn Names** check box is selected and the **Learn Address** check box is NOT selected in the **Name Table Settings** dialog box. OPV-PE will only add an item to the name table when it discovers a character string associated with an address from a DNS, SAP, or NetBIOS packet.

You can display the ASCII characters for well-known vendor names in the MAC address. Check **Display Vendor Names** in the **Name Table Settings** dialog box to display vendor names. Vendor names will be displayed in the monitoring and capture views as well as in the name table.

13-3

Name tables are limited to 5,000 entries. The **Maximum Number of Entries** field in the **Name Table Settings** dialog box must be at least 100 and no more than 5,000.

For remote resources, OPV-PE uses names learned from remote as well as local resources when displaying capture or monitor views. A local copy of the remote name table is updated at a specified time interval. The time interval for refreshing the remote name table is set in the **Configuration** menu of OPV-PE. If there are duplicate names between remote and local resources, local names take precedence and the name table will display the local name only.

The active name table can be loaded from a file. Loading the name table from a file will overwrite all existing entries in memory. Keep this in mind when using the network to learn names; until names are saved to a file, they can be lost if you exit OPV-PE or overwrite the name table contents.

Entries in the currently active name table appear in a **Name Table** area that is within the dialog boxes for appropriate filter statements. The **Name Table** window shows all name and address associations, including the protocol and the frame type. Before starting to write a capture or display filter, make sure the name table you want is the currently active name table (loaded into memory). This ensures that the proper symbolic names are available.

To use the same name table information for all systems running OPV-PE, you can set up a common default name table. All OPV-PE users can configure the path and name of the default name table, which can be the same file stored on a server. See "Providing a Name Table to OPV-PE" in Chapter 3 for more information.

Building a Name Table From the Network

The following provides a general outline of how to build a name table for the names in your network.

1. Run OPV-PE in monitor mode. Do not use any filters. The **Learn Names** check box must be selected in the **Name Table Settings** dialog box; if you also select the **Learn Address** option, OPV-PE places any addresses it sees on the network into the name table as they are discovered in the data stream.

2. If you have names you want to associate with addresses learned from the network, edit the name table using the **Name Table** dialog box. This step can also be performed after the name table is saved.

3. Save the name table to a file. You must save the name table before you exit OPV-PE or new name table data will be lost. If you save the name table data to the default name table, `hosts.nam`, the new name table data will be loaded automatically whenever you restart OPV-PE. If you save the name table to a new file, use the `.nam` file extension for easy reference.

NIS-to-Name Table Conversion Utility

The NIS2NAM.SH utility converts an NIS name table on a UNIX system to the name table format used by OPV-PE. It provides a method of creating a OPV-PE name table with addresses and associated symbolic names without having to re-enter information.

NIS2NAM.SH is installed in the ...\scripts directory. It is a UNIX shell script, designed to run under a Bourne shell. To use the conversion utility, copy the NIS2NAM.SH file to a UNIX system as a text file. The UNIX system must have NIS running for the utility to produce the new name table for use with OPV-PE.

To execute the command on the UNIX system, type:

NIS2NAM <output-name-table>

<output-name-table> is the name you select for the new OPV-PE name table. The UNIX system is searched for the NIS name table. If no NIS name table exists, the utility returns an error message. Once the new name table is created, copy it as a text file to the directory where OPV-PE is installed on your Windows system.

Note

The name table automatically loaded by OPV-PE is hosts.nam. If you use another name for your converted name table, you will need to load the name table before performing other OPV-PE functions.

The default name table loaded by OPV-PE may be changed. Change the Name Table= parameter in the OPV-PE.ini file to set a new default name table file.

Sniffer™ Translator Utility

Translators convert captured data back and forth between OPV-PE capture file format (.cap files) and Sniffer uncompressed trace format (.enc or .trc files). Capture files are stored in 'Snoop' format, compliant with RFC 1761. Capture files include extensions that provide additional information fields not found in RFC 1761. Start a translator by selecting one of the following options from the **Tools** menu.

Table 13-2. Sniffer Translator Utility, Tool Menu Options

Tool Menu Option	Description
Snoop to Sniffer™	Converts OPV-PE capture files to uncompressed trace files that can be viewed with the Sniffer.
Sniffer™ to Snoop	Converts uncompressed trace files (.enc or .trc format) to OPV-PE capture files.

Get Version Information Utility

From Summary View, click on the **Description** tab for a resource. The following information displays:

- Base address for the module

- Revision level

- Module type

- Serial number for the module board

- Capture memory size

- Error counters supported

Module Identification Utility

You may want to verify that the correct PMM or GMM is connected to the correct network or network segment. If you have multiple modules in a system, you can identify which is which. An LED next to the interface connections for the board will blink for the selected module.

1. From the Summary View, make sure that the resource you want to check is the currently active resource.

2. From the **Module** menu, choose **Identify**.

3. Look at the back of the system where modules are connected to the network. The LED for the selected module will blink.

Split Capture Files

The split capture files utility allows you to split capture files. The utility creates two capture files of approximately equal size from a single capture file. Splitting capture files is advantageous if your system resources are limited and you have a very large capture file. You may not be able to open large capture files if you do not have a significant amount of virtual memory. A full-duplex buffer capture using the synchronized modules in an OPV-LA creates a capture file of about 256MB. Depending on the options you have set in OPV-PE, this file could take more than a gigabit of virtual memory to open. If you have a system with 2 Gigabytes of virtual memory, you should be able to view any capture file without having to split it.

To split capture files, do the following:

1. After capture is complete and the capture buffer is saved to a file, select **Split Capture Files…** from the **Tools** menu.

2. In the dialog box, specify the name of capture file to split in the **Input Name** field.

3. The split files are given the name of input file with _part1 and _part2 appended to the name. You can change the output file names in the **Output File** fields.

You can split files that have already been split, thereby further reducing the size of the capture file.

Logging Utilities

OPV-PE creates log files of counter, expert, and alarm information. Log file size, log file name, and disabling or enabling log files can be configured in OPV-PE. To configure log files, see the "Configuring OPV-PE" chapter.

To access counter log files, see the section called "Counter Log File Overview" in the "Counters" chapter. For information on exporting counter log file information to an Excel spreadsheet, see the section called "Export Counter Log Files to Excel" in the following section.

Export Utilities

Data from OPV-PE can be exported to other formats. Use the procedures below to export packet information, counter data, graphs, and tables to other formats. Packet decodes can be exported to a text format. Tables or counter log files can be exported to CSV format. Graphics can be exported as bitmaps.

Exporting Packets

You can export packet decode information to another source. However, this cannot be done directly from the Capture View window. You must copy the data to an intermediate window.

To export packet decode information, do the following:

1. Set the Summary Pane of the Capture View window to display the protocol decode information you want to export. For example, packets numbered -0004 through 0013.

2. Select a packet within the window.

3. Press the ▣ button. A window displays containing the protocol decode data that was visible in the summary pane of the Capture View window.

4. Select the data you want from the window and press Ctrl + C.

5. Switch to the application where you want to store the packet information.

6. Press Ctrl + V.

7. Click on a OPV-PE window to return to OPV-PE.

If you select a portion of the current packet within the detail decode of the packet, the entire decode for this single packet is moved to the copy window for export.

Exporting Tables to CSV Format or Graphs to a Bitmap

You can export tables to CSV format (Excel) or charts to BMP format (bitmapped graphic). When saving a chart to a bitmap, it is recommended that the display settings for your monitor be greater than 256 colors to create an image with accurate colors.

1. Select the view you want to export. Press one of view buttons on the Data Views or the Capture View toolbar. If you already have the desired view window open, click the window to make it the currently selected view.

2. Click the Table tab to export to CSV format or click the Chart tab to export to a bitmap.

3. Choose **Export…** from the **File** menu.

4. Enter the file name in the **Save As...** dialog box. Table views will automatically be saved in CSV format and the file is given an extension of .csv. Chart views will automatically be saved in BMP format and the file is given an extension of .bmp.

5. Click the **Save** button.

Exporting to Optimal CSV Format

Optimal Performance, from Optimal Networks Inc., is a tool for planning, deploying, and troubleshooting distributed applications on large enterprise networks. OPV-PE exports data into a special .csv file format that can be easily read by the Optimal Performance product.

Perform the following steps to export data to Optimal Performance format:

1. Select Application Layer Matrix from the Monitor View or Capture View menus.

2. Select the Table tab to view the data in tabular format.

3. Choose **View Options** from the **View** menu. Using the check boxes, select six additional columns to display:

   Station Address 1
   Station Address 2
   Frames 2 --> 1
   Frames 1--> 2
   Bytes 1 --> 2
   Bytes 2 --> 1

4. Choose **Export to Optimal Performance** from the **File** menu.

5. Enter the file name in the **Save As** dialog box. Table views will automatically be saved in Optimal CSV format and the file is given an extension of .csv.

6. Click the **Save** button.

OPV-PE logs both a start and stop time to the .csv file. The start time is the time the table/chart window is first opened and the stop time is the last time the file is exported or saved to disk.

Exporting Counter Log Files to Excel

Use these steps to view the counter data in the log files as Excel™ 5.0 graphics. The Excel template, charts.xlt, is located in the ...\examples directory.

1. Start Excel 5.0 and open charts.xlt. You should see an empty worksheet called "Data Sheet". Worksheets are named using tabs at the bottom of the Excel rows and columns.

2. Open the log file. Remember to set the **Files of Type** field in the **Open** dialog box, to .csv or to All Files (*.*) so you can see the log file.

3. Select the entire worksheet. Move the mouse to the small button at the top left corner of the worksheet. Click the button to highlight everything on the worksheet.

4. Use **Copy** from the **Edit** menu or Ctrl + C to copy the contents of the worksheet into the Windows clipboard.

5. Switch to the previously opened **Charts** window. To change windows, pull down the Windows menu and click on **Charts**.

6. Click cell **A1** of **Data Sheet** in the **Charts** window, the cell in the top-left corner of the worksheet.

7. Use **Paste** from the **Edit** menu or Ctrl + V to paste the data into the worksheet named **Data Sheet**.

8. Select one of the names on the bottom tabs to see a graph. Twelve graphs and one spreadsheet showing computed data are available. Select a graph by clicking on one of the tabs at the bottom of the spreadsheet.

The rows of counter data displayed in a graph are the most current rows. For example, when displaying 500 rows of counter information, only the 500 most recently captured sets of counter information are used in the graph. Three types of graphs are available, each with four different row counts.

•   Network Utilization (500, 1,000, 2,000, or 4,000 rows)

•   Bytes (500, 1,000, 2,000, or 4,000 rows)

•   Packets (500, 1,000, 2,000, or 4,000 rows)

•   Refer to Excel documentation for more information on using templates in Microsoft Excel.

Appendix A
Implementation Profile

Buffers

Two types of buffers are essential to the execution of OPV-PE's features:

Table A-1. Buffer Types Used By OPV-PE

Buffer Type	Description
Real-Time Buffer	A real-time buffer provides the transient data storage area for on-the-fly frame analysis which, in conjunction with MAC statistics and error counters, produces real-time LAN analysis and monitoring information. Data captured from the network is copied to this area after filtering. The data is immediately available for evaluation, and for streaming copy to disk, after which it is discarded from the buffer. This buffer is not present for the GMM card.
Capture/Transmit Buffer	A separate capture buffer provides a durable data store of LAN traffic filtered and captured in real-time, which is kept for later analysis or to be saved to disk. The same buffer is used as storage for packets to be transmitted when performing LAN component testing. The capture buffer is a "wrap-around" buffer; once filled, it begins filling again from the beginning and older data is lost unless saved to disk.
	OPV-PE supports IMM, GMM, PMM, and NDIS (Ethernet or Token Ring) LAN interfaces. Buffering is Implemented with these interfaces as described in Table A-2. Cumulative system resource demands can limit performance of any features which require system resources, as noted.

How Resources Use Buffers

Table A-2 describes how the primary device types use capture and real-time buffers:

Table A-2. Resources Using Capture and Real-Time Buffers

Resource	Capture and Real-Time Buffer Usage
IMM	IMM is a high speed network analyzer card with a single on-board buffer. IMM supports full line-speed capture for RJ45 10/100 Mbps Ethernet or fiber optic Gigabit Ethernet. Filtering and all other OPV-PE features are supported on IMM modules. The entire IMM buffer can be allocated for capture, monitor, or transmit functions. There is little demand for system resources, regardless of the number of cards being controlled. Real-time functions introduce some system resource dependency: the need to copy periodic real-time monitor, analysis, and/or protocol decode updates to OPV-PE, and optionally to copy the real-time buffer to disk.
PMM	This is a high speed network analyzer card with on-board capture/transmit buffer and filtering. This, along with other hardware features, guarantees full line-speed capture and transmit for 10/100 Mbps Ethernets. Due to this on-board implementation, there is no demand for system resources, regardless of the number of cards being controlled. PMMs include on-board real-time buffer and data slicing capabilities to provide full real-time functionality. Simultaneous data copies to the capture and real-time buffers are an option. Real-time functions introduce some system resource dependency: the need to copy periodic real-time monitor, analysis, and/or protocol decode updates to OPV-PE, and optionally to copy the real-time buffer to disk. Using real-time functions on multiple PMMs will increase resource demands, but much less than when using multiple NDIS cards. All OPV-PE features are supported on PMMs.
GMM	This is a high speed network analyzer card with on-board capture/transmit buffer and filtering for fiber-optic networks. This, along with other hardware features, guarantees full line-speed capture and transmit for Gigabit Ethernets. Due to this on-board implementation, there is no demand for system resources, regardless of the number of cards being controlled. However, because GMM does not include a real-time buffer, the real-time functionality it provides is limited to network statistics and MAC error counters.

Table A-2. Resources Using Capture and Real-Time Buffers

NDIS	OPV-PE NDIS supports up to four Ethernet adapters. The first Ethernet adapter found during system initialization is seen by OPV-PE software as module #1, the second as module #2, and so on.
	When OPV-PE uses Ethernet adapter cards, both buffers are implemented in software, thus requiring system resources. To the extent that a system can keep up with traffic captured by an NDIS card, all LAN traffic will be copied to OPV-PE and filtered, sliced if necessary, then routed to the capture buffer, real-time buffer, or both if desired. System resource demands increase with the complexity of analysis and monitoring configured, and very much by the number of NDIS interfaces OPV-PE is controlling. All OPV-PE real-time functions will be available, excluding any MAC error counters which are not implemented on the card.
Fast Ethernet Traffic Analyzer	Fast Ethernet Traffic Analyzer is a multi-port RMON probe that gathers statistics. Data for all probe ports in the Fast Ethernet Traffic Analyzer (version 1.1 and higher) device can be seen from OPV-PE. Fast Ethernet Traffic Analyzer can gather monitoring statistics at line rate and stores them in its local hardware.
	For Fast Ethernet Traffic Analyzer, OPV-PE merely looks at the statistics passed from the probe; there is no use of a real-time or a capture buffer. Only those OPV-PE real-time functions that can make use of the RMON statistics are available.

Hardware Dependencies

The tables that follow in this section list functions supported by OPV-PE that have hardware dependencies.

Table A-3. Hardware Real-Time Functions

Real-Time Monitoring Functions	NDIS	PMM	GMM	IMM
Buffer Size	64KB	512KB	N/A	128MB
Network Statistics	All but error rate	All	Utilization, error/sec, packets/sec, bytes/sec	All
Packet Decode Summary	Yes	Yes	N/A	Yes
Alarm Thresholds	All except errors not passed by NDIS	All	Utilization, errors, packets, bytes, and MAC error counters	All
Sync View, Full-Duplex	No	Yes	Yes	Yes
Packet Slicing	Yes	Yes	N/A	Yes
Monitor Filter	Yes	Yes	N/A	Yes

Table A-4. Hardware Capture Functions

Capture Functions	NDIS Card	PMM	GMM	IMM
Capture Buffer Size	64KB-16MB*	16MB, 32MB	64MB	128MB
Performance	10Mbps: 5-10Mbps 100Mbps: 5-15Mbps	Full Line Rate, 10/100 Mbps	Full Line Rate, 1000 Mbps	Full Line Rate, 10/100/1000 Mbps
7-Layer Decode	Yes	Yes	Yes	Yes
Sync View, Full-Duplex	No	Yes	Yes	Yes
Filter	Yes	Yes	Yes	Yes
Error Frame Capture	No	Yes	Yes	Yes
Post Capture Views	Yes	Yes	Yes	Yes
Frame Error Counter	depends on adapter	Yes	Yes	Yes
Packet Slicing	Yes	Yes	Yes	Yes

*Limited by available PC system memory. Smaller when running Windows NT.

Table A-5. Hardware Connectivity

Connectivity	NDIS Card	PMM	GMM	IMM
Media	10/100 Ethernet, 4/16 TR	10/100 Ethernet RJ45 for Copper or MII for Fiber	Gigabit Ethernet Fiber only Swapple G-BIC, Single mode or Multi-mode Fiber	10/100 Ethernet RJ45 for Copper or Gigabit Ethernet for Fiber Swappable G-BIC, Single mode or Multi-mode Fiber
Max Interfaces/ System	4	15	15	15
On-Board Transceivers	No	No	Yes	Yes
Portability	Laptop	DPI-1XX	GPI-1XX	OPV-LA
Remote Management	Yes	Yes	Yes	Yes

Table A-6. Hardware Transmit Functions

Transmit Functions	NDIS	PMM	GMM	IMM
Transmit Buffer	64K-16M*	16MB or 32MB	64MB	128MB
Intelligent Frame Edit	Yes	Yes	Yes	Yes
Transmit Frame Size	64 -1518 (valid sizes only)	8 - 15,000 Bytes	16 - 15,000 Bytes	16 - 15,000 Bytes
Transmit Captured Files & User-Generated Frames	Yes	Yes	Yes	Yes
Transmit Error Frames	No	Yes	Yes	Yes
Simultaneous Transmit and Receive	No	Yes	Yes	Yes

About NDIS Mode

OPV-PE in NDIS mode uses an NDIS driver and interfaces to a variety of network adapters. All basic capture, transmit, and monitor functions are the same in NDIS mode. However, it is not recommended that an NDIS module be used to transmit packets; the transmit rate is likely to fall below the specified transmission rate and transmission of error packets is not supported.

The unique capabilities in the software interface due to using an NDIS driver are described below:

Captured Packets

Since the NDIS interface filters out frames with errors, only "good" Ethernet frames are captured. In addition, OPV-PE in NDIS mode captures both frames received by the Ethernet adapter as well as frames transmitted by the Ethernet adapter.

Capture Rate / Transmit Speed

Capture/transmit rates depend on the network adapter and the CPU. Typically, the rate will fall below the full line-rate of the network.

Counters

The error counters supported through the NDIS interface are those counters supported by the network adapter. Some vendors do not support any error counters. Only supported error counters are incremented and shown within data views.

Rx Counter Display

Counters not supported by the NDIS module will display with an "N/A" next to the counter.

Transmit Specification

Transmission of error packets is not supported.

The minimum and maximum values for the **Packet Size** field are 64 and 1518 bytes. The radio button for setting the packet gap in microseconds is grayed. Packet gaps in microseconds are not supported.

Entering a zero in the **Packet Gap** field forces the shortest gap possible.

NDIS Configuration Options

Setting the Interface

The **Interface** and **Interface Mode** options are grayed on the **Module** menu when an NDIS module is the currently selected module. The **Identify** option on the **Module** menu is grayed and does not function when the current module is an NDIS module.

Set Capture Buffer and Packet Slicing Size

The capture buffer memory size can be set in increments that double from 64K to 16MB. To set the buffer size, select the **Buffer Size** tab from the **Configuration -> Module Settings** menu and click the radio button corresponding to the buffer size. Since the buffer uses virtual memory, the system is not required to have more physical memory than the buffer size (e.g., you can set the buffer size to 16MB on a machine with 8MB of memory).

Pre-Defined Filter Templates

Filter Templates

All filter templates supplied with OPV-PE are described below. Templates are defined by an offset(s) and a value(s). These templates can be used in a capture or display filter to capture or display common protocol packets.

An OR in the Offset column indicates that the associated value will cause the frame to be captured/displayed if the value is found in either offset. An OR in the Value column indicates that any of the ORed values found in the associated offset will cause the frame to be captured/displayed. HEX indicates hexadecimal format and DEC indicates decimal format in the Value column.

Filter values are interpreted on byte boundaries. Therefore, port numbers expressed in decimal are shown in the table in "dot" notation. For example, port 1719 (H.323_GD) is shown as "6.183" in decimal; the "6" displays in offset 34 and "183" displays in offset 35. For more information on converting decimal numbers to byte values, see "Entering Values that Cross Byte Boundaries" on page 7-10.

For devices other than IMM, the **No. of Filters Used** column indicates the number of hardware filters used by the template. Each device has maximum number of filters and this value can be useful in making sure you do not exceed this value.

Table B-1. OPV-PE Filter Templates, Ethernet EV2

Filter Template	Description	Offset	Value	No. of Filters Used
AppleTalk	Collect all AppleTalk packet types embedded in Ethernet Version II frames.	12	HEX 809B	1
ARP	Collect all ARP packet types embedded in Ethernet Version II frames.	12	HEX 0806	1
DECNET Phase IV	Collect all DECNET packet types embedded in Ethernet Version II frames.	12	HEX 6003	1
MAC_Destination _Address	Template for setting a destination address. Filters for addresses at the MAC level.	0	Brings up a dialog box for entering the 12-character address.	1
MAC_DA_BROADCAST	Collect all broadcast frames.	0	HEX FFFFFFFFFFFF	1
MAC_DA_MULTICAST	Collect all multicast frames.	0	HEX 01005E	1
MAC_Source_Address	Template for setting a source address.	6	Brings up a dialog box for entering the 12-character address.	1
Packet_Type	Template for setting the packet type.	12	Brings up a dialog box for entering the 4-character address.	1
Packet_Type_ Novell8023	Filter template for collecting Novell 802.3 packet types.	12	Brings up a dialog box for entering the 8-character address.	1
VLAN	Template for collecting VLAN packet types.	12	HEX 8100	1

Table B-2. OPV-PE Filter Templates, IP and IPX over Ethernet EV2

Filter Template	Description	Offset	Value	No. of Filters Used
EIGRP	Collect all frames where EIGRP is embedded in Ethernet II frames.	12 23	HEX 0800 DEC 88	1
ICMP	Filter template for collecting all PING activity.	12 23	HEX 0800 HEX 01	1
IGMP	Filter template for collecting all IGMP activity.	12 23	HEX 0800 DEC 2	1
IP	Filter template for collecting IP packet types embedded in Ethernet Version II frames.	12	HEX 0800	1
IP_Destination_Address	Template for setting the IP destination address when IP is embedded in Ethernet Version II frames.	12 30	Brings up a dialog box for entering the IP address.	1
IP_Source_Address	Template for setting the IP source address when IP is embedded in Ethernet Version II frames.	12 26	Brings up a dialog box for entering the IP address.	1
IPX	Collect all IPX packet types embedded in Ethernet Version II frames.	12	HEX 8137	1
NetBIOS	Collect all frames with a NetBIOS port in IPX packet types embedded in Ethernet II frames.	12 30 OR 42	HEX 8137 HEX 0455 HEX 0455	2
OSPF	Collect all frames where OSFP is embedded in Ethernet II frames.	12 23	HEX 0800 DEC 89	1

Table B-2. OPV-PE Filter Templates, IP and IPX over Ethernet EV2 (continued)

Filter Template	Description	Offset	Value	No. of Filters Used
RIP (IPX)	Collect all frames with a RIP port in IPX packet types embedded in Ethernet II frames.	12 30 OR 42	HEX 8137 HEX 0453 HEX 0453	2
RSVP	Collect all frames where RSVP is embedded in Ethernet II frames.	12 23	HEX 0800 DEC 46	1
SAP (IPX)	Collect all frames with a SAP port in IPX packet types embedded in Ethernet II frames.	12 30 OR 42	HEX 8137 HEX 0452 HEX 0452	2

Table B-3. OPV-PE Filter Templates, TCP/IP over Ethernet EV2

Filter Template	Description	Offset	Value	No. of Filters Used
DNS (TCP)	Collect all frames with a DNS port when TCP is embedded in an Ethernet II frame.	12 23 34 OR 36	HEX 0800 HEX 06 DEC 0.53 DEC 0.53	2
FTP	Collect all frames with an FTP port when TCP is embedded in an Ethernet II frame.	12 23 34 OR 36	HEX 0800 HEX 06 DEC 0.21 DEC 0.21	2
HTTP	Collect all frames with a HTTP port when TCP is embedded in Ethernet II frames.	12 23 34 OR 36	HEX 0800 HEX 06 DEC 0.80 DEC 0.80	2
IMAP	Collect all frames with an IMAP port when TCP is embedded in an Ethernet II frame.	12 23 34 OR 36	HEX 0800 HEX 06 DEC 0.143 DEC 0.143	2
LDAP	Collect all frames with an LDAP port when TCP is embedded in Ethernet II frames.	12 23 34 OR 36	HEX 0800 HEX 06 DEC 1.133 (389) DEC 1.133 (389)	2
MGCP (TCP)	Collect all frames with a MGCP port when TCP is embedded in Ethernet II frames.	12 23 34 OR 36	HEX 0800 HEX 06 DEC 9.123 (2427) DEC 9.123 (2427)	2
NB-SESSION	Collect all frames with an NB-SESSION port when TCP is embedded in Ethernet II frames.	12 23 34 OR 36	HEX 0800 HEX 06 DEC 0.139 (008B) DEC 0.139 (008B)	2
NNTP	Collect all frames with an NNTP port when TCP is embedded in Ethernet II frames.	12 23 34 OR 36	HEX 0800 HEX 06 DEC 0.119 DEC 0.119	2
POP	Collect all frames with a POP port when TCP is embedded in Ethernet II frames.	12 23 34 OR 36	HEX 0800 HEX 06 DEC 0.110 DEC 0.110	2

Table B-3. OPV-PE Filter Templates, TCP/IP over Ethernet EV2 (continued)

Filter Template	Description	Offset	Value	No. of Filters Used
Q.931	Collect all frames with a Q.931 port when TCP is embedded in Ethernet II frames.	12 23 34 OR 36	HEX 0800 HEX 06 DEC 6.184 (1720) DEC 6.184 (1720)	2
SCCP	Collect all frames with an SCCP port when TCP is embedded in an Ethernet II frame.	12 23 34 OR 36	HEX 0800 HEX 06 HEX 07D0 HEX 07D0	2
SMTP	Collect all frames with an SMTP port when TCP is embedded in an Ethernet II frame.	12 23 34 OR 36	HEX 0800 HEX 06 DEC 0.25 DEC 0.25	2
T.120	Collect all frames with a T.120 port when TCP is embedded in Ethernet II frames.	12 23 34 OR 36	HEX 0800 HEX 06 DEC 5.223 (1503) DEC 5.223 (1503)	2
TCP	Collect all frames where TCP is embedded in Ethernet II frames.	12 23	HEX 0800 HEX 06	1
TELNET	Collect all frames with a TELNET port when TCP is embedded in Ethernet II frames.	12 23 34 OR 36	HEX 0800 HEX 06 DEC 0.23 DEC 0.23	2
XWIN	Collect all frames with a XWIN port when TCP is embedded in Ethernet II frames.	12 23 34 OR 36	HEX 0800 HEX 06 DEC 23.112 (6000) DEC 23.112 (6000)	2

Table B-4. OPV-PE Filter Templates, UDP/IP over Ethernet EV2

Filter Template	Description	Offset	Value	No. of Filters Used
DHCP	Collect all frames with a DHCP port when UDP is embedded in an Ethernet II frame.	12 23 34 OR 34	HEX 0800 HEX 11 HEX00440043 HEX00430044	2
DNS (UDP)	Collect all frames with a DNS port when UDP is embedded in an Ethernet II frame.	12 23 34 OR 36	HEX 0800 HEX 11 DEC 0.53 DEC 0.53	2
H.323-GD	Collect all frames with an H.323_GD port when UDP is embedded in Ethernet II frames.	12 23 34 OR 36	HEX 0800 HEX 11 DEC 6.182 (1718) DEC 6.182 (1718)	2
H.323-RAS	Collect all frames with an H.323_RAS port when UDP is embedded in Ethernet II frames.	12 23 34 OR 36	HEX 0800 HEX 11 DEC 6.183 (1719) DEC 6.183 (1719)	2
HSRP	Collect all frames with an HSRP port when UDP is embedded in Ethernet II frames.	12 23 34	HEX 0800 HEX 11 HEX 07C107C1	2
MGCP (UDP)	Collect all frames with a MGCP port when UDP is embedded in Ethernet II frames.	12 23 34 OR 36	HEX 0800 HEX 11 DEC 9.123 (2427) DEC 9.123 (2427)	2
NB-DATAGRAM	Collect all frames with an NB-DATAGRAM port when UDP is embedded in Ethernet II frames.	12 23 34 OR 36	HEX 0800 HEX 11 HEX 008A HEX 008A	2
NB-NAME	Collect all frames with an NB-NAME port when UDP is embedded in Ethernet II frames.	12 23 34 OR 36	HEX 0800 HEX 11 HEX 0089 HEX 0089	2
NFS	Collect all frames with an NFS port when UDP is embedded in Ethernet II frames.	12 23 34 OR 36	HEX 0800 HEX 11 DEC 8.1 (2049) DEC 8.1 (2049)	2

Table B-4. OPV-PE Filter Templates, UDP/IP over Ethernet EV2 (continued)

Filter Template	Description	Offset	Value	No. of Filters Used
NTP	Collect all frames with an NTP port when UDP is embedded in Ethernet II frames.	12 23 34	HEX 0800 HEX 11 HEX 007B007B	2
RIP (UDP)	Collect all frames with a RIP port when UDP is embedded in Ethernet II frames.	12 23 34 OR 36	HEX 0800 HEX 11 DEC 2.8 (520) DEC 2.8 (520)	2
RTCP	Collect all frames with an RTCP port when UDP is embedded in Ethernet II frames.	12 23 43	HEX 0800 HEX 11 DEC 200 OR DEC 201 OR DEC 202 OR DEC 203 OR DEC 204 OR DEC 205	2
SIP	Collect all frames with an SNMP port when UDP is embedded in an Ethernet II frame.	12 23 34 OR 36	HEX 0800 HEX 11 HEX 13C4 HEX 13C4	2
SNMP	Collect all frames with an SNMP port when UDP is embedded in an Ethernet II frame.	12 23 34 OR 36	HEX 0800 HEX 11 DEC 0.161 DEC 0.161	2
UDP	Collect all frames where UDP is embedded in Ethernet II frames.	12 23	HEX 0800 HEX 11	1

Table B-5. OPV-PE Filter Templates, Ethernet LLC/Novell

Filter Template	Description	Offset	Value	No. of Filters Used
DSAP	Template for setting the LLC destination address point.	14	HEX XX	1
IEEE_802.1D	Template for collecting IEEE-802.1D packets.	14	HEX 4242	2
NetBEUI	Template for collecting NetBEUI packets.	14	HEX F0F0	2
Novell	Collect Novell frames.	14	HEX E0E0	1
NMPI	Collect packets with NMPI ports embedded in Novell frames.	14 33 OR 45	HEX E0E0 HEX 0553 HEX 0553	2
RIP (LLC)	Collect packets with RIP ports embedded in Novell frames.	14 33 OR 45	HEX E0E0 HEX 0453 HEX 0453	2
SAP (LLC)	Collect packets with SAP ports embedded in Novell frames.	14 33 OR 45	HEX E0E0 HEX 0452 HEX 0452	2
SSAP	Template for setting the LLC source address.	15	HEX XX	1

Table B-6. OPV-PE Filter Templates, Ethernet SNAP

Filter Template	Description	Offset	Value	No. of Filters Used
SNAP	Collect SNAP frames.	14	HEX AAAA03	1
SNAP_AppleTalk	Filter template for collecting AppleTalk packet types embedded in Ethernet SNAP frames.	14 20	HEX AAAA03 HEX 809B	1
SNAP_ARP	Filter template for collecting ARP packet types embedded in Ethernet SNAP frames.	14 20	HEX AAAA03 HEX 0806	1
SNAP_CDP	Filter template for collecting CDP packet types embedded in Ethernet SNAP frames.	14 20	HEX AAAA03 HEX 2000	1
SNAP_IP	Filter template for collecting IP packet types embedded in Ethernet SNAP frames.	14 20	HEX AAAA03 HEX 0800	1
SNAP_IP_Destination _Address	Template for setting the IP destination address, when IP is embedded in an Ethernet SNAP frame.	14 38	Brings up a dialog box for entering the IP address.	1
SNAP_IP_Source _Address	Template for setting the IP source address, when IP is embedded in an Ethernet SNAP frame.	14 34	Brings up a dialog box for entering the IP address.	1
SNAP_IPX	Filter template for collecting IPX packet types embedded in Ethernet SNAP frames.	14 20	HEX AAAA03 HEX 8137	1

Table B-7. OPV-PE Filter Templates, Ethernet ISL

Filter Template	Description	Offset	Value	No. of Filters Used
ISL_ARP	Filter template for collecting ARP packet types embedded in ISL frames.	38	HEX 0806	1
ISL_DNS (TCP)	Collect all frames with DNS ports when TCP is embedded in ISL frames.	38 49 60 OR 62	HEX 0800 DEC 06 DEC 0.53 DEC 0.53	2
ISL_EIGRP	Collect all frames where EIGRP is embedded in ISL frames.	38 49	HEX 0800 DEC 88	1
ISL_FTP	Collect all frames with FTP ports when TCP is embedded in ISL frames.	38 49 60 OR 62	HEX 0800 DEC 06 DEC 0.21 DEC 0.21	2
ISL_HTTP	Collect all frames with HTTP ports when TCP is embedded in ISL frames.	38 49 60 OR 62	HEX 0800 DEC 06 DEC 0.80 DEC 0.80	2
ISL_ICMP	Collect all frames where ICMP is embedded in ISL frames.	38 49	HEX 0800 DEC 01	1
ISL_IGMP	Collect all frames where IGMP is embedded in ISL frames.	38 49	HEX 0800 DEC 02	1
ISL_IMAP	Collect all frames with IMAP ports when TCP is embedded in ISL frames.	38 49 60 OR 62	HEX 0800 DEC 06 DEC 0.143 DEC 0.143	2
ISL_IP	Collect IP packet types embedded in ISL frames.	38	HEX 0800	1

Table B-7. OPV-PE Filter Templates, Ethernet ISL

Filter Template	Description	Offset	Value	No. of Filters Used
ISL_LDAP	Collect all frames with LDAP ports when TCP is embedded in ISL frames.	38 49 60 OR 62	HEX 0800 DEC 06 DEC 1.133 (389) DEC 1.133 (389)	2
ISL_MAC_DA_Broadcast	Collect all broadcast frames in ISL packets.	26	HEX FFFFFFFFFFFF	1
ISL_MAC_DA_Multicast	Collect all multicast frames in ISL packets.	26	HEX 01005EFFFFFF	1
ISL_MGCP (TCP)	Collect all frames with MGCP ports when TCP is embedded in ISL frames.	38 49 60 OR 62	HEX 0800 DEC 06 DEC 9.123 (2427) DEC 9.123 (2427)	2
ISL_NB-SESSION	Collect all frames with NB-SESSION ports when TCP is embedded in ISL frames.	38 49 60 OR 62	HEX 0800 DEC 06 DEC 0.139 DEC 0.139	2
ISL_NNTP	Collect all frames with NNTP ports when TCP is embedded in ISL frames.	38 49 60 OR 62	HEX 0800 DEC 06 DEC 0.119 DEC 0.119	2
ISL_OSPF	Collect all frames where OSPF is embedded in ISL frames.	38 49	HEX 0800 DEC 89	1
ISL_POP	Collect all frames with POP ports when TCP is embedded in ISL frames.	38 49 60 OR 62	HEX 0800 DEC 06 DEC 0.110 DEC 0.110	2
ISL_Q.931	Collect all frames with Q.931 ports when TCP is embedded in ISL frames.	38 49 60 OR 62	HEX 0800 DEC 06 DEC 6.184 (1720) DEC 6.184 (1720)	2
ISL_RSVP	Collect all frames where RSVP is embedded in ISL frames.	38 49	HEX 0800 DEC 46	1

Table B-7. OPV-PE Filter Templates, Ethernet ISL

Filter Template	Description	Offset	Value	No. of Filters Used
ISL_SMTP	Collect all frames with SMTP ports when TCP is embedded in ISL frames.	38 49 60 OR 62	HEX 0800 DEC 06 DEC 0.25 DEC 0.25	2
ISL_SSP	Collect all frames with SSP ports when TCP is embedded in ISL frames.	38 49 60 OR 62	HEX 0800 DEC 06 DEC 7.208 (2000) DEC 7.208 (2000)	2
ISL_T.120	Collect all frames with DNS ports when TCP is embedded in ISL frames.	38 49 60 OR 62	HEX 0800 DEC 06 DEC 5.223 (1503) DEC 5.223 (1503)	2
ISL_TCP	Collect all where TCP is embedded in ISL frames.	38 49	HEX 0800 DEC 06	1
ISL_TELNET	Collect all frames with TELNET ports when TCP is embedded in ISL frames.	38 49 60 OR 62	HEX 0800 DEC 06 DEC 0.23 DEC 0.23	2
ISL_XWIN	Collect all frames with XWIN ports when TCP is embedded in ISL frames.	38 49 60 OR 62	HEX 0800 DEC 06 DEC 23.112 (6000) DEC 23.112 (6000)	2

Table B-8. Standard Filter Templates, Token Ring

Filter Template	Description	Offset	Value	No. of Filters Used
MAC_Active_Monitor_Present	Collect all Active Monitor Token Ring MAC frames.	1 17	HEX 05 HEX 05	1
MAC_Beacon	Collect all Beacon Token Ring MAC frames.	1 17	HEX 02 HEX 02	1
MAC_Change_Parameters	Collect all Change Parameters Token Ring MAC frames.	17	HEX 0C	1
MAC_Claim_Token	Collect all "Claim Token" Token Ring MAC frames.	1 17	HEX 03 HEX 03	1
MAC_Duplicate_Address	Collect all Duplicate Address Token Ring MAC frames.	17	HEX 07	1
MAC_Initialize_Ring_Station	Collect all Initialize Ring Station Token Ring MAC frames.	17	HEX 0D	1
MAC_Lobe_Test	Collect all Lobe Test Token Ring MAC frames.	17	HEX 08	1
MAC_Poll_Error	Collect all Poll Error Token Ring MAC frames.	17	HEX 27	1
MAC_Remove_Ring_Station	Collect all Remove Ring Station Token Ring MAC frames.	17	HEX 0B	1
MAC_Report_Error	Collect all Report Error Token Ring MAC frames.	17	HEX 29	1
MAC_Report_Monitor_Error	Collect all Report Monitor Error Token Ring MAC frames.	17	HEX 28	1

Table B-8. Standard Filter Templates, Token Ring (continued)

Filter Template	Description	Offset	Value	No. of Filters Used
MAC_Report_NAUM_Change	Collect all Report NAUM Change Token Ring MAC frames.	17	HEX 26	1
MAC_Report_New_Active_Monitor	Collect all Report New Active Monitor Token Ring MAC frames.	17	HEX 25	1
MAC_Report_Ring_Station_Address	Collect all Report Ring Station Address Token Ring MAC frames.	17	HEX 22	1
MAC_Report_Ring_Station _Attachments	Collect all Report Ring Station Attachments Token Ring MAC frames.	17	HEX 24	1
MAC_Report_Ring_Station_State	Collect all Report Ring Station State Token Ring MAC frames.	17	HEX 23	1
MAC_Report_Transmit_Forward	Collect all Report Transmit Forward Token Ring MAC frames.	17	HEX 2A	1
MAC_Request_Initialization	Collect all Request Initialization Token Ring MAC frames.	17	HEX 20	1
MAC_Request_Ring_Station_Address	Collect all Request Ring Station Address Token Ring MAC frames.	17	HEX 0E	1
MAC_Request_Ring_Station _Attachments	Collect all Request Ring Station Attachments Token Ring MAC frames.	17	HEX 10	1
MAC_Request_Ring_Station_State	Collect all Request Ring Station State Token Ring MAC frames.	17	HEX 0F	1
MAC_Response	Collect all Response Token Ring MAC frames.	17	HEX 00	1

Table B-8. Standard Filter Templates, Token Ring (continued)

Filter Template	Description	Offset	Value	No. of Filters Used
MAC_Ring_Purge	Collect all Ring Purge Token Ring MAC frames.	1 17	HEX 04 HEX 04	1
MAC_Standby_Monitor_Present	Collect all Standby Monitor Present Token Ring MAC frames.	1 17	HEX 06 HEX 06	1
MAC_Transmit_Forward	Collect all Transmit Forward Token Ring MAC frames.	17	HEX 09	1
NON_MAC	Collect all non-MAC Token Ring frames.	1	HEX 40	1

Appendix C
Keyboard Shortcuts

Function Keys

Function keys perform different operations depending on the window from which they are used. A table of the function keyboard shortcuts is provided below:

Table C-1. Shortcut Keys from Summary and Detail View

Key	Summary View	Detail View
F1	Help	Help
F2	System Settings	Capture View Display Options
F3	Module Settings	Module Settings
F4	Module Monitor View Preferences	Create Display Filter
F5	Connect to Remote	Create Capture Filter
F6	Load Capture Filter	Load Capture Filter
F7	Open Capture File	Expert Summary View
F8	Save Capture	Save Capture
F9	Go to Detail View	Capture View
F10	Start/Stop	Start/Stop

Standard and Navigational Keys

Function keys perform different operations depending on the window from which they are used. Tables of standard and navigational keyboard shortcuts are provided below:

Table C-2. Shortcut Keys from All Windows

Key(s)	Action
Alt + F4	Close Window
Ctrl + O	Open
Ctrl + S	Save

Table C-3. Shortcut Keys from Summary View

Key(s)	Action
Ctrl + T	Start Module
Ctrl + P	Stop Module
Ctrl + R	Go to Detail View

Table C-4. Shortcut Keys from Detail View

Key(s)	Action
Ctrl + T	Start Module
Ctrl + P	Stop Module

Table C-5. Shortcut Keys from the Capture View Window

Key(s)	Action
F11	Toggle Show/Hide of capture view details
Home	Select the first line
End	Select the last line
Page up	Scroll up one page
Page down	Scroll down one page
Up arrow	Select the preceding line
Down arrow	Select the next line
Right arrow	Move data in Summary pane one character to the right
Left arrow	Move data in Summary pane one character to the left

Table C-6. Shortcut Keys from the Capture Filter Window

Key(s)	Action
Ctrl + N	Bring up new default capture filter
Ctrl + P	Print capture filter
Home	Select the first statement
End	Select the last statement
Page up	Scroll up one page
Page down	Scroll down one page
Up arrow	Select the preceding statement
Down arrow	Select the next statement
Tab	Select next state
Shift + Tab	Select previous state
Plus	Expand state (Numeric pad only)
Asterisk (*)	Expand branch (Numeric pad only)
Minus (-)	Collapse branch (Numeric pad only)
Ctrl + Asterisk	Expand all branches (Numeric pad only)
Space	Bring up dialog box to edit statement
Double-click	Bring up dialog box to edit statement
Right mouse	List possible actions
Insert	Add a statement or add a state.
	If a ROOT or ELSE statement is selected, add a state.
	If an IF statement is selected, add an ELSE IF statement before the ELSE statement.
	If an ELSE IF selected, add an ELSE IF statement after the currently selected statement.
	If a state is selected, add an IF statement; if an IF statement already exists for the state, add an ELSE IF statement.
Delete	Delete statement or state.
	If an ELSE IF selected, remove the statement.
	If a state is selected, remove the entire state.
	If any other statement is selected, Delete performs no action.

Parser Names

Recognized Parser Names

The Parser Names recognized by OPV-PE are organized by protocol suite in the following tables. Parser Names must be spelled exactly as shown when used in the `ANALYSIS.INI` file. See "Advanced Configuration" in the "Customizing OPV-PE" chapter for information on using Parser Names.

Table D-1. Parser Names, DLC Suite

Parser Name	Protocol
ETHERNETV2	Ethernet Version 2
IEEE8023	IEEE 802.3 (RAW)
IEEE8022	IEEE 802.2 (LLC - Logical Link Control
IEEESNAP	IEEE Sub-Network Access Protocol
IEEE8025	IEEE 802.5 Token Ring
LOOPBACK	IEEE 802.1d
IEEE8021P	IEEE 802.1p - Generic Attribute Registration Protocol (GARP)
IEEE8021Q	IEEE 802.1q - Virtual Bridged Local Area Networks Protocol

Table D-2. Parser Names, Applications and Others

Parser Name	Protocol
CCMAIL	CC:Mail
NOTES	Lotus Notes
TDS	Sybase Tabular Data Stream
TNS	Oracle's Transparent Network Substrate Protocol
SMB	Server Message Block

Table D-3. Parser Names, Apple Talk Suite

Parser Name	Protocol Name
AARP	AppleTalk Address Resolution Protocol
ADSP	AppleTalk Data Stream Protocol
AEP	AppleTalk Echo Protocol
AFP	AppleTalk Filing Protocol
ASP	AppleTalk Session Protocol
ATP	AppleTalk Transaction Protocol
AURP	AppleTalk Update-based Routing Protocol
DDP	Datagram Delivery Protocol
LAP	Link Access Protocol
NBP	Name Binding Protocol
PAP	Printer Access Protocol
RTMP	Routing Table Maintenance Protocol
ZIP	Zone Information Protocol

Table D-4. Parser Names, Banyan Suite

Parser Name	Protocol Name
VARP	Vines Address Resolution Protocol
VFRP	Vines Fragmentation Protocol
VICP	Vines Internet Control Protocol
VIP	Vines Internet Protocol
VIPC	Vines Interprocess Communication Protocol
VNETRPC	Vines Network Remote Procedure Call
VRTP	Vines Routing Update Protocol
VSSP	Vines Sequenced Packet Protocol

Table D-5. Parser Names, Cisco Suite

Parser Name	Protocol Name
CDP	Cisco Discovery Protocol
DISL	Dynamic Inter-Switch Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol (see Internet Protocol suite)
HSRP	Hot Standby Router Protocol
IGRP	Interior Gateway Routing Protocol (see Internet Protocol suite)
iSCSI	Internet Small Computer System Interface
ISL	Inter-Switch Link Protocol
VTPADVT	VLan Trunk Protocol - Advertisement
VTPSTAT	VLan Trunk Protocol - Status

Table D-6. Parser Names, DECnet Suite

Parser Name	Protocol Name
CTERM	Network Command Terminal
DAP	Data Access Protocol
DRP	DECnet Routing Protocol
FOUND	Foundation Services
LAT	Local Area Transport
MOP	Maintenance Operation Protocol
NICE	Network Information and Command Exchange Protocol
NSP	Network Service Protocol

Table D-7. Parser Names, Fujitsu Suite

Parser Name	Protocol Name
FNA	Fujitsu network Architecture
DAP	Local Network Flow Control

Table D-8. Parser Names, IBM Suite

Parser Name	Protocol Name
3270	3270 Terminal
NETBEUI	NetBIOS Extended User Interface
SNA	Server Network Architecture
XID	XID

Table D-9. Parser Names, Internet Suite

Parser Name	Protocol Name
ARP	Address Resolution Protocol
DVMRP	Distance Vector Multicast Routing Protocol
EGP	Exterior Gateway Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
GGP	Gateway to Gateway Protocol
ICMP	Internet Control Message Protocol
iFCP	Internet Fibre Channel Storage Networking Protocol
IGMP	Internet Group Management Protocol
IGRP	Interior Gateway Routing Protocol
IP	Internet Protocol
MOSPF	Enhanced Interior Gateway Routing Protocol
OSPF	Open Shortest Path First
PIM	Protocol Independent Multicast
RARP	Reverse Address Resolution Protocol
RSVP	Resource Reservation Protocol
RTCP	Real Time Transport Control Protocol
RTP	Real Time Transport Protocol
SLP	Service Location Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
BGP	Boarder Gateway Protocol
BOOTP	Bootstrap Protocol

Table D-9. Parser Names, Internet Suite (continued)

Parser Name	Protocol Name
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
FTP	File Transfer Protocol
GOPHER	Gopher
HTTP	Hyper Text Transfer Protocol
HTTPS	Secure Hyper Text Transfer Protocol
IMAP	Internet Message Access Protocol
LDAP	Lightweight Directory Access Protocol
LPR	Printer
MIME	Multipurpose Internet Mail Extensions
Mobile_IP (A11)	Mobile IP Protocol
MOUNT	NFS Mount
NBNAME	NetBIOS Name Service over IP
NBDATAGRAM	NetBIOS Datagram Service over IP
NBSESSION	NetBIOS Session Service over IP
NETCP	NetScout Control Protocol
NFS	Network File Server
NIS	Network Information Services
NNTP	Network News Transfer Protocol
NTP	Network Time Protocol
POP	Post Office Protocol
PORTMAP	Port Mapper
RADIUS	Remote Authentication Dial In User Service
REXEC	Remote Program Execution
RIP	Routing Information Protocol
RLOGIN	Remote Login
RSHELL	Remote Shell
RTSP	Real-Time Streaming Protocol
SGCP	Simple Gateway Control Protocol

Table D-9. Parser Names, Internet Suite (continued)

Parser Name	Protocol Name
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol (versions 1, 2, and 3)
SNMPTRAP	Simple Network Management Protocol Trap
SUNRPC	Sun's Remote Procedure Call
TELNET	Remote Terminal Protocol
TFTP	Trivial File Transfer Protocol
TPKT	ISO Transport service over TCP
XDMCP	X Display Manager Control Protocol
XWIN	X Windows

Table D-10. Parser Names, Internet Next Generation Suite

Parser Name	Protocol Name
DNCPNG	Dynamic Host Configuration Protocol over IPng
ICMPNG	Internet Control Message Protocol over IPng
IDRPNG	Interdomain Routing Protocol over IPng
IPNG	Internet Protocol (Version 6) Next Generation
OSPFNG	Open Shortest Path First over IPng
RIPNG	Routing Information Protocol over IPng
RSVPNG	Resource Reservation Protocol over IPng

Table D-11. Parser Names, Netware Suite

Parser Name	Protocol Name
IPX	Internet Packet Exchange
IPXBURST	IPX Packet Burst Mode
IPXDIAG	IPX Diagnostic Protocol
IPXNB	NetBIOS over IPX
IPXRIP	Routing Information Protocol over IPX
IPXWAN	Wide Area Network Protocol over IPX
NBCAST	Netware Broadcast Message Protocol

Table D-11. Parser Names, Netware Suite (continued)

Parser Name	Protocol Name
NCP	Netware Core Protocol
NDS	Netware Directory Services
NLSP	Netware Link State Protocol
NMPI	Name Management Protocol
SAP	Service Advertising Protocol
SERIAL	Serialization Protocol
SPX	Sequenced Packet Exchanged
SPX2	Sequenced Packet Exchanged Version 2 (use SPX)
WDOG	Netware Watch Dog Protocol

Table D-12. Parser Names, PPP Suite

Parser Name	Protocol Name
PPPCHAP	Challenge Handshake Authentication Protocol
PPPIPCP	IP Control Protocol
PPPIPXCP	IPX Control Protocol
PPPLCP	Link Control Protocol
PPPNBFCP	NetBIOS Control Protocol
PPPoE	PPP over Ethernet

Table D-13. Parser Names, XNS Suite

Parser Name	Protocol Name
IDP	Internetwork Datagram Protocol
PEP	Packet Exchange Protocol
SSP	Sequence Packet Protocol
XECHO	XNS Echo Protocol
XERROR	XNS Error Protocol
XRIP	XNS Routing Information Protocol

Table D-14. Parser Names, H.323 Suite

Parser Name	Protocol Name
ASN.1	Abstract Syntax Notation 1
H323GD	H.323 - Gatekeeper Discovery
H.225.0	H.225.0 - Call Signaling Protocols
H245	H.245 - Control Protocol For Multimedia Communication
H4501	H.450.1 - Supplementary Services for Multimedia
Q921	Q.921 - Call Signaling Protocol
Q931	Q.931 - Call Signaling Protocol
H323RAS	H.323 - Gatekeeper Registration/Administration/Status
T120	T.120 - Data Protocols for Multimedia Conferencing
T.38	T.120 / Fax over IP

Table D-15. Parser Names, ITU Codecs

Parser Name	Protocol Name
CELLB	Sun's CellB video coding
G711	G.711 Audio Codec
G721	G.721 Audio Codec
G722	G.722 Audio Codec
G723	G.723 Speech Decoders (5.3/6.3 kbs)
G728	G.728 Coding for Speech at 16kbs using Low-Delay Code Excited Linear Prediction
G729	G.729 Coding of Speech at 8kbs using Conjugate-Structure Algebraic-Code-Excited Linear-Prediction (AS-ACELP)
H261	H261 Video Codec for Audiovisual Services at p x 64kbits
H263	G.711 Video Codec for Low Bit Rate Communication
JPEG	Video Coding for Joint Photographic Experts Group
MPEG	Moving Pictures Expert Group - Video

Table D-16. Parser Names, Cisco IP Telephony Suite

Parser Name	Protocol Name
SSP	Skinny Station Protocol
SCCP	Skinny Client Control Protocol
RUDP	Reliable UDP

Table D-17. Parser Names, Other Multimedia

Parser Name	Protocol Name
MGCP	Multimedia Gateway Control Protocol (over TCP)
RTCP	Real-Time Transport Control Protocol
RTP	Real-Time Transport Protocol
SIP	Session initiation Protocol

Table D-18. Parser Names, Intel Suite

Parser Name	Protocol Name
H.248/Megaco	H.248 / Megaco Protocol
MGCP	Multimedia Gateway Control Protocol (over TCP)
MTP2	Multicasting Transport Protocol 2
MTP3	Multicasting Transport Protocol 3
RTSP	Real-Time Stream Control Protocol
SCCP	Skinny Client Control Protocol
SIP	Session Initiation Protocol
TCAP	Transaction Capabilities Procedures

Table D-19. Parser Names, VPN Suite

Parser Name	Protocol Name
L2TP	Layer 2 Tunneling Protocol
LDP	Label Distribution Protocol
PPPOEDS	PPP over Ethernet - Discovery Stage
PPPOESS	PPP over Ethernet - Session Stage

Glossary

10/100 Ethernet Analyzer Card

10/100 Ethernet Analyzer Card is an adapter/analyzer card for 10/100 Ethernet networks in a portable PC environment.

.CAP extension

File extension for all capture files.

.CFD extension

File extension for all capture filters.

.DFD extension

File extension for all view filters.

.NAM extension

File extension for all name tables.

.TSP extension

File extension for all transmit specifications.

Abort Delimiter

A counter that records events where a reporting Ring Station encounters recoverable internal errors, forcing it to transmit an Abort Delimiter frame.

AC Error

A counter that records events where the reporting Ring Station's nearest active upstream neighbor could not set the address recognized bits or frame copied bits in the newly transmitted frame after copying the bits on the last frame received.

Actions

Events that occur as the result of testing conditions within statements in a filter.

Activated Stream

A defined packet or set of packets that is included in a transmit specification. Activated streams are loaded to a module for transmission.

Address

A character or group of characters that identifies some other data source or destination.

Alarm

A message posted to OPV-PE indicating a certain condition has occurred or a threshold has been reached.

Alarm Browser

A window used to list, select, and set alarms.

Alarm Falling Threshold

Falling threshold value to be compared to counter data. If the counter value or its delta value over time falls below the threshold, an alarm event is triggered.

Alarm Generation Type

Is this a rising, falling or "rising or falling" type of alarm. Used at the time of comparing the sampled value against a corresponding rising or falling threshold.

Alarm Interval

The interval, in seconds, over which data is sampled and compared.

Alarm Log

A list of all alarms triggered by incoming data to OPV-PE.

Alarm Rising Threshold

Rising threshold value to be compared to counter data. If the counter value or its delta value over time raises above the threshold, an alarm event is triggered.

Alarm Sample Type

The type of the alarm, Delta or Absolute. Delta alarm types measure increases or decreases over time; absolute alarm types measure only the absolute value of a counter.

Alarm Setting

A set of conditions that when satisfied will cause OPV-PE to record an entry in the alarm log.

Alarm Severity

Type of notification to be posted to the Message window upon alarm trigger. Valid types are informational, warning, and serious.

Alarm Value

The Alarm variable value from the last sample period.

Analysis Table

Table in OPV-PE's Expert system that lists all expert symptoms discovered over time.

Application Response Time

The time required to establish a session with an application protocol, measured in milliseconds. OPV-PE tracks average time, the shortest time, and the longest time required for connections to a protocol over the monitored network segment.

Base Address

The address of the Protocol Media Module or other resource within the PC system's low memory.

Burst

For transmission from OPV-PE, a flood of frames sent at the maximum speed of the network.

Burst Error

A counter that records events where the reporting Ring Station encounters signal transition or signal error on the Token Ring physical medium.

Burst Gap

For transmission from OPV-PE, a pause between a set of packets sent at the maximum network speed and another set of packets sent at the maximum network speed.

Capture

The processing of receiving frames from the network and storing them in the OPV-PE capture buffer.

Capture Buffer

The DRAM memory in Protocol Media Modules (or system memory on an NDIS host) that stores packets captured from the network. The PMM buffer size can be 4MB, 16MB, 32MB, or 64MB depending on the Protocol Media Module model in use.

Capture File

File used to store frames captured from the network. A capture file must be given a name with an extension of .cap. Captured frames are not automatically stored in a file - the contents of the capture buffer must be saved using the Save or Save As options.

Capture Filter

A set of conditions that determine the frames to be captured and how the captured frames are counted. The capture filter consists of programming-like statements that set variables and specify conditions and actions for the capture of frames.

Capture Filter Window

A window for defining capture filters.

Capture Mode

The mode in which OPV-PE receives network data and stores it in the Capture Buffer.

Capture View

A window for viewing and decoding network packets saved to a file or in the capture buffer.

Captured Frames

Frames stored within OPV-PE's capture buffer.

Collision

A counter that shows the best estimate of the total number of collisions (packets arriving at exactly the same time) on this Ethernet segment. Transmit collisions are not counted.

CRC/Align Error

A counter that shows the total number of packets received that had a length between 64 and 1518 octets, inclusive, but had either a bad FCS with an integral number of octets (FCS/CRC Error) or a bad FCS with a non-integral number of octets (Alignment Error).

CRC Errors

Cyclical Redundancy Check (CRC) errors.

DA

Destination address. MAC level station address of where a frame is sent.

Deactivated Stream

A defined packet or set of packets defined in a transmit specification but not currently active. Deactivated streams are NOT loaded to a module for transmission.

Defined Stream

In transmission mode, a sequence of bytes you specify for transmission on the network. Multiple streams can be defined for transmission.

Detail Pane

See Packet Detail Pane.

Detail View

The primary monitoring view for a single network resource. Multiple views of each resource can display in the Detail View.

Device

A single hardware device that provides data to OPV-PE.

Display Filter Window

A window for defining display filters.

DPI-1XX

A network troubleshooting and monitoring system available from Fluke Networks. Portable and rack mountable, DPI-1XX is designed for field service and network operations personnel. DPI-1XX can by accessed locally or remotely by OPV-PE software and provides tools to diagnose, troubleshoot and monitor any full or half-duplex 10/100 Ethernet network.

OPV-LA

A network troubleshooting and monitoring system available from Fluke Networks. OPV-LA is designed for field service and network operations personnel. OPV-LA can by accessed locally or remotely by OPV-PE software and provides tools to diagnose, troubleshoot, and monitor any full or half-duplex 10/100 Ethernet copper or Gigabit Ethernet fiber-optic network.

DRAM

Direct Random Access Memory.

Drop Events

A counter that shows the total number of events in which packets were dropped by the probe due to lack of resources. Note that this number is not necessarily the number of packets dropped; it is just the number of times this condition was detected.

Duplicate Network Address

An IP or IPX address that is discovered in packets that contain the same MAC address.

ELSE statement

The last statement for a level in a capture filter. If no combination of conditions in other statements for this level are met, the actions in the ELSE statement are taken.

ELSE IF statement

Statement in a capture or display filter. Always comes between an IF statement and an ELSE statement. Provides for the specification of additional conditions and actions for a state.

Expert Alarms

Messages posted to Expert Analysis indicating a certain condition has occurred or a threshold has been reached. Expert alarms are based on a set of counters related to Expert Symptoms or to other conditions that can signal a network problem.

Expert Diagnosis

Discussion of probable causes and possible solutions for Expert Symptoms detected by OPV-PE.

Expert Symptom

A network condition that may indicate a network problem. Expert symptoms are detected by OPV-PE's expert logic and logged in the Expert Analysis table.

Expert View

OPV-PE data view showing expert symptoms and expert counters for a time period.

Fragments

A counter showing the total number of packets received that were less than 64 octets and had either an FCS/CRC error or an Alignment Error.

Fast Ethernet

EEE 802.3 compliant MII (Media Independent Interface) network. Capable of speeds up to 100 Mbps.

Fast Ethernet Traffic Analyzer

A multi-port RMON/RMON2 probe.

Frame

Sequence of contiguous bits bracketed by and including beginning and ending flag sequences. A recognizable sequence of bits within a data stream.

Frame Copy

A counter that records when a reporting Ring Station copies a frame containing the Ring Station's own (duplicate) address.

Frame Rate

The speed at which frames are received/transmitted on the network.

Frequency

A counter that records events where the reporting Ring Station attempts to receive a frame containing an improper ring-clock frequency.

Frozen Window

Condition where the TCP/IP window size remains the same for all packets over a time period.

GMM (Gigabit Media Module)

The Gigabit Media Module (GMM) is a hardware analyzer card in a GPI-1XX hardware device. GMM provides data capture and transmit for fiber optic networks at one gigabit per second. The GMM card is for use with 1000BASE-SX or 1000BASE-LX networks only. The network interface for GMM is a removable G-BIC interface connector.

Good Frames

Frames that pass all alignment and CRC checks are counted as good frames.

GoTo

In the Filter window, "GoTo" shows jumps to levels within the capture filter. Selecting a level other than the current level in the action portion of a statement dialog box creates a GoTo phrase in the Filter window. The object of the GoTo phrase is always a state in the filter.

GPI-1XX

A network troubleshooting and monitoring system available from Fluke Networks. GPI-1XX is designed for field service and network operations personnel. GPI-1XX can by accessed locally or remotely by OPV-PE software and provides tools to diagnose, troubleshoot, and monitor any full or half-duplex Gigabit Ethernet fiber-optic network.

Hex Pane

Portion of the Capture View window that displays the hex values of a packet stored in a capture file or capture buffer.

Host

A computer upon which a particular program or resource is located. In the context of OPV-PE, the host is the computer upon which the OPV-PE program is running.

IF Statement

First statement for a level in a filter. Specifies conditions and actions. Use the IF statement dialog box to create a condition filter comprised of filter elements and operators specify the actions to take if the condition filter is satisfied.

IMM (Integrated Media Module)

A hardware device available from Fluke Networks that allows the capture/transmit of network data at full line rate and supports real-time monitoring functions for 10/100/1000 Ethernets. The IMM card is for use with 1000BASE-SX or other 1000Mbps interface or 10/100 copper-wire networks. The fiber-optic network interface for IMM is a removable G-BIC interface connector. The copper-wire network interface is an RJ45 connector.

Internal Error

A counter that records events where the reporting Ring Station encounters a recoverable internal error.

Jabbers

A counter that shows the total number of packets that were received that were longer than 1518 octets and had either an FCS/CRC error or an Alignment Error.

Line Error

A counter that records events where the reporting Ring Station's checksum process detects an error in a received data frame or token that the Ring Station transmitted.

Link Speed

The maximum rate at which a device can transmit/receive data on the network, typically described in bits/second.

Local Host

A networked computer that is running the program or resource being described. In the context of OPV-PE, a local host is the computer that is(1) running the OPV-PE program under discussion and (2) located on a network where at least one other computer (remote host) is also running a copy of the OPV-PE program.

Log Files

Files containing snapshots of OPV-PE counter information.

Lost Frame

A counter that records events where a reporting Ring Station generates a frame to a specific address and does not receive the returned frame.

Message Window

A window that displays all alarm, log, and error messages received by OPV-PE.

Mode of Operation

Defines the current relationship between OPV-PE and a resource. OPV-PE can transmit data from a resource (transmit), receive data from a resource (capture), view a resource (monitor), or view and receive data from a resource simultaneously (monitor + capture)

Module

A hardware device attached to the network that can be used by OPV-PE software to perform LAN analysis and monitoring functions. OPV-PE can use NDIS-compatible network interface cards and Protocol Media Modules as modules.

Module Speed

The rate at which OPV-PE will capture/transmit packets on the network. The speed is either 10 or 100 Mbps.

Module Status

Indicates whether or not the module is actively capturing/transmitting frames. "Arm" indicates that the module is capturing/transmitting.

Monitor

View activity on the network in real time.

Monitor and Capture Mode

Allows OPV-PE to view and receive data from a resource simultaneously.

Monitor Mode

Allows OPV-PE to view in real time the data coming to a resource.

Name Table

Table containing name and address associations for stations on the network. The address can be in the format of the MAC, IP, or IPX protocol.

NDIS

Network Driver Interface Specification.

Network

An interconnected group of nodes.

Network Adapter

Hardware board for connecting a station or node to an Ethernet LAN.

NIS

Name Information Service.

Oversize

A counter showing the total number of packets received that were longer than the 1518 octets and were otherwise well formed (good FCS).

Overview Table

Table in Expert Analysis's Expert system that lists all counters for expert events discovered over time.

Packet

A sequence of digits including data and control signals that is switched as a composite whole. Data, control signals, and error control information are arranged in a specific format. For OPV-PE, packet and frame are used interchangeably.

Packet Detail Pane

A portion of the Capture View window that displays the detailed breakdown of a packet that is stored in a capture file or capture buffer. Packets are broken down by protocol and field value within the protocol.

Packet Drop

A counter that shows the number of dropped packets when running in NDIS mode. This counter is always zero when using an Protocol Media Module and capturing packets at line rate.

Packet Editor

A dialog box available from Capture View for changing or creating packets.

Packet Gap

Time interval between packets. A packet gap can be specified when transmitting packets.

Packet Size

The size of a packet sent during transmission mode. Any packet size up to 15,000 bytes can be transmitted.

Packet Summary Pane

In Capture View, the top portion of the window that provides a summary view of all the captured packets.

Packet Summary View

Real-time protocol decode summary.

Packet Type

The type of packet sent in transmission mode. Packet types are IP, IPX, ARP, and AARP, or any other type specified by the user. It can also be the packet length field for 802.2 and SNAP frames.

Pause

Stop the continuous update of the data when viewing any resource.

Post Trigger Buffer Position

Percentage of the capture buffer used to store frames after the module is triggered.

Protocol

Set of rules, format, and timing governing the operation of functional units of a communications system.

PMM (Protocol Media Module)

A hardware device available from Fluke Networks that allows the capture of network data at full line rate and supports real-time monitoring functions.

Real-Time Buffer

Buffer used in Protocol Media Modules to store data received from the network. This circular buffer is continuously updated and overwritten as information is received. The Real-Time buffer supports monitoring functions.

Remote Host

A remote, networked computer that is running the particular program or resource. OPV-PE can serve as a Remote Host, but cannot access Remote Hosts unless you have the Remote Control.

Remote Server Protocol (RSP)

Remote Server Protocol is the protocol based on TCP/IP to transfer data or commands for OPV-PE between the local station and the remote host. You can encrypt packets passed back and forth between the local station and the remote host when using RSP to transfer data and commands.

Resource

Any source that provides data to OPV-PE. This can be an Protocol Media Module, an Ethernet Adapter, multiple devices synchronized to provide a single data stream, or a data file.

Resource Browser

The resource browser is a single window through which you can access all local and remote resources available in the network.

Root Statement

The first statement in all capture filters. Specifies global variables and global values.

SA Source address

MAC level station address of where a frame is coming from.

Start Sequence Number

A number assigned in the transmit specification that indicates where the transmission sequence starts. The number can be used at the receiving end to note the start of a sequence.

State

A symbolic label used as an address for a set of statements in a filter.

Stop Sequence Number

A number assigned in the transmit specification that indicates where the transmission sequence stops. The number can be used at the receiving end to note the end of a sequence.

Stream

A continuous sequence of data elements transmitted in a defined format.

Summary Pane

In Capture View, the top portion of the window that provides a summary of all the captured packets.

Summary View

The primary monitoring view for all network devices. One view of every device can display in the Summary View. This window has three docking windows; the Resource Browser window, the Alarm Browser window, the Summary View window, and the Message window.

Synchronized Resource

Multiple hardware devices logically joined to provide a single data source to OPV-PE.

Token Error

A counter that records events where the Token Ring Active Monitor does not detect a token.

Undersize

A counter showing the total number of packets received that were shorter than the 64 octets and were otherwise well formed (good FCS).

Total Tx Collision Counter

A counter showing the total number of collisions that have occurred when attempting to transmit.

Traffic

Transmitted and received frames or packets.

Traffic Rate

When transmitting from OPV-PE, a percentage of the maximum capacity of the network to carry packets.

Transmit Mode

One of the modes for using OPV-PE. In transmit mode, data streams loaded are transmitted on the network when the resource is started.

Transmit Specification

A definition of packets to be transmitted on the network by OPV-PE.

Tx Attempt Counter

A counter of the number of transmission attempts that have failed.

Tx Defer Counter

A counter that shows the number of times the transmitter had transmit data available and was ready to transmit but had to defer transmission due to sensing other traffic.

Tx Excessive Collision Counter

A counter that shows the number of times packets collided 16 times without successful transmission.

Tx Excessive Defer Counter

A counter that shows the number of times the transmitter had to defer for greater than 3,036 byte times.

Tx Late Collision Counter

A counter that shows the number of collisions that occur greater than 512 bit times after a transmission has started.

View

Any one of many displays of network data provided by OPV-PE.

Very Long Event Counter

A counter that shows the number of times the transmitter is active for greater than a maximum event length. The maximum event length is 4ms to 7ms for 10Mbps network speeds and 0.4 to 0.75ms for 100Mbps network speeds.

Voice over IP (VoIP)

Industry term for the carrying of voice traffic over the Internet Protocol. This term is sometimes used more broadly to indicate VoIP/Multi-Media communications via the H.323 or SCCP protocols.

WKP

Abbreviation for "well known port", a known port address on the network.

Zero Window

Condition where the TCP/IP window size remains zero for all packets over a time period.

Index

Symbols