

---

Sniffer Pro

# Getting Started Guide

Release 3.5

## **COPYRIGHT**

Copyright © 1999 Networks Associates Technology, Inc. All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of Networks Associates Technology, Inc., or its suppliers or affiliate companies.

## **TRADEMARK ATTRIBUTIONS**

\* *ActiveHelp, Bomb Shelter, Building a World of Trust, CipherLink, Clean-Up, Cloaking, CNX, Compass 7, CyberCop, CyberMedia, Data Security Letter, Discover, Distributed Sniffer System, Dr Solomon's, Enterprise Secure Cast, First Aid, ForceField, Gauntlet, GMT, GroupShield, HelpDesk, Hunter, ISDN Tel/Scope, LM 1, LANGuru, Leading Help Desk Technology, Magic Solutions, MagicSpy, MagicTree, Magic University, MagicWin, MagicWord, McAfee, McAfee Associates, MoneyMagic, More Power To You, Multimedia Cloaking, NetCrypto, NetOctopus, NetRoom, NetScan, Net Shield, NetShield, NetStalker, Net Tools, Network Associates, Network General, Network Uptime!, NetXRay, Nuts & Bolts, PC Medic, PCNotary, PGP, PGP (Pretty Good Privacy), PocketScope, Pop-Up, PowerTelnet, Pretty Good Privacy, PrimeSupport, RecoverKey, RecoverKey-International, ReportMagic, RingFence, Router PM, Safe & Sound, SalesMagic, SecureCast, Service Level Manager, ServiceMagic, Site Meter, Sniffer, SniffMaster, SniffNet, Stalker, Statistical Information Retrieval (SIR), SupportMagic, Switch PM, TeleSniffer, TIS, TMach, TMeg, Total Network Security, Total Network Visibility, Total Service Desk, Total Virus Defense, T-POD, Trusted Mach, Trusted Mail, Uninstaller, Virex, Virex-PC, Virus Forum, ViruScan, VirusScan, VShield, WebScan, WebShield, WebSniffer, WebStalker WebWall, and ZAC 2000* are registered trademarks of Network Associates and/or its affiliates in the US and/or other countries. All other registered and unregistered trademarks in this document are the sole property of their respective owners.

## **LICENSE AGREEMENT**

NOTICE TO ALL USERS: FOR THE SPECIFIC TERMS OF YOUR LICENSE TO USE THE SOFTWARE THAT THIS DOCUMENTATION DESCRIBES, CONSULT THE README.1ST, LICENSE.TXT, OR OTHER LICENSE DOCUMENT THAT ACCOMPANIES YOUR SOFTWARE, EITHER AS A TEXT FILE OR AS PART OF THE SOFTWARE PACKAGING. IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH THEREIN, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.

# Table of Contents

<b>Preface</b> .....	<b>vii</b>
About This Manual .....	vii
Help Topics .....	vii
Other Manuals for the Sniffer Pro .....	vii
How to Contact Network Associates .....	viii
Technical Support .....	viii
Network Associates Training .....	ix
International Contact Information .....	x
<b>Chapter 1. Introducing Sniffer Pro</b> .....	<b>1-1</b>
Major Components .....	1-2
<b>Chapter 2. Monitoring Your Network</b> .....	<b>2-1</b>
Monitor Filters .....	2-2
Monitor Applications .....	2-2
Dashboard .....	2-3
Host Table .....	2-5
Single Station Functions .....	2-6
Matrix .....	2-8
Single Station Functions .....	2-9
History Samples .....	2-11
Protocol Distribution .....	2-14
Global Statistics .....	2-16
Smart Screens (ATM Adapters) .....	2-17
Physical Layer Statistics (ATM Adapters) .....	2-19
Switch Statistics .....	2-20
Monitor Alarms .....	2-21
Exporting Monitor Data .....	2-21
Generating Reports on Monitor Data .....	2-22
Saving Monitor Data to a Database File .....	2-23
<b>Chapter 3. Capturing Packets</b> .....	<b>3-1</b>

Capture Controls .....	3-1
Capture Panel .....	3-2
Capture Buffer .....	3-3
Saving the Capture Buffer to a File .....	3-4
Capturing from Specific Stations .....	3-5
Capture Filters .....	3-6
Capture Triggers .....	3-6
Expert Options .....	3-6
Expert Layers and Objects .....	3-6
Expert Thresholds .....	3-9
Subnet Masks .....	3-10
RIP Settings .....	3-11
<b>Chapter 4. Displaying Captured Data .....</b>	<b>4-1</b>
Display Filters .....	4-2
Packet Display .....	4-3
Decode Tab .....	4-3
Navigating the Display .....	4-4
Selecting Packets .....	4-5
Setting Display Options .....	4-5
Using Protocol Forcing .....	4-9
Matrix Tab .....	4-10
Host Table Tab .....	4-12
Protocol Distribution Tab .....	4-14
Statistics Tab .....	4-16
Expert Display .....	4-17
Displaying Context-Sensitive Explain Messages .....	4-19
Rearranging the Expert Display .....	4-20
Exporting the Contents of the Expert Database .....	4-21
Automatically Exporting Expert Analyzer Data .....	4-22
<b>Chapter 5. Defining Filters and Triggers .....</b>	<b>5-1</b>
Defining Filters .....	5-1
Filtering by Address .....	5-2
Filtering by Data Pattern .....	5-3

---

Filtering by Packet Size, Protocol, and Error Type .....	5-6
Setting Capture Buffer Options .....	5-7
Filtering on ATM VPI.VCIs .....	5-8
Filtering on ATM Station Addresses .....	5-9
Filtering on Payload Type (ATM Book Only) .....	5-10
Filtering by WAN Synchronous Frame Types .....	5-11
Defining Triggers .....	5-12
<b>Chapter 6. Using the Address Book .....</b>	<b>6-1</b>
Creating an Address Book .....	6-1
Entering Names Manually .....	6-2
Importing Address Tables .....	6-2
Autodiscovering Addresses and Names .....	6-3
Configuring Autodiscovery for Routers .....	6-4
Netware 4.x Names and Addresses .....	6-4
Adding Discovered Addresses to the Address Book .....	6-5
<b>Chapter 7. Managing Alarms .....</b>	<b>7-1</b>
The Alarm Log .....	7-1
Setting Alarm Severity Levels .....	7-2
Monitor Alarms .....	7-2
Expert Alarms .....	7-4
Setting Alarm Notification Actions .....	7-5
Enabling Alarm Actions .....	7-6
Alarm Beeps and Sounds .....	7-6
<b>Chapter 8. Using Sniffer Pro Tools .....</b>	<b>8-1</b>
Ping .....	8-1
Trace Route .....	8-3
DNS Lookup .....	8-4
Finger .....	8-5
Who Is .....	8-6
Adding Tools to the Tools Menu .....	8-7
<b>Chapter 9. Using the Packet Generator .....</b>	<b>9-1</b>
Using the Standard Packet Generator .....	9-1

Transmitting a Single Packet .....	9-2
Transmitting the Capture Buffer or a File .....	9-3
Using the ATM Packet Generator .....	9-5
Transmitting a Single Packet .....	9-5
Transmitting the Capture Buffer or a File .....	9-7
Using Packet Setup Files and Buffer Setup Files .....	9-9
Using Scripts To Generate Traffic .....	9-9
Saving Script Files .....	9-10

**Chapter 10. Using the Sniffer Reporter Agent with Sniffer Pro ..... 10-1**

**Chapter 11. Network Adapters and Settings ..... 10-1**

Creating Sniffer Local Agents .....	10-2
-------------------------------------	------

**Appendix A. Network Associates**

<b>Support Services .....</b>	<b>A-1</b>
Adding Value to Your Network Associates Product .....	A-1
PrimeSupport Options for Corporate Customers .....	A-1
The PrimeSupport KnowledgeCenter Plan .....	A-1
The PrimeSupport Connect Plan .....	A-2
The PrimeSupport Connect 24-By-7 Plan .....	A-3
The PrimeSupport Enterprise Plan .....	A-4
Ordering a Corporate PrimeSupport Plan .....	A-5
PrimeSupport Options for Home Users .....	A-7
How to Reach International Home User Support .....	A-9
Ordering a PrimeSupport Plan for Home Users .....	A-9
Network Associates Consulting and Training .....	A-9
Professional Services .....	A-10
Jumpstart Services .....	A-10
Network Consulting .....	A-10
Total Education Services .....	A-11

**Index**

# Preface

## About This Manual

This manual provides a comprehensive overview of Sniffer Pro, a network visibility and troubleshooting tool for Windows 95/98 and Windows NT.

## Help Topics



*Help topic*

In this manual, references to the program's online Help system are shown in the margin, next to the help book icon.

Use the Help topic to search Sniffer Pro's online Help index and obtain further information about the feature currently being discussed.

## Other Manuals for the Sniffer Pro

*Table i* lists other manuals provided by Network Associates to describe specific Sniffer Pro features.

**Table i. Other Sniffer Pro Manuals**

Manual	Contents
<i>Switch Expert Connection and Configuration Guide</i>	Describes how to connect and configure the Sniffer Pro to use Switch Expert features.
<i>ATM Installation, Connection, and Configuration Guide</i>	Describes how to install, connect, and configure the Sniffer Pro when using ATM hardware. Describes ATM interface pods.
<i>Installing, Connecting, and Configuring WAN Hardware</i>	Describes how to install, connect, and configure the Sniffer Pro when using the LM2000 or HSSI adapter.
<i>Using the SnifferBook</i>	Describes how to install, connect, and configure the Sniffer Pro when using the SnifferBook.
<i>Using the WANBook</i>	Describes how to install, connect, and configure the Sniffer Pro when using the WANBook.



For corporate-licensed customers:

Phone	(408) 988-3832
Fax	(408) 970-9727

For retail-licensed customers:

Phone	(972) 855-7044
Fax	(408) 970-9727

To provide the answers you need quickly and efficiently, the Network Associates technical support staff needs some information about your computer and your software. Please have this information ready before you call:

- Product name and version number
- Computer brand and model
- Any additional hardware or peripherals connected to your computer
- Operating system type and version numbers
- Network type and version, if applicable
- Contents of your AUTOEXEC.BAT, CONFIG.SYS, and system LOGIN script
- Specific steps to reproduce the problem

## Network Associates Training

For information about scheduling on-site training for any Network Associates product, call (800) 338-8754.

## International Contact Information

To contact Network Associates outside the United States, use the addresses, phone numbers and fax numbers below.

### **Network Associates Australia**

Level 1, 500 Pacific Highway  
St. Leonards, NSW  
Sydney, Australia 2065  
Phone: 61-2-8425-4200  
Fax: 61-2-9439-5166

### **Network Associates Austria**

Pulvermuehlstrasse 17  
Linz, Austria  
Postal Code A-4040  
Phone: 43-732-757-244  
Fax: 43-732-757-244-20

### **Network Associates Belgique**

BDC Heyzel Esplanade, boîte 43  
1020 Bruxelles  
Belgique  
Phone: 0032-2 478.10.29  
Fax: 0032-2 478.66.21

### **Network Associates do Brasil**

Rua Geraldo Flausino Gomez 78  
Cj. - 51 Brooklin Novo - São Paulo  
SP - 04575-060 - Brasil  
Phone: (55 11) 5505 1009  
Fax: (55 11) 5505 1006

### **Network Associates Canada**

139 Main Street, Suite 201  
Unionville, Ontario  
Canada L3R 2G6  
Phone: (905) 479-4189  
Fax: (905) 479-4540

### **Network Associates People's Republic of China**

New Century Office Tower, Room 1557  
No. 6 Southern Road Capitol Gym  
Beijing  
People's Republic of China 100044  
Phone: 8610-6849-2650  
Fax: 8610-6849-2069

### **Network Associates Denmark**

Lautruphoej 1-3  
2750 Ballerup  
Danmark  
Phone: 45 70 277 277  
Fax: 45 44 209 910

### **NA Network Associates Oy**

Sinikalliontie 9, 3rd Floor  
02630 Espoo  
Finland  
Phone: 358 9 5270 70  
Fax: 358 9 5270 7100

**Network Associates  
France S.A.**

50 Rue de Londres  
75008 Paris  
France  
Phone: 33 1 44 908 737  
Fax: 33 1 45 227 554

**Network Associates Hong Kong**

19th Floor, Matheson Centre  
3 Matheson Way  
Causeway Bay  
Hong Kong 63225  
Phone: 852-2832-9525  
Fax: 852-2832-9530

**Network Associates Japan, Inc.**

Toranomon 33 Mori Bldg.  
3-8-21 Toranomom Minato-Ku  
Tokyo 105-0001 Japan  
Phone: 81 3 5408 0700  
Fax: 81 3 5408 0780

**Network Associates  
de Mexico**

Andres Bello No. 10, 4 Piso  
4th Floor  
Col. Polanco  
Mexico City, Mexico D.F. 11560  
Phone: (525) 282-9180  
Fax: (525) 282-9183

**Network Associates  
Deutschland GmbH**

Ohmstraße 1  
D-85716 Unterschleißheim  
Deutschland  
Phone: 49 (0)89/3707-0  
Fax: 49 (0)89/3707-1199

**Network Associates Srl**

Centro Direzionale Summit  
Palazzo D/1  
Via Brescia, 28  
20063 - Cernusco sul Naviglio (MI)  
Italy  
Phone: 39 02 92 65 01  
Fax: 39 02 92 14 16 44

**Network Associates Latin America**

1200 S. Pine Island Road, Suite 375  
Plantation, Florida 33324  
United States  
Phone: (954) 452-1731  
Fax: (954) 236-8031

**Network Associates  
International B.V.**

Gatwickstraat 25  
1043 GL Amsterdam  
The Netherlands  
Phone: 31 20 586 6100  
Fax: 31 20 586 6101

**Network Associates  
Portugal**

Av. da Liberdade, 114  
1269-046 Lisboa  
Portugal  
Phone: 351 1 340 4543  
Fax: 351 1 340 4575

**Network Associates  
South East Asia**

78 Shenton Way  
#29-02  
Singapore 079120  
Phone: 65-222-7555  
Fax: 65-220-7255

**Network Associates Sweden**

Datavägen 3A  
Box 596  
S-175 26 Järfälla  
Sweden  
Phone: 46 (0) 8 580 88 400  
Fax: 46 (0) 8 580 88 405

**Network Associates  
Taiwan**

Suite 6, 11F, No. 188, Sec. 5  
Nan King E. Rd.  
Taipei, Taiwan, Republic of China  
Phone: 886-2-27-474-8800  
Fax: 886-2-27-635-5864

**Net Tools Network Associates  
South Africa**

Bardev House, St. Andrews  
Meadowbrook Lane  
Epson Downs, P.O. Box 7062  
Bryanston, Johannesburg  
South Africa 2021  
Phone: 27 11 706-1629  
Fax: 27 11 706-1569

**Network Associates  
Spain**

Orense 4, 4ª Planta.  
Edificio Trieste  
28020 Madrid, Spain  
Phone: 34 9141 88 500  
Fax: 34 9155 61 404

**Network Associates AG**

Baeulerwissenstrasse 3  
8152 Glattbrugg  
Switzerland  
Phone: 0041 1 808 99 66  
Fax: 0041 1 808 99 77

**Network Associates  
International Ltd.**

Minton Place, Victoria Street  
Windsor, Berkshire  
SL4 1EG  
United Kingdom  
Phone: 44 (0)1753 827 500  
Fax: 44 (0)1753 827 520

Sniffer Pro is a powerful network visibility tool that enables you to:

- Monitor network activity in real time
- Collect detailed utilization and error statistics for individual stations, conversations, or any portion of your network
- Save historical utilization and error information for baseline analysis
- Generate visible and audible real-time alarms
- Notify network administrators when troubles are detected
- Capture network traffic for detailed packet analysis
- Probe the network with active tools to simulate traffic, measure response times, count hops, and troubleshoot problems

Sniffer Pro is designed to take full advantage of Windows 32-bit multitasking features. You can run multiple instances of the program and its individual tools, and it can run concurrently with other Windows applications. The intuitive Windows user interface makes Sniffer Pro easy to learn and simple to use.

You can use Sniffer Pro on network segments running:

- Ethernet
- Gigabit Ethernet
- Fast Ethernet (100BASE-T)
- Token Ring
- ATM
- WAN/Synchronous
  - RS/V interfaces using the LM2000 adapter.
  - HSSI interfaces using the HSSI adapter
  - RS/V, T1, E1, and ISDN (BRI and PRI) interfaces using the SnifferBook and a corresponding interface module.
  - RS/V, T1, E1, and ISDN (BRI and PRI) interfaces using the WANBook and a corresponding interface module.

# Major Components

Figure 1-1 shows the major components of Sniffer Pro.

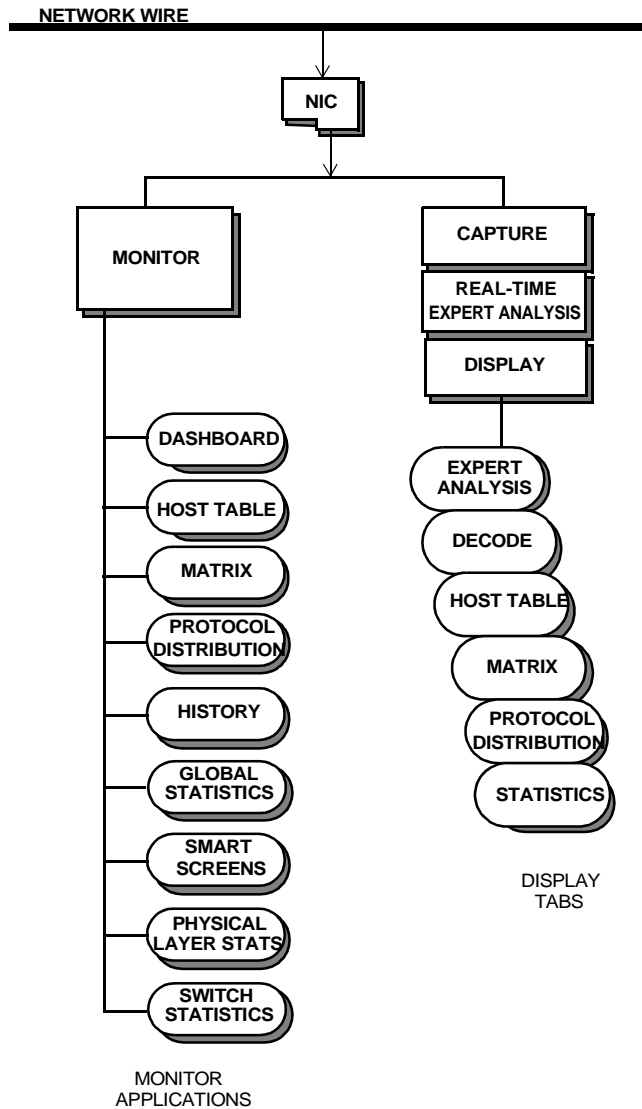


Figure 1-1. Sniffer Pro Major Components

Figure 1-1 shows the main functional blocks of Sniffer Pro: monitor, capture, real-time Expert analysis, and display.

- The *monitor* calculates and displays real-time network traffic data.
- The *capture* function captures network traffic and stores the actual packets in a buffer (and optionally to a file) for later analysis.
- The *Real-time Expert analysis* function analyzes the network packets during capture and alerts you to potential problems on your network. These problems are categorized as either symptoms and/or diagnoses.
- The *display* function decodes and analyzes the packets in the capture buffer, and displays them in a variety of formats.





*Real-Time  
Monitoring*

The Sniffer Pro *monitor* stores statistical measurements and calculations about your network traffic, providing an accurate picture of network activity in real time. It can generate alarms to notify you when errors are detected, and can save historical records of network activity that you can use later for traffic and fault analysis.

The monitor provides the following kinds of information:

- Network load statistics, including the number of frames/bytes of network traffic per time interval, the percentage of utilization, and broadcast and multicast counts.
- Network error statistics, including:
  - For Ethernet; CRC errors, runts, oversize packets, fragments, jabbers, alignment errors, and collision counts.
  - For Gigabit Ethernet; CRC errors, code violation errors, jabbers, and runts.
  - For Token Ring; Ring purge packets, beacon packets, NAUN changes, token errors, soft errors, and so on.
  - For ATM; CRC errors, length errors, and timeout errors.
- Protocol use statistics.
- Individual station and conversation-pair traffic statistics.
- Packet size distribution statistics.

---

**NOTE:** To report some of the network error statistics, you need to have a supported network interface card (NIC) and an enhanced driver. Refer to the installation guide provided with your shipment for information about installing the enhanced NDIS drivers.

---

The data collected by the monitor can help you find traffic overloads, troubleshoot bottlenecks, and locate faulty equipment. The data can also be an important factor in deciding how to allocate your company's resources for network maintenance and upgrades.

# Monitor Filters

Sniffer Pro lets you apply predefined filters to the monitor. The filter you apply to the monitor affects all the monitor applications.

Using a monitor filter, you can look at your network traffic from several different views. You can precisely focus on the data you need to troubleshoot network problems and minimize the size of files you collect for your historical records.

For a description of how to define a filter, see *Chapter 5, Defining Filters and Triggers*.

# Monitor Applications

You display monitor data by using *Monitor Applications*. The monitor applications are listed under the **Monitor** menu and are also available on the main toolbar (see *Figure 2-1*). The two ATM-specific monitor applications (Smart Screens and Switch Statistics) are available on their own individual toolbar (also shown in *Figure 2-1*), along with a **Media Options** button used to access configuration options for the ATM analyzer.

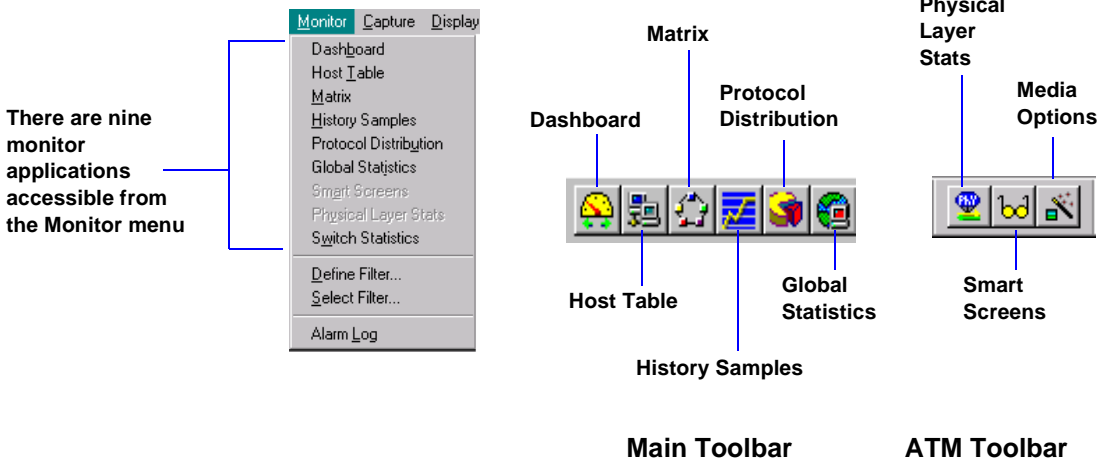


Figure 2-1. The Monitor Menu and Toolbar Buttons (Main and ATM)

## Dashboard



[Viewing the Dashboard](#)

[Monitor Applications](#)

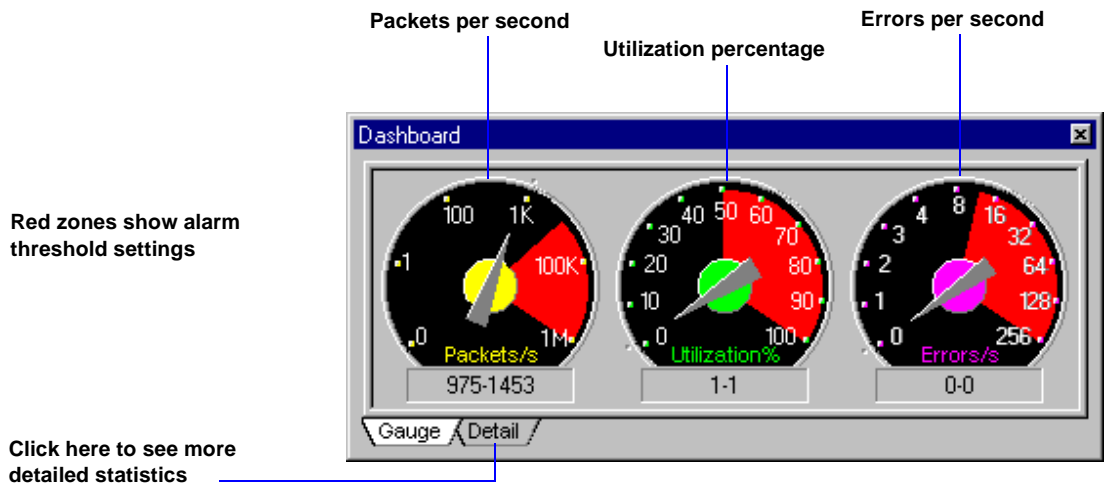
[Arranging the Dockable Windows](#)

Use the Dashboard to display a network segment's packet rate, utilization, and error rate in real time on a graphical display called the *Dashboard*.

You can use various tabs to view accumulated detail statistics or average-per-second statistics for a number of important network parameters. The exact tabs depend on the currently selected adapter:

- Ethernet (including Gigabit Ethernet) adapters provide the **Detail** tab.
- Token ring adapters provide the **LLC** and **MAC** tabs.
- WAN/Synchronous adapters provide the **WAN**, **Line Status**, **SDLC**, **U-Frame**, **LAPB**, **Frame Relay**, and **HDLC** tabs.
- When using the SnifferBook or WANBook to monitor an ISDN network, the **ISDN** tab is provided. Additionally, if using the ISDN BRI interface module to monitor the S/T interface of an ISDN link, the **S/T** tab is provided.
- ATM adapters provide the **ATM** tab. When using the ATM Book, statistics in the Dashboard are multicolored. Black statistics are those that are calculated using hardware on the ATM Book. Blue statistics are those that are calculated using software on the Sniffer Pro PC.

*Figure 2-2* shows the Dashboard for an Ethernet adapter.



**Figure 2-2.** The Dashboard Gauge View

You can set alarm thresholds for each of the dials on the Dashboard (as well as many other network statistics). When a threshold is exceeded, an entry is made in the alarm log. You can monitor the alarm log to keep watch over your network.

To set a threshold value, select **Options** from the **Tools** menu and click the **Threshold** tab. You can also access the **Threshold** tab by right-clicking the Dashboard and selecting its **Properties** page.

You will see a complete list of network parameters that can trigger a threshold alarm. The exact parameters depend on the currently selected adapter. *Figure 2-3* shows the network parameters for an Ethernet adapter.

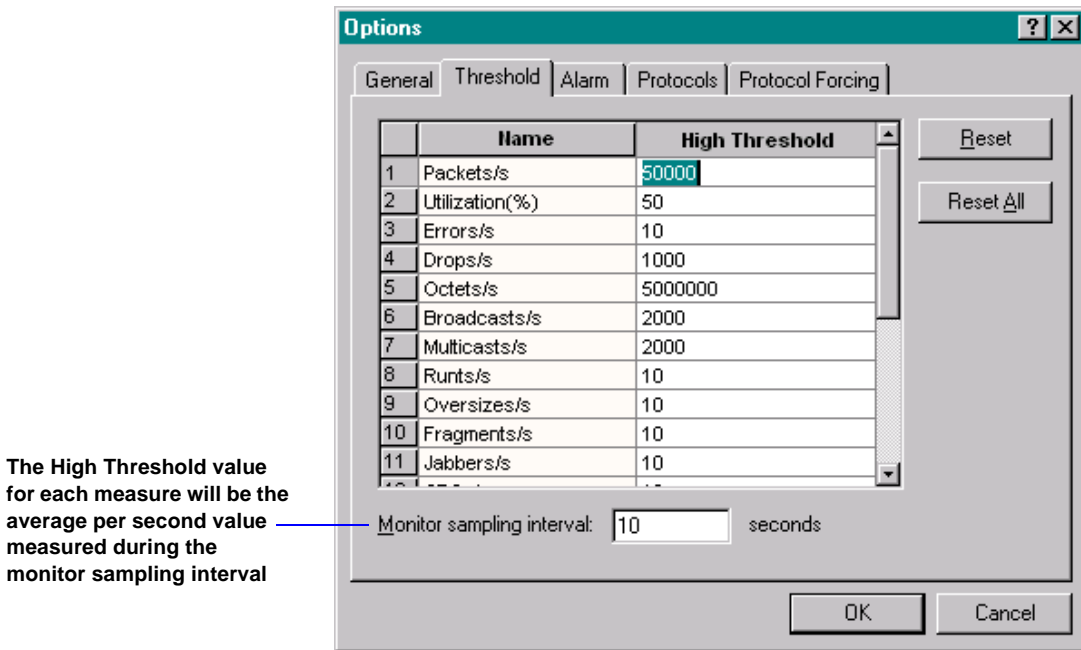


Figure 2-3. Setting Threshold Options

## Host Table

The Host Table collects each network node's traffic statistics in real time:

- For LAN adapters, the Host Table accumulates MAC, IP network, IP application, IPX network, and IPX transport-layer information.
- For ATM adapters, the Host Table also includes the ATMCNX tab, listing connections (both PVCs and SVCs) detected on the network.
- For WAN adapters, the Host Table accumulates SDLC, LCN, Virtual Circuit, or HDLC link-layer information depending on the encapsulation protocol currently selected in the **Options** menu. Transport layer information is also provided when available (particularly for Frame Relay).



### Monitor Applications

#### Host Table View - LAN Adapters

#### Host Table View - WAN Adapters

#### Displaying Top Talkers


#### Sorting the Host Table

You can view the Host Table data as a *table*, *bar chart*, or *pie chart*.

- The *table* views display traffic count statistics for each network node in real time.
  - The *outline table* provides a quick summary of total bytes and packets transmitted in and out of each network node.
  - The *detail table* provides a quick summary of the higher-layer protocol type and its traffic load transmitted in and out of each network node.


You can sort a Host Table by clicking on a column heading (for example, to sort the statistics by incoming packets, click on the **In Pkts** column heading). Click a second time to sort in reverse order.


- The *bar chart* displays the top *x* busiest host nodes in real time, where *x* is a user-configurable number. (The default is 10.)
- The *pie chart* displays the top *x* busiest host nodes as relative percentages of the total load of top *x* traffic. *x* is a user-configurable number (the default is 10).

You can configure settings (such as the update and sort interval, and the top *x* variable in the bar and pie chart) by clicking on the  button in the Host Table toolbar.

In the table views, you can export the statistics for tabulation or charting. Refer to [Exporting Monitor Data on page 2-21](#).

## Single Station Functions

To capture data to or from a single station, click on the station's icon in the outline table and then click on the  button. (For more information, see [Capturing from Specific Stations on page 3-5](#).)

To display a single station's statistics, click on the station's icon in the outline table and click on the  button. You can view a single station's statistics in a traffic map, table, bar chart, or pie chart.

[Figure 2-4](#) shows a Host Table for an Ethernet adapter and describes the Host Table toolbar.

**Host Table: 169 stations**

Hw Addr	In Pkts	Out Pkts	In Bytes	Out Bytes	Broadcast
00A024932FAA	50101	25457	5110870	1639696	12
00608CE8675D	6500	6533	678191	418884	12
Cisco F4CFD9	31859	39193	5677945	9553892	2423
Broadcast	22815	40	3941964	2560	0
00608CBC3A7D	1729	354	116178	35444	52
0020AFD3364A	3810	3731	473220	701384	239
0060972D053A	527	653	219847	101631	123
HP D6E524	1568	1620	100512	106444	52
006008BD842B	3029	3342	431846	279725	141
00A024C65EC8	7263	7005	920733	496352	224
Cisco 011688	125982	147166	67454290	17856273	1068
SynOpt111989	646866	698452	109291428	238024266	8601
Novell4C80A5	168016	172064	18995249	19707340	141
0020AF1A3208	58977	58999	6230317	3955191	62
NGC 090003	1503	10	96192	640	0
00609759D728	2430	2287	1578651	341349	39

MAC / IP / IPX

Click to display traffic by MAC, IP, or IPX

Outline table view

Detail table view

Bar chart view

Pie chart view

Capture data to or from a single station (first select a station from outline table view)

Define filter

Pause screen updates

Refresh display

Restart data collection

Export data to spreadsheet (Table views only)

Display statistics for the selected station

Properties:

- Show raw address instead of symbolic name
- Define update and sort interval
- Define sort variable and top-N

Figure 2–4. The Host Table (Outline Table View) and Toolbar

## Matrix

The Matrix collects statistics for conversations between network nodes in real time:

- For LAN and ATM adapters, the Matrix accumulates MAC, IP network, IP application, IPX network, and IPX transport-layer information.
- For WAN adapters, the Matrix accumulates SDLC, LCN, Virtual Circuit, or HDLC link-layer information depending on the encapsulation protocol currently selected in the **Options** menu. Transport layer information is also provided when available (particularly for Frame Relay).



### Monitor Applications

#### Matrix View


#### Monitoring Traffic Volume Between Nodes: Matrix

You can view Matrix data as a traffic map, as a table, or as a bar or pie chart.

- The *traffic map* provides a birds-eye view of network traffic patterns between nodes in real time.
- The *matrix tables* display traffic count statistics for node pairs:
  - The *outline table* provides a quick summary of total bytes and packets transmitted between pairs of network nodes.
  - The *detail table* provides a quick summary of the higher-layer protocol type and its traffic load transmitted in and out of each conversation node pair.


You can sort a Matrix table by clicking on a column heading (for example, to sort the statistics by packets, click on the **Packets** column heading). Click a second time to sort in reverse order.

- The *bar chart* displays the top *x* busiest conversation node pairs in real time, where *x* is a user-configurable number. (The default is 10.)
- The *pie chart* displays the top *x* busiest conversation node pairs in their relative percentage load of the total top *x* traffic. *x* is a user-configurable number (the default is 10).

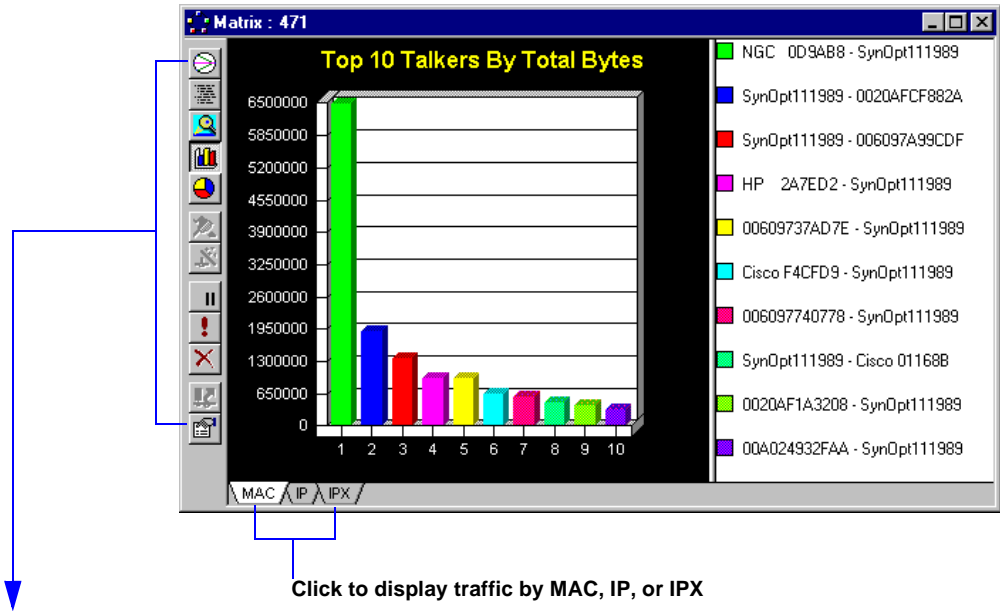
You can configure settings (such as the colors used in the traffic map, the top *x* variable in the bar and pie chart, and the update and sort interval) by clicking on the  button in the Matrix toolbar.

In the table views, you can export the statistics for tabulation or charting. Refer to [Exporting Monitor Data on page 2-21](#).

## Single Station Functions

To capture data between two specific stations, click on the icon for one of the stations in the traffic map or outline table view, then click on the  button. (For more information, see [Capturing from Specific Stations on page 3-5](#).)

[Figure 2-5](#) shows a Matrix bar chart for an Ethernet adapter and describes the Matrix toolbar.



- Traffic map view
- Detail table view
- Pie chart view
- Define a filter
- Refresh display
- Export data to spreadsheet (Table views only)
- Outline table view
- Bar chart view
- Capture data between two stations (first, select a station in the traffic map or outline table view)
- Pause screen updates
- Restart data collection
- Properties
  - Define update and sort interval
  - Select colors used in the traffic map
  - Define sort variable and top-N

Figure 2–5. The Matrix (Bar Chart View) and Toolbar

## History Samples



[Monitor Applications](#)

[History Samples](#)

[History Overview](#)

[Customizing the History Samples View](#)

You can use History Samples to collect a variety of network statistics over a period of time to establish your network performance baseline.

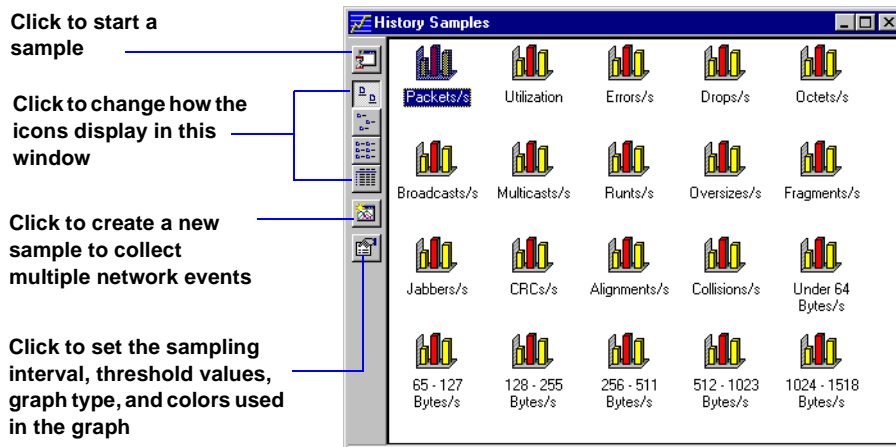
Baseline statistics help you set alarm thresholds to notify you when abnormal network behavior occurs. You can also use history samples to determine long-term network traffic trends, and help plan for future network expansion and reorganization.

You can launch as many as 10 history sample processes concurrently. These can be 10 different samples, or multiple instances of the same sample so that both short-term and long-term trends can be recorded simultaneously.


The network events available for history sample monitoring vary according to the type of adapter you have selected in the Adapter dialog box. For example, when monitoring a token ring network, you can collect history samples of various token ring frame types (such as beacon frames). When monitoring a Frame Relay network, you can collect history samples of various Frame Relay frame types (such as LMI frames). When monitoring an ATM network, you can collect history samples of different cell types.

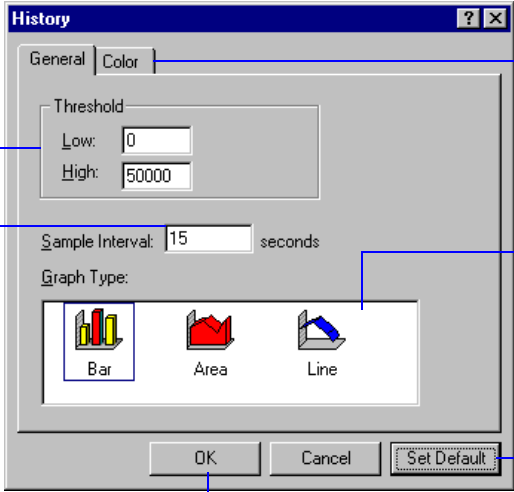
The sample data can be displayed in a bar chart, a line chart, or an area chart.

[Figure 2-6](#) shows the History Samples window for an Ethernet adapter.



**Figure 2-6. The History Samples Window**

Before launching a sample, set the sampling interval, the high and low threshold values, the graph type, and the colors used in the graph. First select the sample you want to use from the History Samples window. Then click the  button. The History properties dialog box is shown in [Figure 2-7](#).



Specify the threshold values here

Specify the sample interval. (Sniffer Pro maintains a maximum of 3,600 samples. If you specify 15 seconds, you will get up to 3,600 15-second samples.)

Click to select the colors used in the graph

Click to select the graph type

Click to restore factory settings

Click OK to save the settings

**Figure 2-7. Configuring History Sample Settings**



*Exporting History Trend Data*

The history sample will stop automatically when the maximum number of samples are collected or when you close the History window.

Sniffer Pro lets you export the history data for tabulation or charting. Refer to [Exporting Monitor Data on page 2-21](#).

[Figure 2-8](#) shows a **Packets/s** history sample in bar chart format and describes the toolbar.

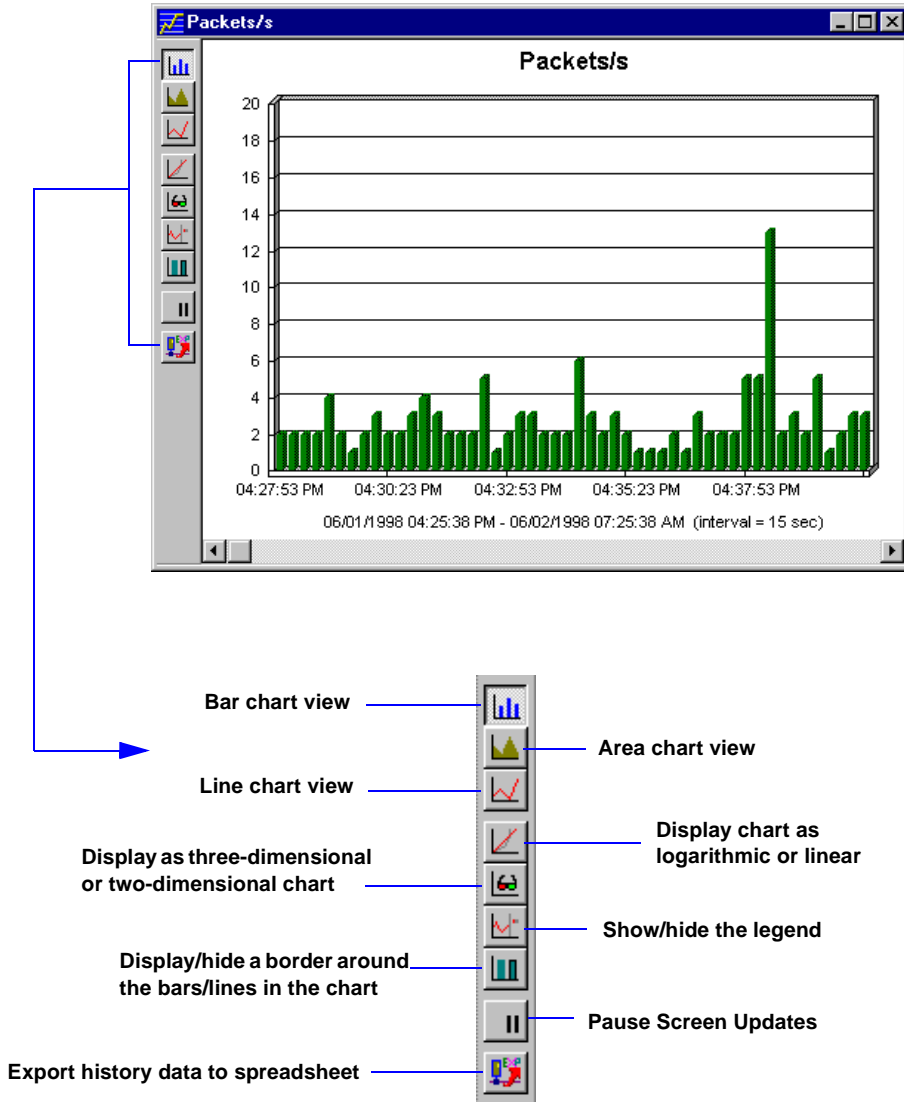


Figure 2–8. History Samples (Packets/s Bar Chart) and Toolbar

## Protocol Distribution



### *Monitor Applications*

### *Monitoring Network Protocol Distribution*

You can use Protocol Distribution to report network usage based on the network-, transport-, and application-layer protocols. For example, you can monitor IPX/SPX, TCP/IP, NetBIOS, AppleTalk, DECnet, SNA, Banyan, and many other protocols.

Protocol distribution monitors popular IP applications, such as NFS, FTP, Telnet, SMTP, POP2, POP3, HTTP (WWW), Gopher, NNTP, SNMP, X-Window, and others. It also monitors IPX transport-layer protocols such as NCP, SAP, RIP, NetBIOS, Diagnostic, Serialization, NMPI, NLSP, SNMP, and SPX.

For WAN and ATM adapters, tabs are also provided to monitor network usage based on link layer protocols – for example, by PVC for Frame Relay circuits. The WAN tabs available depend on the encapsulation protocol currently selected in the Options dialog box.

You can view the protocol distribution in a table, or as a bar or pie chart. You can also view the number and percentage of packets or bytes for a protocol.

Sniffer Pro lets you export the protocol distribution data for tabulation or charting. Refer to *Exporting Monitor Data on page 2–21*.

*Figure 2–9* shows a Protocol Distribution bar chart for an Ethernet adapter.

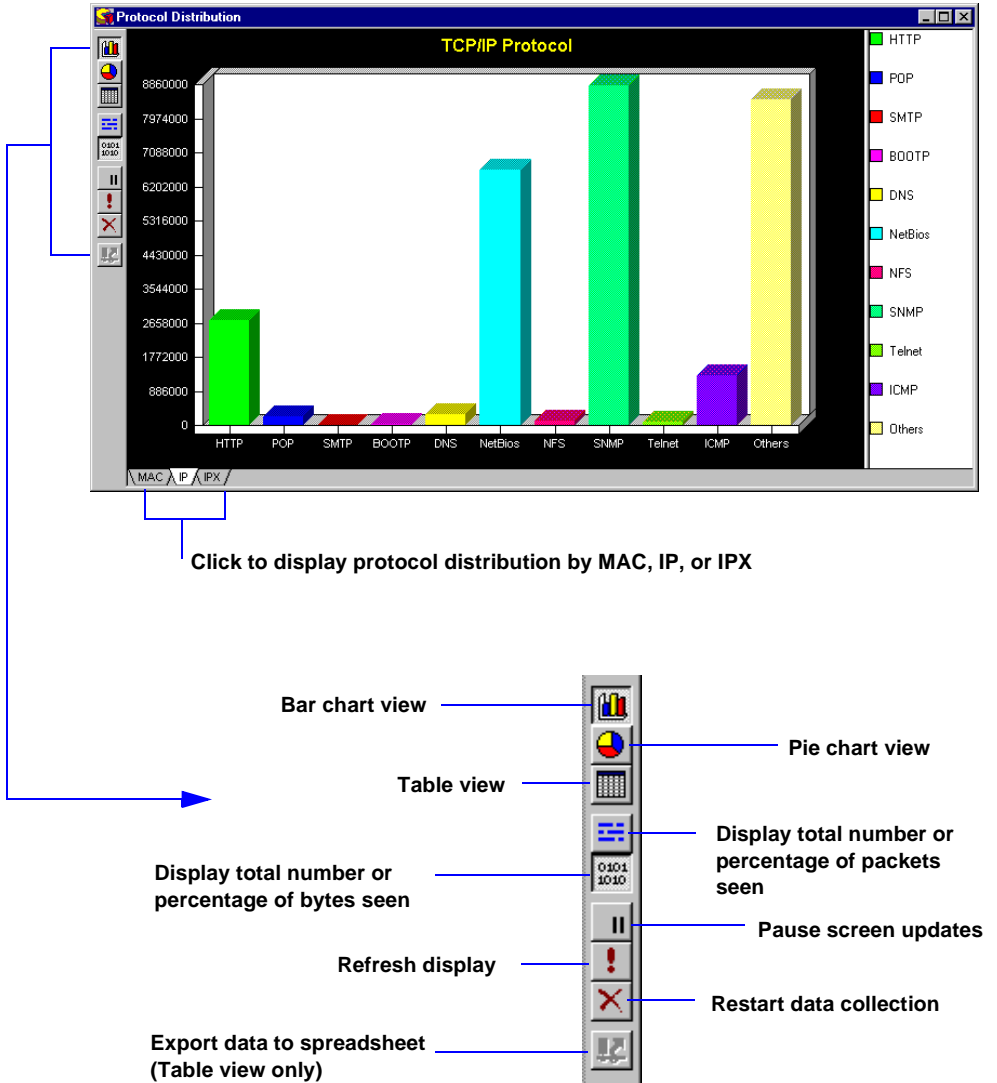


Figure 2–9. Protocol Distribution (Bar Chart View) and Toolbar

## Global Statistics



### *Monitor Applications*

### *Viewing Packet Size and Utilization Distribution*

Global Statistics help you understand the overall activity levels in the network and pinpoint large- and small-size packet traffic loads, each of which can have a different effect on overall network performance and availability.

Global statistics provides various tabs with statistical measures pertinent to network traffic analysis:

- The Size Distribution tab shows the frequency of each packet size as a percentage of all monitored traffic.
- The Utilization Distribution tab shows network bandwidth consumption distributed among each 10% grouping – 0 to 10%, 11% to 20%, ..., 91% to 100%.
- The WAN Link tab (WAN adapters only) shows WAN traffic in both graphic and tabular format. Packets/second, Utilization/second, and Errors/second are all monitored separately for DTE and DCE, in addition to various error frame counters and frame size distribution counters.
- The ATM tab (ATM adapters only) shows ATM traffic in both graphic and tabular format. Packets/second, Utilization/second, and Errors/second are all monitored separately for DTE and DCE, in addition to various error frame counters and frame size distribution counters.

You can view global statistics in a bar or pie chart.

*Figure 2–10* shows a packet size distribution graph for an Ethernet adapter.

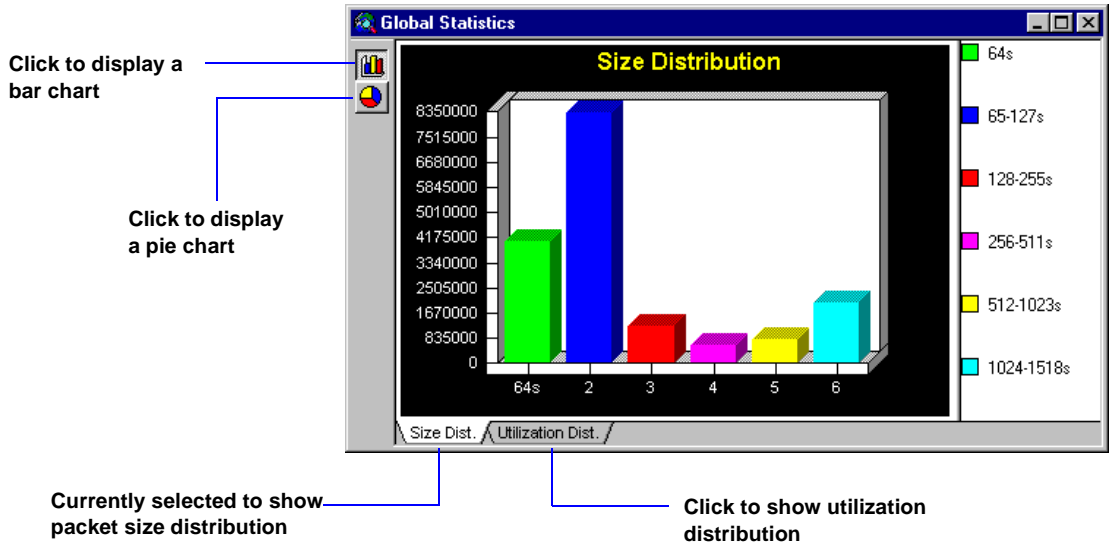


Figure 2–10. Global Statistics (Bar Chart View)

## Smart Screens (ATM Adapters)



*Monitor Applications*

*Viewing ATM Smart Screens*

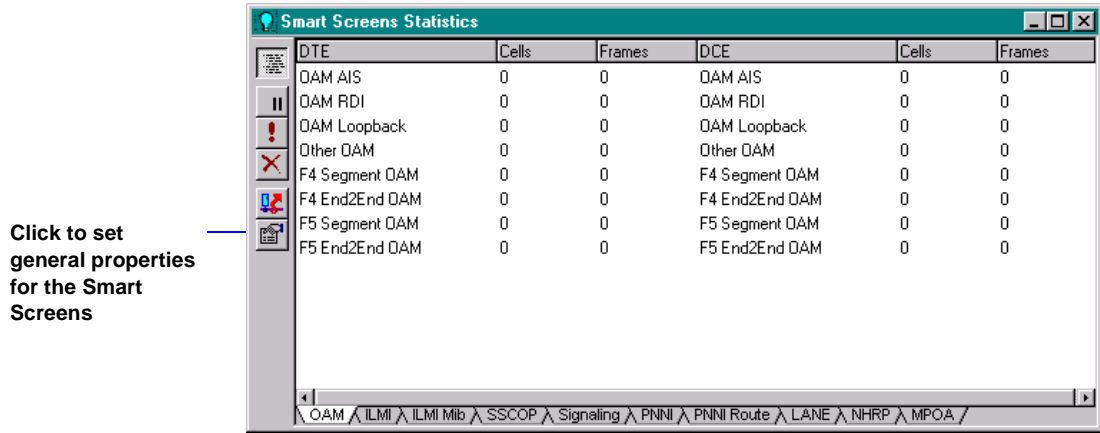
*Setting ATM Smart Screens Properties*

ATM Smart Screens provide tabular counters for various ATM-related cell/frame types. There are separate Smart Screens for different sets of cell/frame types (for example, OAM cell types, ILMI cell types, and so on).

To view the ATM Smart Screens, select **Smart Screens** from the **Monitor** menu or click the **Smart Screens** button in the ATM toolbar.

A window opens showing counters of various frame types, broken out by direction (DTE and DCE). At the bottom of the Smart Screens window, there are multiple tabs for different protocol-specific sets of cell/frame types. You can click on each tab to see the counters for that set of cell/frame types.

*Figure 2–11* shows the OAM tab of the Smart Screens display.



Click to set general properties for the Smart Screens

Currently selected to show OAM cell types.

Click other tabs to see different frame/cell counters.

Figure 2–11. ATM Smart Screens (OAM tab)

## Physical Layer Statistics (ATM Adapters)



### Monitor Applications

### Viewing ATM Physical Layer Statistics

### Overview of Physical Layer Statistics

The Physical Layer Statistics screen provides counters and status indicators monitoring the current status of the connected ATM physical interface. The exact counters will depend on the interface pod (or the ATM Book interface module) used to connect to the ATM network (for example, Multimode Fiber STS3c, Single Mode Fiber STS3c, Unshielded Twisted Pair (UTP-5) STS3c, DS3, E1, E3, OC-3, OC-12, and so on).

To view the ATM Physical Layer Statistics screen, select **Physical Layer Stats** from the Monitor menu or click the **Physical Statistics** button in the ATM toolbar. A window opens showing counters of various physical layer statistics and alarms, broken out by direction (DTE and DCE).

**NOTE:** The counters in the Physical Layer Statistics screen are the same for the Multimode Fiber STS3c, Single Mode Fiber STS3c, and UTP-5 STS3c OC3\_Physical\_Layer\_Statistics Interface Pods.

*Figure 2–12* shows the Physical Layer Statistics screen for a T1 interface pod.

DS1 Physical Layer Statistics									
DTE					DCE				
	Status	Error Sec	Error Cnt	Error Rate		Status	Error Sec	Error Cnt	Error Rate
CHEC		--	0	0.0000-00	CHEC		--	0	0.0000-00
UCHEC		--	0	0.0000-00	UCHEC		--	0	0.0000-00
LOS	🔴	119	--	--	LOS	🔴	119	--	--
ODF	🔴	119	--	--	ODF	🔴	119	--	--
AIS	🟢	0	--	--	AIS	🟢	0	--	--
CRC6	🟢	0	0	0.0000-00	CRC6	🟢	0	0	0.0000-00
Yel	🟢	0	--	--	Yel	🟢	0	--	--
LCV	🔴	119	9185	0.4999-04	LCV	🔴	119	203913	0.1110-02

The display shows the status of different line indicators. A green circle means that the indicator is not in an error state. A red circle means that the indicator is in an error state.

Figure 2–12. ATM Physical Layer Statistics (T1 Pod shown)

# Switch Statistics



Monitor Applications

About the Sniffer Pro Switch Analysis Features

Understanding the Switch Statistics Display

Using a Switch Alarm as a Trigger To Start Capture Automatically

The Switch Statistics application retrieves and displays statistics from the MIB on the switch selected in the Switch Connection Settings dialog box. Each switch port is listed in the Switch Statistics display with a set of counters and identifiers. The following information is provided:

- Traffic statistics for each port, including the number of bytes, unicast packets, broadcast packets, error packets, and discarded packets seen both in and out of each port.
- Identifying information, including the name of each module and port on the switch.
- Operational status information, including whether each module and port is functional, idle, or down.

Depending on the tab selected in the display, switch ports are listed sequentially either by the **Module** in which they are found or by the **VLAN** to which they belong.

Use the **Alarm Config** tab of the Switch Statistics display to set threshold based alarms on the connected switch. When a particular threshold is crossed, the switch reports the alarm back to the Sniffer Pro where it is recorded in the Alarm Log. You can also set triggers on these alarms to start capture on the offending switch port automatically.

Figure 2-13 shows the Switch Statistics display with the **Module** tab enabled.

Starts capture on selected Port or VLAN.

View Module Details

Module Name	Module Status	Port Name	Port Status	VLAN	In Bytes	Out Bytes	In Unicast Pkts
Module 1	ok	1/1	Ok	Trunk	73337229	3417955	0
Module 1	ok	1/2	No Connect	default	0	0	0
JeffM	ok	2/1	SPAN	Trunk	0	75108421	0
JeffM	ok	2/2	No Connect	VLAN022	0	0	0
JeffM	ok	2/3	Ok	VLAN022	49634	20373673	246
JeffM	ok	2/4	Ok	VLAN022	0	20856178	0
JeffM	ok	2/5	Ok	VLAN022	251632	7725372	0
JeffM	ok	2/6	No Connect	VLAN022	0	0	0
JeffM	ok	2/7	No Connect	VLAN022	0	0	0
JeffM	ok	2/8	No Connect	VLAN022	0	0	0
JeffM	ok	2/9	No Connect	VLAN022	0	0	0
JeffM	ok	2/10	No Connect	VLAN022	0	0	0
JeffM	ok	2/11	No Connect	VLAN022	0	0	0
JeffM	ok	2/12	Ok	Trunk	1306477	69019937	0

Currently selected to show switch ports by module.

Select this tab to display switch ports by the VLAN to which they belong.


Select this tab to configure alarms to be set on the switch.

Figure 2-13. The Switch Statistics Display (Module Tab Enabled)

## Monitor Alarms

Sniffer Pro provides a comprehensive method of detecting and logging unusual network events during monitoring.

The alarm manager logs an event in the *alarm log* when a user-specified threshold parameter is exceeded. By reviewing the events listed in the alarm log, you can identify network exception conditions that might require immediate attention.

To view the alarm log, select **Alarm Log** from the **Monitor** menu, or click on the  button in the Sniffer Pro main toolbar.

For information about configuring alarms and setting options, see [Chapter 7, Managing Alarms](#).

## Exporting Monitor Data

You can export data from the following application displays for tabulation or charting:


- The Dashboard gauge view and tab views
- The Monitor and Matrix outline table view
- The History data view
- The Protocol Distribution table view
- The Smart Screens table view.
- The Physical Layer Statistics table view.
- The Switch Statistics table view.

Right-click on the application's display and select **Export**. You can also click the  button if available.

You can save data in several formats:

- Comma Separated Value format (.csv)
- Tab-delimited text file (.txt)
- Space-delimited formatted text file (.prn).

## Generating Reports on Monitor Data

The Sniffer Reporter Agent is an optional application provided by Network Associates for generating a wide variety of customizable reports based on data collected by the Sniffer Pro application. If you have installed the optional Sniffer Reporter Agent on the Sniffer Pro PC, the Reporter's icon  appears in the following monitor applications:

- Matrix
- Host Table
- Protocol Distribution
- Global Statistics

You can click the Reporter's icon to launch the setup dialog box for a report based on the data collected by the corresponding monitor application. For more information on using the Sniffer Reporter Agent, see the documentation and online help accompanying your product shipment.

## Saving Monitor Data to a Database File



Sniffer Pro saves the real-time statistics generated by the Monitor applications to a Microsoft Access database file. The file (netdb.mdb) is located in the current local agent's folder in the Sniffer Pro Program directory. By default, Sniffer Pro updates the database file for all statistics every 60 minutes.

The **Database** menu in the Sniffer Pro menu bar provides configuration options for the database file. You can turn off database collection for all or specific statistics, change the update interval for statistics, and delete all or specific database records. You can also save the Sniffer Pro address book in the database file.

*Database*

*Turning Off  
Database Collection*

*Deleting Database  
Records*

*Changing the  
Database Update  
Interval*

*Saving the Address  
Book to the Database  
File*



Unlike the monitoring function, which stores statistical measurements and calculations about your network traffic, the *capture* function collects and stores the actual packets from your network in a capture buffer.

During capture, the Expert analyzes the packets and displays the results in real time. To disable the real-time Expert analysis, select **Expert Options** from the **Tools** menu and uncheck the **Expert During Capture** box.

After a capture is stopped, you can use the Sniffer Pro display function to decode and display the packets in the capture buffer, providing you with detailed information about network transactions (*packet display*). The display function also displays Expert analysis (*Expert display*). Both the packet display and the Expert display are described in [Chapter 4, Displaying Captured Data](#).

Sniffer Pro provides *capture controls* on the main toolbar and in the **Capture** menu to control the capture process, configure the *capture buffer* (which stores the captured packets), and define capture *filters*. A capture panel is also provided so that you can view the status of a capture session.

Before starting a capture, you should configure the Expert options that determine how Expert data is processed and displayed. Expert options are described on [page 3-6](#).

## Capture Controls

Use the capture buttons on the main toolbar or the menu items in the **Capture** menu to:

- Start, stop, and pause a capture session
- Display the results of a capture
- Create a new filter to use for capture
- Select a filter to use for capture

[Figure 3-1](#) shows the capture buttons located in the main toolbar.

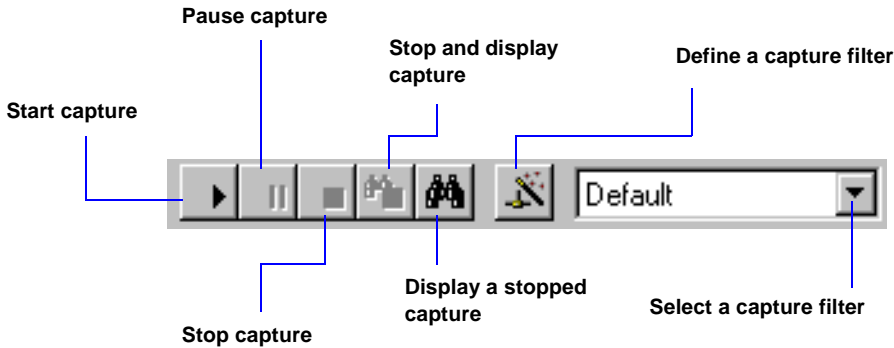


Figure 3–1. The Capture Controls

## Capture Panel



### *Capturing Packets From the Network*

### *Viewing the Status of the Capture Buffers On the Gigabit Ethernet Card*

Use the capture panel to view the status of the capture process. Two tabs are provided at the bottom of the panel. The **Gauge** tab displays the number of packets captured and indicates how full the capture buffer is (as a percentage). The **Detail** tab shows detailed statistics about the current capture session.

If you are using the Gigabit Ethernet adapter or the ATM Book, there is also a **Channel Info** tab providing information on the status of the onboard capture buffers on the Gigabit Ethernet interface card or the ATM Book, respectively.

To open the capture panel, select **Capture Panel** from the **Capture** menu, or click the  button in the main toolbar.

The capture panel (like the Packet Generator and the Dashboard) is a *dockable* window. You can dock it on the Sniffer desktop (select **Options** from the **Tools** menu and click the **Workspace** tab, or right-click the Capture Panel window and select the **Docking View** toggle). If not docked, the capture panel is a normal window.

*Figure 3–2* shows the Capture Panel window.

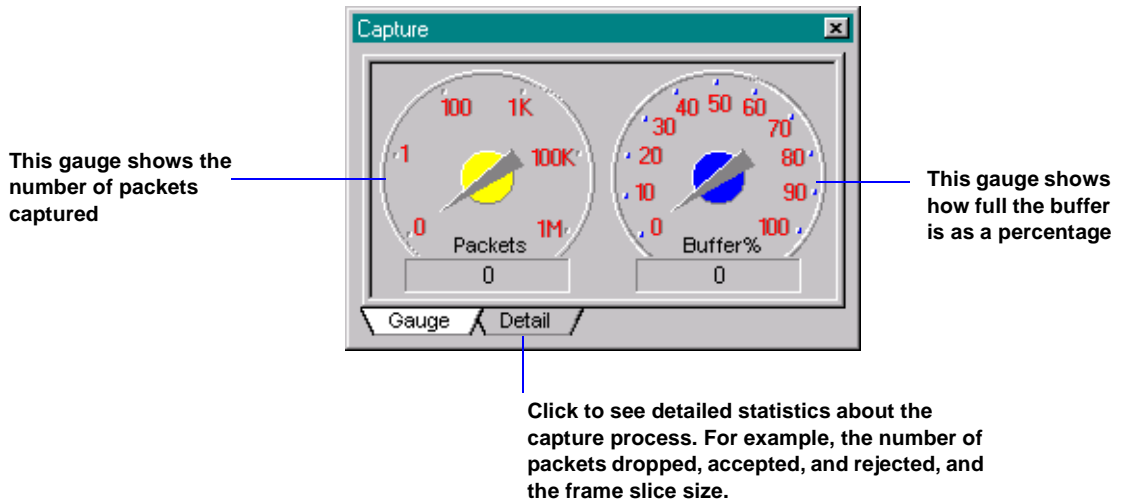


Figure 3–2. The Capture Panel Gauge Display

## Capture Buffer

Captured packets are stored in a *capture buffer*. You can display and analyze the packets currently in the capture buffer or save the packets to disk. You can load and display previously saved capture files (trace files). You can even spool captured packets to files in real time, effectively increasing the size of your capture buffer.

By loading previously captured packets from a disk file, you can display and analyze data as if it were captured live at that moment. Sniffer Pro treats the data loaded from a disk file in the same way as data captured live off the network.

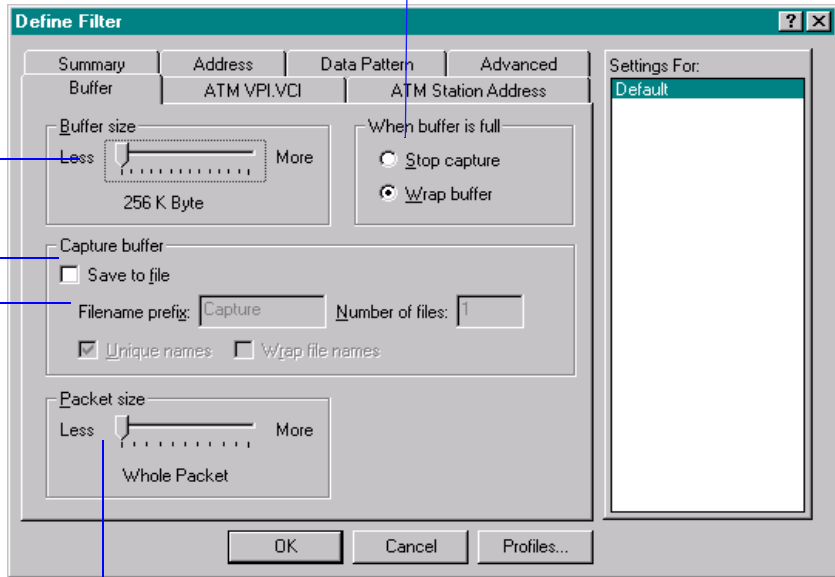


*Define Filter Buffer Tab*

Capture buffer options are tied to the Define Filter function. To set capture buffer options, select **Define Filter** from the **Capture** menu, then click the **Buffer** tab (see [Figure 3–3](#)).

Select to stop capture when the buffer is full or overwrite older data in the buffer (Wrap). You can select these options only if Save to File option is disabled.

Select the memory size for the capture buffer. If you specify a large buffer, there may be a delay while Sniffer Pro allocates memory. Do not specify a buffer larger than the amount of RAM available in your system.



Click to save buffer contents to a file automatically when full. Specify a filename prefix and number of files to be spooled. (Each file will be the same size as the defined capture buffer.)

Select the packet size. You can save the whole packet in the buffer or a truncated version. (Truncated packets save disk space, reduce capture file size, and help eliminate lost frames when network traffic is very high.)

Figure 3–3. Setting Capture Buffer Options


**IMPORTANT:** You can configure the size of the capture buffer from 256 K bytes to up to 192 MB on Windows 95 and up to 64 MB on Windows NT. In Windows NT, although Sniffer Pro lets you specify 192 MB, the maximum buffer size is only 64 MB. If you create a filter specifying 192 MB, the capture will fail to start.

## Saving the Capture Buffer to a File

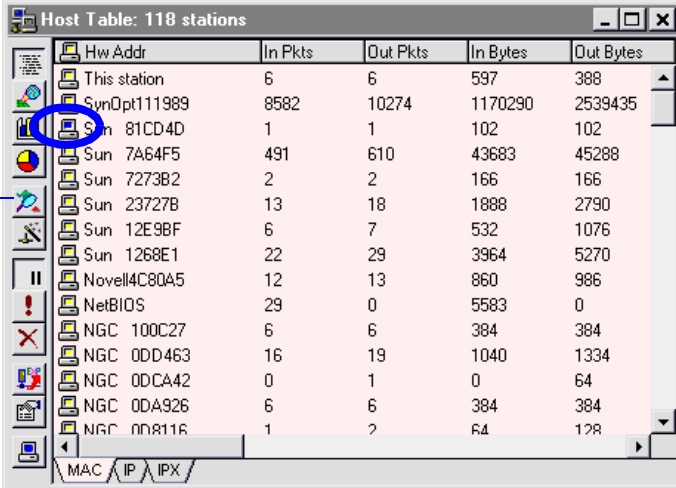
You can save the capture buffer contents to a file automatically when the buffer is full by selecting **Save to file** on the **Buffer** tab. Specify the filename prefix and the number of files to be spooled. For example, if you specify 5 in the **Number of files** field and click **Wrap file names**, the sixth

file overwrites the first file. If you do not select **Wrap file names**, capture will stop when the fifth file is full.

## Capturing from Specific Stations

To capture packets for a particular station, select the station from the monitor's host table display. To capture packets between two specific stations, select one of the stations from the monitor's matrix display. Then, click the  button. (To view the host table or matrix table, select **Host Table** or **Matrix** from the **Monitor** menu, or use a toolbar button.)

*Figure 3-4* shows an example of how to capture from a single station in the host table.



**1. Select station (turns blue)**

**2. Click Capture Button**

You can see the progress of the capture on the status line of the main Sniffer Pro window, or on the Capture Panel

Hw Addr	In Pkts	Out Pkts	In Bytes	Out Bytes
This station	6	6	597	388
SynOpt111989	8582	10274	1170290	2539435
Sun 81CD4D	1	1	102	102
Sun 7A64F5	491	610	43683	45288
Sun 7273B2	2	2	166	166
Sun 23727B	13	18	1888	2790
Sun 12E9BF	6	7	532	1076
Sun 1268E1	22	29	3964	5270
Novel4C80A5	12	13	860	986
NetBIOS	29	0	5583	0
NGC 100C27	6	6	384	384
NGC 0DD463	16	19	1040	1334
NGC 0DCA42	0	1	0	64
NGC 0DA926	6	6	384	384
NGC 0DA116	1	2	64	128

**Figure 3-4. Single-Station Capture from the Host Table**

## Capture Filters

You can define *filters* to capture only the particular packets you need, so that you can focus on the data necessary for troubleshooting network problems.

When you apply a filter to the capture process it is called a *capture filter*. A capture filter allows only certain frames to be saved in the capture buffer. For a description of how to define a filter, see [Chapter 5, Defining Filters and Triggers](#).

## Capture Triggers

The *trigger* feature allows you to start and stop captures based on date and time, alarms, and specific network events. Use triggers to capture data while Sniffer Pro is unattended, such as on off-hours or weekends, or to start captures when specific events occur, such as alarm conditions.

For a description of how to define a capture trigger, see [Chapter 5, Defining Filters and Triggers](#).

## Expert Options



[Configuring the Expert](#)

For effective network analysis, and depending on your network's protocol environment, you should configure Expert options before you start capturing data. The Expert options are described below.

## Expert Layers and Objects



[Objects Tab](#)

[Recycling Expert Objects](#)

During capture, the Expert constructs a database of network objects from the traffic it sees and categorizes network problems according to the Expert layer at which they occur. (The Expert's network layering structure is similar to the OSI model. However, the two schemes do not always map on a one-to-one basis.)

The Expert has configuration options that enable you to:

- Exclude certain layers from Expert processing.

In addition to using capture filters, which let you select the particular traffic you need for network analysis, you can exclude certain Expert layers from processing. This enables you to focus on specific network problems precisely.

- Specify the maximum number of objects that can be created in the database for each Expert layer.

To reduce the amount of memory needed to create network objects, you can specify the maximum number of objects that the Expert can create for each Expert layer. To help with configuration, the Expert shows the estimated amount of memory needed for the number of objects selected for each layer.

- Specify whether to recycle Expert objects (the default) or stop creating new objects when there is no more room in the database.

The Expert builds a database of network objects from the information in the packets accumulated in the capture buffer. Because some networks can be immensely complex in their structure, at some point the Expert will have no more memory for new network objects. If you recycle objects, the Expert continues to add new objects to the database, overwriting the least interesting objects when it runs out of memory (objects with no associated errors are considered “least interesting”). If you do not recycle objects, the Expert stops creating new objects when it runs out of memory, and instead, continues to interpret traffic in accordance with the information it has already stored in its database.

- Enable/disable real-time Expert analysis during capture.

By default, when you start a capture, the Sniffer Pro Expert analyzes the packets coming into the buffer and displays the results in real time in the Expert window. You can observe the network objects, symptoms, and diagnoses that the Expert analyzer creates while the capture progresses. You can disable real-time Expert analysis if you prefer.

To configure network object and Expert layer options, select **Expert Options** from the **Tools** menu. The Expert Options dialog box opens displaying the **Objects** tab. See [Figure 3-5](#).

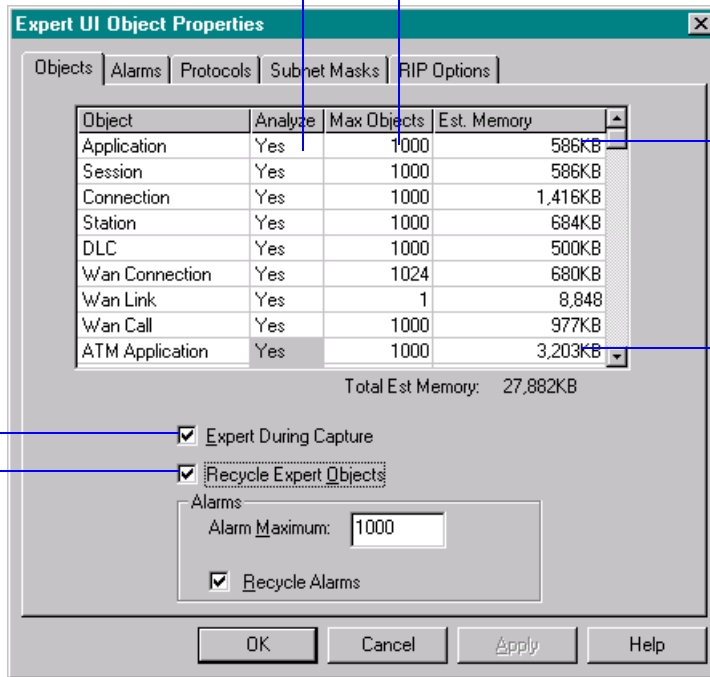
Click in the Analyze column for a layer and select No to exclude the layer from Expert processing

Specify the maximum number of objects that can be created in the database for each Expert layer

Sniffer Pro shows the estimated amount of memory needed for the number of objects specified for each layer.

Uncheck this box to disable Expert analysis during capture

This check box determines what the Expert does when it runs out of memory:



- Continues to create new objects by overwriting older objects in the database (checked)
- Stops creating new objects and continues interpreting traffic according to information already in the database (unchecked)

Figure 3–5. Setting Expert Object and Layer Options

# Expert Thresholds



## Alarms Tab

### Expert Alarm Thresholds

Expert thresholds determine whether the Expert generates a symptom or a diagnosis (also called an alarm) based on a given network event.

To change Expert thresholds, select **Expert Options** from the **Tools** menu and click the **Alarms** tab. The Alarms tab is shown in *Figure 3-6*.

**IMPORTANT:** The default thresholds supplied with Sniffer Pro have been carefully calculated to ensure accurate and informative symptom and diagnosis detection. Before changing any of the thresholds, make sure you understand your network.

Click to expand/collapse all Expert layers

Click the + to open an Expert layer and display all symptoms and diagnoses (alarms)

Click the + to display the settings for this alarm.

The thresholds display at the end of the settings list

Expert UI Object Properties

Objects | Alarms | Protocols | Subnet Masks | RIP Options

0 1	Description	Value
+	<b>ATM App</b>	
+	<b>ATM Flow</b>	
+	<b>ATM Cnx</b>	
+	<b>ATM Host</b>	
+	<b>Global</b>	
+	Bad CRC	Minor
+	Broadcast/Multicast Storm	40, Minor, Logged
-	Broadcast/Multicast Storm Diag	120, Critical/Diag, Log
	Severity	Critical/Diag
	Alarm Logged	Yes
	Broadcast Frames/sec	120
+	Collisions over threshold	10, Minor
+	LAN overload	50%, Minor
+	LAN overload percentage	20%, Critical/Diag, Log
+	Spanning Tree Topology Change	Minor
+	VLAN Not Operational	Minor

Reset | Reset All

OK | Cancel | Apply | Help

Click in the Threshold Value cell and type the new threshold value

Click to reset the selected value to the factory default.

Click to reset all settings for all layers to the factory defaults

**Figure 3-6. Setting Expert Thresholds**

For information about alarm severity levels and the alarm log, refer to *Chapter 7, Managing Alarms*.

## Subnet Masks



*Subnet Masks Tab*  
*Using an Incorrect Subnet Mask*

TCP/IP subnet masks traditionally reserve specific bits within an IP network address for the subnet mask depending on the class of address. The Expert comes with default subnet mask settings.

Certain networks may use nontraditional subnet masks. If the Expert is attached to a network segment that uses nontraditional subnet masks, it may register spurious network objects and diagnoses. This happens because the Expert expects address information at a location within the address field other than where it actually is.

If your networks use nontraditional subnet masks, you must add the IP network address and appropriate subnet mask for the networks from which the Expert will see frames.

Select **Expert Options** from the **Tools** menu, then click the **Subnet Masks** tab (see *Figure 3-7*). Click the **Add** button to create a new entry. Type your IP address in the **IP Net Address** column in the format *n.n.n.n* where each *n* is less than 256. Type the subnet mask associated with the IP address in the **Subnet Mask** column, then click **Apply**.

Click to add the IP address and appropriate subnet mask for the networks from which the Expert sees frames

Click to delete the selected IP address/subnet mask from the table

The Expert comes with default subnet mask settings for each class of IP address

#	IP Net Address	Subnet Mask
1	<ClassA>	255.255.0.0
2	<ClassB>	255.255.255.0
3	<ClassC>	255.255.255.0

Figure 3-7. Setting Subnet Masks

## RIP Settings



### *RIP Options Tab*


The Expert performs RIP (Routing Information Protocol) analysis during capture and builds a routing table by parsing RIP and other routing protocols in captured frames. RIP analysis is shown in the “Route” layer in the Expert window and enables you to detect common routing problems.

You can disable RIP analysis, or specify the level of analysis you want to perform (traffic counts and misdirected frames, or traffic counts only).

The Expert tracks the routers it discovers over the network and any default routers that you configure. When you configure a default router, the Expert constructs a default static route to that gateway. The destination IP address for this route is [0.0.0.0]. (You can enter either the MAC address or the IP address of the default router.) This feature allows the RIP Expert to be aware of routers that provide routes that they are not advertising.

Some hosts may be configured to route traffic to default gateways, but a route from such a host to a default gateway might never be advertised. Unless you configure static default routes, the RIP Expert will incorrectly diagnose frames sent from a host to a default gateway as misdirected. If a default route you have configured is also advertised, the other route is ignored, since the one you configured is permanently in the table.

---

 **IMPORTANT:** For RIP packets to be analyzed by the Expert, the connection layer or the application layer must be set to Analyze in the **Objects** tab of the Expert Properties dialog box. RIP sits above UDP; the RIP interpreter must be called from the UDP interpreter. Sniffer Pro considers UDP to be a transport layer; for the transport layer and above to be interpreted, at least the connection layer must be selected.

---

To configure or disable RIP analysis, select **Expert Options** from the **Tools** menu, then click the **RIP Options** tab. The RIP Options tab is shown in [Figure 3–8](#).

Select the level of RIP analysis you want to perform:

- *No traffic analysis (RIP disabled)* disables the RIP Expert.
- *Full traffic analysis (counts and analysis)* produces traffic counts and detects misdirected frames.
- *Traffic counts only* produces only traffic counts.

Expert discovers the routers on the network during capture and displays them in the router table

Select if you want Expert to discover the subnets on your network automatically during capture

This table displays the subnets that Expert detects on your network automatically during capture and the subnets you add manually.

The Source column indicates if the subnet is detected by the Expert (Network) or added manually (User).

Click to add a default router to the router table



Click to delete a router from the router table

Click to add or delete a subnet to or from the subnet table.

**IMPORTANT:** The RIP Expert requires that the IP subnet address and subnet mask be set properly in the Subnet Masks Tab.

Figure 3–8. Setting RIP Options

Use the *Display* feature to decode and view the packets stored in the capture buffer or in a capture file (packet display) and view the results of Expert analysis (Expert display).

To display the contents of the capture buffer and the associated Expert analysis, click  in the main toolbar during a capture session, or click  after a capture session. To open a capture file, select **Open** from the **File** menu.

The Expert display also opens when you start a capture showing Expert analysis in real time. (To disable real-time Expert analysis during capture, select **Expert Options** from the **Tools** menu and uncheck the **Expert During Capture** box.)

---

**NOTE:** The first time you view the results of a capture, the Expert display shows all traffic analyzed during the capture session. If you reopen the display, the Expert reanalyzes the packets in the capture buffer and displays the results. The results may differ if the capture buffer wrapped during capture.

---

Before displaying decoded packets and Expert analysis, you can apply a display filter. Display filters enable you to view the specific data needed for your network analysis. You should also configure Expert options, which determine how the Expert data is displayed. Expert options are described in [Expert Options on page 3–6](#).

## Display Filters

A filter applied to the display of captured data is called a *display filter*. Display filters let you select the packets you want to display. You can use display filters to view only:



### *Filters*

- Packets transmitted between network nodes (or address pairs)
- Packets that belong to one or more protocol groups
- Packets that match predefined data patterns
- Error packets
- Packets that belong to a certain size range
- Packets that match various combinations of the above specifications

Display filters do not affect the contents of the capture buffer. They just prevent some of the data from being displayed.

For a description of how to define a filter, see [Chapter 5, Defining Filters and Triggers](#).

## Packet Display



### Display Format Tabs

When you display the contents of the capture buffer or a capture file, Sniffer Pro interprets and decodes the higher-level protocols within the captured packets using its *protocol interpreters*. Sniffer Pro decodes over 200 different network protocols.

You can display the decoded packets in a variety of formats. Each format appears on a tab in the Display window. The formats are: Decode, Matrix, Host Table, Protocol Distribution, Statistics, and Expert.

---

**NOTE:** The Matrix, Host table, Protocol Distribution, and Statistics tabs appear at the bottom of the Display window *only* if the **Post analysis tabs** box is checked on the **General** tab of the **Display Setup** dialog box. Similarly, the Expert tab only appears if the **Expert tab** box is checked.

---

## Decode Tab



### ecode Tab

The Decode tab shows packets in three color-coded viewing panes: *summary*, *detail*, and *hex*.

- The *summary pane* shows an overview of the packets captured in line-by-line summarized format.
- The *detail pane* displays the detailed contents of the packet currently selected in the summary pane. Each layer of the protocol is interpreted and displayed.

You can display the detailed protocol layers in three different views — fully expanded decode, one-line summary, or a mixture of the two.

By default, Sniffer Pro expands underlying protocol layers in the detail pane. To save viewing space, click the minus (-) sign in front of the protocol sublayer line. To expand the protocol display again, click the plus (+) sign.

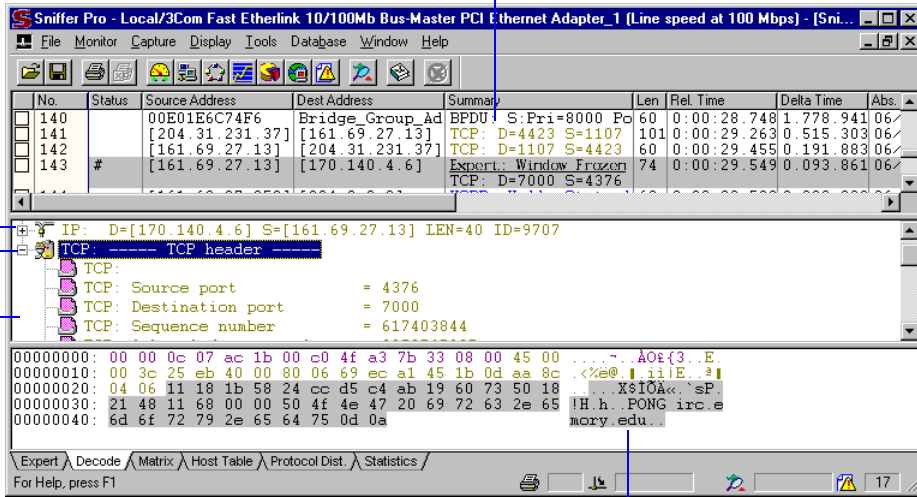
- The *hex pane* shows the selected packet in hexadecimal and ASCII (or EBCDIC) format.

When you select a packet on the summary pane, or a detailed protocol field in the detail pane, the equivalent hexadecimal octets in the packet are highlighted in the hex pane. This quickly shows you the correspondence between the protocol field and its equivalent bytes in the packet.

*Figure 4-1* shows the Decode display.

Click the minus (-) sign to reduce the protocol display  
 Click the plus (+) sign to expand the display

The *summary pane* shows an overview of the packets captured in line-by-line summarized format



The *detail pane* displays the detailed contents of the packet currently selected in the summary pane

The *hex pane* shows the selected packet in hexadecimal and ASCII (or EBCDIC) format

Figure 4–1. The Decode Tab

## Navigating the Display

Use the following keys to navigate the display. You can also use the commands in the **Display** menu.

- Page Up                      View the previous page in the active pane.
- Page Down                  View the next page in the active pane.
- Cursor Up                    View the previous line in the active pane.
- Cursor Down                View the next line in the active pane.
- F2                             Search the next selected packet in the summary pane.



### Keyboard Usage

Shift+F2	Search the previous selected packet in the summary pane.
Control+F2	Toggle the packet between selected and unselected state.
F3	Search for the next instance of a text string, data pattern, or status.
Alt+F3	Open the Search Packet dialog box.
F4	Zoom in/out of a Decode display.
F7	View the previous packet in the summary pane.
F8	View the next packet in the summary pane.

## Selecting Packets



*Selecting Packets for Separate Viewing*

*Selecting Packets for Separate Viewing or as Book Marks*

Sniffer Pro lets you select individual packets or a group of packets in the summary pane. Selecting packets allows you to mark key packets that are of interest to you, so that you can use them more easily. You can:

- Save the selected packets into a separate window for viewing
- Save the selected packets to a file
- Treat the selected packets as bookmarks, and use F2 to advance from one selected packet to the next.

## Setting Display Options



*Special Viewing Tips*

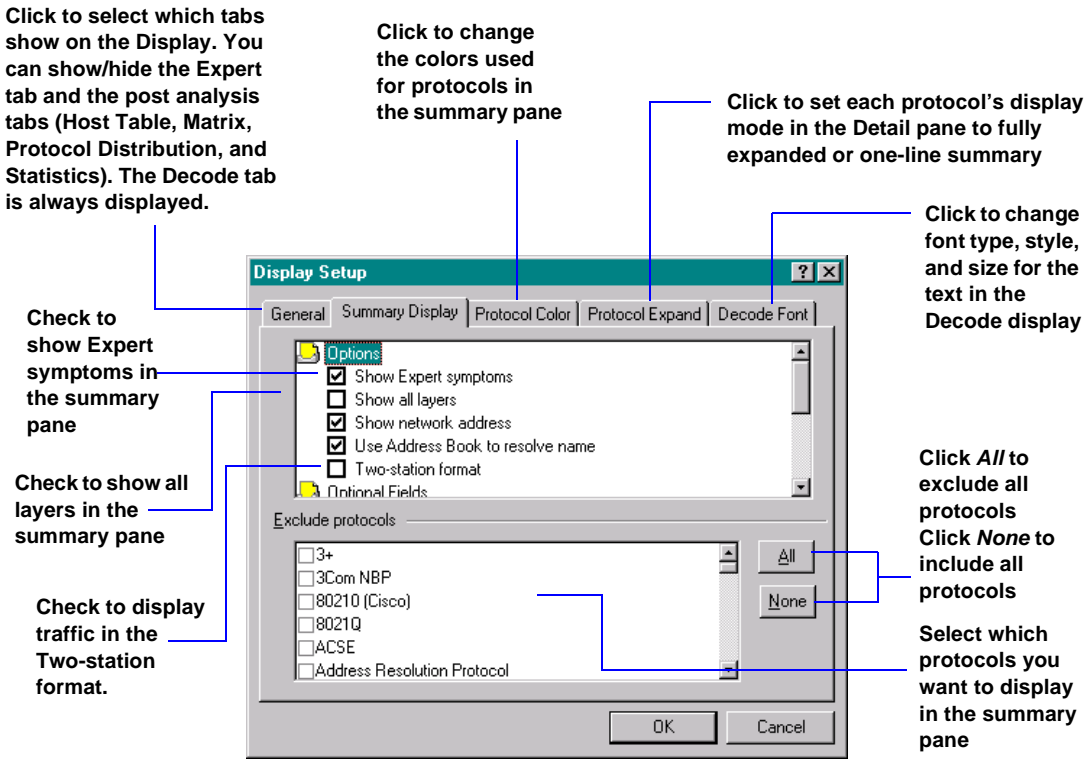
*Two-station format*

You can customize the way data is displayed in the decode display. You can:

- Exclude certain subprotocols from the summary pane (this is a more detailed control than a display filter)
- Set the summary address field format (network or hardware).
- Specify whether the two-station display format should be used.
- Select optional fields to be shown in the summary display.
- Color-code packets displayed in the summary pane based on their protocol
- Select the font for the detail display

To set the display options, select **Display Setup** from the **Display** menu.

*Figure 4-2* shows the Display Setup dialog box.



**Figure 4-2. Setting Display Options**

### About the Summary Display Options

You can set the following Summary Display options in *Figure 4-2*.

- Show Expert symptoms** If enabled, the Summary display shows the last symptom found (if any) for each frame.
- Show all layers** If enabled, the Summary view shows one line for each protocol level contained in a frame. If disabled, only one line (for the highest enabled protocol level) is shown.

<b>Show network address</b>	If enabled, the Summary view shows addresses as network addresses. If disabled, the Summary view shows addresses as hardware (DLC) addresses.
<b>Resolve name on MAC address</b>	If enabled, the Summary view shows names for MAC addresses instead of numerical addresses.
<b>Resolve name on Network address</b>	If enabled, the Summary view shows names for network addresses instead of numerical addresses.
<b>Use Address Book to resolve name</b>	If enabled, the Summary view will substitute names for addresses for any stations that are named in the Address Book.
<b>Two-station format</b>	If enabled, splits the display into left and right panes, showing traffic between two stations.

### Optional Fields

<b>Flags</b>	Shows flags associated with a frame.
<b>Absolute time</b>	Shows when the frame was received.
<b>Delta time</b>	Shows the interval between the current frame and the previous frame.
<b>Relative time</b>	Shows the interval between the current frame and the marked frame.
<b>Bytes</b>	Shows the frame's length.
<b>Cumulative bytes</b>	Shows the length of all frames, starting with the marked frame and including the current frame.

### About the Two-Station Format

When you examine network activity, you often want to focus on traffic between a pair of stations. To do this, you can set up display filters that define the two stations and enable the **Two-station format** in the

Summary Display tab of the Display Setup dialog box. You access this dialog box by selecting **Display Setup** from the **Display** menu.

The two-station format shows transmission from one station (the station that was detected first) on the left side of the screen and transmissions from the other station on the right. The Source and Destination columns from the single station display are removed. Instead, there are two columns, title **From xxx** and **From yyy**. A frame from the station on the left is assumed to be addressed to the station on the right, and vice versa.

## Using Protocol Forcing



### Using Protocol Forcing

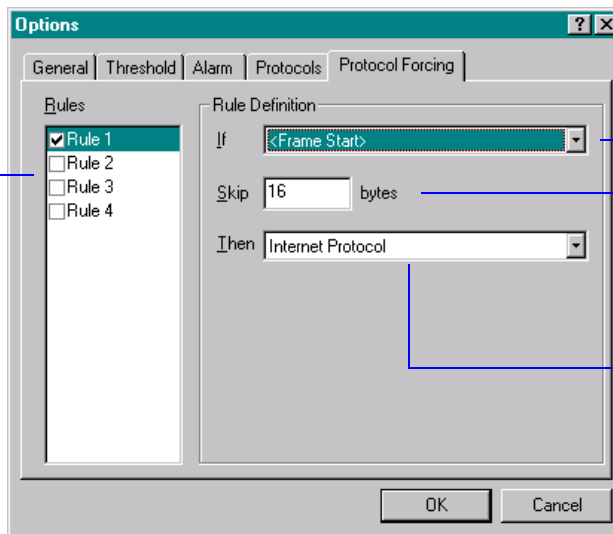
### Defining a Protocol Forcing Rule

Protocol forcing is useful when capturing frames that use a mixture of standard and non-standard (for example, proprietary) protocols that the Sniffer Pro might not otherwise be able to decode. For example, in some situations, networks may include standard IP data within a proprietary lower layer packet format unknown to the analyzer. Protocol forcing essentially lets you tell the analyzer "if you see this condition, skip this many bytes (to where the standard data is), then apply this protocol interpreter."

You specify protocol forcing rules in the **Protocol Forcing** tab of the Options dialog box, displayed by selecting the **Options** command from the analyzer's **Tools** menu (Figure 4-3).

You can define up to four rules. Checked rules are enabled and applied to decoded data.

Use the dropdown list to specify the protocol that should be used as the "force from" protocol. When the analyzer encounters the condition specified here, it will skip the number of bytes specified in the Skip x bytes field and apply the protocol interpreter specified in the Then field.



Specify the number of bytes to skip once the "If" condition is detected.

Use the dropdown list to specify the protocol that should be used as the "force to" protocol (that is, the protocol to be expected at the offset you specified in the Skip x bytes field).

Figure 4-3. Defining Protocol Forcing Rules

## Matrix Tab



[Showing the Traffic Map](#)

[Using a Visual Filter in the Traffic Map](#)

[Using the Matrix Map](#)

The Matrix tab collects statistics for conversations between network nodes.

- For LANs, the matrix tab accumulates MAC, IP network, IP application, IPX network, and IPX transport-layer information.
- For WANs, the matrix tab accumulates link layer (SDLC, LCN, Virtual Circuit, or HDLC, depending on the encapsulation protocol selected in the Options dialog box), IP network, IP application, IPX network, and IPX transport-layer information.

You can view accumulated data as a traffic map, as a table, or as a bar or pie chart.

- The *traffic map* provides a birds-eye view of network traffic patterns between nodes. You can filter out unwanted traffic by unchecking certain protocols, or by selecting specific network nodes to display.
- The *matrix tables* display traffic count statistics for node pairs:
  - The *outline table* provides a quick summary of total bytes and packets transmitted between pairs of network nodes.
  - The *detail table* provides a quick summary of the higher layer protocol type and its traffic load transmitted in and out of each conversation node pair.

You can sort a matrix table by clicking on a column heading (for example, to sort the statistics by packets, click on the **Packets** column heading). Click a second time to sort in reverse order.

- The *bar chart* displays the top 10 busiest conversation node pairs.
- The *pie chart* displays the top 10 busiest conversation node pairs as relative percentages of the total load of traffic.

In all views, you can display conversation traffic at the link layer, MAC layer, or selectively view only the IP or IPX layers.

In the table views, you can export the statistics for tabulation or charting.

[Figure 4-4](#) shows the Matrix display (bar chart view) and toolbar.

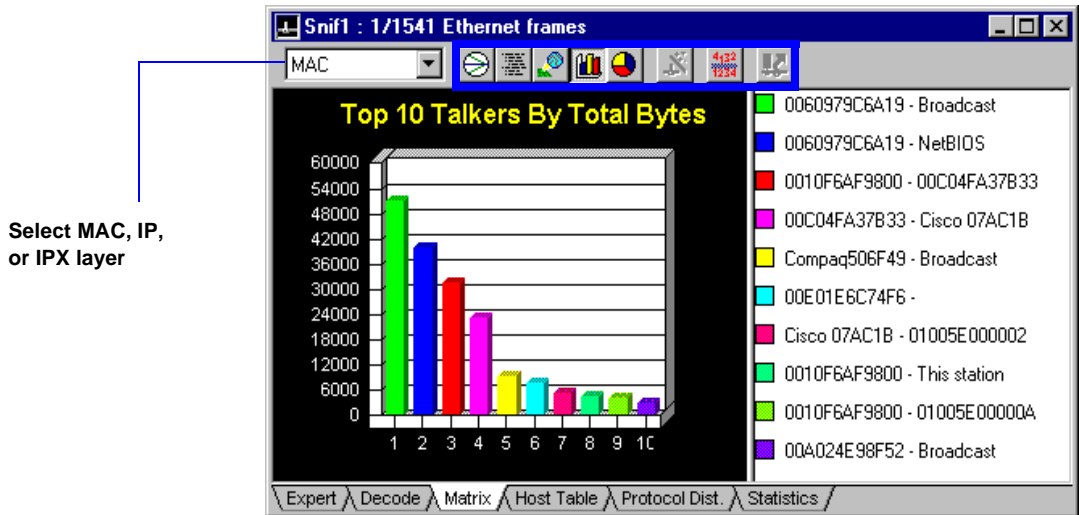
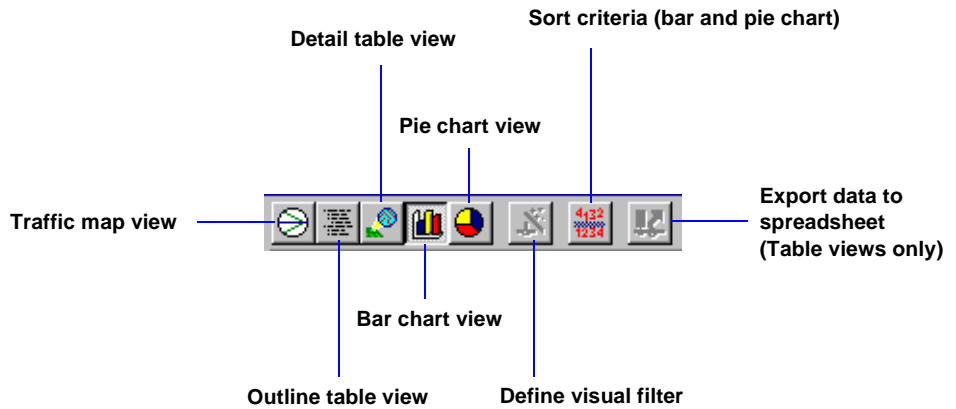


Figure 4-4. Matrix Display (Bar Chart View) and Toolbar

## Host Table Tab

The Host Table collects each network node's traffic statistics.

- For LANs, the matrix tab accumulates MAC, IP network, IP application, IPX network, and IPX transport-layer information.
- For WANs, the matrix tab accumulates link layer (SDLC, LCN, Virtual Circuit, or HDLC, depending on the encapsulation protocol selected in the Options dialog box), IP network, IP application, IPX network, and IPX transport-layer information.



### Host Table Tab

Identifying the  
TCP/IP Application  
Protocol Used by  
Each Host Node

You can view accumulated data as a table, bar chart, or pie chart.

- The *table* views display traffic count statistics for each network node.
  - The *outline table* provides a quick summary of total bytes and packets transmitted in and out of each network node.
  - The *detail table* provides a quick summary of the higher layer protocol type and its traffic load transmitted in and out of each network node.

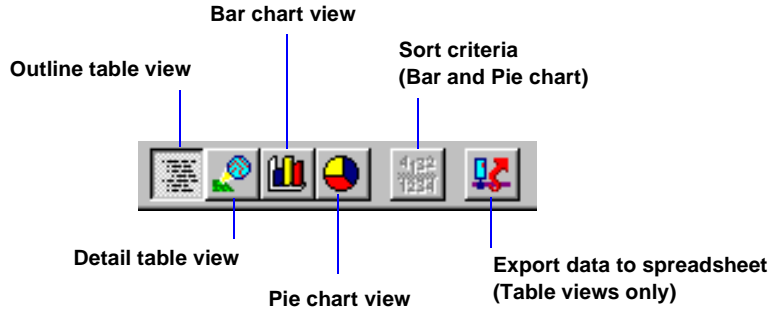
You can sort a host table by clicking on a column heading (for example, to sort the statistics by incoming packets, click on the **In Pkts** column heading). Click a second time to sort in reverse order.

- The *bar chart* displays the 10 busiest host nodes in real time.
- The *pie chart* displays the 10 busiest host nodes as relative percentages of the total load of traffic.

In all views, you can display traffic at the link layer, MAC layer, or selectively view only the IP or IPX layers.

In the table views, you can export the statistics for tabulation or charting.

*Figure 4-5* shows the Host Table display and toolbar.



Select MAC, IP, or IPX layer

Click the plus (+) sign to see protocol information. Click the minus (-) sign to hide it.

The screenshot shows a window titled "Sniff : 1/1541 Ethernet frames". The toolbar at the top has a dropdown menu set to "MAC". The table below shows the following data:

	Address	In Packets	In Bytes	Out Packets	Out Bytes	Total Packets	Total Bytes
+	0060979C6A19	0	0	382	90732	382	90732
	Broadcast	426	81045	0	0	426	81045
-	00C04FA37B33	297	31434	320	23300	617	54734
	IP	297	31434	320	23300	617	54734
+	0010F6AF9800	0	0	406	43958	406	43958
+	NetBIOS	195	42788	0	0	195	42788
+	Cisco 07AC1B	330	25076	80	5280	410	30356
+	Compaq506F49	0	0	58	9460	58	9460
+	00E01E6C74F6	0	0	124	8440	124	8440
+	Bridge_Group_Adv	120	7680	0	0	120	7680
+	This station	10	4760	10	1608	20	6368
+	01005E000002	80	5280	0	0	80	5280
+	01005E00000A	51	3978	0	0	51	3978
+	00A024E98F52	0	0	26	3450	26	3450

Expert Decode Matrix Host Table Protocol Dist. Statistics

Figure 4–5. Host Table Display (Outline Table View) and Toolbar

## Protocol Distribution Tab



### *Protocol Distribution Tab*

### *Showing IPX Protocol Distribution*

The **Protocol Distribution** tab reports network usage based on the network-, transport-, and application-layer protocols. For example, you can monitor IPX/SPX, TCP/IP, NetBIOS, AppleTalk, DECnet, SNA, Banyan, and many other protocols.

Protocol distribution monitors popular IP applications, such as NFS, FTP, Telnet, SMTP, POP2, POP3, HTTP (WWW), Gopher, NNTP, SNMP, X-Window, and others. It also monitors IPX transport-layer protocols such as NCP, SAP, RIP, NetBIOS, Diagnostic, Serialization, NMPI, NLSP, SNMP, and SPX.

You can view the protocol distribution in a table, or as a bar or pie chart. You can also view the number and percentage of packets or bytes for a protocol.

Sniffer Pro lets you export the protocol distribution data for tabulation or charting. To export data, the display must be in the table view.

*Figure 4-6* shows the Protocol Distribution display and toolbar.

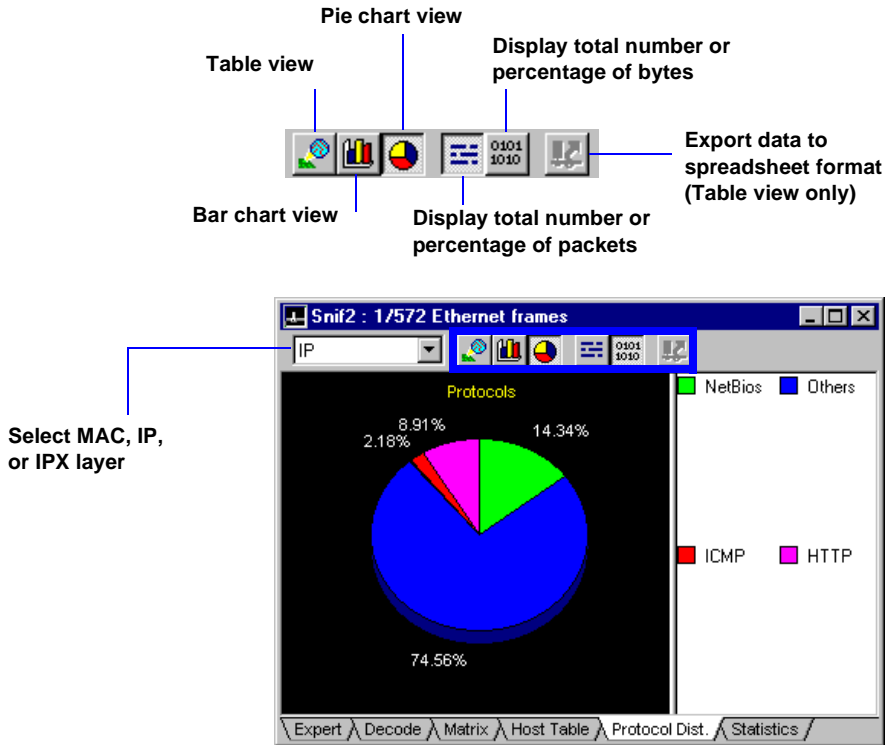


Figure 4–6. Protocol Distribution Display (Pie Chart View) and Toolbar


## Statistics Tab




### Statistics Tab

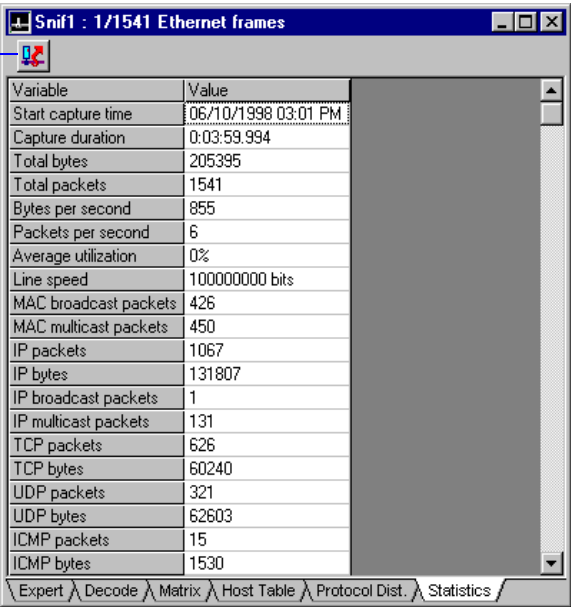
For each capture session, Sniffer Pro accumulates statistical information to help you analyze the network traffic during the capture period. A summary of this information is displayed in a table on the **Statistics** tab. The table displays:

- The date and time of the capture
- The amount of traffic seen during the capture period
- Utilization statistics

You can export this information to a spreadsheet using the  button.

*Figure 4-7* shows the Statistics display.

Export data to spreadsheet 



Variable	Value
Start capture time	06/10/1998 03:01 PM
Capture duration	0:03:59.994
Total bytes	205395
Total packets	1541
Bytes per second	855
Packets per second	6
Average utilization	0%
Line speed	100000000 bits
MAC broadcast packets	426
MAC multicast packets	450
IP packets	1067
IP bytes	131807
IP broadcast packets	1
IP multicast packets	131
TCP packets	626
TCP bytes	60240
UDP packets	321
UDP bytes	62603
ICMP packets	15
ICMP bytes	1530

**Figure 4-7. The Statistics Display**

## Expert Display



### Expert

### Expert Window

The Expert display shows the results of Expert analysis. Expert analysis can occur during a capture session, showing the results in real time. It can also occur after a capture session when the display function is invoked.

During Expert analysis, Sniffer Pro constructs a database of network objects from the traffic it sees. The Expert protocol interpreters learn all about the network stations, routing nodes, subnetworks, and connections related to the frames in the capture buffer. Using this information, Sniffer Pro detects and alerts you to potential problems that may exist on the network. These problems are categorized as being either *symptoms* or *diagnoses*:

- A *symptom* indicates that a threshold has been exceeded and may indicate a problem on your network.
- A *diagnosis* can be several symptoms analyzed together, high rates of recurrence of specific symptoms, or single instances of particular network events that cause the Expert to conclude that the network has a real problem. A Diagnosis should be investigated immediately.

The Expert analysis results (symptoms and diagnoses) are shown in five viewing panes on the Expert display tab and on the real-time Expert window that displays during capture. These panes function together so that you can view and select information at all levels of detail. See [Figure 4-8](#).

Each pane is described below:

- The *Expert Overview* pane shows the network analysis layers (similar in concept to the ISO layers) and the Expert overview statistics (objects, symptoms, or diagnoses) for each layer. By selecting a combination of layer and statistic type, you control the display of Expert analysis data in the other Expert panes.

---

✦ **TIP:** You can configure the window to be wide or narrow by clicking on the arrows in the upper right-hand corner of the Expert overview pane.

---

- The *Expert Summary* pane shows key summary information for the layer and statistic selected in the Expert Overview pane. The column headings for the Expert Summary display will change, depending on what layer and statistic you have selected.

- The *Protocol Statistics* pane displays the amount of traffic (in frames and bytes) for each protocol encountered for the layer you selected in the Expert Overview pane. (This pane is not displayed when the Expert Overview pane is narrow.)
- The *Detail tree* pane shows a hierarchical listing of all layers at or below those selected in the Expert Overview and Expert Summary panes. You can expand or collapse each layer in a manner similar to Windows Explorer. Click on any item in the Detail Tree to display its Expert detail data.
- The *Expert Detail* pane is a collection of information tables for the data selected by the other panes. The content of the Expert Detail pane will vary, depending on what items are selected in the various other panes.

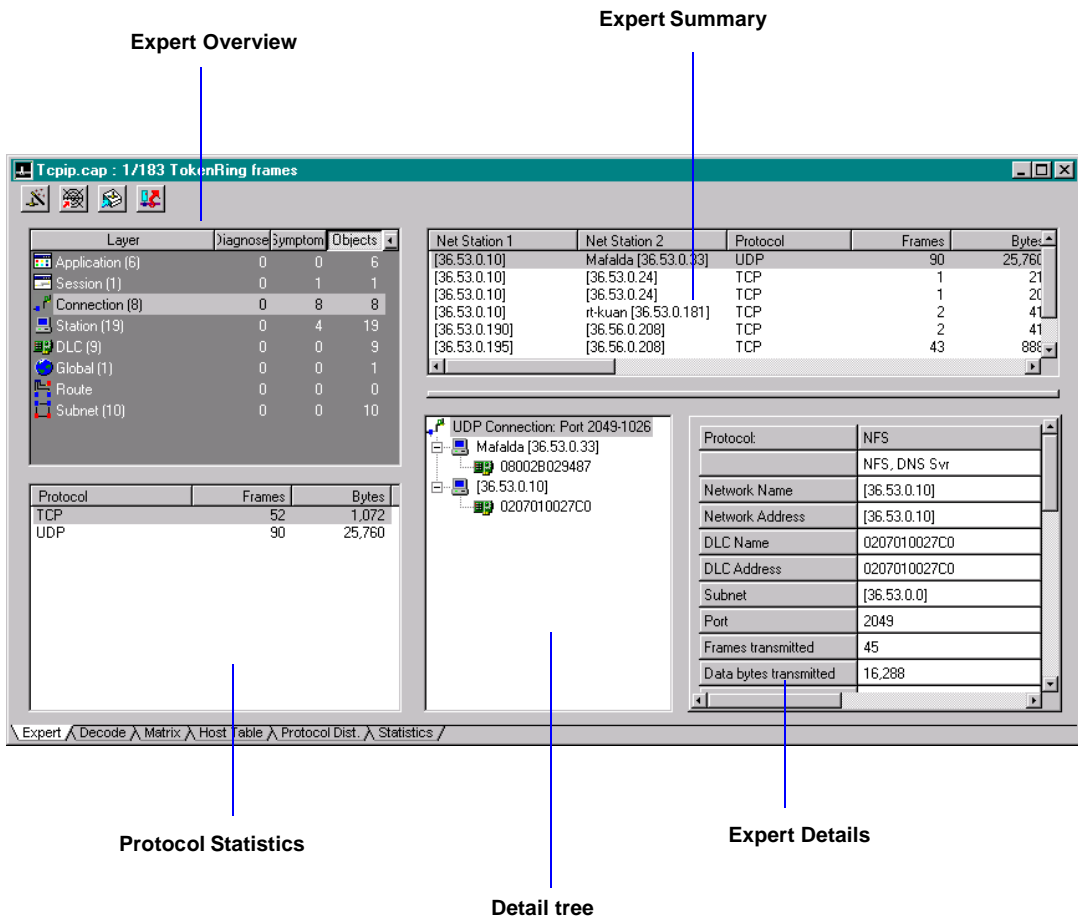


Figure 4–8. The Expert Window Panes

## Displaying Context-Sensitive Explain Messages



### *Displaying Expert Explain Files*

The Expert provides an explanation of the information in each pane of the Expert window. Click inside the pane on which you need information and press F1.

The Expert also provides concise explanations for each symptom and diagnosis generated. To display a detailed explanation of a symptom or diagnosis, click the question mark (?) to the right of the symptom/diagnosis description in the Expert Detail pane. (You may have to scroll to the right of the pane to see the ?.)

## Rearranging the Expert Display



### Arranging the Expert Display

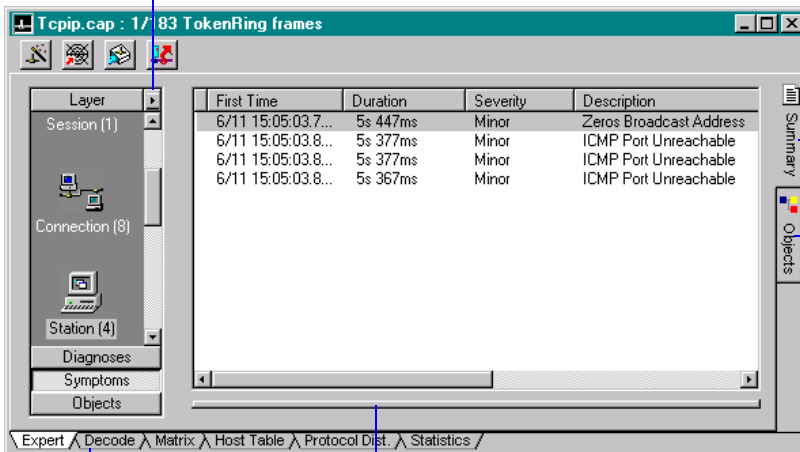
You can change the Expert display to better suit your viewing needs. You can display:

- All five viewing panes at the same time (shown in [Figure 4-8](#)).
- The Expert Overview and Expert Summary panes (with or without the Protocol Statistics pane). This is the default view.
- The Detail tree and Expert Detail panes.

[Figure 4-9](#) shows the default Expert display and demonstrates how to rearrange the different panes.

Click here to expand the Expert Overview pane and display the Protocol Statistics pane underneath

Click the Summary tab to display the Expert Overview and Summary panes (as shown)



Click the Objects tab to display the Detail tree and Expert Detail panes

Click to show the packet display (only available when capture is stopped)


Drag the bar up to the middle of the display to see all five panes at the same time (as in [Figure 4-8](#))

Figure 4-9. Rearranging the Expert Window Panes

## Exporting the Contents of the Expert Database

You can export the contents of the Expert analyzer's database of network objects, symptoms, and diagnoses to a file saved in comma-separated values (CSV). The CSV file format can easily be imported into most spreadsheet programs.

You can export the contents of the Expert analyzer's database in two ways:

- **Manually**, by clicking the Export  button in the Expert window. Then, use the dialog box shown in [Figure 4-10](#) to specify which portions of the database you would like to export.
- **Automatically**, by using the options in the Expert Data tab of the Database Options dialog box. See [Automatically Exporting Expert Analyzer Data](#), below.

The format of the exported file is described in detail in the *Expert Analyzer Output File Format* manual.

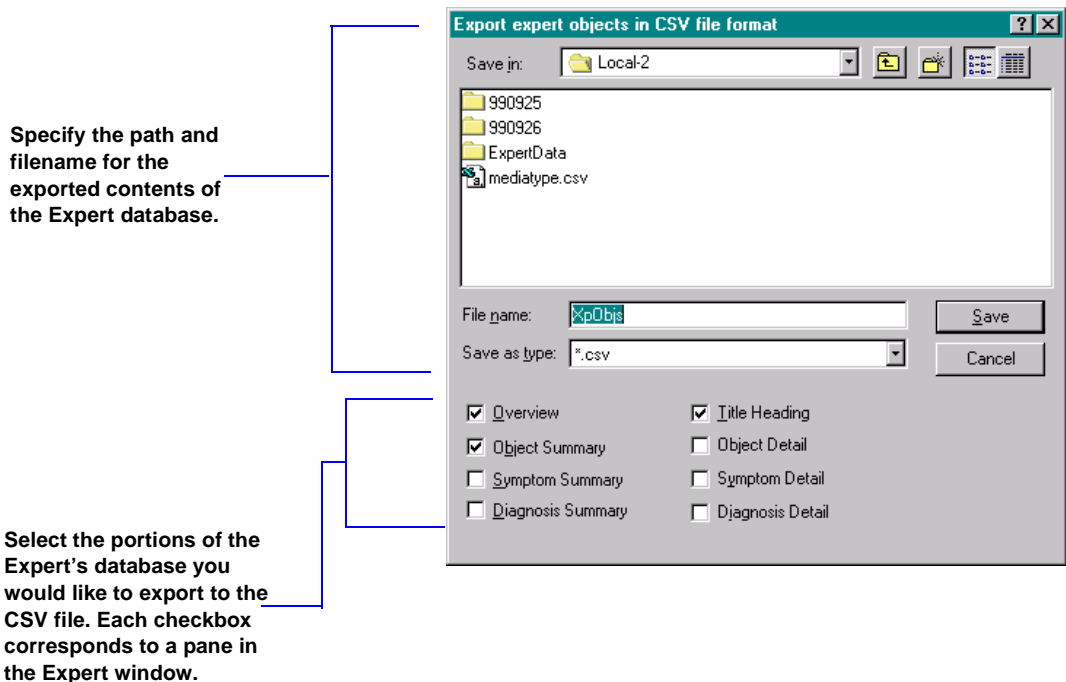


Figure 4-10. Exporting the Contents of the Expert Analyzer's Database

## Automatically Exporting Expert Analyzer Data

You can configure the Sniffer Pro to export the contents of the Expert Analyzer’s database automatically every time capture is stopped. You do so by enabling the **Log Expert Data** option in the **Expert Data** tab of the Database Options dialog box (Figure 4-11). Display this dialog box by selecting the **Options** command from the Sniffer Pro’s **Database** menu.

When the **Log Expert Data** option is enabled, the Sniffer Pro exports the Expert Analyzer’s database to a CSV file each time capture is stopped. The portions of the database exported depend on the options selected in the **Log Following Data** section of the **Expert Data** tab (Figure 4-11).

Automatically exported files are saved in the ExpertData subdirectory of the current adapter’s subdirectory in the Program Files\NAI\Program directory (each adapter defined in the Select Settings dialog box has its own subdirectory in this directory). For example, if the currently selected adapter’s name is Local-2, automatically exported files would be saved in the following directory:

\Program Files\NAI\Program\Local-2\ExpertData\yyymmddhhmmexpert.csv

As indicated above, saved files are named with the **yyymmddhhmm**expert.csv naming convention, where **yy**=year, **mm**=month, **dd**=day, **hh**=hour, and **mm**=minutes.

When this option is enabled, Expert data is exported automatically each time capture is stopped.

Select the portions of the Expert’s database you would like to export to the CSV file. Each checkbox corresponds to a pane in the Expert window.

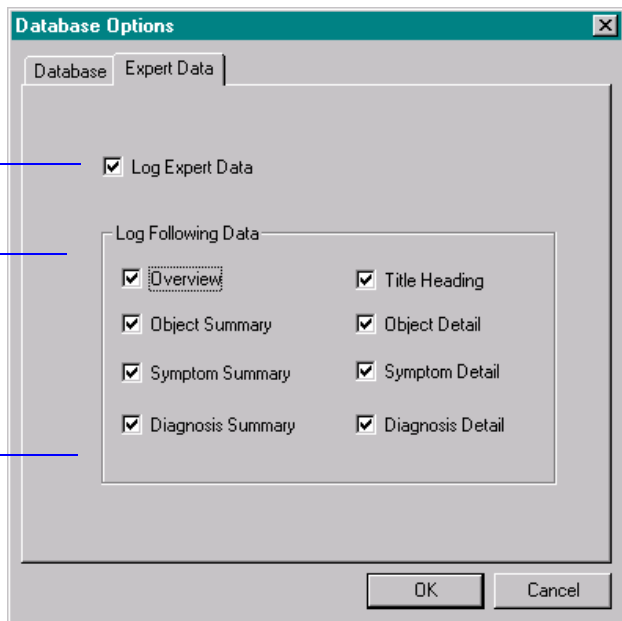


Figure 4-11. Configuring Automatic Export of Expert Data

Use *filters* to select the particular traffic you need for your network analysis so that you can precisely focus on the data you need to troubleshoot network problems and minimize the size of files you collect for historical records.

Use *triggers* to capture data while Sniffer Pro is unattended, such as on off-hours or weekends, or to start captures when specific events occur, such as alarm conditions.

## Defining Filters



[Define Filter Overview](#)

[Define Filter](#)

All filters used in Sniffer Pro are defined using the same procedure. The type of filter is determined by its use:

- When selecting what traffic to monitor, the filter becomes a *monitor filter*.
- When selecting what traffic to admit into the capture buffer, the filter becomes a *capture filter*.
- When selecting what data in the capture buffer to display, the filter becomes a *display filter*.
- When selecting what data will be used to start or stop capturing (using the trigger feature), the filter becomes an *event filter*.

---

✦ **TIP:** When you define a filter, you give it a name. You then apply a named filter to become a monitor, capture, display, or event filter. To easily differentiate different kinds of filters, use a distinctive naming convention.

---

To define a filter, select **Define Filter** from the **Monitor**, **Capture**, or **Display** menu. You can also click the  button (located in many Sniffer Pro windows). The Filter Settings dialog box opens and displays five tabs:


- The **Summary** tab shows the settings for the currently selected filter. This tab also displays the buffer size and the buffer action (stop capture or overwrite older data when buffer is full).
- The **Address** tab lets you set up filters based on network node addresses.
- The **Data Pattern** tab lets you set up filters based on data patterns.

- The **Advanced** tab lets you set up filters based on packet size, protocol, and error type.
- The **Buffer** tab lets you set capture buffer options.
- For WAN adapters (including the WANBook), the **SDLC**, **X.25**, **Frame Relay**, or **HDLC** tab let you specify various WAN packet types on which to filter. The exact tab available will depend on the setting of the Encapsulation option in the **Options** dialog box.
- For ATM adapters, the **ATM VPI.VCI** tab lets you set up filters on specific VCCs on the network using their VPI.VCIs. These filters are useful for setting up filters on PVCs.
- For ATM adapters, the **ATM Station Address** tab lets you set up filters on specific ATM end station addresses. These filters are useful for setting up filters on all SVCs in which a specified station takes part.

## Filtering by Address

Use the options on the **Address** tab of the Filter Settings dialog box to set up a filter to capture or display packets between up to ten pairs of network nodes by their addresses.

---

 **IMPORTANT:** To define a new filter, first click on the **Profiles** button and give the new filter a name. Then, configure your settings.

---

*Figure 5-1* shows the **Address** tab of the Filter Settings dialog box.

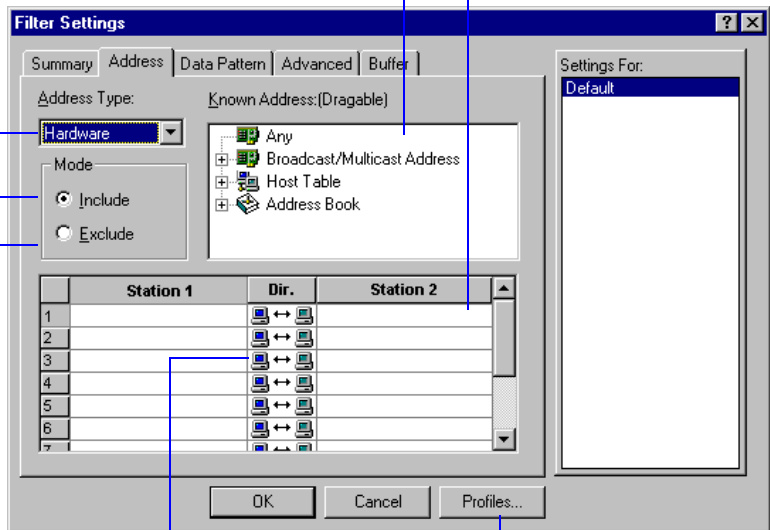
Drag and drop a symbolic address from the known address list into the Station 1 or Station 2 fields. Known addresses come from Broadcast Addresses, the Host Table, or the Address Book.

You can also just type in an address manually

Define the address as either a network hardware address (6 bytes in hexadecimal value) or a network IP or IPX address (4 octets)

Select to include or exclude packets that match the address specification

Select which direction the traffic flows by setting the *Dir* option



First, click to name the new filter

Figure 5–1. Setting Address Filters

## Filtering by Data Pattern

Use the **Data Pattern** tab to define a filter that will only capture or display packets that match a data pattern you specify. A data pattern filter can be simple, consisting of a single data pattern, or very sophisticated, involving multiple data patterns connected by Boolean operators AND, OR, and NOT.



*Define Filter Data Pattern Tab*

**NOTE:** A complex filter is limited to no more than 20 Boolean operators and data patterns.

A *data pattern* is:

- A particular sequence of bits
- The length of the sequence
- Its offset position within the packet.

The maximum data pattern length is 32 octets. You can specify the offset from the beginning of the packet or from the protocol boundary.

You can copy the data pattern for your filter from the display decode screen. To do this, select the packet *before* you invoke the define filter function. In the **Data Pattern** tab, select **Add Pattern**, then **Set Data**. This copies the data field from the selected packet into the data pattern fields, and calculates the offset and length.

To construct a complex data pattern filter, link data patterns using Boolean operators. The result is displayed in a tree-like diagram on the **Data Pattern** tab.

The **Data Pattern** tab displays the workspace for creating your filter, and displays the current data pattern equation. Buttons below the display control the process of defining the Boolean expression and data patterns.

*Figure 5-2* shows the **Data Pattern** tab of the Filter Settings dialog box.

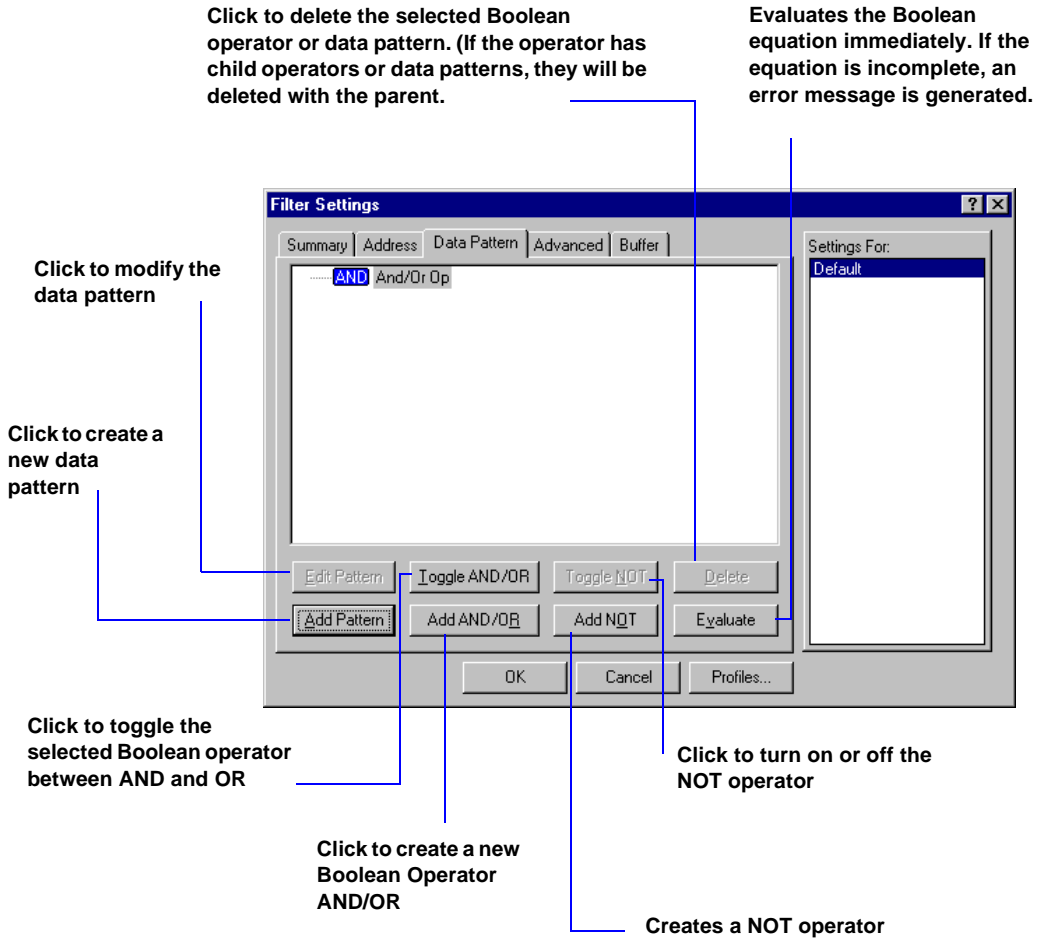


Figure 5–2. Setting Data Pattern Filters

## Filtering by Packet Size, Protocol, and Error Type



### *Define Filter Advanced Tab*

Use options on the **Advanced** tab to define a filter based on packet size, protocol type, or error type.

You can specify packets that are equal to, greater than, or less than a specific packet size, or in a range or outside of a range of packet sizes.

You can select one or more protocols or subprotocols to act as a filter. If the packet matches one of the selected protocol types, it will pass through the filter. (If no protocol is selected, Sniffer Pro captures *all* protocol types.)

---

**NOTE:** If a protocol you need is not defined in the protocol list, you can define your own protocol filter using the data pattern filter controls.

---



### *Protocol Interpreters*


---

**NOTE:** Not all protocols in the list are supported by the Expert. For a list of currently supported protocols for Expert, see the online Help.

---

Sniffer Pro captures and displays a full range of error packets, including CRC errors, runts, fragments, and so on. You can select one or more **Packet Types** to create an error-type filter. Packet types you select will be passed through the filter.

---

 **IMPORTANT:** To collect error packet information, you must install one of the NAI enhanced network drivers provided with Sniffer Pro.

---

*Figure 5-3* shows the **Advanced** tab of the Filter Settings dialog box.

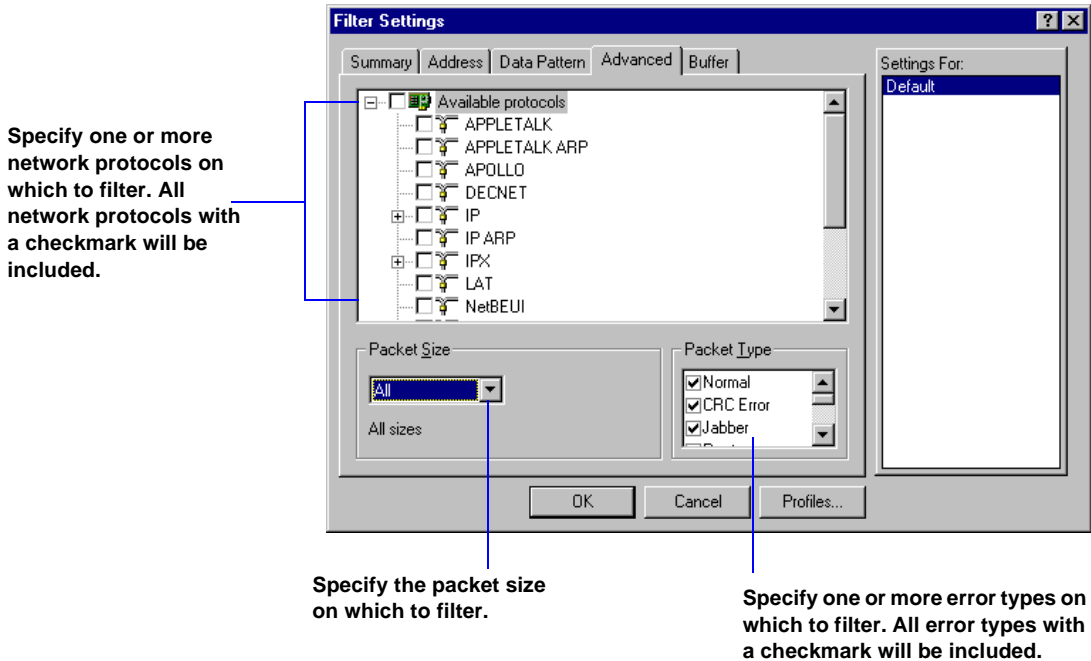


Figure 5–3. Setting Advanced Filters

## Setting Capture Buffer Options



### Define Filter Buffer Tab

Set options for the capture buffer on the **Buffer** tab. (These settings are used only if the filter is being used as a *capture filter*.) For a description of the capture buffer settings, refer to [Capture Buffer on page 3–3](#).

## Filtering on ATM VPI.VCIs

Use the **ATM VPI.VCI** tab to define filters to capture data on specific PVCs (Permanent Virtual Connections). *Figure 5-4* shows the **ATM VPI.VCI** tab. You can also set Protocol filters on each PVC using the dropdown lists in the **Proto Type** field.

**NOTE:** The **Include\Exclude** settings are not available for the ATM Book. PVC filters for the ATM Book are Include filters by default.



### ATM VPI.VCI Tab

In *Figure 5-4*, PVC filters have been set to capture traffic on VPI.VCI 0.5 (the standard signaling channel) and VPI.VCI 0.16 (the standard ILMI channel). Also, a PVC filter is set to capture only SPANS traffic on the PVC with the VPI.VCI 1.450.

Use the **Filter** field to specify whether you want to include or exclude the specified traffic (non-ATM book only).

Use the **VPI** and **VCI** fields to add the VPI.VCIs of the PVCs you would like to include or exclude from capture. Use the **Proto Type** field to apply a protocol filter to the selected PVC.

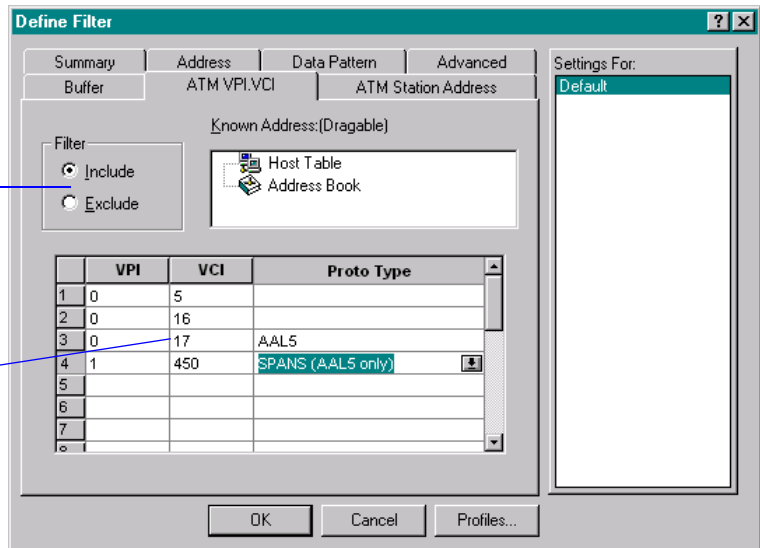


Figure 5-4. Setting ATM VPI.VCI Filters

## Filtering on ATM Station Addresses



### ATM Station Address Tab

Because SVCs (Switched Virtual Connections) are set up dynamically on different VPI.VCIs, you need a way to capture the data sent between different stations on the ATM network, regardless of the VPI.VCI on which the data is sent. The **ATM Station Address** tab lets you do this.

**IMPORTANT:** To define a new filter, first click on the **Profiles** button and give the new filter a name. Then, configure your settings.

Figure 5–5 shows the **ATM Station Address** tab of the Filter Settings dialog box.

Drag and drop a symbolic address from the known address list into the Station 1 or Station 2 fields. Known addresses come from Broadcast and Well-Known Addresses, the Host Table, or the Address Book.

You can also just type in an address.

Select to include or exclude packets that match the address specification

Select which direction the traffic flows by setting the *Dir* option

First, click to name the new filter

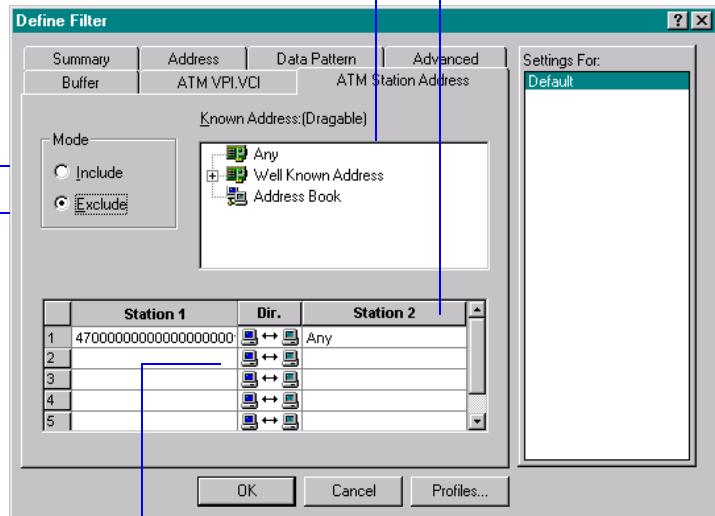


Figure 5–5. Setting ATM Station Address Filters

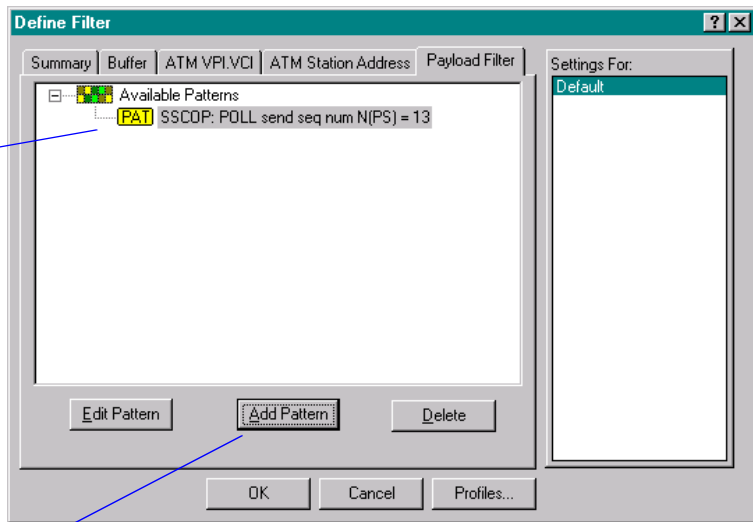
## Filtering on Payload Type (ATM Book Only)



*Define Filter  
Payload Filter Tab*

If you are using the ATM Book, you can use the Define Filter dialog box's **Payload Filter** tab to set filters to capture only those packets that match the data pattern criteria you specify. Pattern filters apply to the first 48 bytes of each captured cell (that is, the cell payload and not the 5 byte header of each 53 byte cell).

Select from available payload patterns.



Click here to open a dialog box in which you can add a new pattern. You can select frames from the Decode display and have them automatically added.

**Figure 5–6. Setting a Payload Filter (ATM Book Only)**

## Filtering by WAN\Synchronous Frame Types



*Define Filter SDLC Tab*

*Define Filter X.25 Tab*

*Define Filter Frame Relay Tab*

*Define Filter HDLC Tab*

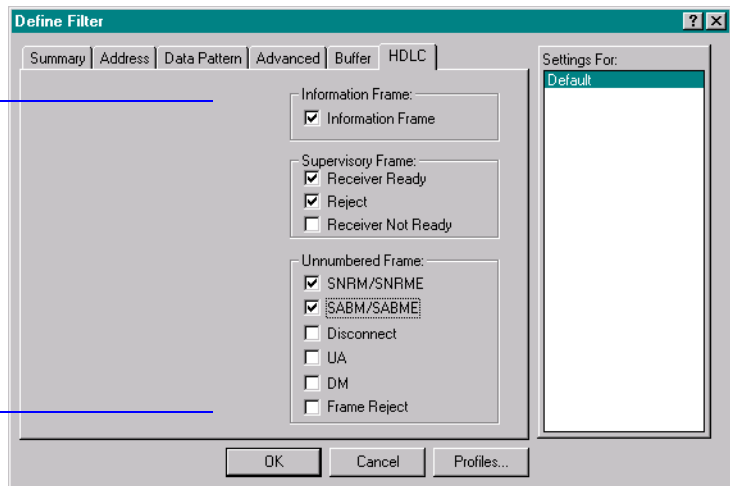
When a WAN\Synchronous adapter is selected as the current probe, a new tab appears in the Filter Settings dialog box. Depending on the encapsulation protocol currently selected in the Options dialog box, this tab can be one of the following:

- SDLC
- X.25
- Frame Relay
- HDLC

You use these tabs to select various frame types that you want either to include or exclude from capture. The frame types available as filters correspond to the currently enabled encapsulation protocol. For example, if you have selected HDLC/Router/Bridge as the encapsulation protocol, you can include or exclude HDLC Information Frames, Receiver Ready frames, Reject frames, and so on.

*Figure 5–7* shows the **HDLC** tab of the Filter Settings dialog box.

**Specify one or more packet types on which to filter. All packet types with a checkmark will be included.**



**Figure 5–7. Setting WAN\Synchronous Frame Type Filters**

# Defining Triggers



*Specifying a Capture Filter for a Trigger*

*Configuring Start and Stop Triggers for Packet Capture*

Triggers enable you to start and stop captures based on date and time, alarms, and specific network events. Use triggers to capture data while Sniffer Pro is unattended, such as on off-hours or weekends, or to start captures when specific events occur, such as alarm conditions.

You can define three kinds of triggers — *start triggers*, which will start a capture session, *stop triggers*, which will stop a capture session, and *start and stop triggers*, which do both. As with a filter, once you define a trigger and give it a name, you can reuse it whenever appropriate.

To define a trigger, select **Trigger Setup** from the **Capture** menu. The Trigger Setup dialog box opens (shown in *Figure 5–8*).

Click to specify which events to use as a start trigger (start time and date, threshold alarm, and/or event filter)

Specify what capture filter to use when the trigger event occurs

This picture graphically depicts your trigger definition

Define how to control packet capture: Start trigger, stop trigger, delay after trigger, or repeat mode

Click to specify which events to use as a stop trigger (start time and date, threshold alarm, and/or event filter)

Figure 5–8. Defining a Trigger

Sniffer Pro's *address book* lets you assign familiar, recognizable names for your network nodes. These symbolic names are used in place of six-byte hardware addresses, IP addresses, and ATM addresses in:

- Filter definitions
- The capture decode display
- The Expert display
- Host Table displays (both monitor and capture)
- Matrix displays (both monitor and capture)

## Creating an Address Book



### Address Book Entries

You create an address book to maintain a symbolic names table for your own network. You can enter names manually, import an external address table, or automatically discover names with the address book's autodiscovery feature.

To open the address book, select **Address Book** from the **Tools** menu or click the button in the main toolbar.

**Add a new address**

**Edit selected address**

**Delete selected address**

**Undo and redo previous action**

**Sort and unsort address book.**

Name	HW Address	Network Address	Type	Description
Finance	ETHER 00609737AE58	IP 11.11.11.1	Server	
Eng_21	ETHER 0020AF252FDD	IP 111.11.1.1	Printer Server	
Bob's PC	ETHER 006504545451	IP 206.94.93.12	WorkStation	

**Export table to spreadsheet**

**Autodiscover IP addresses and Domain names**

**Delete all entries.**


Figure 6-1. The Address Book

## Entering Names Manually

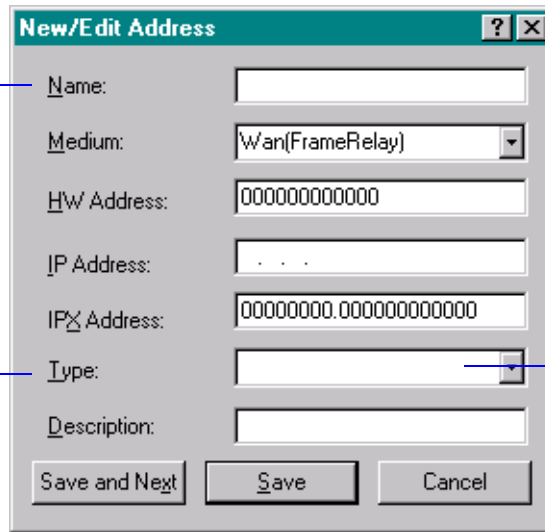


### Creating an Entry

You can build your own address book by getting hardware addresses and IP addresses from the host table.

To add a new address in the book, select **Address Book** from the **Tools** menu then click the **New Address** button  in the Address Book toolbar. The New/Edit Address dialog box opens, in which you can enter address information for a network node, see [Figure 6-2](#).

Specify the name, medium, hardware address, IP/IPX address, and type of network node in these fields.



A node Type can be:

- Workstation
- Server
- File Server
- Printer Server
- Router
- Bridge
- Hub

Figure 6-2. Entering Names Manually

## Importing Address Tables



### Importing Address Tables

Sniffer Pro lets you import address tables from other applications (such as NetXRay and WebXRay, and from local host files into the Sniffer Pro address book. The address tables must be in Comma Separated Value (CSV) format and must be imported into the address book using the Visual Basic scripts provided in the Sniffer Pro Program directory.

---

**NOTE:** You can have up to 5,000 entries in the address book.

---

To import an address table, select **Run Script** from the **File** menu. Select the appropriate script from the Sniffer Pro Program directory, then click **Open**. From the Open dialog box, select your .csv file and click **Open**.

## Autodiscovering Addresses and Names




### *Auto-discovering Network Addresses and Domain Names*


Sniffer Pro provides an autodiscovery feature that learns the following names and addresses automatically and saves them in the Address Book:

- A network node's IP address, its associated hardware address, and domain name
- A network node's NetBIOS name and hardware (MAC address)
- An IPX network node's Netware user name and hardware (MAC) address
- An ATM address seen on the signaling channel.

---

 **IMPORTANT:** During autodiscovery of Netware user names and MAC addresses, you must log in to a Netware Server from a DOS window and type the command `userlist /a`. This procedure enables Sniffer Pro to extract *login user names* and hardware addresses.

---

To use the autodiscovery feature, click the **autodiscovery** button  in the Address Book toolbar or click the right mouse button and select **Auto Discovery**. The Discovery Option dialog box opens, in which you select the type of address to resolve (see [Figure 6-3](#)).

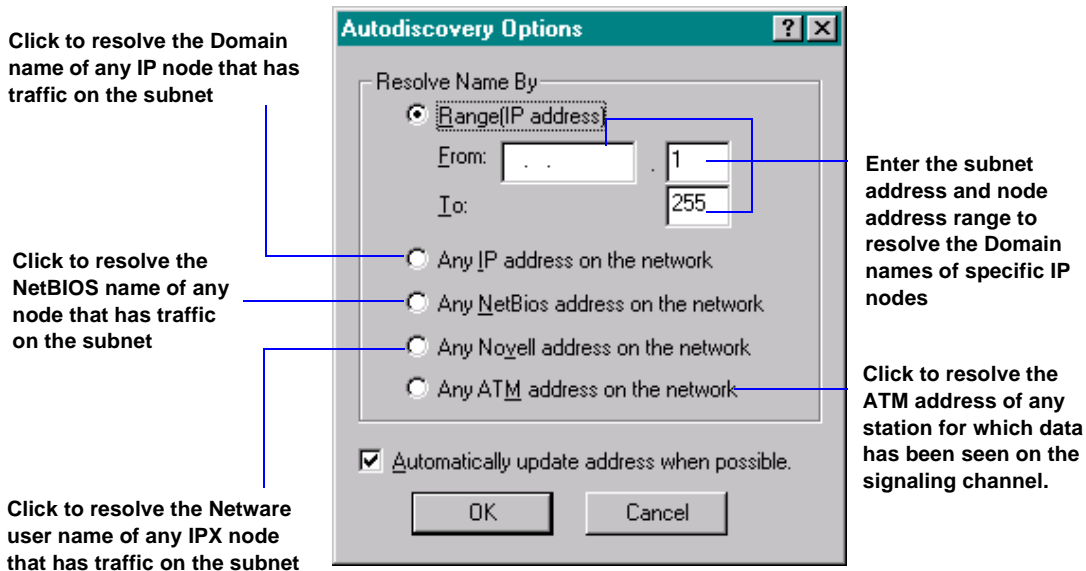


Figure 6–3. Setting Autodiscovery Options

## Configuring Autodiscovery for Routers

A router carries traffic between other subnets and the local segment where your Sniffer Pro resides, therefore, the router’s hardware address will be associated with any IP address that passes through it. This appears as a duplicate IP address to the autodiscovery process. When autodiscovery finds duplicate IP addresses, it adds an entry into the alarm log and sounds an audible alarm. To prevent these false duplicate IP address alarms, you must manually enter your IP network router’s IP address, hardware address, and domain name in the address book first, and specify the **Type** as Router.

## Netware 4.x Names and Addresses

If you are using Novell Netware 4.x, you can perform the following procedure *instead* of using the autodiscovery feature to compile a user list from a Netware server. (The list will include only users currently logged on to the server.)

1. From a DOS window, type the command:  
`nlist user /a > \install-directory\program\novell.txt`

**NOTE:** Replace *install-directory* with the directory in which Sniffer Pro is installed.

2. From the Sniffer Pro **File** menu, select **Run Script**.
3. Select ImpNovAddr.bas (located in the Sniffer Pro Program directory), then select the novell.txt file you created in [Step 1](#).


## Adding Discovered Addresses to the Address Book

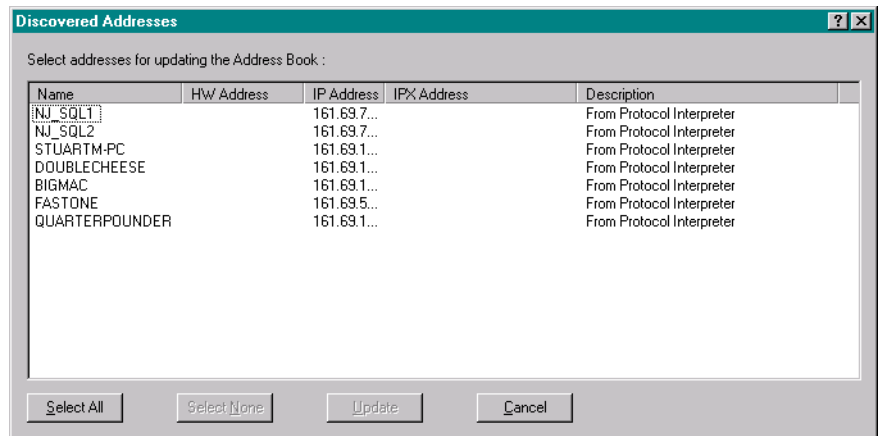


### Adding Discovered Addresses to the Address Book

During capture, the Expert analyzer automatically discovers name and address pairs on the network. You can add these discovered addresses to the analyzer's Address Book using the Discovered Addresses dialog box.

#### To add name and address pairs discovered by the Expert to the Address Book:

1. After a capture, display the Expert tab of the display window.
2. Click the **Discovered Addresses** button  in the Expert tab of the display window. The Discovered Addresses dialog box appears ([Figure 6-4](#)). It lists the new name and address pairs that have been discovered during the capture session. Only name and address pairs not already in the address book are listed.



**Figure 6-4.** The Discovered Addresses Dialog Box

3. Select the addresses in the list that you would like to add to the Address Book. You can use the standard Shift-Click and Ctrl-Click methods to select multiple entries. You can also use the **Select All** and **Select None** buttons to speed the selection process.
4. When you have finished selecting the addresses you would like to add to the Address Book, click the **Update** button.
5. The Address Book appears with the newly added entries

---

**TIP:** The **General** tab of the Options dialog box (accessed from the **Tools** menu) provides a means to ensure that you are reminded to save discovered name and address pairs. If you enable the **Discovered Address** checkbox in the **Prompt to save/update** list, the analyzer will always ask you if you want to save discovered addresses that have not yet been saved when you close a capture window.

---

Sniffer Pro's alarm features provide a comprehensive method of detecting and logging network alarm events:

- The Sniffer Expert generates alarms during data capture. It can log an event in the alarm log when it detects a symptom or diagnosis.
- The monitor's alarm manager starts automatically when you start Sniffer Pro. It logs an event in the alarm log when a user-specified threshold parameter is exceeded.
- The Switch Statistics application's Alarm Config tab provides a means of setting threshold-based alarms on different switch ports. When thresholds are exceeded, alarms are reported back to the Sniffer Pro.

You can configure Sniffer Pro to notify you by email, beeper, or pager when an alarm of a particular severity level occurs. An alarm can be assigned to one of five different severity levels: Critical/Diag, Major, Minor, Warning, or Informational.

## The Alarm Log



### *Alarm Log*

All alarm events (Monitor alarms and Expert alarms) are listed in the *alarm log*, which you display by selecting **Alarm Log** from the **Monitor** menu or by clicking the **Alarm** button .

For each alarm event, you see the type of node that triggered the alarm (for example, server, bridge, hub), a description of the alarm, the time it occurred, and the severity level.

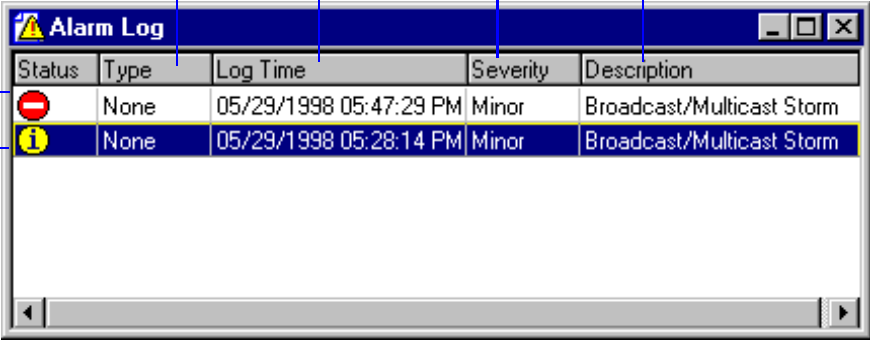
*Figure 7-1* shows the alarm log.

Type of node triggering the alarm (as defined in your address book)

Date and time the alarm was triggered

Level of severity assigned to this type of alarm (1 through 5)

Description of the error



Status	Type	Log Time	Severity	Description
	None	05/29/1998 05:47:29 PM	Minor	Broadcast/Multicast Storm
	None	05/29/1998 05:28:14 PM	Minor	Broadcast/Multicast Storm

The Status can be new or acknowledged (i). To acknowledge an alarm, right-click on the alarm entry and select Acknowledge.

Figure 7-1. The Alarm Log

## Setting Alarm Severity Levels

You can assign a severity level to both Monitor and Expert alarms (symptoms and diagnoses).

### Monitor Alarms



*Assign a Severity Level to an Alarm Event Type*

By default, Sniffer Pro defines four event types and assigns each one a severity level. You can change the default severity level assigned to each event to suit your specific network operating environment. *Table 7-1* lists the default severity levels.

Table 7–1. Default Severity Levels

Alarm Event	Severity Level
Threshold: Over upper limit	Critical
Address: Duplicate IP address	Critical
Address: Duplicate data in address book	Informational
Probe: Not responding	Minor

To change an alarm severity level, select **Options** from the **Tools** menu, then click the **Alarm** tab. Click the **Define Severity** button to open the Define Severity dialog box (Figure 7–2). Click on the **Severity** cell for an alarm to display a list of severity-level options. Select the one you want to use and click **OK**.

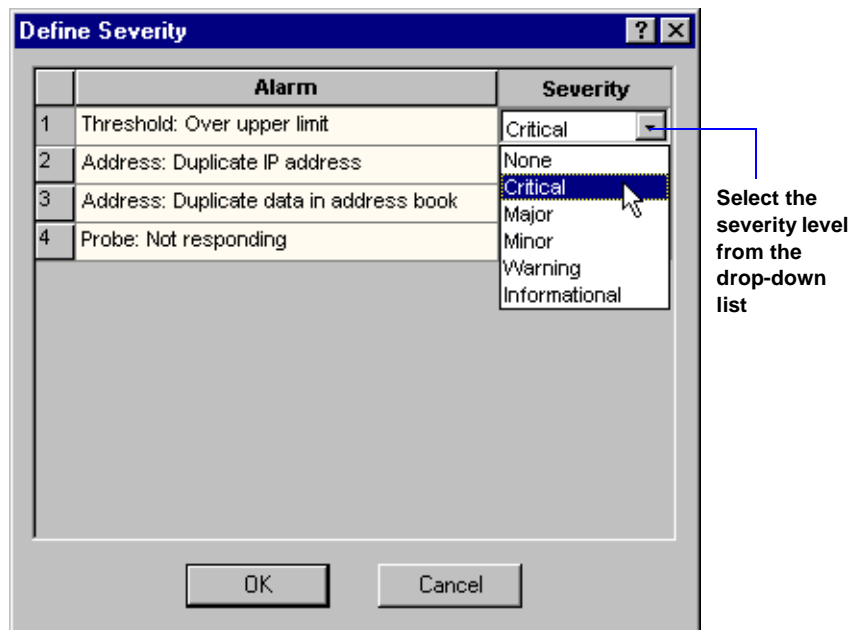


Figure 7–2. Setting Severity Levels for Monitor Alarms

# Expert Alarms



## Assigning Severity Levels to Expert Alarms

Expert alarms (symptoms and diagnoses) can be assigned one of five different severity levels: Critical/Diag, Major, Minor, Warning, and Informational. The severity level for a symptom or diagnosis displays in the summary pane of the Expert window. It is also recorded in the alarm log if the alarm setting **Alarm Logged** is set to YES in the **Tools/Expert Options/Alarms** tab.

**NOTE:** The alarm must be recorded in the alarm log for notification to take place. Refer to [Setting an Alarm Notification Action on page 7-6](#).

To change the severity level for an Expert alarm, select **Expert Options** from the **Tools** menu and click the **Alarms** tab. [Figure 7-3](#) shows the Alarms tab.

Click to expand/collapse all Expert layers

1. Click the + to open an Expert layer and display all alarms

2. Click the + to display an alarm's settings

Alarm Logged must be set to Yes to record the alarm in the alarm log.

3. Click the Value cell for the severity to display the drop-down box.

4. Click the drop-down box to display the severity levels. Select the one you want to use.

0	1	Description	Value
		ATM App	
		ATM Flow	
		ATM Cnx	
		ATM Host	
		Global	
		Bad CRC	Minor
		Broadcast/Multicast Storm	40, Minor, Logged
		Broadcast/Multicast Storm Diag	120, Critical/Diag, Log
		Severity	Critical/Diag
		Alarm Logged	Yes
		Broadcast Frames/sec	120
		Collisions over threshold	10, Minor
		LAN overload	50%, Minor
		LAN overload percentage	20%, Critical/Diag, Log
		Spanning Tree Topology Change	Minor
		VLAN Not Operational	Minor

Figure 7-3. Setting Severity Levels for Expert Alarms

---

## Setting Alarm Notification Actions



### *Define Alarm Notification Actions*

Each severity level that can be assigned to an alarm (Critical/Diag, Major, Minor, Warning, and Informational) can be associated with up to four alarm notification actions. These notification actions can be enabled for specified time periods within a day, and on specified days of the week. When an alarm is triggered, Sniffer Pro can:

- Sound an audible alarm signal
- Send email
- Call a beeper number
- Call a pager number with alarm text attached
- Invoke a Visual Basic script to open an application or send an alarm notification as an SNMP trap to an SNMP console

---

**NOTE:** You must have a modem (with a functioning phone line) attached to your computer to call a beeper or pager.

---

To set up a notification action, select **Options** from the **Tools** menu and select the **Alarm** tab. Click **Define Actions** to open the Define Actions dialog box (*Figure 7-4*). Click **Add** and select the radio button for the type of alarm response you want. A wizard will guide you through the setup procedure.

---

**NOTE:** Expert alarms must be recorded in the alarm log for notification to take place. Refer to *Expert Alarms on page 7-4*.

---

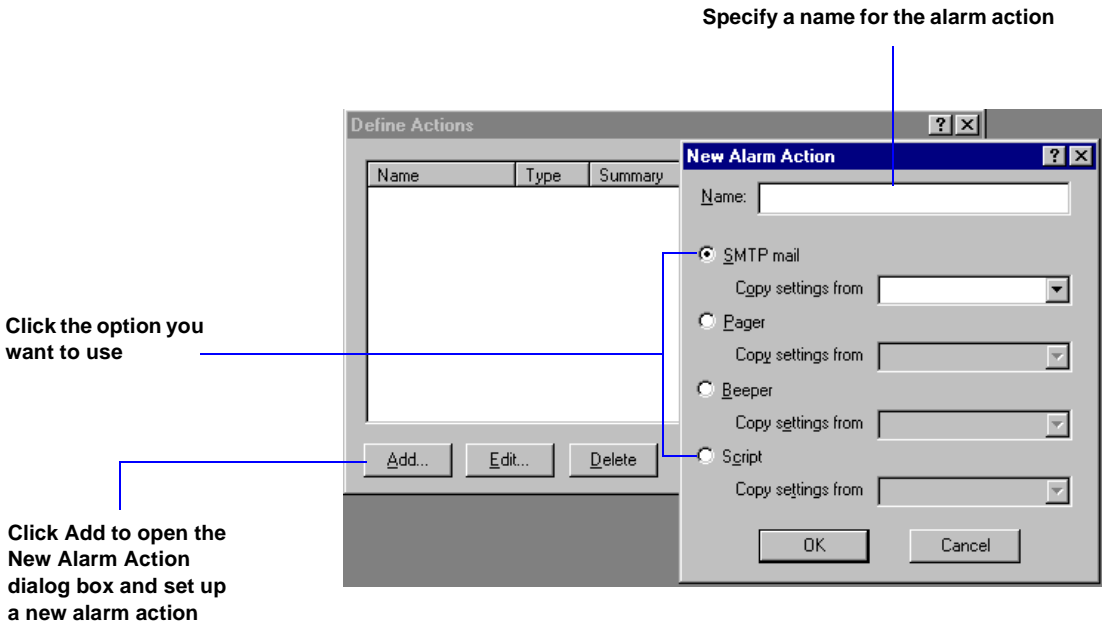


Figure 7–4. Setting an Alarm Notification Action

## Enabling Alarm Actions

After you complete the definition of an alarm action, you must assign it to a *severity level*. Up to four actions can be assigned to a severity level. When an alarm of a particular severity level occurs, all actions assigned to it are executed (unless disabled by time and date settings).



*Assign Alarm Actions*

---


**NOTE:** You must *enable* alarms for alarm actions to take place. Check the **Enable New Alarm** check box on the **Alarm** tab to enable alarm actions.

---

## Alarm Beeps and Sounds



*Define an Audible Alarm*

By default, Sniffer Pro makes a single beep sound when an alarm occurs. If you prefer another sound, you can replace the standard beep with any .wav sound file. To do this, click the  button on the **Alarm** tab and select the file.

Sniffer Pro includes a set of common tools that you can use to identify and troubleshoot IP network problems. These tools are *Ping*, *Trace Route*, *DNS Lookup*, *Finger*, and *Who Is*. You can access them from the **Tools** menu.

This chapter describes the tools provided with Sniffer Pro and discusses how to add your own tools.

## Ping

Use Ping to identify the availability of an IP host node on the network.

Ping utilizes the ICMP protocol's mandatory ECHO REQUEST datagram to elicit an ICMP ECHO RESPONSE from a host or network gateway that you specify.

- If the host responds, Ping displays the number of bytes sent and received, the response time, and the TTL (Time to Live).
- If there is no response for the defined timeout period, Ping displays the message Error: Request timeout in the Ping log window.



*Ping*

The default timeout period is 300 milliseconds. You can adjust it to an appropriate value for your network conditions.

*Figure 8-1* shows the Ping log window.

Click to check the Ping application version number

Click to specify the host name of the node you want to ping and the timeout period

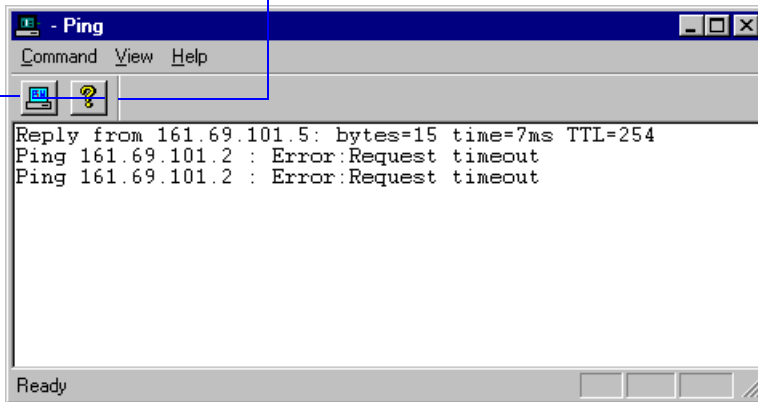


Figure 8-1. The Ping Log Window

## Trace Route



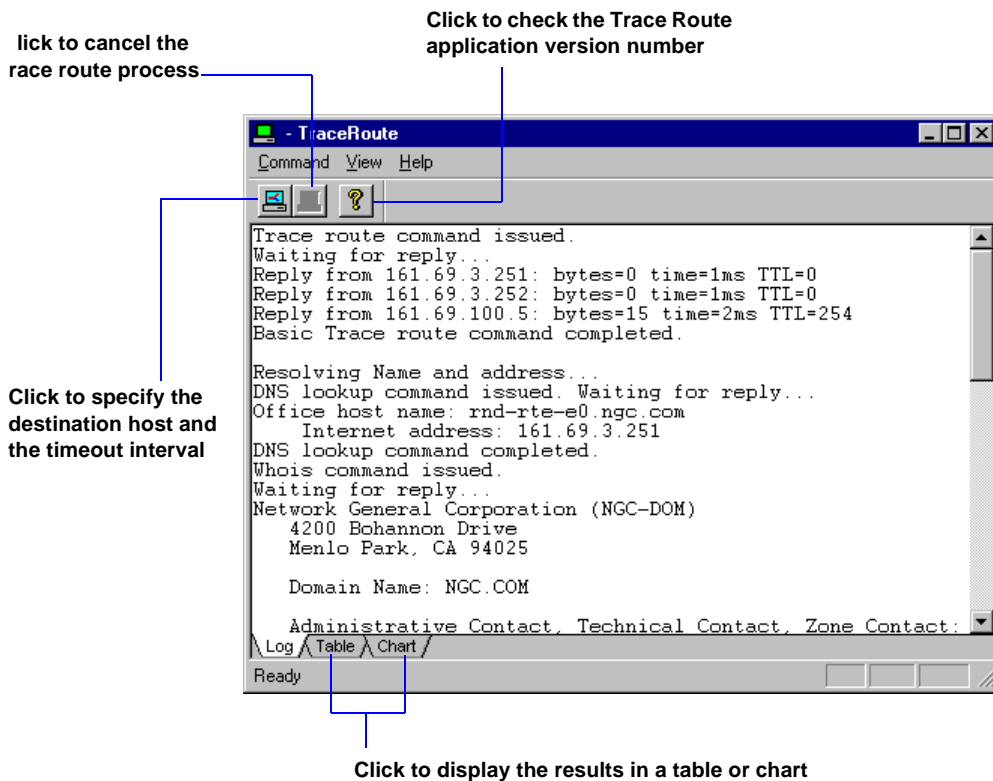
### Trace Route

Use Trace Route to identify all the intermediate router IP addresses and access time delays between your Sniffer Pro and a destination host.

You specify the IP address or DNS name of your destination host and a time-out interval (the default is 300 milliseconds). Trace Route sends out ICMP Trace Route packets. Routers along the way report back, and Trace Route builds and displays a Trace Route log, showing the path between your PC and the destination host.

When the trace route process completes, Trace Route issues a DNS Lookup and displays the results in the Trace Route log window. You can also display the results in a table or a chart by clicking the **Table** or **Chart** tab at the bottom of the Trace Route log window.

*Figure 8-2* shows the Trace Route log window.



**Figure 8-2. The Trace Route Log Window**

# DNS Lookup



Use DNS Lookup to find the domain name of an IP address, or vice versa. DNS Lookup sends a query to the DNS host and displays the results of the query in the DNS Lookup log window, see [Figure 8-3](#).

## DNS Lookup

Click to check the DNS Lookup application version number

Click to specify the domain name or IP address

Click to cancel the lookup process

The screenshot shows a Windows-style application window titled "DnsLookup". The window has a menu bar with "Command", "View", and "Help". Below the menu bar is a toolbar with three icons: a globe, a document, and a question mark. The main area of the window is a text log with the following text: "DNS lookup command issued. Waiting for reply...", "Office host name: atlantis.ngc.com", "Internet address: 161.69.100.1", and "DNS lookup command completed.". At the bottom left of the window, the status bar says "Ready". Three blue lines with text labels point to the toolbar icons: the question mark icon is labeled "Click to check the DNS Lookup application version number", the globe icon is labeled "Click to specify the domain name or IP address", and the document icon is labeled "Click to cancel the lookup process".

Figure 8-3. The DnsLookup Log Window

# Finger

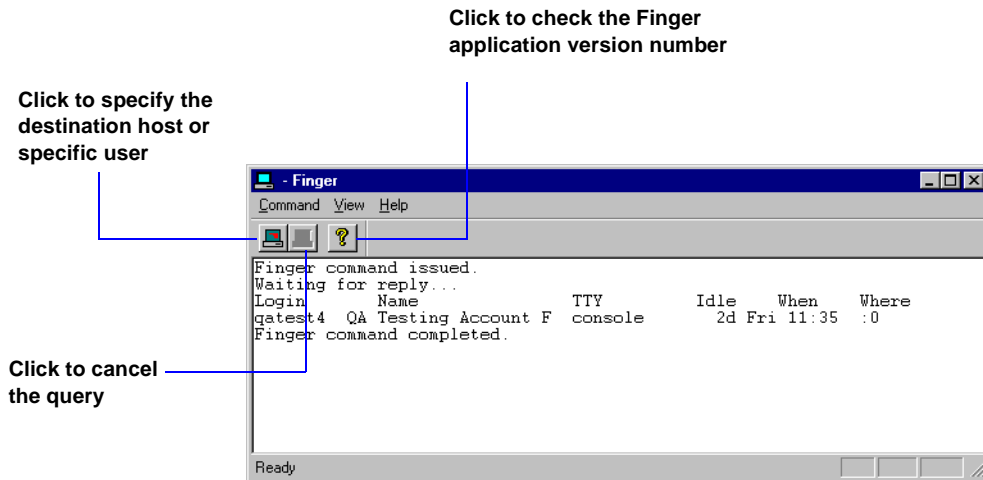


## Finger

Use Finger to display information about each logged-in user on a specified host. You can enter the host name or IP address.

To query for a particular user, enter a username in the **Query** field. To see all users, leave the **Query** field blank.

Finger displays the results of its query in the Finger log window, see [Figure 8-4](#).



**Figure 8-4. The Finger Log Window**

# Who Is



## Whois

Use Who Is to search for a TCP/IP directory entry for a registered domain name, user's name, or user ID.

You specify the target for the Who Is search in the **Query** field. Enter:

- *name.dom* for a domain; for example, netscape.com
- *Firstname Lastname* or *Lastname, Firstname* for a registered user; for example, Mary Smith or Smith, Mary
- *userid* for a user ID; for example, eric\_hua

You can also restrict the search to a particular server by specifying the server in the **Server** field.

The results of the search are displayed in the WhoIs log window, see [Figure 8-5](#).

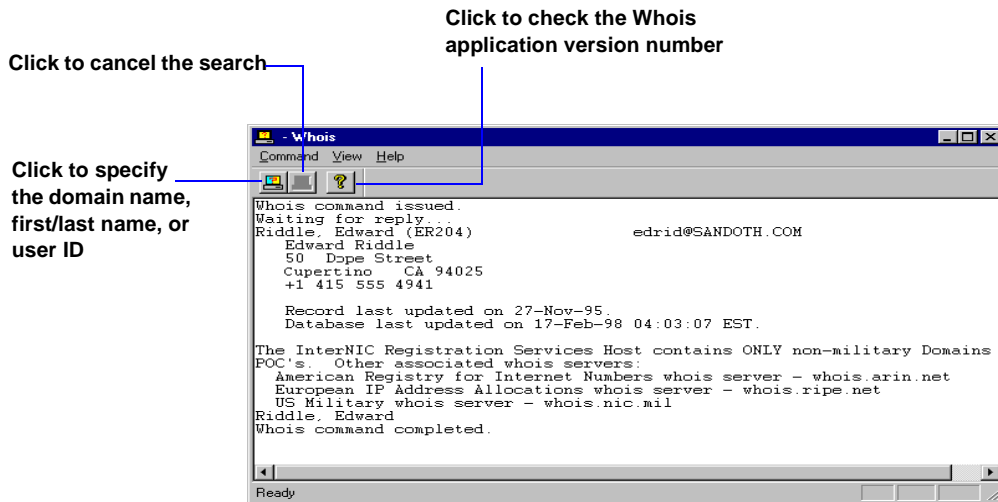


Figure 8-5. The Whois Log Window

## Adding Tools to the Tools Menu



[Adding Tools to the Tools Menu](#)

[Removing Tools from the Tools Menu](#)

In addition to the standard set of Sniffer Pro tools provided, you can add your own tools to the **Tools** menu. A tool can be any Windows or DOS executable file currently installed or accessible to your machine.

When adding a new tool, specify the path, filename, and any command-line parameters needed to start the program.

To add a tool, select **Customize User Tools** from the **Tools** menu. The Customize dialog box opens (*Figure 8-6*). Enter the requested information in the fields provided.

To assign a shortcut key (Alt + t, *letter*), place an ampersand character (&) in front of an appropriate letter in the name. The program automatically assigns an Alt + *number* shortcut as well, visible to the right of the menu item.

To change the order of the tools in the **Tools** menu, select a tool in the **Menu Contents** box and click **Move Up** or **Move Down**.

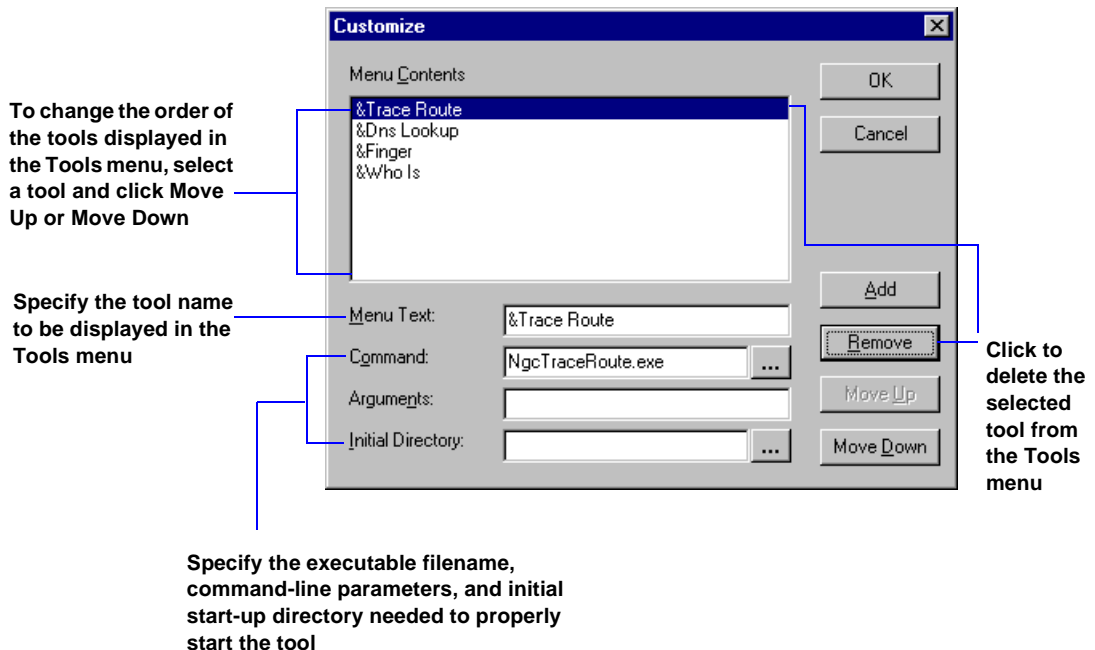


Figure 8-6. Adding Tools to the Tools Menu



Use the Packet Generator to transmit test packets on your network so that you can:

- Reproduce network problems to troubleshoot and verify fixes for your network equipment or applications
- Generate a level of network traffic load to simulate realistic network conditions and test your equipment or applications

---

**⚠ WARNING:** Transmitting packets to a real network may produce unexpected results which may cause difficulties. Make sure you transmit only *benign* packets to a production network, or isolate your test network from the production network before proceeding with packet generation.

---

The packet generator shares CPU resources with other Sniffer Pro operations. You can generate traffic, capture packets, and monitor the network load at the same time. However, running multiple processes at the same time can impact performance.

---

**🔦 IMPORTANT:** The ATM Packet Generator is different from the Packet Generator used by other network topologies (Ethernet, token ring, and so on). It is described on [page 9-5](#).

---

## Using the Standard Packet Generator



### [Packet Generator](#)

To start the Packet Generator, select **Packet Generator** from the **Tools** menu.

From the Packet Generator, you can transmit a single packet, either one that you create or one that you have captured from the network. You can also transmit the entire contents of the capture buffer or a capture file.

You can send a packet, the capture buffer, or a capture file a single time, a specified number of times, or continuously. If you send multiple packets, or you send a packet continuously, you can specify the time delay between each packet (either in milliseconds, or as a percentage of line utilization you would like the transmitted packet to achieve).

The packet generator has two views. The *animation view* shows when packets are being transmitted. The *detail view* shows the progress of packet transmission in detail.



## Transmitting a Single Packet

Before transmitting a packet, you must prepare the message you want to send. You can create a packet, use a captured packet, or use a captured packet that you have modified.



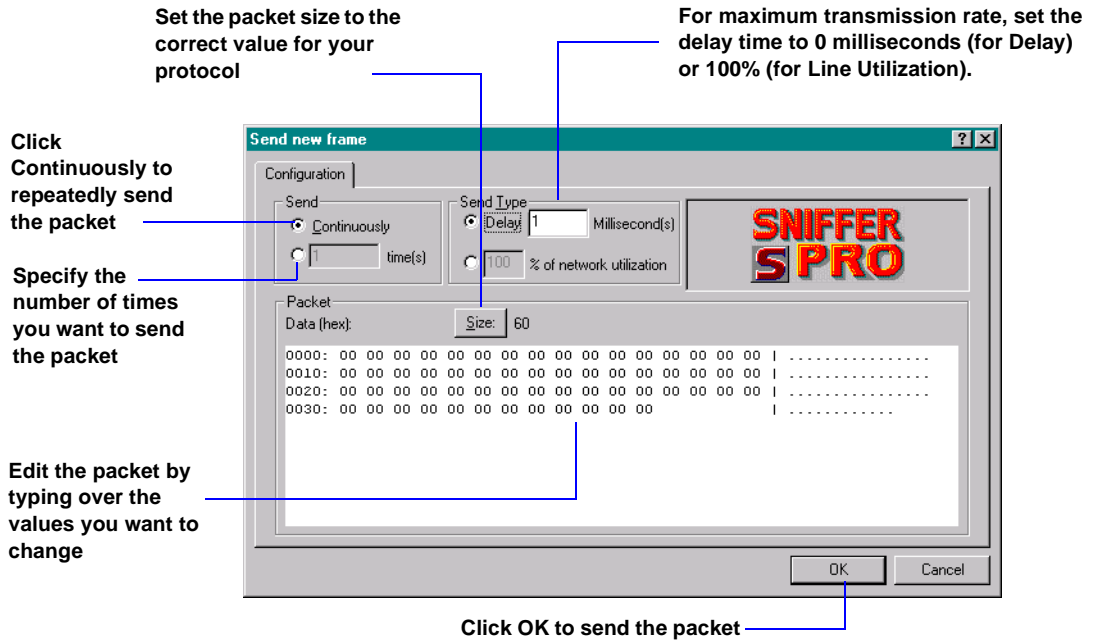
[Sending a Single Packet](#)

[Editing Packet Contents](#)

- To create a new packet, click the  button in the Packet Generator window to open the Send new frame dialog box. You can directly edit the hexadecimal display on the **Configuration** tab.
- To select an existing (captured) packet or edit an existing packet, you must first select the packet from the summary pane of the decode display. Then, click the  button in the Packet Generator window to open the Send current frame dialog box. You can edit the hexadecimal display on the **Configuration** tab.

You can control how you want to send the packets by selecting the options in the dialog box.

*Figure 9-1* shows the Send new frame dialog box (the Send current frame dialog box is identical).




**Figure 9–1. Transmitting a Single Packet**

**NOTE:** The maximum rate of transmission depends on the size of the packet, the performance of your network, your computer's CPU speed, and whether any other processes are running on your system.

## Transmitting the Capture Buffer or a File



### *Playing Back a Capture File*

To send the current capture buffer or a capture file, you must first display the contents. To display the current buffer, select **Display** from the **Capture** menu. To display a capture file, select **Open** from the **File** menu. Then, click the  button in the Packet Generator window. The Send current buffer dialog box displays information about the buffer/file contents and lets you control how you want to send the packets.

*Figure 9–2* shows the Send current buffer dialog box.

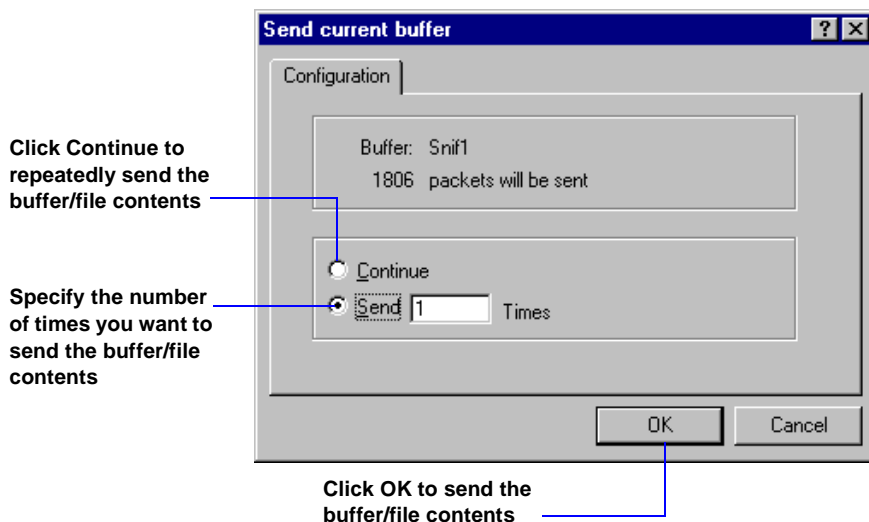


Figure 9–2. Transmitting the Current Buffer Contents

## Using the ATM Packet Generator



*TM Packet  
enerator  
view*


To start the ATM Packet Generator, make sure that you currently have the ATM adapter selected for monitoring. Then, select **Packet Generator** from the **Tools** menu.

From the ATM Packet Generator, you can transmit a single packet, either one that you create or one that you have captured from the network. You can also transmit the entire contents of the capture buffer or a capture file.

You can send a packet, the capture buffer, or a capture file a single time, a specified number of times, or continuously. If you send multiple packets, or you send a packet continuously, you can specify the time delay between each packet.

The ATM Packet Generator window has two tabs. The **Detail** tab shows the progress of packet transmission on a per-port basis. The **Connections** tab shows the progress of packet transmission on a per-connection basis (detailed statistics for each VPI.VCI on which the ATM Packet Generator is transmitting).

---

 **IMPORTANT:** The ATM Packet Generator is only supported for use with the Zeitnet ATM adapter card. It is not supported for use with the ATM Book.



---



## Transmitting a Single Packet

Before transmitting a packet, you must prepare the message you want to send. You can create a packet, use a captured packet, or use a captured packet that you have modified. You can also open a Packet Setup file to transmit. Packet Setup files include a both a saved packet and a set of options defining how that packet should be transmitted.



*Generating Traffic  
in Single Frame  
Mode*

- To create a new packet, click the  button in the Packet Generator window to open the Packet Setup dialog box. You can directly edit the hexadecimal display in the Packet Setup dialog box.
- To select an existing (captured) packet or edit an existing packet, you must first select the packet from the summary pane of the decode display. Then, click the  button in the Packet Generator window to open the Packet Setup dialog box. You can directly edit the hexadecimal display in the Packet Setup dialog box.

- To select a Packet Setup file to transmit, click either the  button or the  button to open the Packet Setup dialog box. Then, select the Open command from the Setup menu to open your saved Packet Setup file.

You can control how you want to send the packets by defining the options in the Packet Setup dialog box. The Packet Setup dialog box contains four tabs:

- The **General** tab lets you specify how many times you would like to send the selected packet and on which ports. It also lets you edit the data field of the packet to be sent.
- The **Rate** tab lets you specify the speed at which the selected packet will be transmitted.
- The **Advanced** tab lets you set various advanced options for the packet to be generated, including whether to generate random packet sizes.
- The **ATM** tab lets you specify the value of the GFC field, PTI field, and CLP bit in traffic to be transmitted. In addition, you can also specify whether to transmit cells or frames, on which VPI.VCIs to transmit the packet, and set traffic shaping parameters for the selected VPI.VCIs.

*Figure 9-1* shows the ATM tab of the Packet Setup dialog box (the dialog box is the same regardless of how you display it).

Specify the value of the GFC field, PTI field, and CLP bit in the cell headers of the packet to be transmitted (in hex, decimal, or binary).

Specify on which VPI.VCIs to transmit the selected packet. You can transmit on a single specified VPI.VCI or click the List button to create a list of up to 15 VPI.VCIs on which to transmit. You can also use the Address Book to select known VPI.VCIs.

Specify traffic shaping parameters to control the rate at which the selected packet will be transmitted. Traffic shaping parameters are only used if the Traffic shaping option is enabled on the Rate tab

Specify whether to transmit raw cells or AAL5 frames.

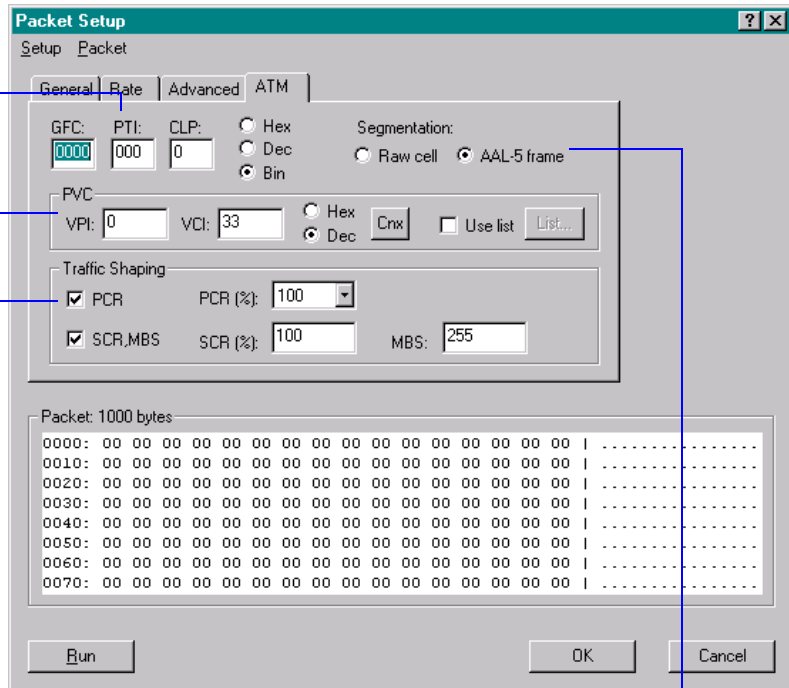


Figure 9–3. Transmitting a Single Packet with the ATM Packet Generator


**NOTE:** The maximum rate of transmission depends on the size of the packet, the performance of your network, your computer’s CPU speed, and whether any other processes are running on your system.

## Transmitting the Capture Buffer or a File



### Generating Traffic in Buffer Mode

In buffer mode, the ATM Packet Generator sends the contents of an open capture buffer or of a saved trace file. Before transmitting a buffer, you must configure the buffer you want to send. You configure the buffer to send in the Buffer Setup dialog box. You can display this dialog box in any of the following ways:

- Select the **Packet Generator** command from the Sniffer Pro's **Tools** menu. In the Packet Generator window that appears, click on the **Send Buffer** button .
- From the Sniffer Pro's Decode display, right-click anywhere to display a context menu. In the context menu that appears, select the **Send Buffer** option.

Regardless of which method you choose, the Buffer Setup dialog box appears. The Buffer Setup dialog box lets you configure the buffer to be transmitted – which buffer to send, how often it will be sent, on which ports it will be sent, and so on. The Buffer Setup dialog box has three tabs:

- The **General** tab lets you specify how many times you would like to send the selected buffer and on which ports.
- The **Rate** tab lets you specify the speed at which the selected buffer will be transmitted.
- The **ATM** tab lets you overwrite the headers of the cells in the selected buffer with your own custom headers. You can also choose whether to transmit the buffer on the VPI.VCIs found in the buffer itself or to send it only on your own custom selected VPI.VCIs.

Each of these three tabs shows the same information at the bottom allowing you to select the File or Buffer which you would like to transmit:

- Select the **File** option to transmit a saved ATM trace file. Click the Browse button to display a common Browse dialog box in which you can navigate to the trace file to be transmitted.
- Select the **Buffer** option to transmit a currently open capture buffer. The drop down list includes all currently open buffers and trace files.

*Figure 9-2* shows the Buffer Setup dialog box.

Use these fields to overwrite the headers of the cells in the selected buffer with your own custom headers.

Specify whether to transmit the buffer on the VPI.VCIs found in the buffer itself or to send it only on your own custom selected VPI.VCIs. If you select to overwrite the VPI.VCIs found in the buffer, you can transmit on a single specified VPI.VCI or create a list of up to 15 VPI.VCIs on which to transmit.

Select the file or buffer to transmit.

Figure 9–4. Transmitting the Current Buffer Contents (ATM Packet Generator)

## Using Packet Setup Files and Buffer Setup Files



### *Saving Packets and Packet Setup Files*


### *Saving Buffer Setup Files*

The ATM Packet Generator lets you save Packet Setup Files and Buffer Setup Files containing different sets of definitions for the various options in the ATM Packet Generator dialog boxes. Packet and Buffer Setup files make it easy to apply carefully-defined settings to a new packet or buffer.

- You save Packet Setup files using the **Save as** command from the **Setup** menu in the Packet Setup dialog box.
- You save Buffer Setup files using the **Save as** command in the **Setup** menu of the Buffer Setup dialog box.

## Using Scripts To Generate Traffic

The ATM Packet Generator provides a sophisticated scripting utility that lets you build complex combinations of saved packets and buffers to transmit onto the network. You can also use various override capabilities to apply different Packet Setup files and Buffer Setup Files to given

packets and buffers. You set up a Packet Generation Script by clicking the Send Script button  on the Packet Generator's toolbar to display the Send Script dialog box.

Scripts consist of a series of steps. Each step can be either a transmitted packet or a transmitted buffer. You create a list of steps by adding packet steps and buffer steps sequentially in the Script Setup dialog box. You can specify that each step run a certain number of times. You can also control the delay between each iteration of a given step (**Step Run Delay**), the delay between the steps themselves (**Step Delay**), and the delay between each run (**Run Delay**). A “run” consists of the entire series of steps in the list.

The figure below shows the Script Setup dialog box for the sample `myscript.scs` script.

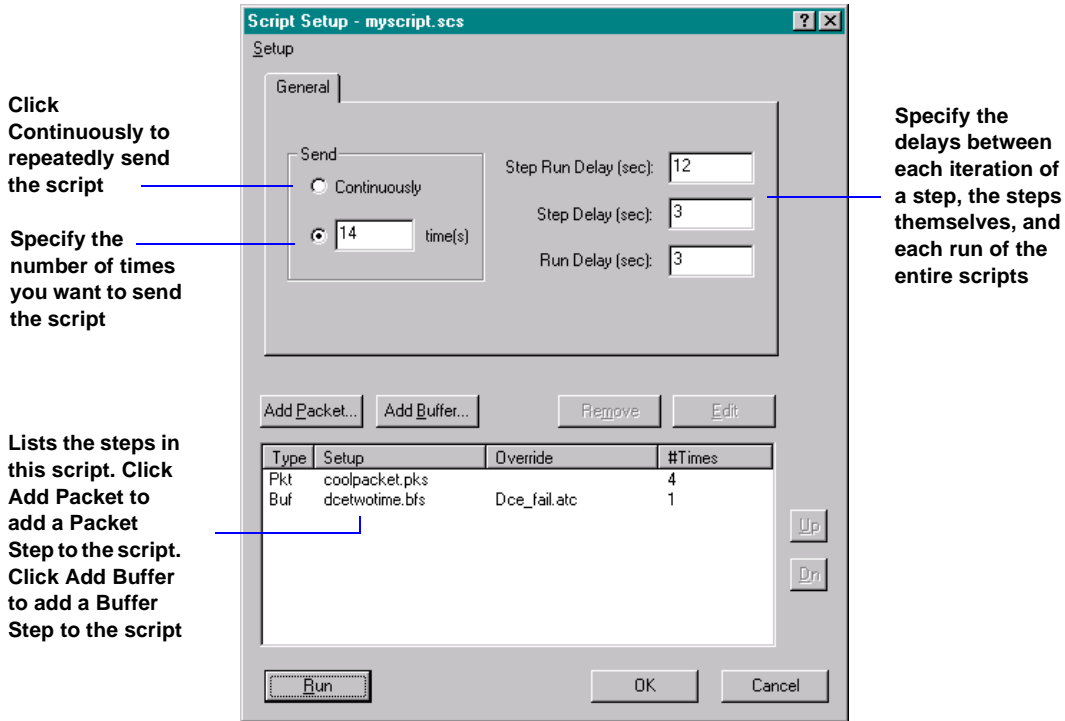


Figure 9–5. Transmitting a Script

## Saving Script Files

You can save your script files so that you can use them over and over again. Save script files by selecting the **Save As** command from the **Setup**

menu in the Script Setup dialog box. Then, when you want to open your saved script file to use it again, use the **Open** command in the **Setup** menu in the Script Setup dialog box. Script files are saved with a .SCS extension.




# Using the Sniffer Reporter Agent with Sniffer Pro

# 10

The Sniffer Reporter Agent is an optional application provided by Network Associates for generating a wide variety of customizable reports based on data collected by the Sniffer Pro application.

You can launch the Sniffer Reporter Agent application from within Sniffer Pro by selecting the **Reporter** option from the Sniffer Pro's **Tools** menu.

Additionally, if you have installed the Sniffer Reporter Agent on the Sniffer Pro PC, the Reporter's icon  appears in the toolbar for each of the following monitor applications:

- Matrix
- Host Table
- Protocol Distribution
- Global Statistics

You can click the Reporter's icon to launch the setup dialog box for a report based on the data collected by the corresponding monitor application.

For more information on using the Sniffer Reporter Agent, see the documentation and online help accompanying your product shipment.



# Network Adapters and Settings

# 11



## Select Network Adapter

### Overview of the WAN Sniffer Pro

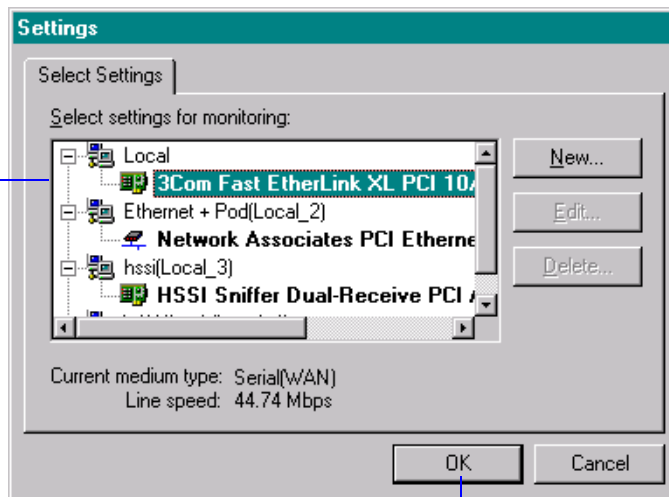
If you have more than one NDIS-compliant network interface card (adapter) installed in your system, you can select which card Sniffer Pro will use.

If you have multiple adapters attached to different network segments, you can select which segment Sniffer Pro will monitor by switching from one adapter to another.

In addition, you can launch multiple instances of Sniffer Pro, setting each one to use a different adapter or the same adapter. In this way, you can monitor several segments at once.

To select an adapter, click **Select Settings** in the Files menu. The Settings dialog box opens (see [Figure 11-1](#)). It contains the local agents you have defined for this Sniffer Pro PC. You can either select a previously defined local agent as the target network for the Sniffer Pro to monitor, or you can click the **New** button to define a new local agent to use for monitoring.

Select the network adapter from the display



Click OK

Figure 11-1. Selecting a Network Adapter

# Creating Sniffer Local Agents



*Monitoring Two or More Network Adapters Concurrently*

*Maintaining Multiple Sniffer Pro Settings Files*

*Defining a New Probe Using the SnifferBook*

*Defining a New Probe Using the Full Duplex Pod*

To run multiple instances of Sniffer Pro, you create separate entities, called *local agents*. A local agent can be thought of as a set of settings — each local agent holds session information, such as the address book, capture filter settings, and packet display options. Each local agent has independent configuration information, so it can be used to globally reconfigure Sniffer Pro when moving from one network to another, one segment to another, or for setting up the options for specific tasks.

✦ **TIP:** If you use a portable Sniffer Pro as a field service tool to troubleshoot different networks, use the local agent feature to maintain configuration information for each client's network.

To create a new local agent, select **Select Settings** from the **File** menu and click on the **New** button. The New Settings dialog box lets you specify a name for the local agent and copy the workspace settings from an existing probe to limit the amount of reconfiguration you need to do.

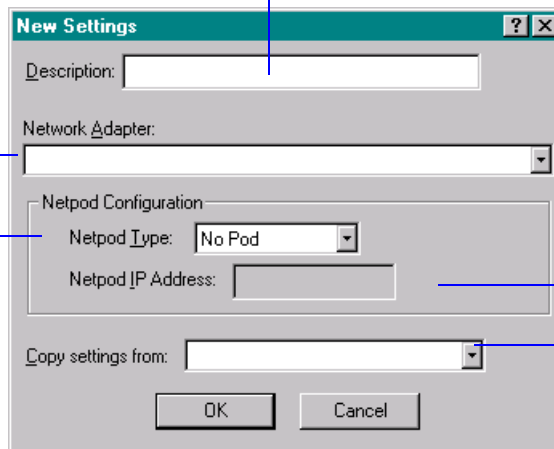
💡 **IMPORTANT:** When you create a new local agent, it automatically uses the settings currently defined in the Sniffer Pro application (the address book, capture filter settings, packet display options, and so on).

Figure 11-2 shows the New Settings dialog box.

Type a description for the local agent.

Select the adapter for this local agent. All NDIS-compliant adapters are listed.

If this local agent will use a netpod (such as NAI's Full Duplex Ethernet Pod or the SnifferBook), select the appropriate pod from the list.



If a Netpod is selected, the Netpod IP Address is automatically filled with an IP address incremented by one from the Sniffer Pro PC's IP address.

Select an existing local agent to copy its settings

Figure 11-2. Creating a Local Agent

## Adding Value to Your Network Associates Product

Choosing Network Associates anti-virus, network management, and security software helps to ensure that the critical technology you rely on functions smoothly and effectively. Taking advantage of a Network Associates support plan extends the protection you get from your software by giving you access to the expertise you need to install, monitor, maintain and upgrade your system with the latest Network Associates technology. With a support plan tailored to your needs, you can keep your system or your network working dependably in your computing environment for months or years to come.

Network Associates support plans come under two general headings. If you are a corporate customer, you can choose from four levels of extended support under the Network Associates Corporate PrimeSupport\* program. If you are a home user, you can choose a plan geared toward your needs from the Home User PrimeSupport program.

## PrimeSupport Options for Corporate Customers

The Corporate PrimeSupport program offers these four support plans:

- PrimeSupport KnowledgeCenter plan
- PrimeSupport Connect plan
- PrimeSupport Connect 24-By-7 plan
- PrimeSupport Enterprise plan

Each plan has a range of features that provide you with cost-effective and timely support geared to meet your needs. The following sections describe each plan in detail.

### The PrimeSupport KnowledgeCenter Plan

The PrimeSupport KnowledgeCenter plan gives you access to an extensive array of technical support information via a Network Associates online knowledge base, and download access to product upgrades from the [Network Associates website](#). If you purchased your Network Associates product with a subscription license, you receive the

PrimeSupport KnowledgeCenter plan as part of the package, for the length of your subscription term.

If you purchased a perpetual license for your Network Associates product, you can purchase a PrimeSupport KnowledgeCenter plan for an annual fee.

To receive your KnowledgeCenter password or to register your PrimeSupport agreement with Network Associates, visit:

[http://www.nai.com/asp\\_set/support/introduction/default.asp](http://www.nai.com/asp_set/support/introduction/default.asp)

Your completed form will go to the Network Associates Customer Service Center. You must submit this form before you connect to the PrimeSupport KnowledgeCenter site.

With the PrimeSupport KnowledgeCenter plan, you get:

- Unrestricted, 24-hour-per-day online access to technical solutions from a searchable knowledge base within the [Network Associates website](#)
- Electronic incident and query submission
- Technical documents, including user's guides, FAQ lists, and release notes
- Online data file updates and product upgrades

## The PrimeSupport Connect Plan

The PrimeSupport Connect plan gives you telephone access to essential product assistance from experienced technical support staff members.

With this plan, you get:

- In North America, unlimited toll-free telephone access to technical support from Monday through Friday, 8:00 a.m. to 8:00 p.m. Central Time
- In Europe, the Middle East, and Africa, unlimited telephone access to technical support, at standard long-distance or international rates, Monday through Friday, from 9:00 a.m. to 6:00 p.m. local time
- In the Asia-Pacific region, unlimited toll-free, telephone access to technical support, Monday through Friday, from 8:00 a.m. to 6:00 p.m. AEST
- In Latin America, unlimited telephone access to technical support, at standard long-distance or international rates, Monday through Friday, from 9:00 a.m. to 5:00 p.m. Central Time

- Unrestricted, 24-hour-per-day online access to technical solutions from a searchable knowledge base within the [Network Associates website](#)
- Electronic incident and query submission
- Technical documents, including user's guides, FAQ lists, and release notes
- Data file updates and product upgrades via the [Network Associates website](#)

## The PrimeSupport Connect 24-By-7 Plan

The PrimeSupport Connect 24-By-7 plan gives you round-the-clock telephone access to essential product assistance from experienced Network Associates technical support staff members. You can purchase PrimeSupport Connect 24-By-7 on an annual basis when you purchase a Network Associates product, either with a subscription license or a one-year license.

The PrimeSupport Connect 24-By-7 plan has these features:

- In North America, unlimited toll-free telephone access to technical support from Monday through Friday, 8:00 a.m. to 8:00 p.m. Central Time
- In Europe, the Middle East, and Africa, unlimited telephone access to technical support, at standard long-distance or international rates, Monday through Friday, from 9:00 a.m. to 6:00 p.m. local time
- In the Asia-Pacific region, unlimited toll-free, telephone access to technical support, Monday through Friday, from 8:00 a.m. to 6:00 p.m. AEST
- In Latin America, unlimited telephone access to technical support, at standard long-distance or international rates, Monday through Friday, from 9:00 a.m. to 5:00 p.m. Central Time
- Priority access to technical support staff members during regular business hours
- Responses within one hour for urgent issues that happen outside regular business hours, including those that happen during weekends and local holidays
- Unrestricted, 24-hour-per-day online access to technical solutions from a searchable knowledge base within the [Network Associates website](#)
- Electronic incident and query submission

- Technical documents, including user's guides, FAQ lists, and release notes
- Data file updates and product upgrades via the [Network Associates website](#)

## The PrimeSupport Enterprise Plan

The PrimeSupport Enterprise plan gives you round-the-clock, personalized, proactive support from an assigned technical support engineer. You'll enjoy a relationship with a support professional who is familiar with your Network Associates product deployment and support history, and who will call you at an interval you designate to verify that you have the knowledge you need to use and maintain Network Associates products.

By calling in advance, your PrimeSupport Enterprise representative can help to prevent problems before they occur. If, however, an emergency arises, the PrimeSupport Enterprise plan gives you a committed response time that assures you that help is on the way. You may purchase the PrimeSupport Enterprise plan on an annual basis when you purchase a Network Associates product, either with a subscription license or a one-year license.

With the PrimeSupport Enterprise plan, you get:

- Unlimited, toll-free telephone access to an assigned technical support engineer on a 24-hour-per-day, seven-day-per-week basis, including during weekends and local holidays.

---

**NOTE:** The availability of toll-free telephone support varies by region and is not available in some parts of Europe, the Middle East, Africa, and Latin America.

---

- Proactive support contacts from your assigned support engineer via telephone or e-mail, at intervals you designate
- Committed response times from your support engineer, who will respond to pages within half an hour, to voice mail within one hour, and to e-mail within four hours
- Assignable customer contacts, which allow you to designate five people in your organization who your support engineer can contact in your absence
- Optional beta site status, which gives you access to the absolute latest Network Associates products and technology

- Unrestricted, 24-hour-per-day online access to technical solutions from a searchable knowledge base within the [Network Associates website](#)
- Electronic incident and query submission
- Technical documents, including user’s guides, FAQ lists, and release notes
- Online data file updates and product upgrades

## Ordering a Corporate PrimeSupport Plan

To order any PrimeSupport plan, contact your sales representative, or

- In North America, call Network Associates at (408) 988-3832, Monday through Friday from 8:00 a.m. to 7:00 p.m. Central Time. Press 3 on your telephone keypad for sales assistance.
- In Europe, the Middle East, and Africa, contact your local Network Associates office. Contact information appears near the front of this guide.

**Table i. Corporate PrimeSupport Plans at a Glance**

Plan Feature	Knowledge Center	Connect	Connect 24-By-7	Enterprise
Technical support via website	Yes	Yes	Yes	Yes
Software updates	Yes	Yes	Yes	Yes

Plan Feature	Knowledge Center	Connect	Connect 24-By-7	Enterprise
Technical support via telephone	—	Monday-Friday technical support North America; 8 a.m.-8 p.m. CT Europe, Middle East, Africa: 9am-6pm local time Asia-Pacific: 8 a.m.-6 p.m. AEST Latin America: 9 am - 5 pm CT	Monday-Friday, after hours emergency access North America; 8 a.m.-8 p.m. CT\ Europe, Middle East, Africa: 9am-6pm local time Asia-Pacific: 8 a.m.-6 p.m. AEST Latin America: 9 am - 5 pm CT	Monday-Friday, after hours emergency access North America; 8 a.m.-8 p.m. CT Europe, Middle East, Africa: 9am-6pm local time Asia-Pacific: 8 a.m.-6 p.m. AEST Latin America: 9 am - 5 pm CT
Priority call handling	—	—	Yes	Yes
After-hours support	—	—	Yes	Yes
Assigned support engineer	—	—	—	Yes
Proactive support	—	—	—	Yes
Designated contacts	—	—	—	At least 5
Response charter	E-mail within one business day	Calls answered in 3 minutes, response in one business day	Within 1 hour for urgent issues after business hours	After hours pager: 30 minutes Voicemail: 1 hour E:mail: 4 hours

The PrimeSupport options described in the rest of this chapter are available only in North America. To find out more about PrimeSupport, Training and Consultancy options available outside North America,

contact your regional sales office. Contact information appears near the front of this guide.

## PrimeSupport Options for Home Users

If you purchased your Network Associates product through a retail vendor or from the Network Associates website, you also receive support services as part of your purchase. The specific level of support you receive depends on which product you purchased. Services you might receive include:

- For anti-virus software products, free data file updates for the life of your product via the Network Associates website, your product's automatic update feature, or the SecureCast service. You can also update your data files by using your web browser to visit:

[http://www.nai.com/asp\\_set/download/dats/find.asp](http://www.nai.com/asp_set/download/dats/find.asp)

- Free program (executable file) upgrades for one year via the Network Associates website. If you purchased a deluxe version of a Network Associates product, you receive free program upgrades for two years. You can also upgrade your software by using your web browser to visit:

[http://www.nai.com/asp\\_set/download/upgrade/login.asp](http://www.nai.com/asp_set/download/upgrade/login.asp)

- Free 24-hour-per-day, seven-days-per-week access to online or electronic support through the Network Associates voice and fax system, the Network Associates website, and through such other electronic services as America Online and CompuServe.

To contact Network Associates electronic services

- Call the automated voice and fax system at (408) 346-3414
- Visit the Network Associates website at <http://support.nai.com>
- Visit the Network Associates CompuServe forum at GO NAI
- Visit Network Associates on America Online: keyword MCAFEE
- Free access to the PrimeSupport KnowledgeBase: online access to technical solutions from a searchable knowledge base, electronic incident submission, and technical documents such as user's guides, FAQs, and release notes. Visit the KnowledgeBase at:

[http://www.nai.com/asp\\_set/support/technical/intro.asp](http://www.nai.com/asp_set/support/technical/intro.asp)

- Thirty days of complimentary technical support from a Network Associates support technician during regular business hours, Monday through Friday from 9:00 a.m. to 5:30 p.m. Central Time. Your thirty-day support period starts from the date of your first support phone call for all Network Associates products. To contact technical support, call (972) 855-7044

If you need additional support, Network Associates offers a variety of other support plans that you can purchase either with your Network Associates product or after your complimentary 30-day support period expires. These include:

---

**NOTE:** The support plans described here are available only in North America—contact your regional sales representative to learn about local support options.

---

- **Small Office/Home Office Annual Plan.** This plan gives you unlimited toll-free access to technical support during regular business hours, Monday through Friday from 9:00 a.m. to 5:00 p.m. Central Time.
- **Pay-Per-Incident Plan.** This plan gives you support on a per-incident basis during business hours, Monday through Friday from 7:00 a.m. to 6:00 p.m. Pacific Time. You call a toll-free number, use a credit card to take care of the transaction, and get transferred to the technical support team within minutes. Your cost will be \$35 per incident.

All McAfee products (800) 950-1165

- **Pay-Per-Minute Plan.** This plan gives you support only when you need it. You get 900-number access to technical support staff members on a priority basis to minimize your hold time. Your first two minutes are free.

All products except PGP encryption software (900) 225-5624

- **Online Upgrades Plan.** This plan gives you the convenience of automatic access to product upgrades via Network Associates online or electronic services.
- **Quarterly Disk/CD Plan.** This plan gives you automatic quarterly delivery of upgrade disks or CDs if you cannot obtain product upgrades online. This service is available for McAfee VirusScan and NetShield software only.

## How to Reach International Home User Support

The following table lists telephone numbers for technical support in several international locations. The specific costs, availability of service, office hours and plan details might vary from location to location. Consult your sales representative or a regional Network Associates office for details.

Country or Region	Phone Number*	Bulletin Board System
Germany	+49 (0)69 21901 300	+49 89 894 28 999
France	+33 (0)1 4993 9002	+33 (0)1 4522 7601
United Kingdom	+44 (0)171 5126099	+44 1344-306890
Italy	+31 (0)55 538 4228	+31 (0)20 586 6128
Netherlands	+31 (0)55 538 4228	+31 (0)20 586 6128
Europe	+31 (0)55 538 4228	+31 (0)20 688 5521
Latin America	+55-11-3794-0125	+55-11-5506-9100

\* long distance charges might apply

## Ordering a PrimeSupport Plan for Home Users

To order the PrimeSupport Small Office/Home Office Annual Plan, Pay-Per-Incident Plan, Pay-Per-Minute Plan, Online Upgrades Plan, or Quarterly Disk/CD Plan for your Network Associates products:

- In North America, call Network Associates Customer Service at (972) 855-7044
- In international locations, contact the Network Associates retail technical support center closest to your location for more information. Some support options may not be available in some locations.

## Network Associates Consulting and Training

The Network Associates Total Service Solutions program provides you with expert consulting and comprehensive education that can help you maximize the security and performance of your network investments. The Total Service Solutions program includes the Network Associates Professional Consulting arm and the Total Education Services program.

## Professional Services

Network Associates Professional Services is ready to assist you during all stages of your network growth, from planning and design, through implementation, and with ongoing management. Network Associates consultants provide an expert's independent perspective that you can use as a supplemental resource to resolve your problems. You'll get help integrating Network Associates products into your environment, along with troubleshooting assistance or help in establishing baselines for network performance. Network Associates consultants also develop and deliver custom solutions to help accomplish your project goals—from lengthy, large-scale implementations to brief problem-solving assignments.

## Jumpstart Services

For focused help with specific problem resolution or software implementation issues, Network Associates offers a Jumpstart Service that gives you the tools you need to manage your environment. This service can include these elements:

- **Installation and optimization.** This service brings a Network Associates consultant onsite to install, configure, and optimize your new Network Associates product and give basic operational product knowledge to your team.
- **Selfstart knowledge.** This service brings a Network Associates consultant onsite to help prepare you to perform your new product implementation on your own and, in some cases, to install the product.
- **Proposal Development.** This service helps you to evaluate which processes, procedures, hardware and software you need before you roll out or upgrade Network Associates products, after which a Network Associates consultant prepares a custom proposal for your environment.

## Network Consulting

Network Associates consultants provide expertise in protocol analysis and offer a vendor-independent perspective to recommend unbiased solutions for troubleshooting and optimizing your network. Consultants can also bring their broad understanding of network management best practices and industry relationships to speed problem escalation and resolution through vendor support.

You can order a custom consultation to help you plan, design, implement, and manage your network, which can enable you to assess the impact of rolling out new applications, network operating systems, or internetworking devices.

To learn more about the options available:

- Contact your regional sales representative.
- In North America, call Network Associates at (408) 988-3832, Monday through Friday from 8:00 a.m. to 7:00 p.m. Central Time.
- Visit the Network Associates website at:  
[http://www.nai.com/asp\\_set/services/introduction/default.asp](http://www.nai.com/asp_set/services/introduction/default.asp)

## Total Education Services

Network Associates Total Education Services builds and enhances the skills of all network professionals through practical, hands-on instruction. The Total Education Services technology curriculum focuses on network fault and performance management and teaches problem-solving at all levels. Network Associates also offers modular product training so that you understand the features and functionality of your new software.

You can enroll in Total Education Services courses year-round at Network Associates educational centers, or you can learn from customized courses conducted at your location. All courses follow educational steps along a learning path that takes you to the highest levels of expertise. Network Associates is a founding member of the Certified Network Expert (CNX) consortium. To learn more about these programs:

- Contact your regional sales representative.
- Call Network Associates Total Education Services at (800) 395-3151 Ext. 2670 (for private course scheduling) or (888) 624-8724 (for public course scheduling).
- Visit the Network Associates website at:  
<http://www.nai.com/services/education/>

