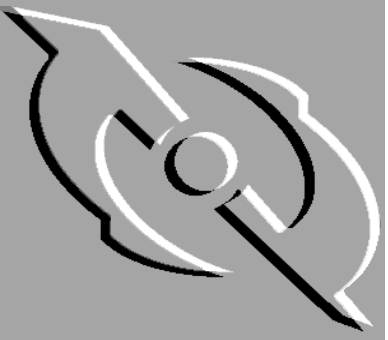


Sniffer Pro
Getting Started Guide

Release 2.0

September, 1998

Part Number: NGC-3044703

Preface

About This Manual

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

Technical Support

Technical Support is available from 6 a.m. to 6 p.m. Pacific time, weekdays. You can contact Technical Support via telephone, FAX, FAX-on-Demand, Internet mail, and the World Wide Web home page. Outside of support hours, you may leave a voice message. Technical Assistance Centers are located in California and the Netherlands.

If you purchased your product from one of our International Distributors, you must contact that distributor for support assistance. Refer to *http://www.nai.com* on the World Wide Web for information on contacting our International Distributors.

Table i describes the various ways to access Technical Support.

Table i. Contacting the Technical Support Department (1 of 2)

North American and International, 0600–1800 (PST), Monday–Friday

Telephone Number (North America only)	+1-408-988-3832
FAX	+1-650-346-5540
FAX-on-Demand (North America)	+1-800-764-3329

Table i. Contacting the Technical Support Department (2 of 2)

Europe, 0730–1730 (GMT), Monday–Friday

Telephone Number	+31 (0) 20 586 6100
FAX	+31 (0) 20 586 6101

Worldwide

Internet Address	tnv_support@nai.com
World Wide Web (Internet) information	*http://www.nai.com*

World Wide Web

You can obtain additional information about Network Associates and its products and services from the World Wide Web at *http://www.nai.com*.

Training

Network Associates offers a comprehensive set of training courses focused on hands-on network analysis, monitoring, and troubleshooting using products from Network Associates. Courses can be conducted at your site, at central locations throughout the globe, or at specific training centers. For more information about these courses, contact your sales representative or call Network Associates.

Introducing Sniffer Pro 1

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

Major Components

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

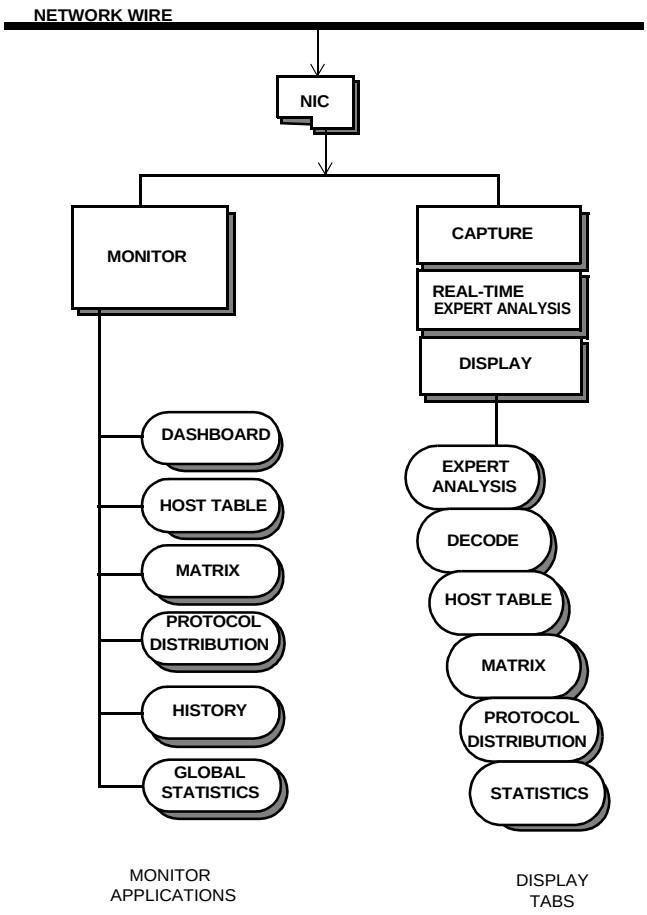


Figure 1–1. Sniffer Pro Major Components

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.

Monitoring Your Network 2

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 Token Ring; Ring purge packets, beacon packets, NAUN changes, token errors, soft errors, and so on.
  - For WAN/Synchronous; U-frame packets, S-frame packets, I-frame packets, LMI packets, and so on.
- 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 document *Installing NAI Enhanced Drivers* 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*).

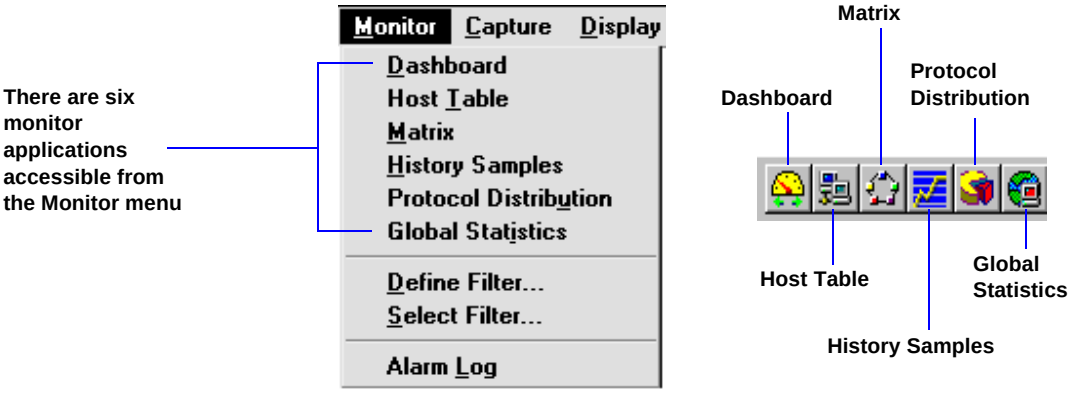


Figure 2–1. The Monitor Menu and Toolbar Buttons

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 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.

Figure 2–2 shows the Dashboard for an Ethernet adapter.

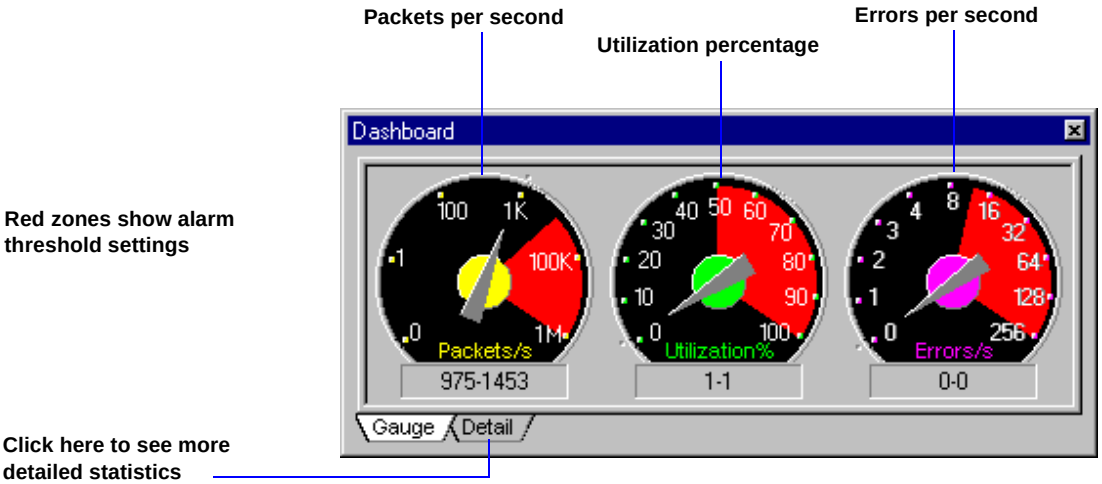
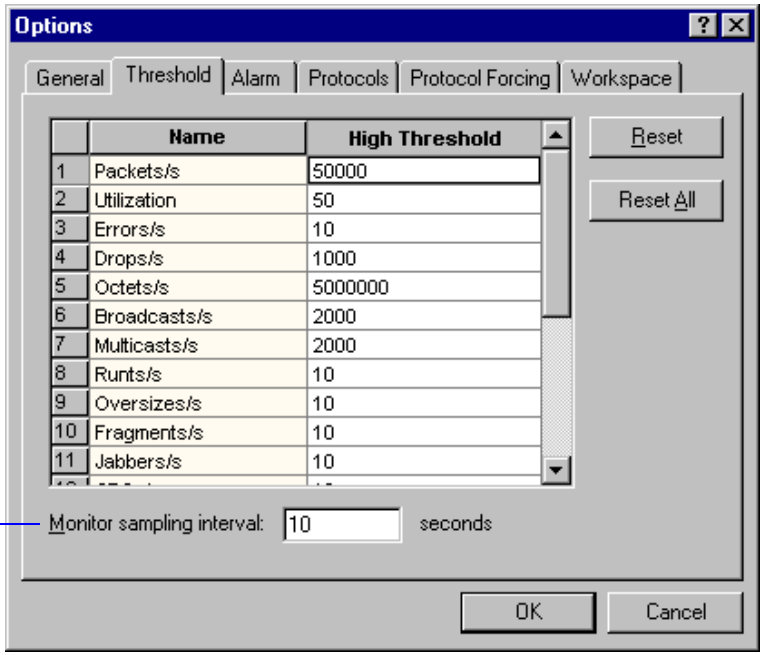


Figure 2–2. The Dashboard Gauge View

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.



The High Threshold value for each measure will be the average per second value measured during the monitor sampling interval

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 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 2–17*.

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 3–4*.)

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.

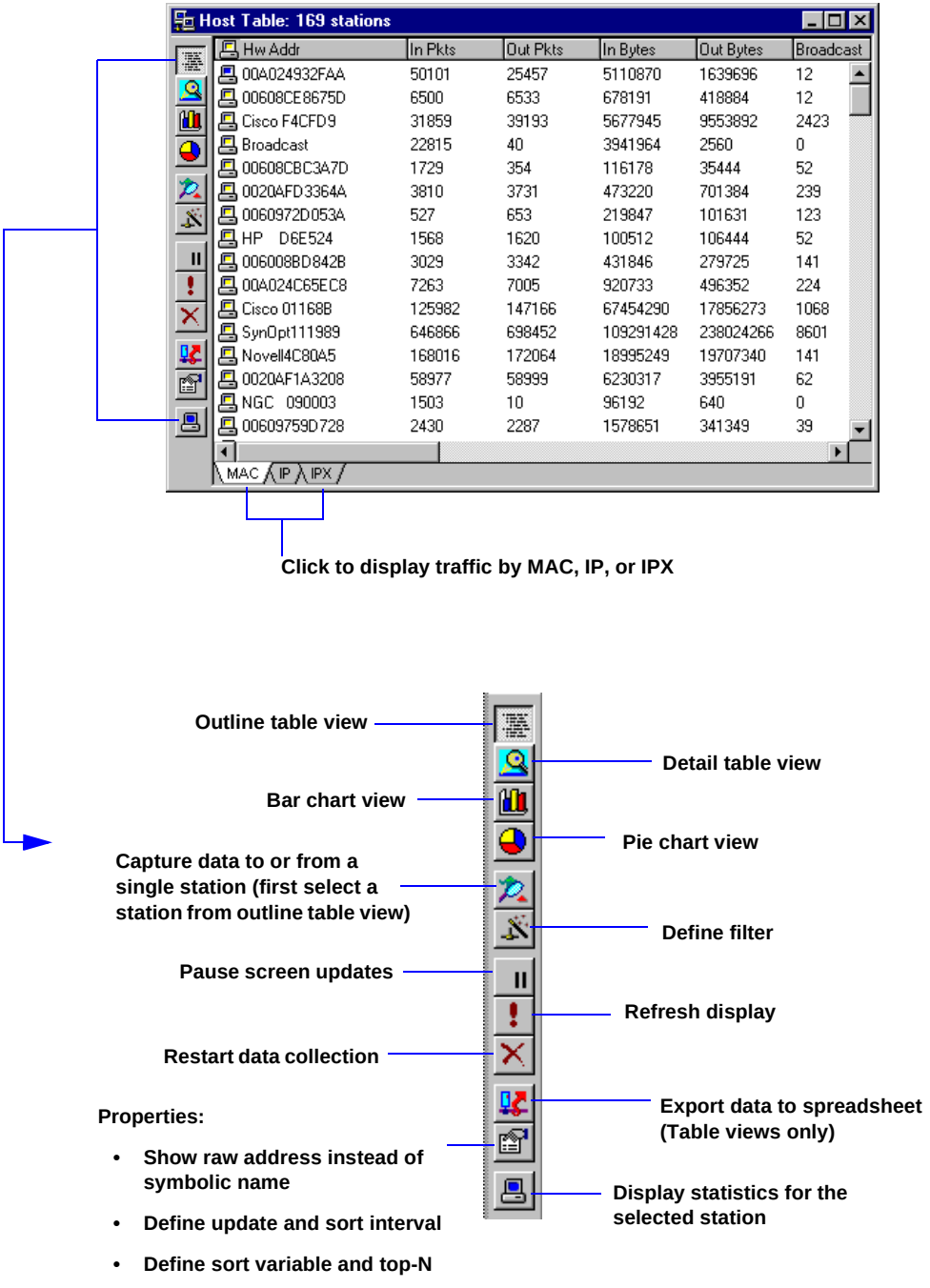


Figure 2–4. The Host Table (Outline Table View) and Toolbar

Matrix

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

- For LAN 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 2–17*.

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 3–4*.)

Figure 2–5 shows a Matrix bar chart for an Ethernet adapter and describes the Matrix toolbar.

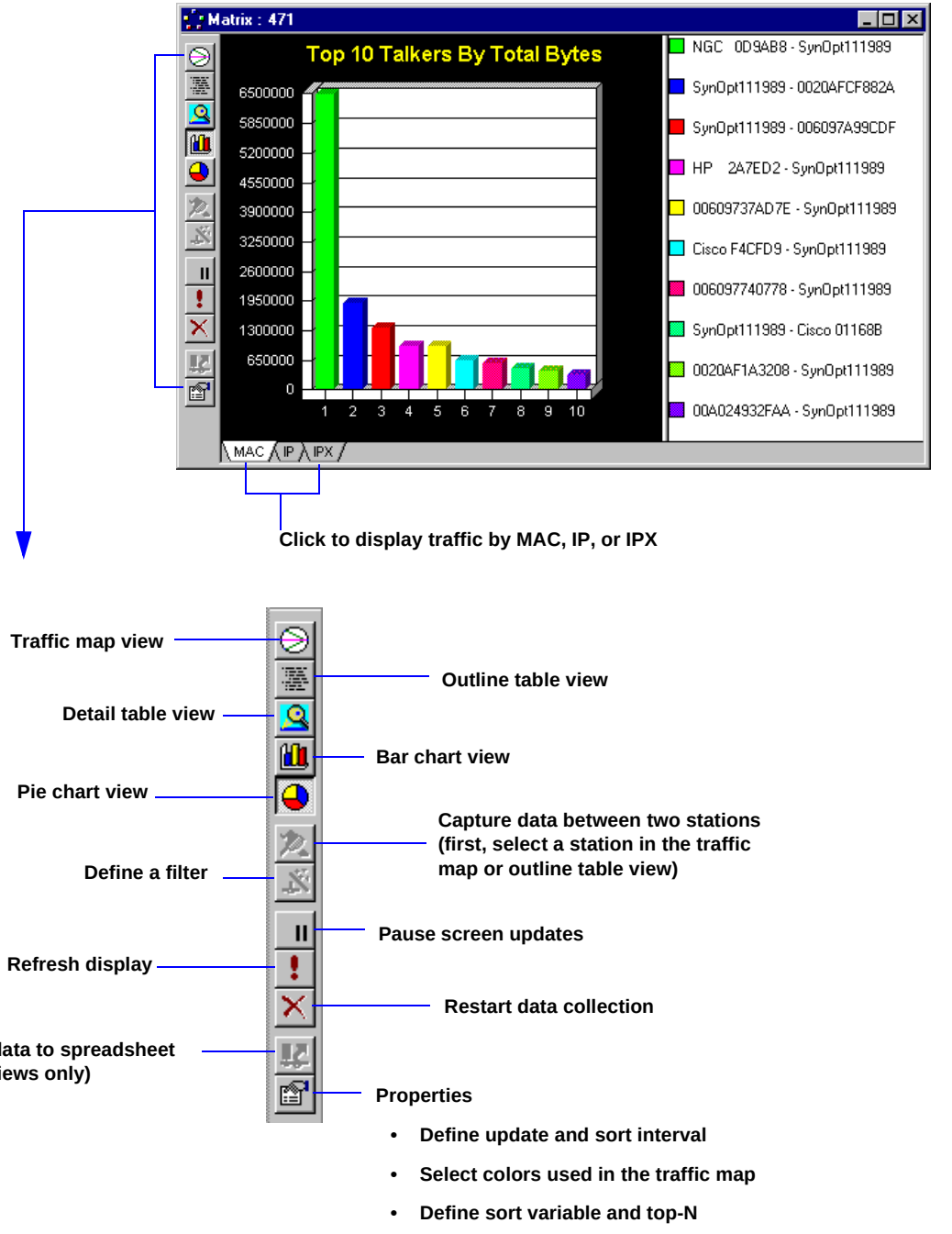


Figure 2–5. The Matrix (Bar Chart View) and Toolbar

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).

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.

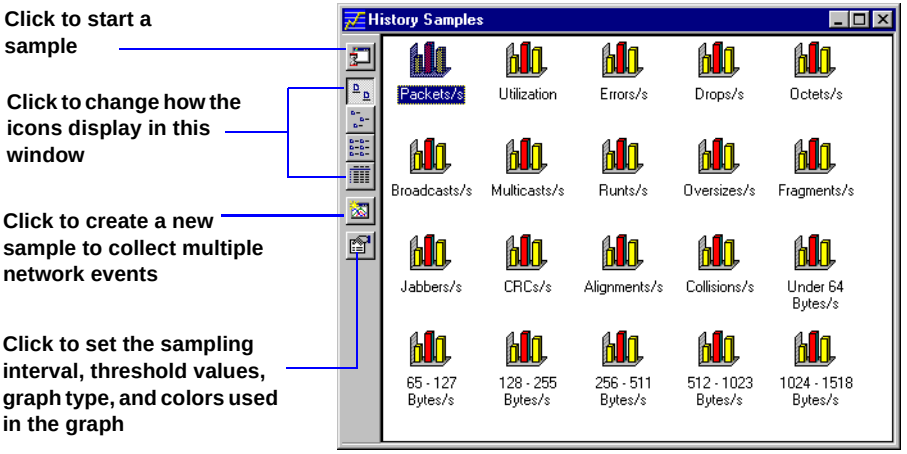


Figure 2–6. The History Samples Window

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*.

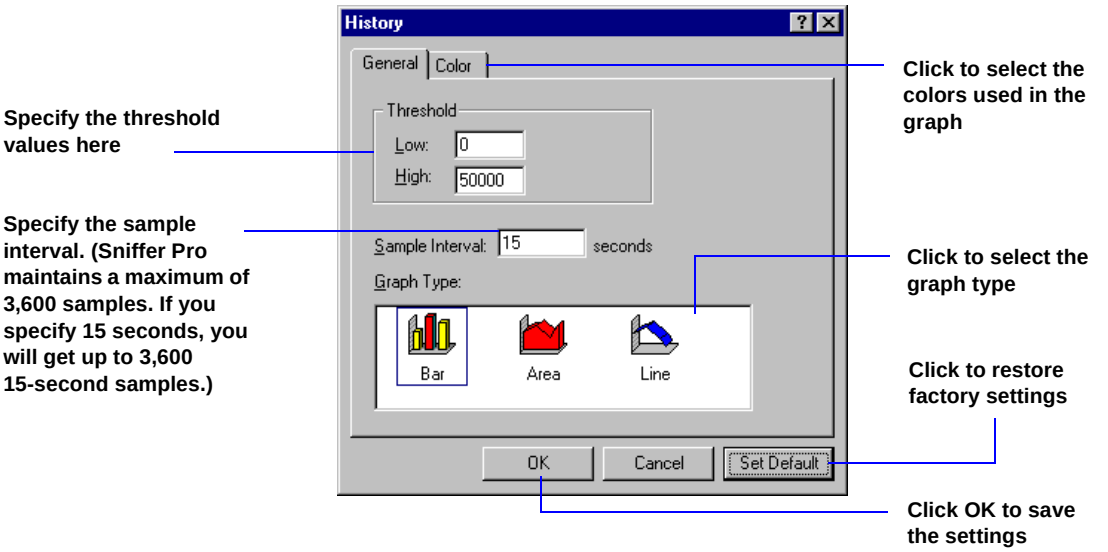


Figure 2–7. Configuring History Sample Settings

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 2–17*.

Figure 2–8 shows a **Packets/s** history sample in bar chart format and describes the toolbar.

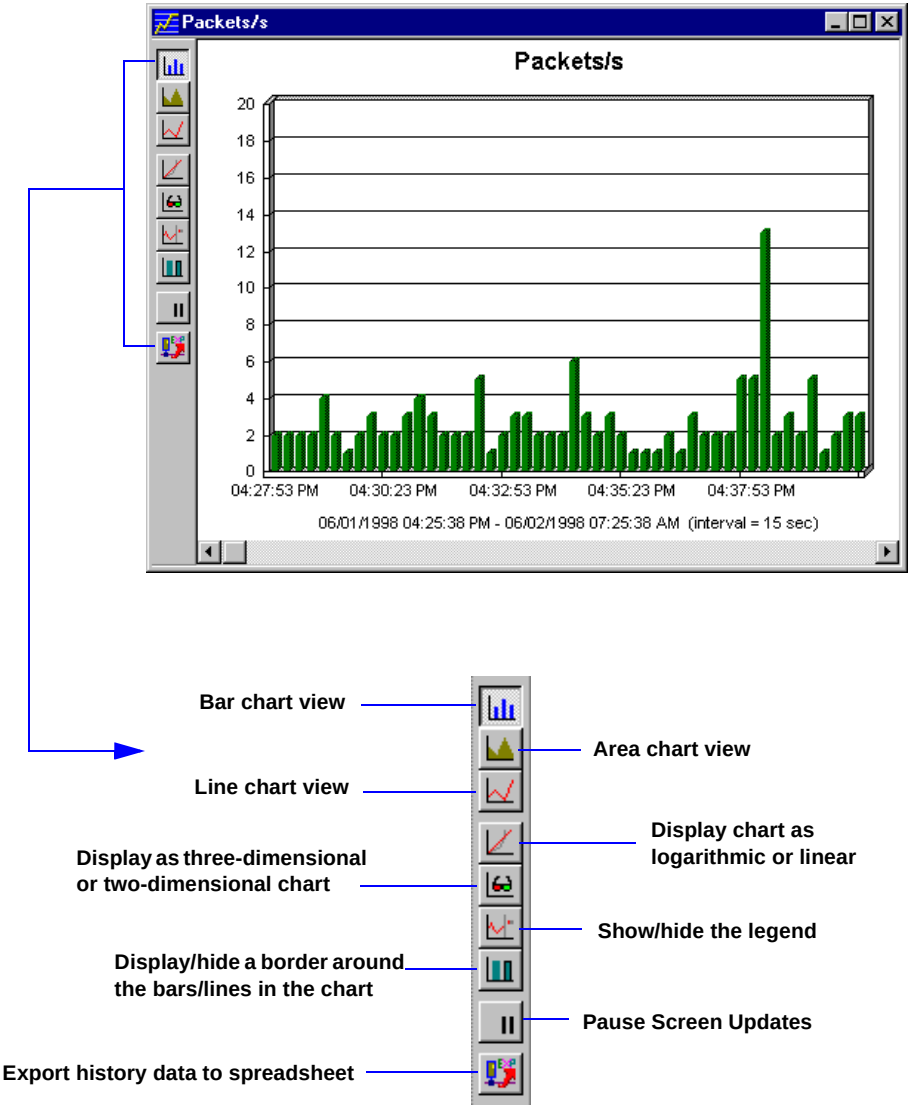


Figure 2–8. History Samples (Packets/s Bar Chart) and Toolbar

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 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 2–17*.

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

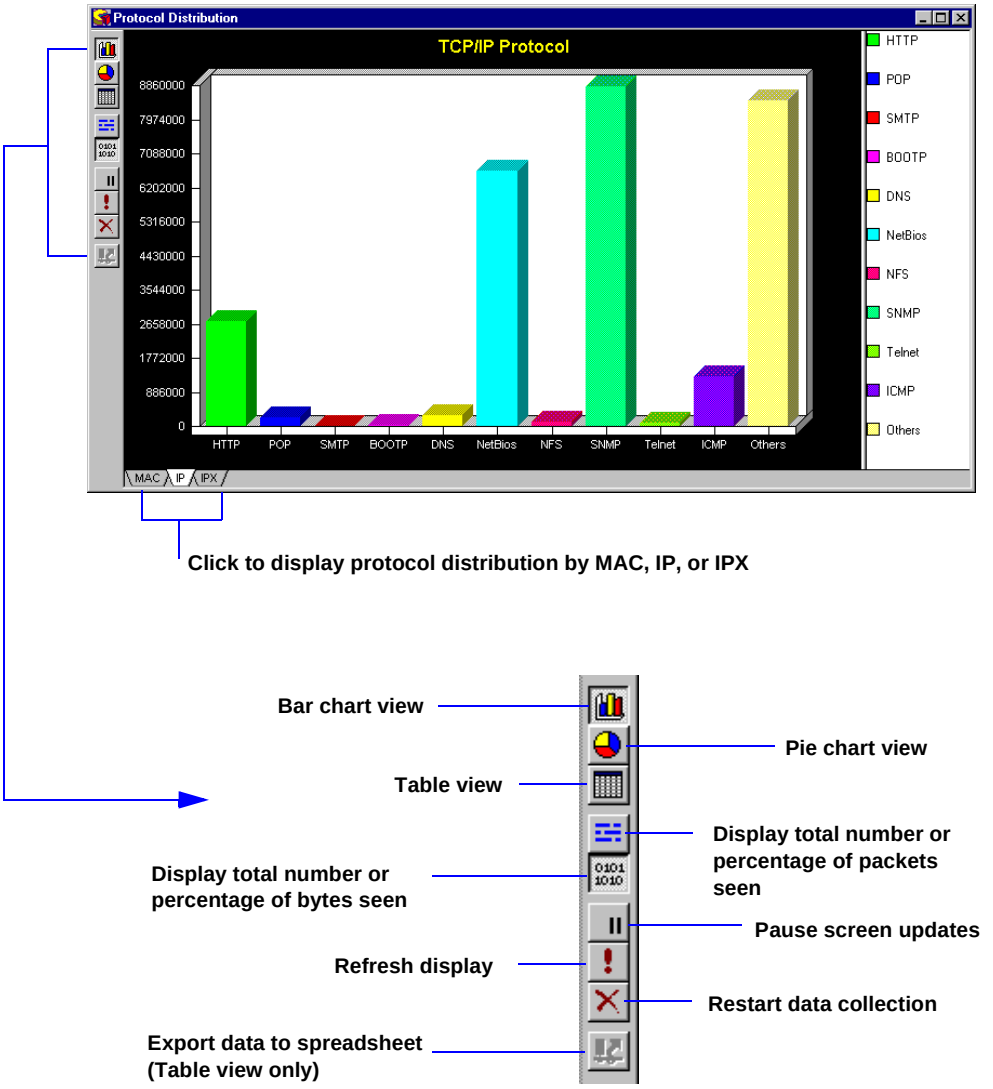


Figure 2–9. Protocol Distribution (Bar Chart View) and Toolbar

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.

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

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

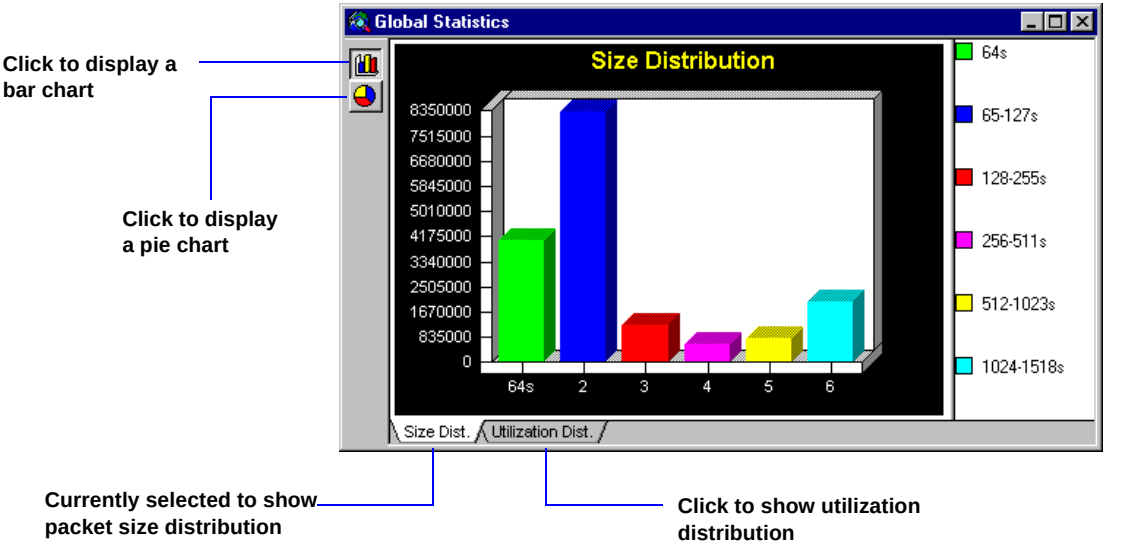


Figure 2–10. Global Statistics (Bar Chart View)

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

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).

Saving Monitor Data to a Database File

Database

Turning Off Database Collection

Deleting Database Records

Changing the Database Update Interval

Saving the Address Book to the 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.

Capturing Packets 3

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 a *capture panel* with which you control the capture process. From the capture panel, you can configure the *capture buffer* (which stores the captured packets), and define capture *filters*.

Before starting a capture, you should configure the Expert options that determine how Expert data is processed and displayed.

Capture Panel

Capturing Packets From the Network

Use the capture panel to:

- Start and stop capturing
- Display the results of a capture
- Select a capture filter to use while capturing
- Access the Define Filter dialog box to create a new filter

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

The capture panel (like the Packet Generator and the Dashboard) is a *dockable* window. You can dock it on the Sniffer Pro 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 3–1 shows the Capture Panel window.

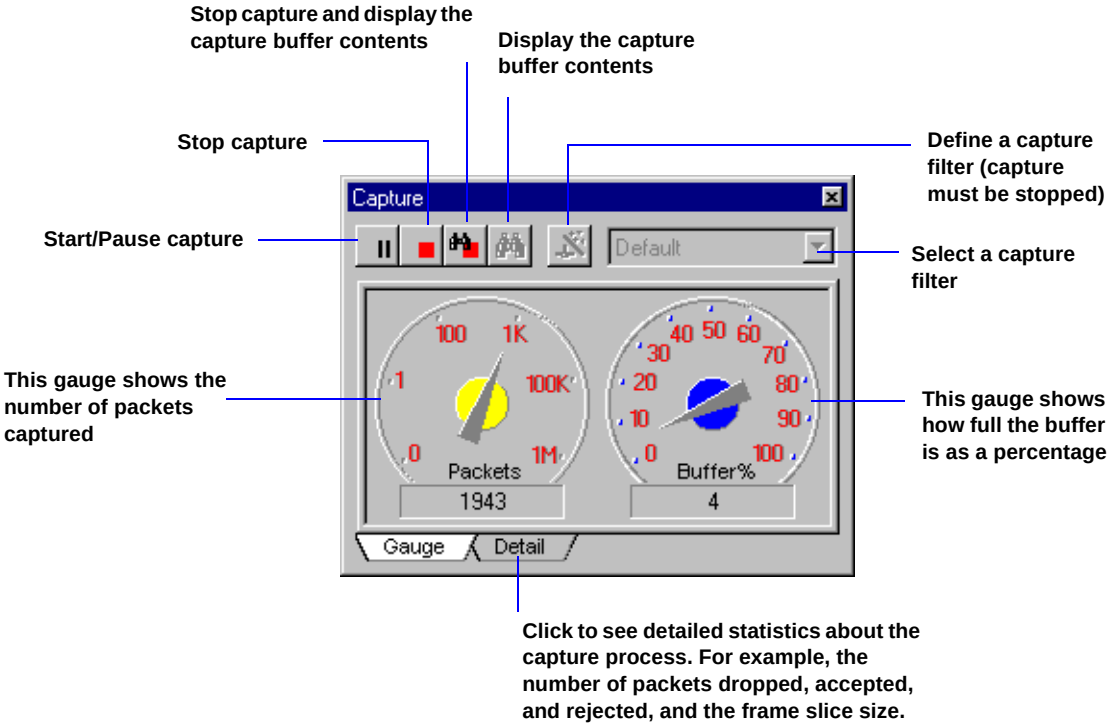


Figure 3–1. The Capture Panel Gauge Display

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.

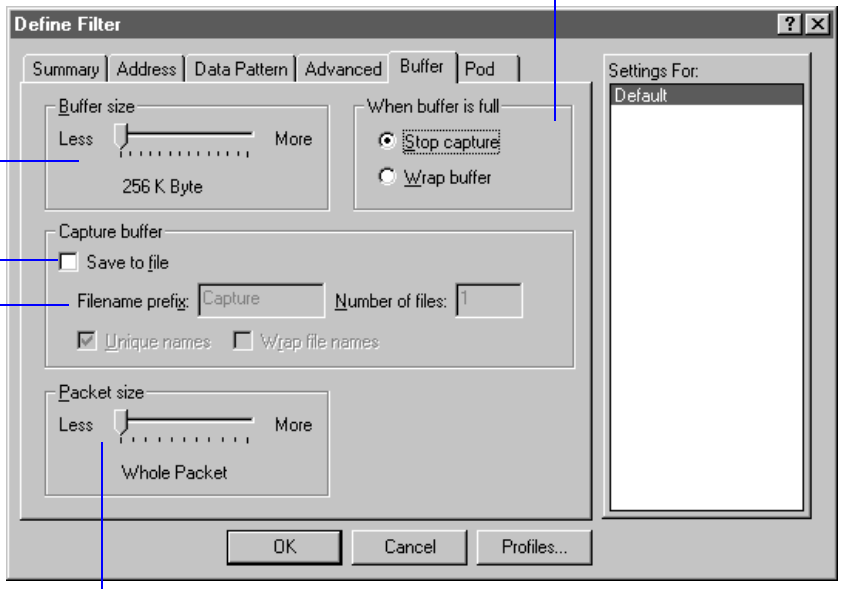
By loading previously captured packets from a disk file, you can display and analyze data as if it were captured live at that moment. Sniffer Pro treats the data loaded from a disk file in the same way as data captured live off the network.

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 3–2*).

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 3–2. 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 3–3 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

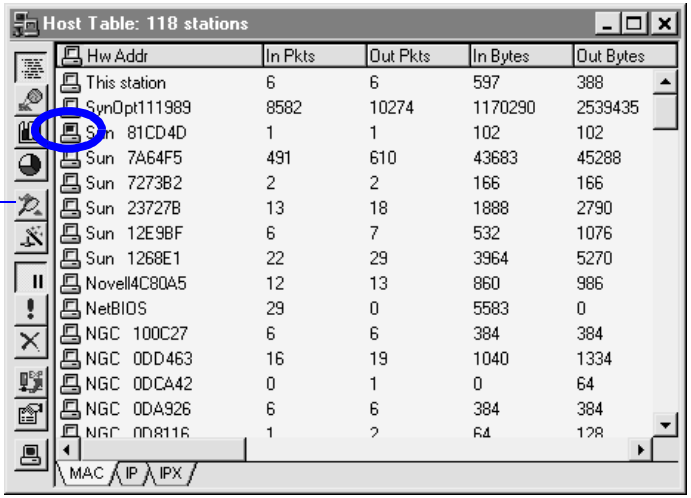


Figure 3–3. Single-Station Capture from the Host Table

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

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.)

Objects Tab

Recycling Expert Objects

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 3–4*.

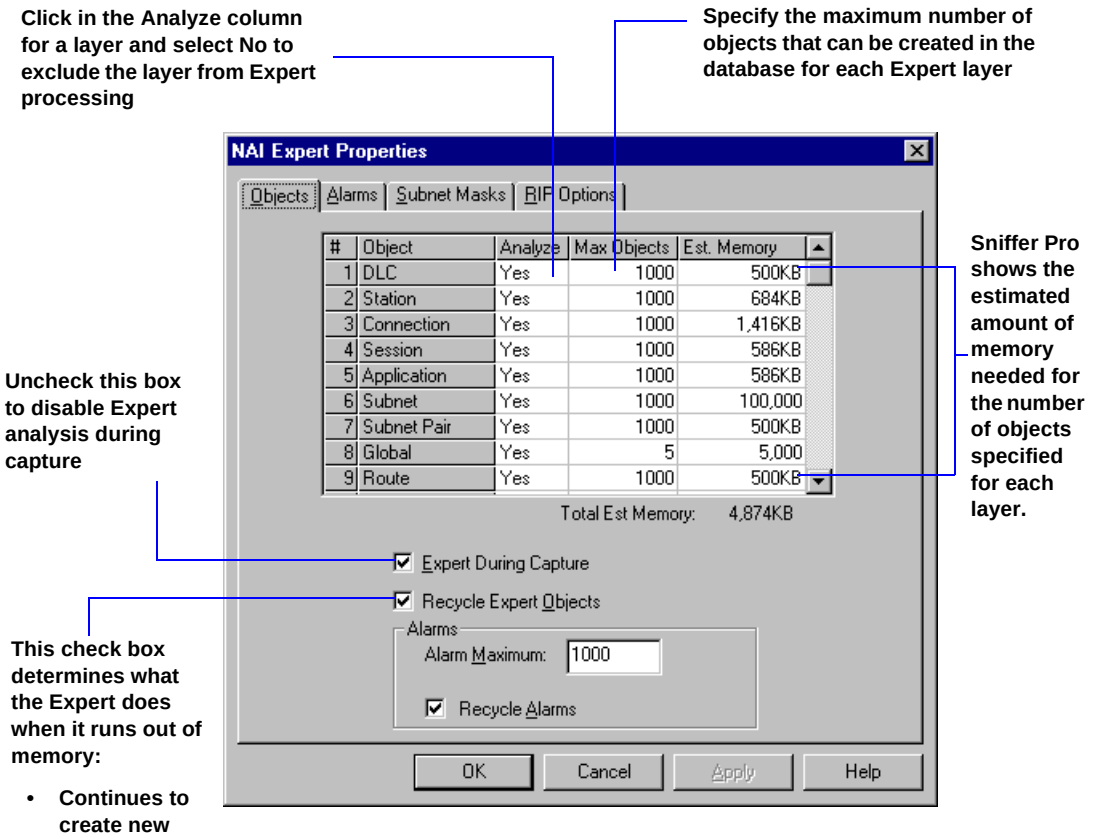


Figure 3–4. Setting Expert Object and Layer Options

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 3–5*.

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.

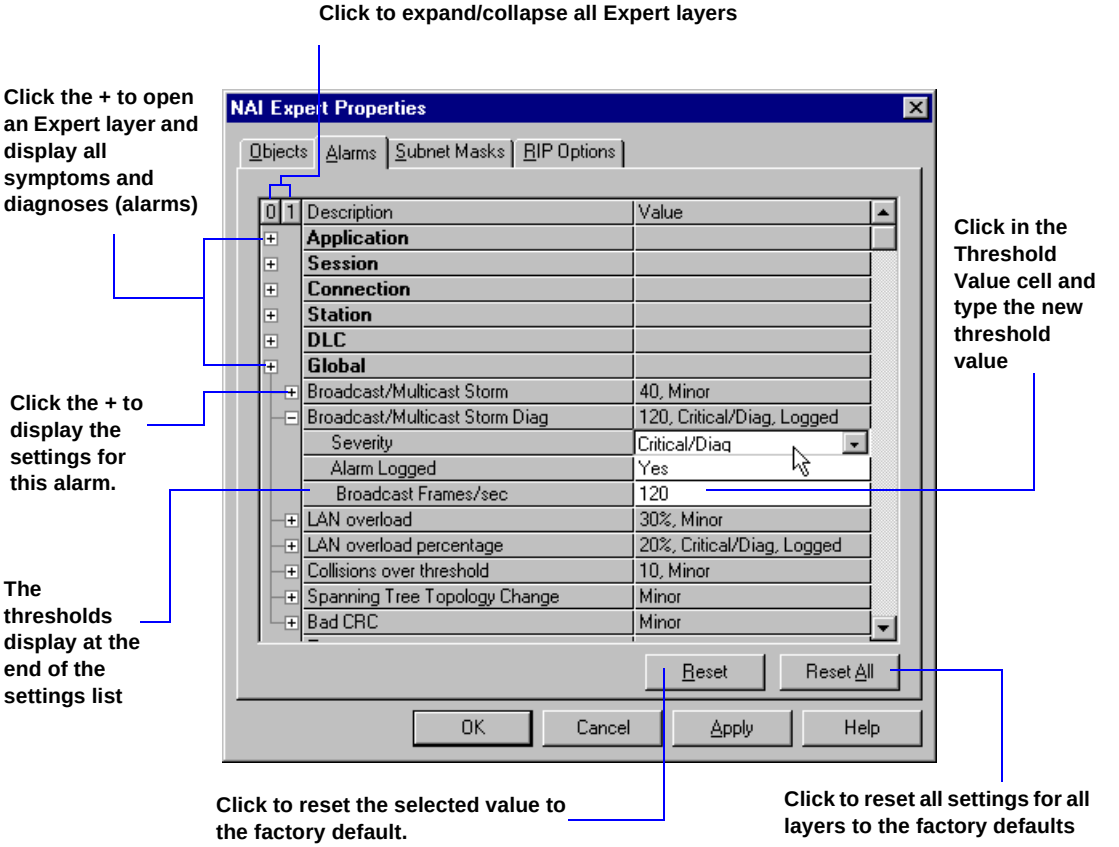


Figure 3–5. Setting Expert Thresholds

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 3–6*). 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**.

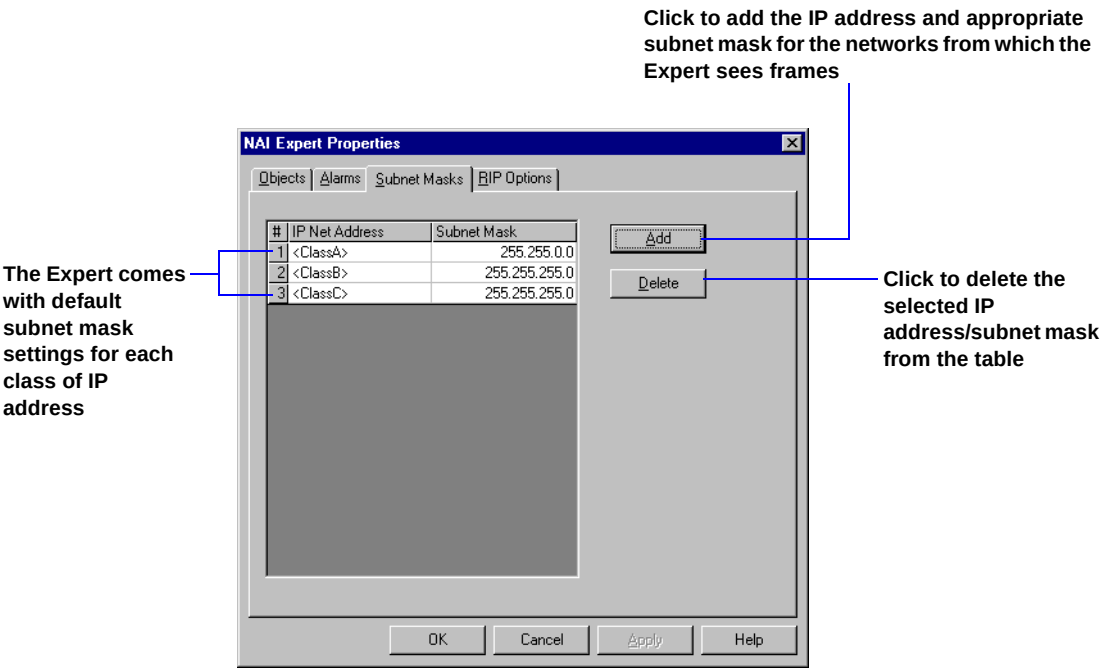


Figure 3–6. Setting Subnet Masks

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.

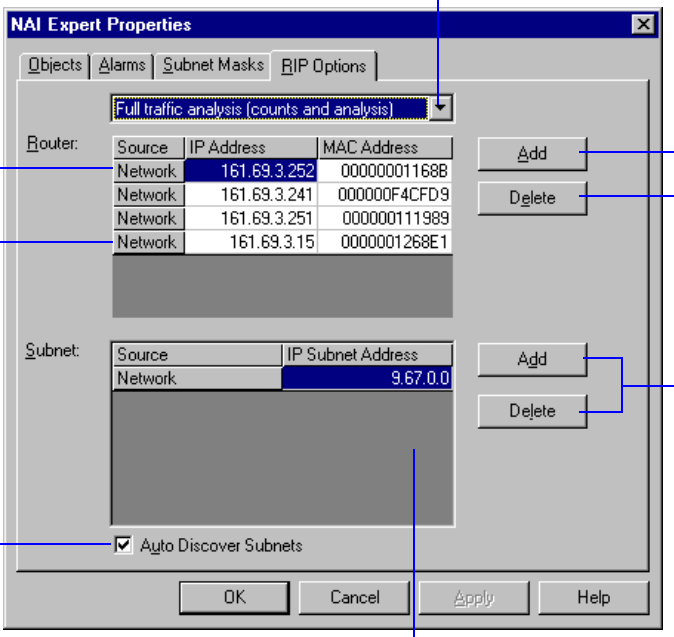
Some hosts may be configured to route traffic to default gateways, but a route from such a host to a default gateway might never be advertised. Unless you configure static default routes, the RIP Expert will incorrectly diagnose frames sent from a host to a default gateway as misdirected. If a default 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 3–7*.

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

Click to add a default router to the router table

Click to delete a router from 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 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 3–7. Setting RIP Options

Displaying Captured Data 4

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 Capture panel 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 3–5*.

Display Filters

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:

- 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

Decode 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.

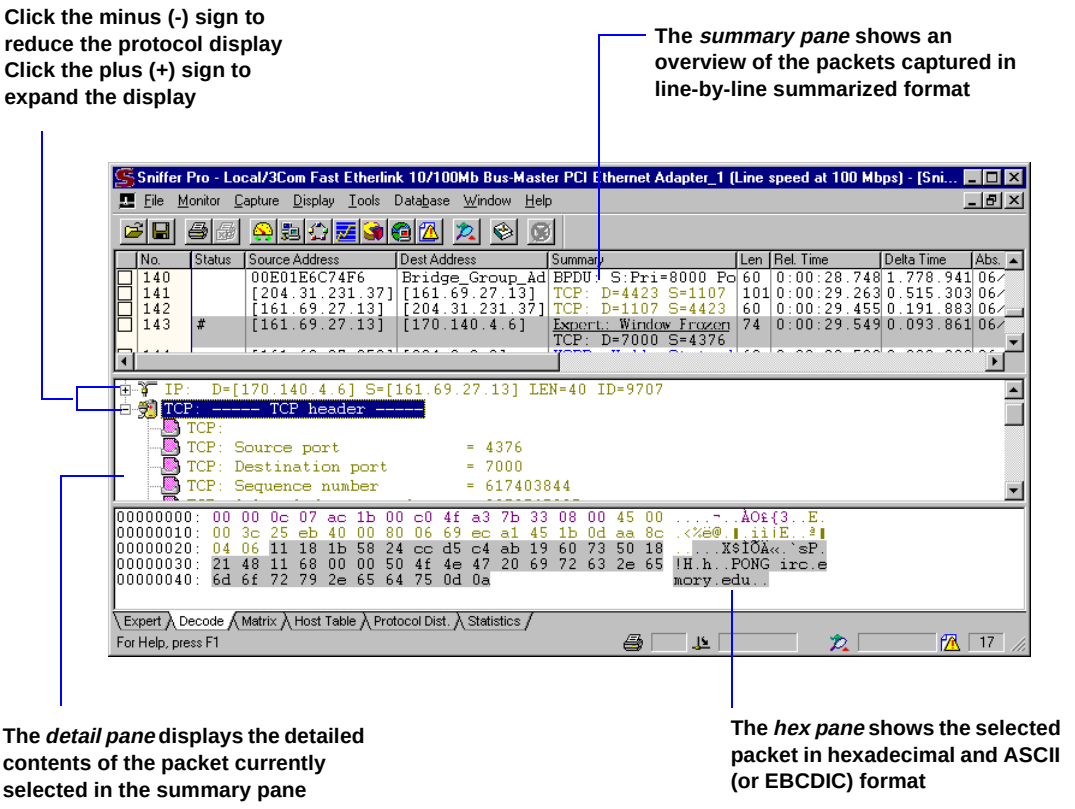


Figure 4–1. The Decode Tab

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.

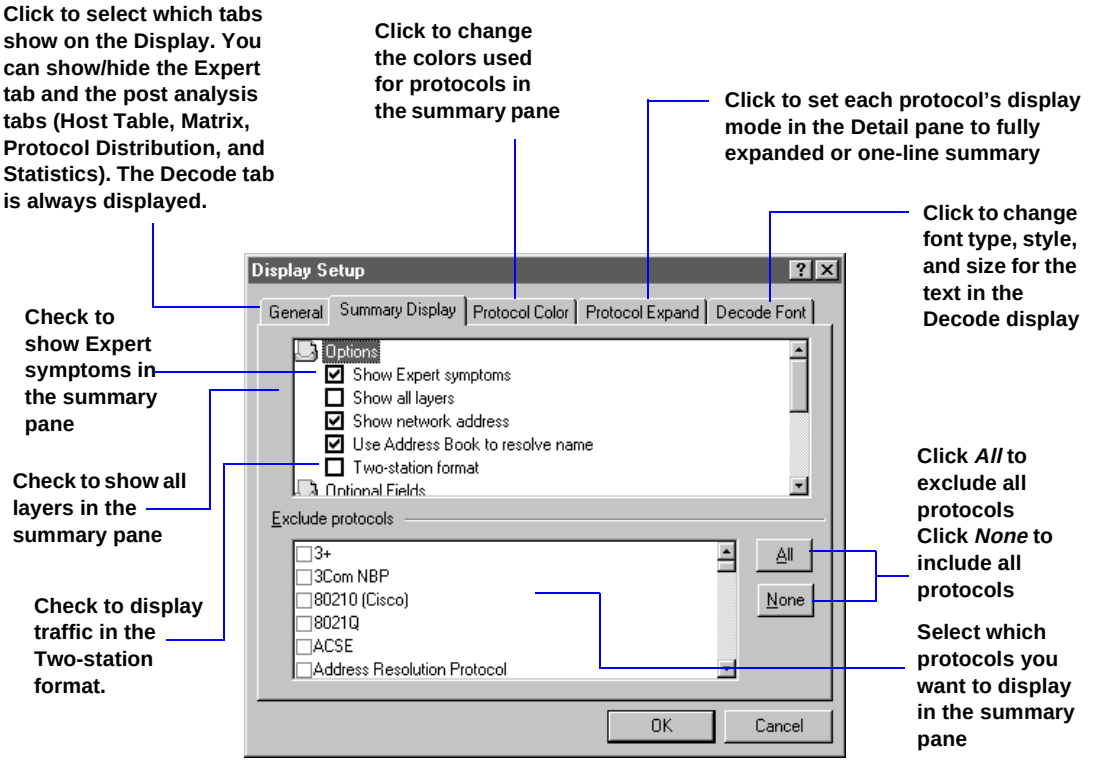


Figure 4–2. Setting Display Options

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.

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

Optional Fields

Flags	Shows flags associated with a frame.
Absolute time	Shows when the frame was received.
Delta time	Shows the interval between the current frame and the previous frame.
Relative time	Shows the interval between the current frame and the marked frame.
Bytes	Shows the frame's length.
Cumulative bytes	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.

Matrix Tab

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.

Showing the Traffic Map

Using a Visual Filter in the Traffic Map

Using the Matrix Map

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 4–3 shows the Matrix display (bar chart view) and toolbar.

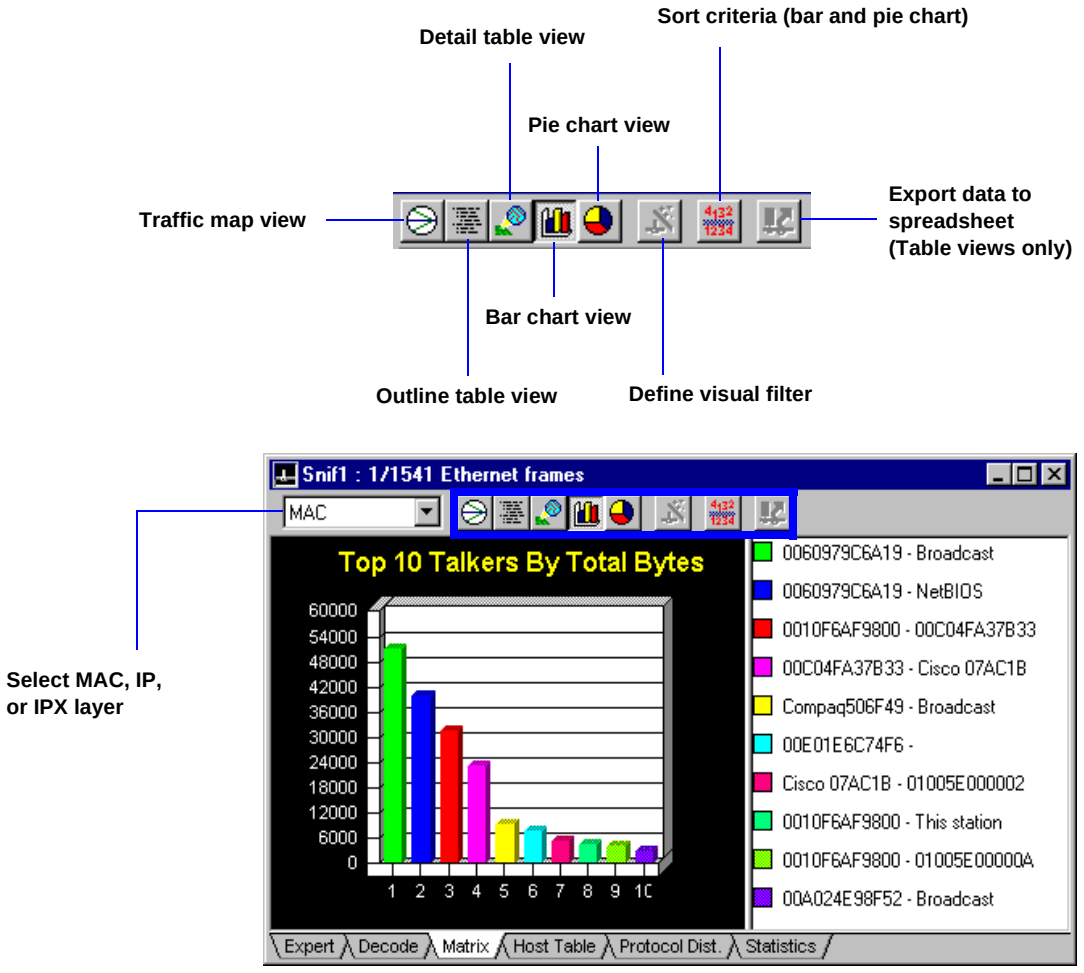


Figure 4–3. Matrix Display (Bar Chart View) and Toolbar

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 4–4 shows the Host Table display and toolbar.

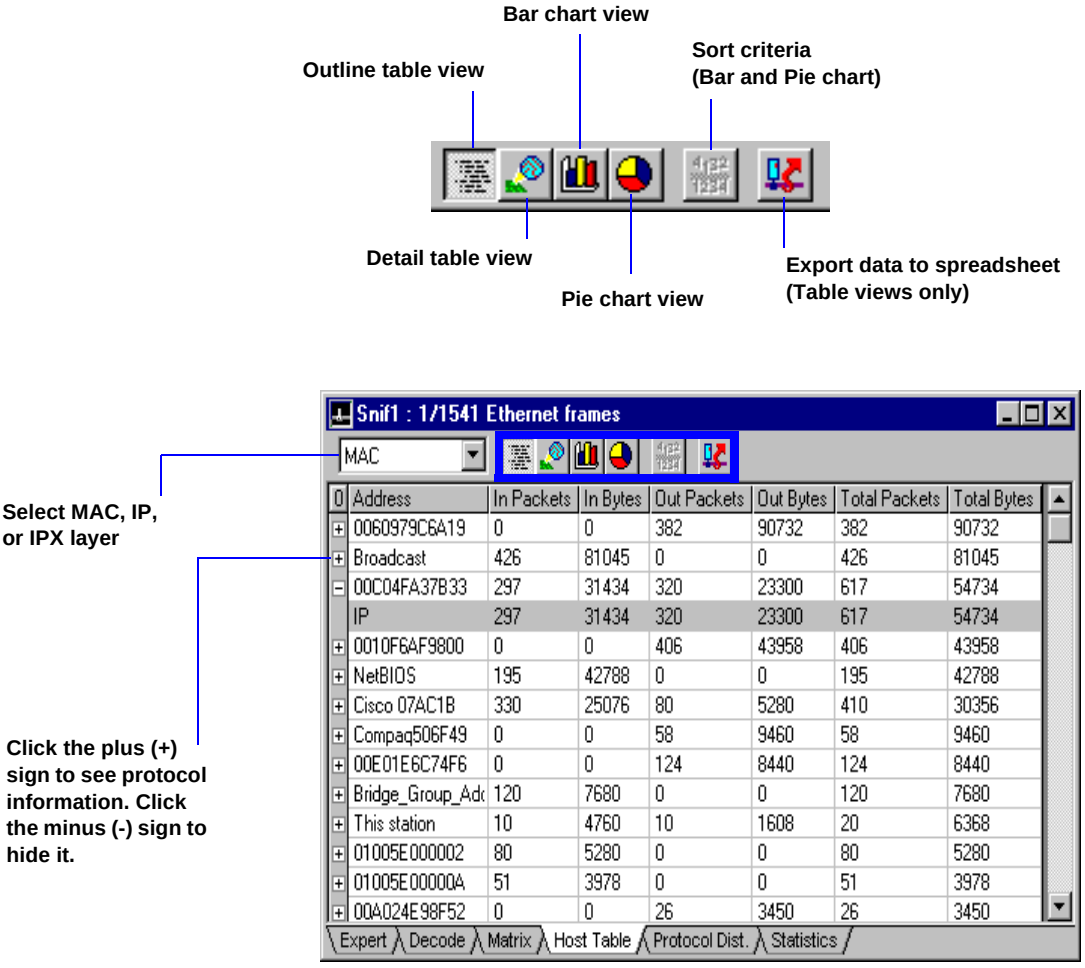


Figure 4–4. Host Table Display (Outline Table View) and Toolbar

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 4–5 shows the Protocol Distribution display and toolbar.

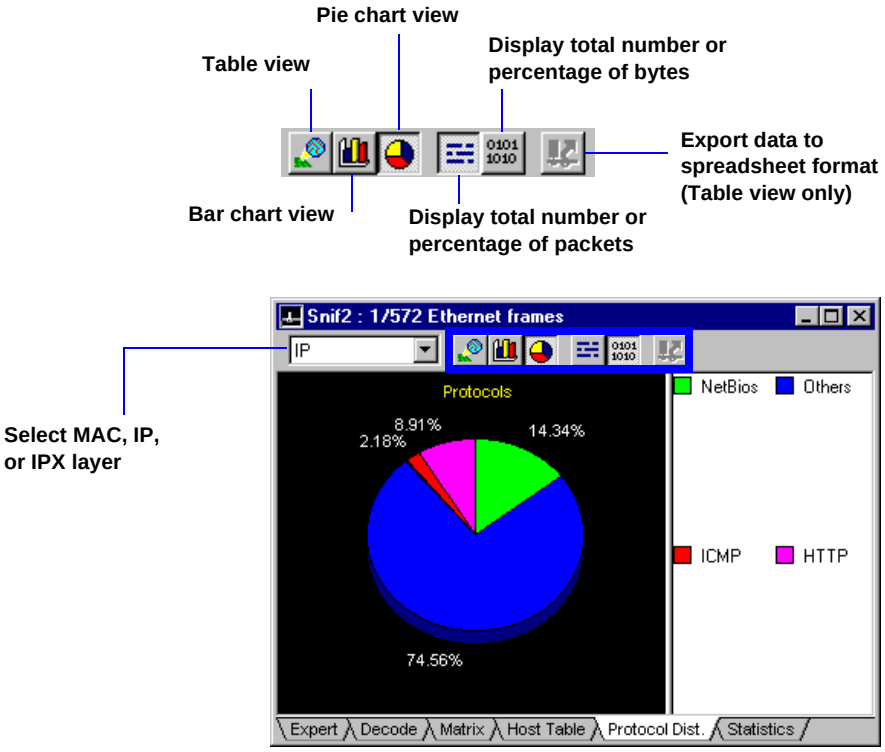


Figure 4–5. Protocol Distribution Display (Pie Chart View) and Toolbar

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 4–6 shows the Statistics display.

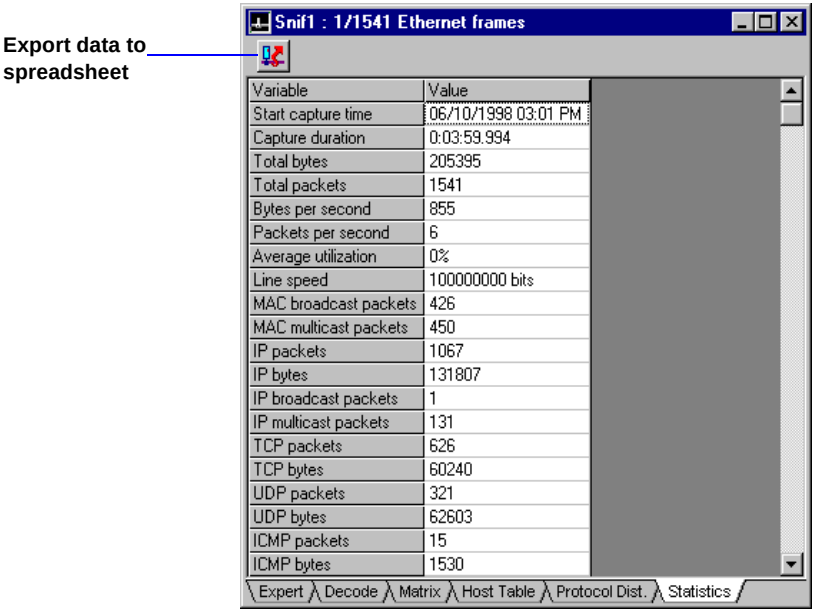


Figure 4–6. The Statistics Display

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 4–7*.

Each pane is described below:

- The *Expert Overview* pane shows the eight 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.

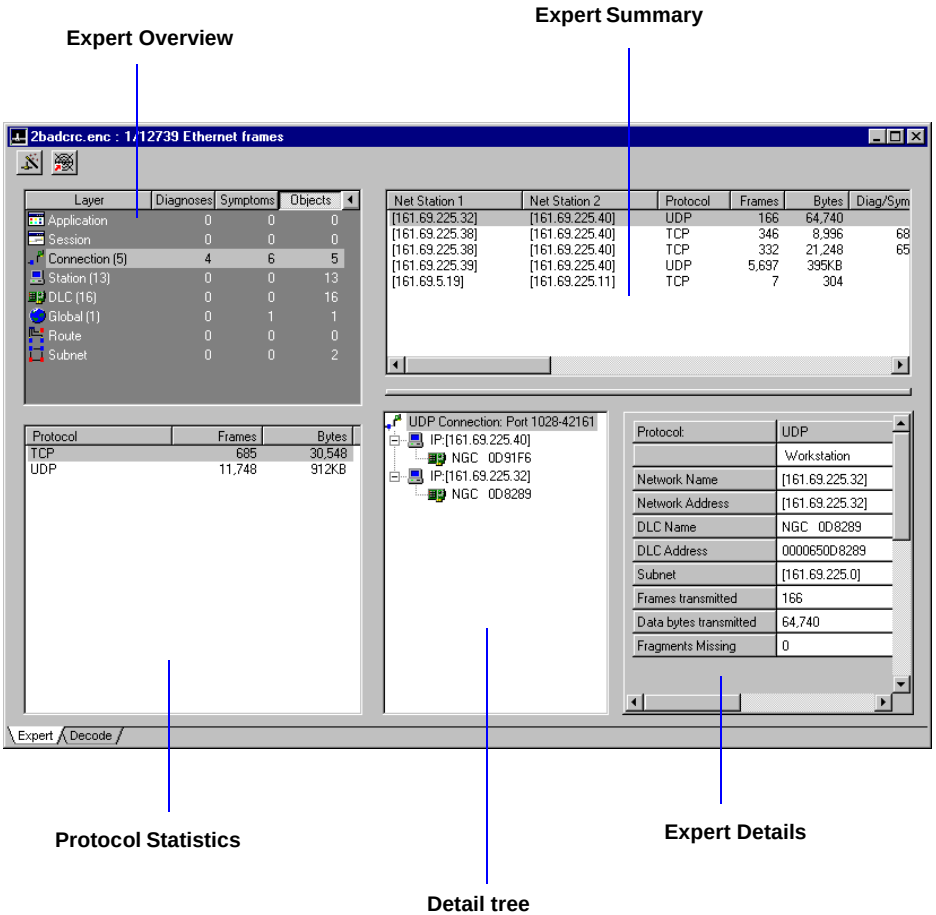


Figure 4–7. The Expert Window Panes

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 ?.)

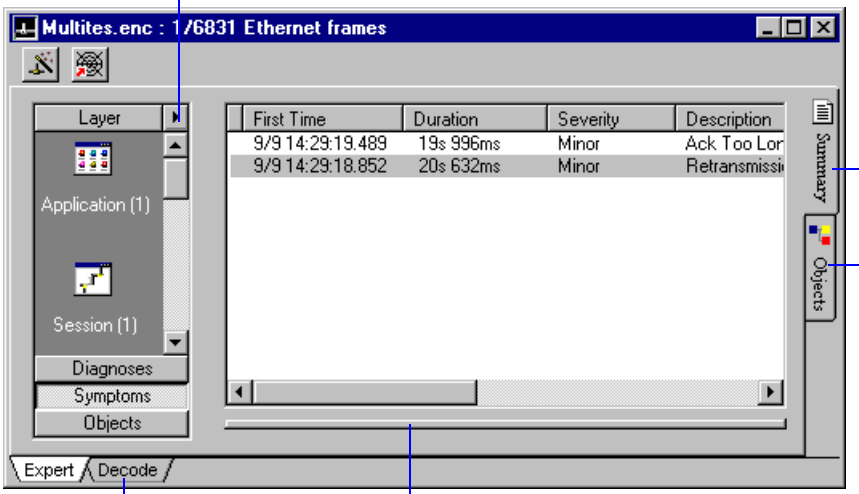
Rearranging the Expert Display

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 4–7*).
- 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 4–8 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 4–7*)

Figure 4–8. Rearranging the Expert Window Panes

Defining Filters and Triggers 5

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.

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.

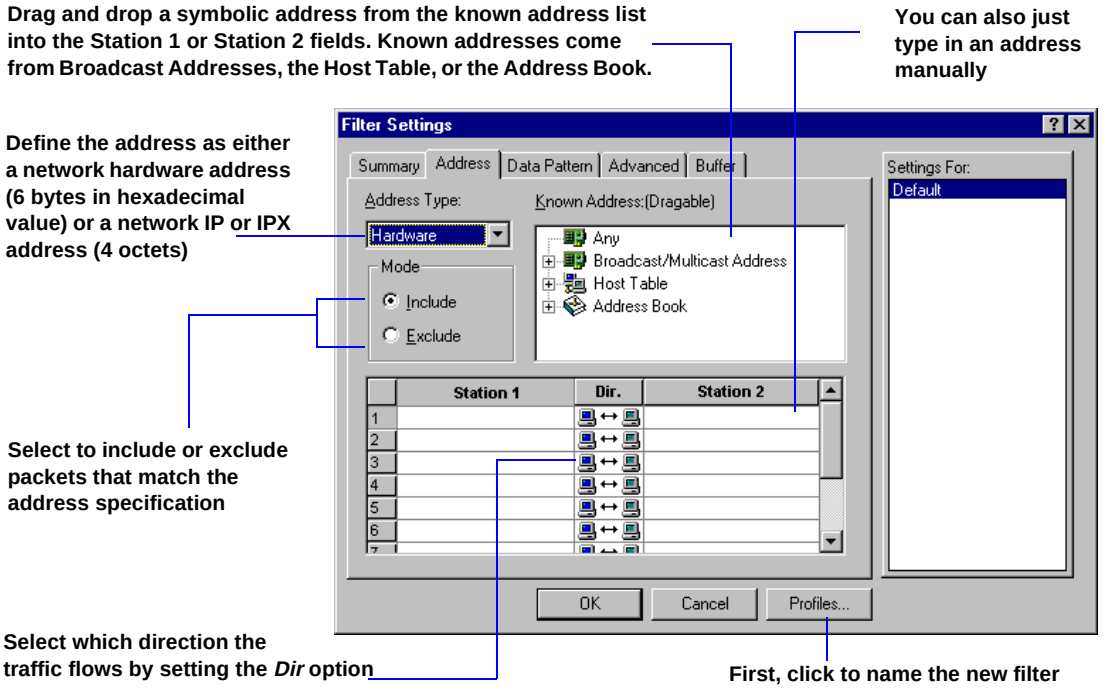


Figure 5–1. Setting Address Filters

Filtering by Data Pattern

Define Filter Data Pattern Tab

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.

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.

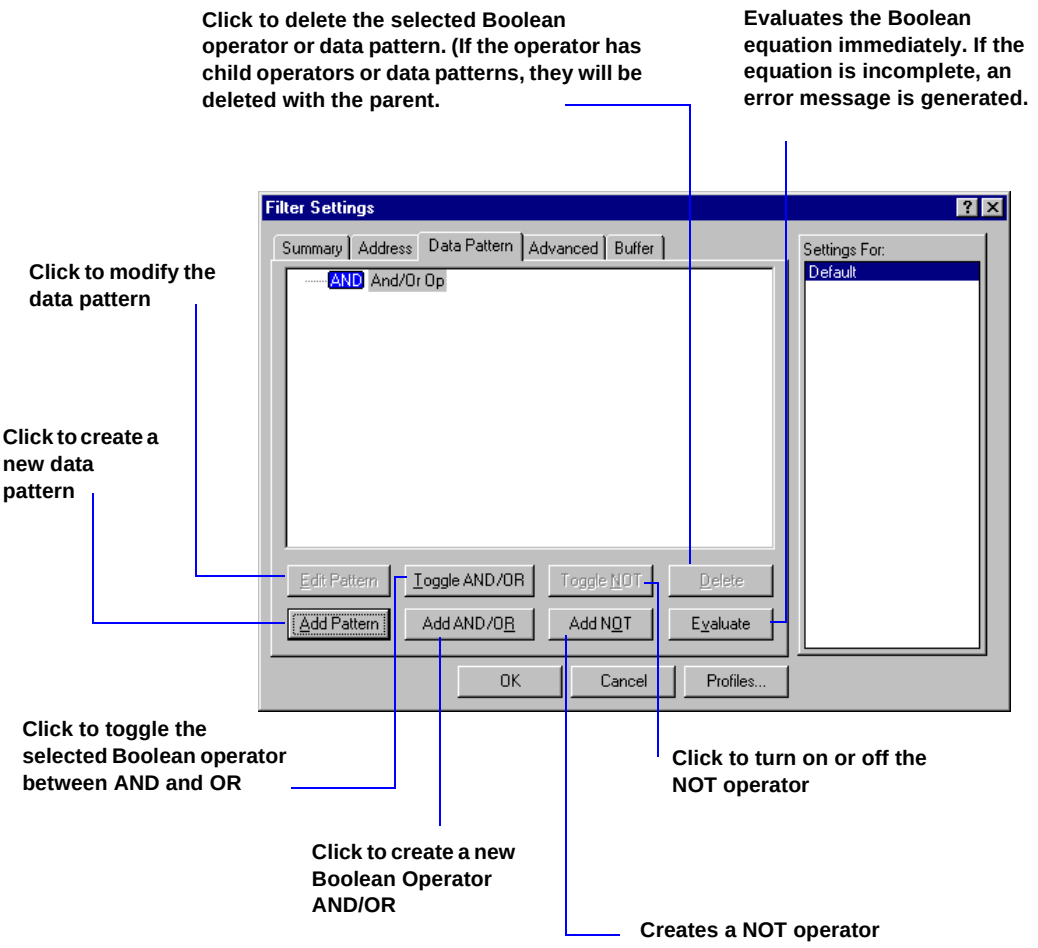


Figure 5–2. Setting Data Pattern Filters

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.

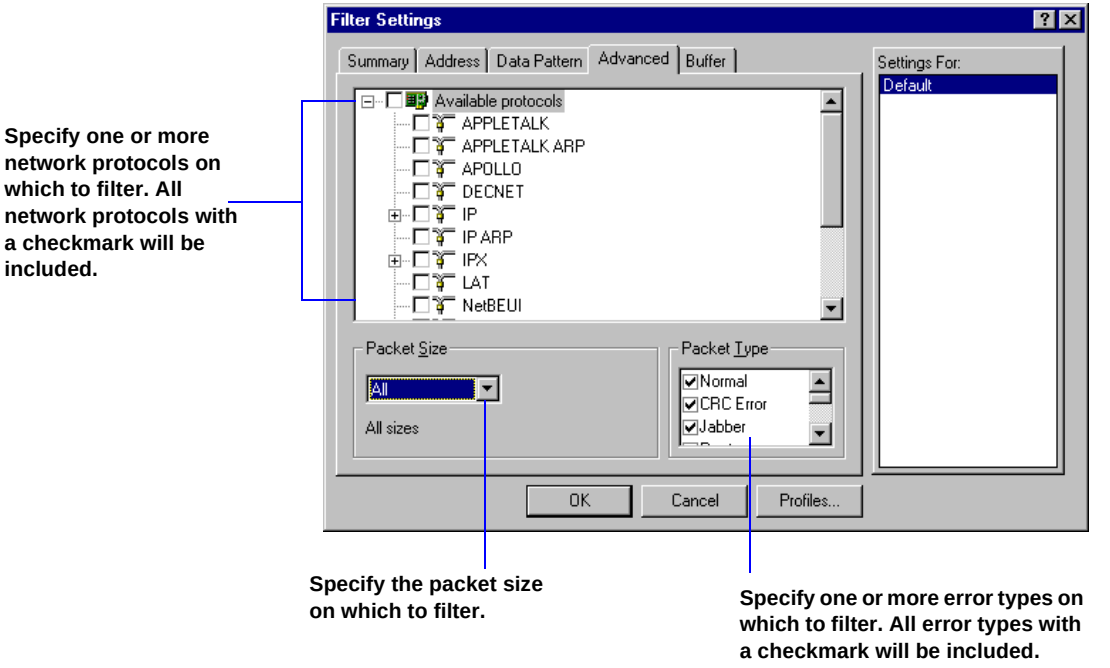


Figure 5–3. Setting Advanced Filters

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 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 5–4 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.

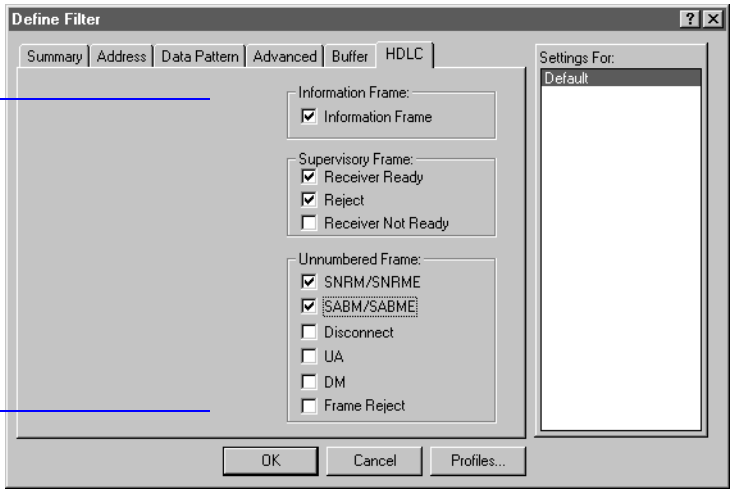


Figure 5–4. Setting WAN\Synchronous Frame Type Filters

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 5–5*).

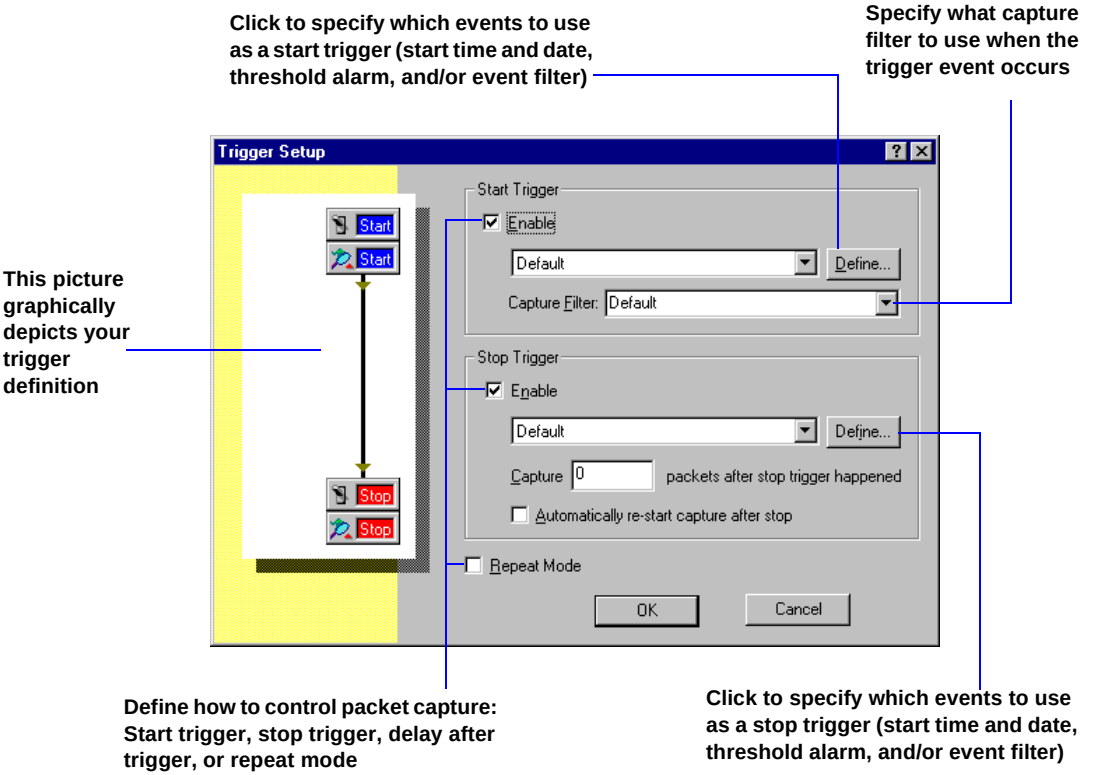


Figure 5–5. Defining a Trigger

Using the Address Book 6

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 and IP 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.

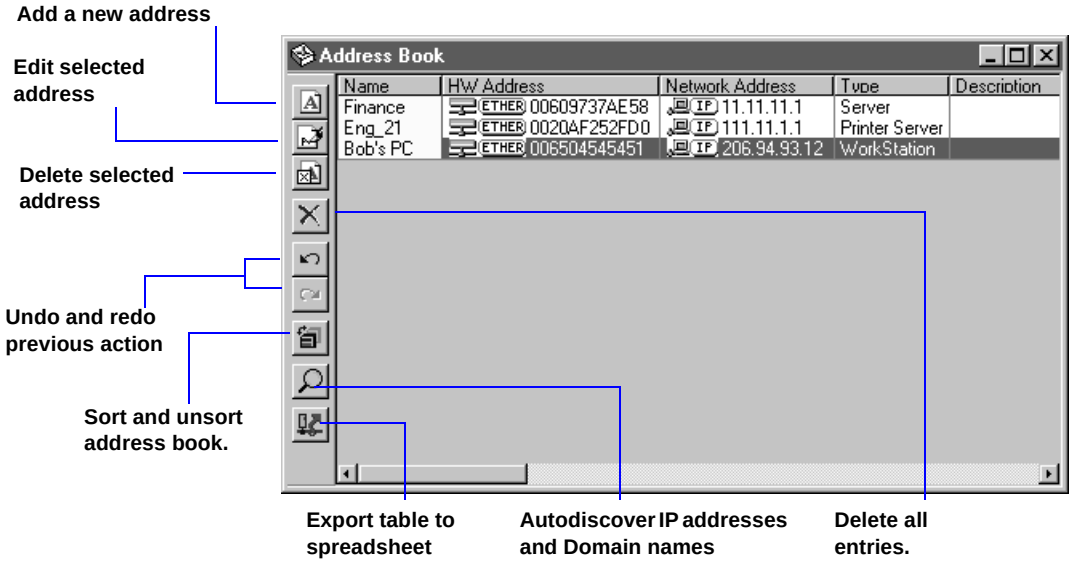


Figure 6–1. The Address Book

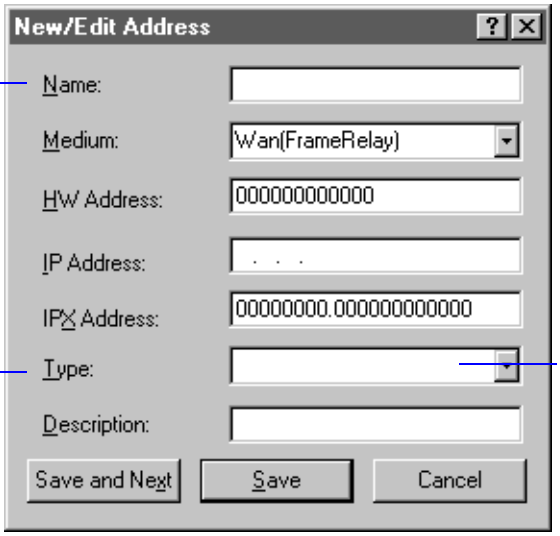
Entering Names Manually

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

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*).

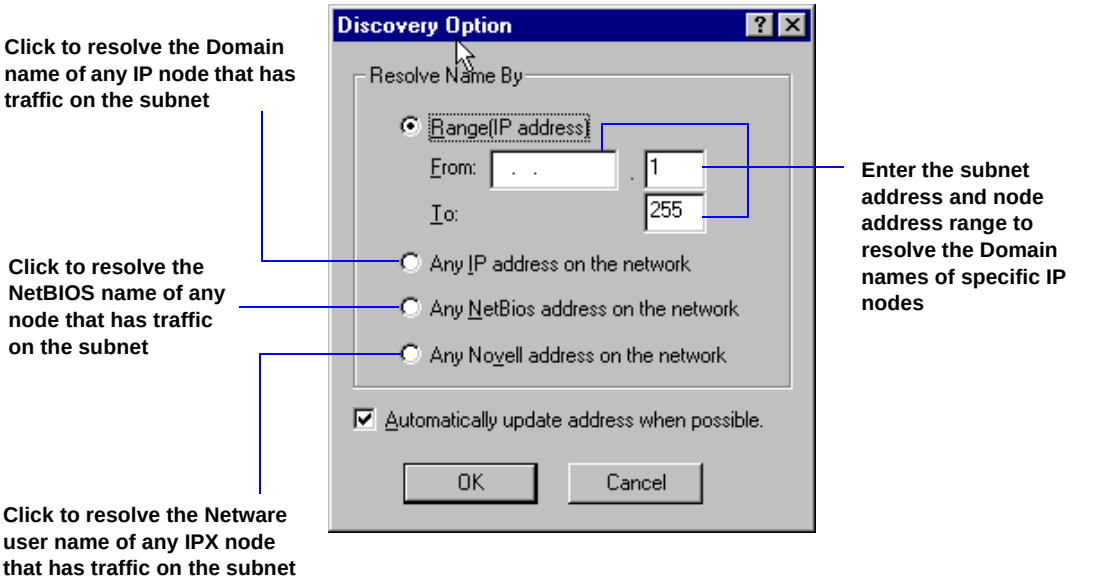


Figure 6–3. Setting Autodiscovery Options

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*.

Managing Alarms 7

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.

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.

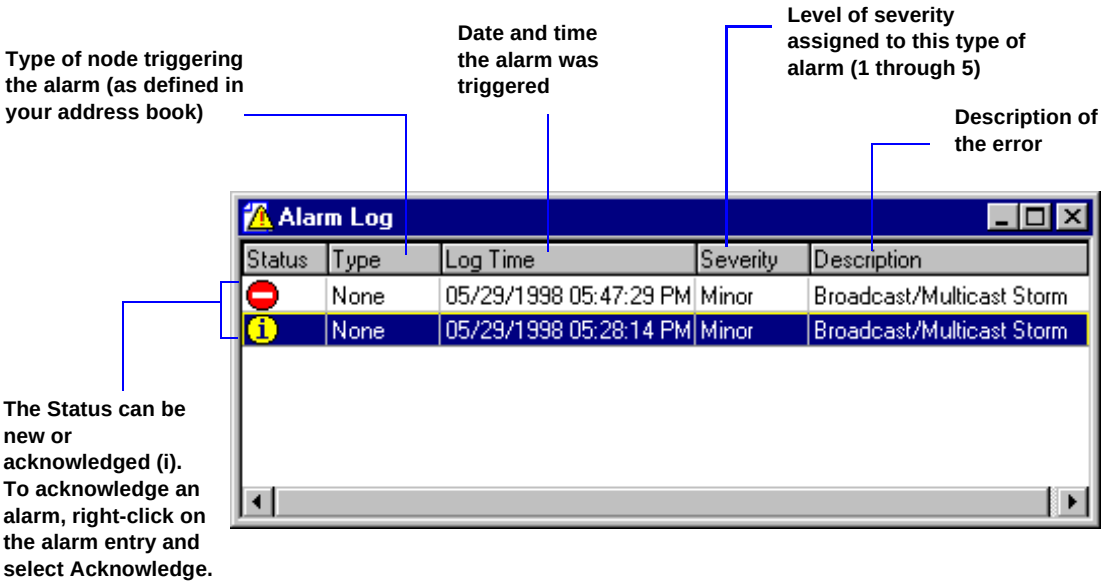


Figure 7–1. The Alarm Log

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**.

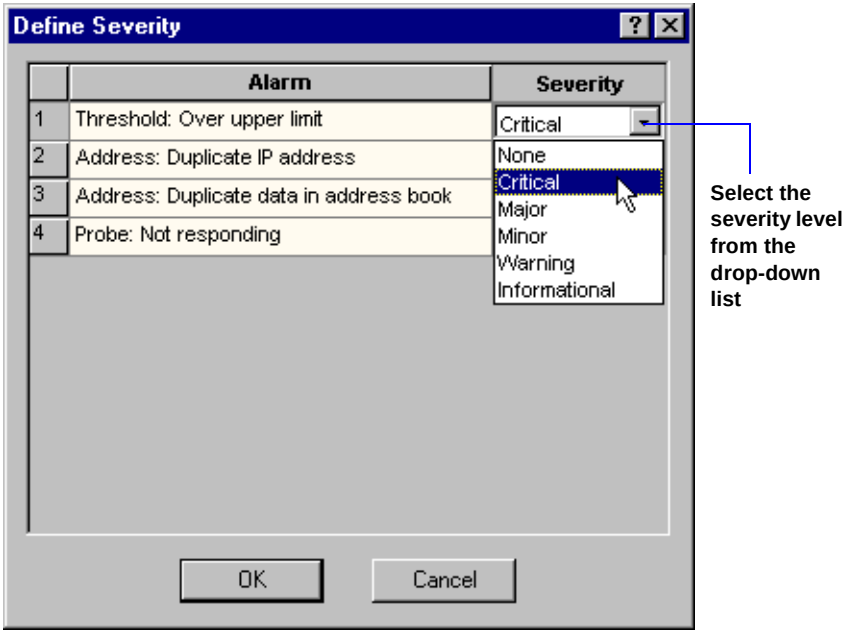


Figure 7–2. Setting Severity Levels for Monitor Alarms

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.

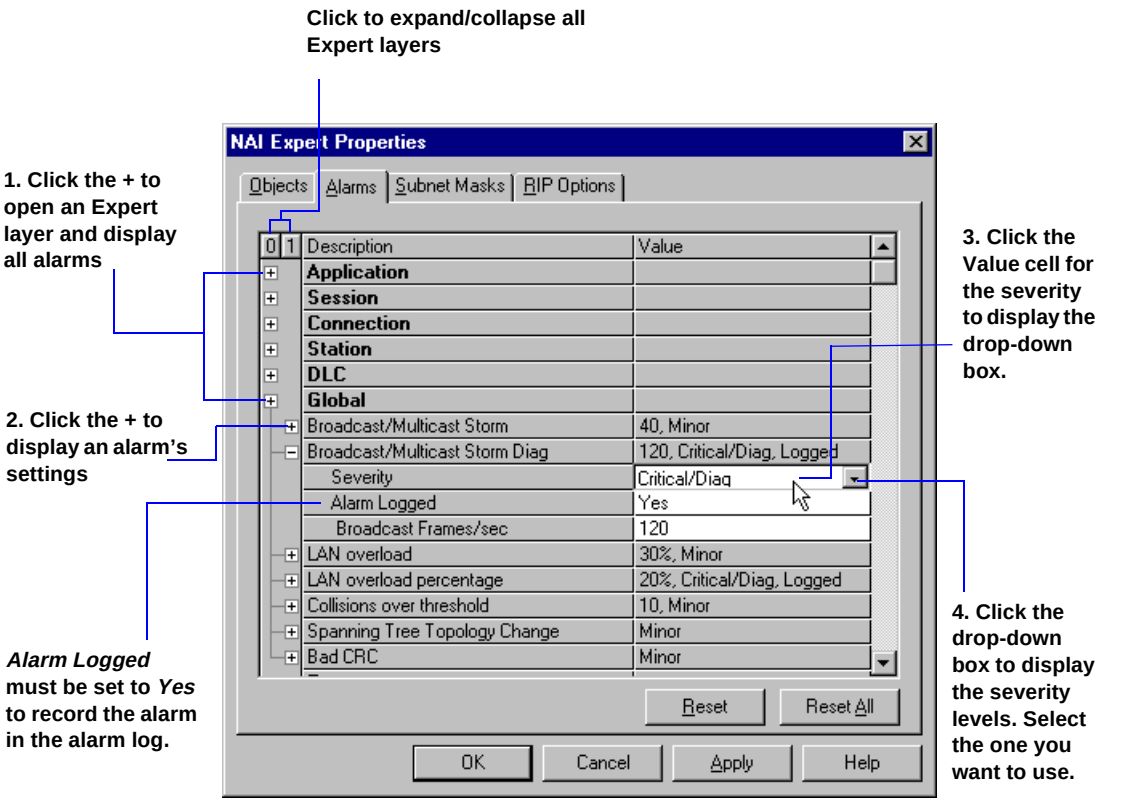


Figure 7–3. Setting Severity Levels for Expert Alarms

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*.

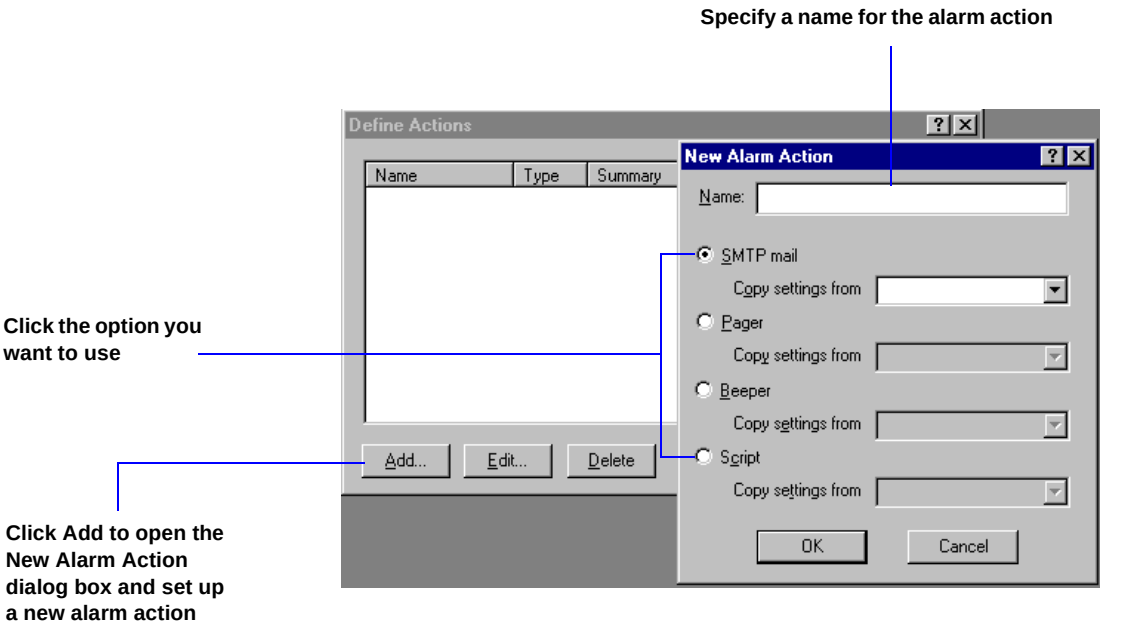


Figure 7–4. Setting an Alarm Notification Action

Enabling Alarm Actions

Assign 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).

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.

Using Sniffer Pro Tools 8

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.

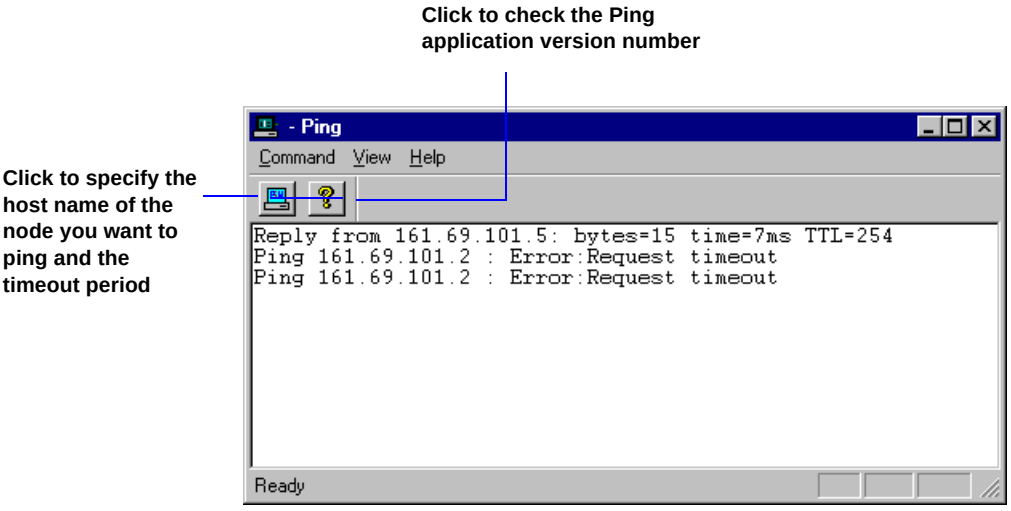


Figure 8–1. The Ping Log Window

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.

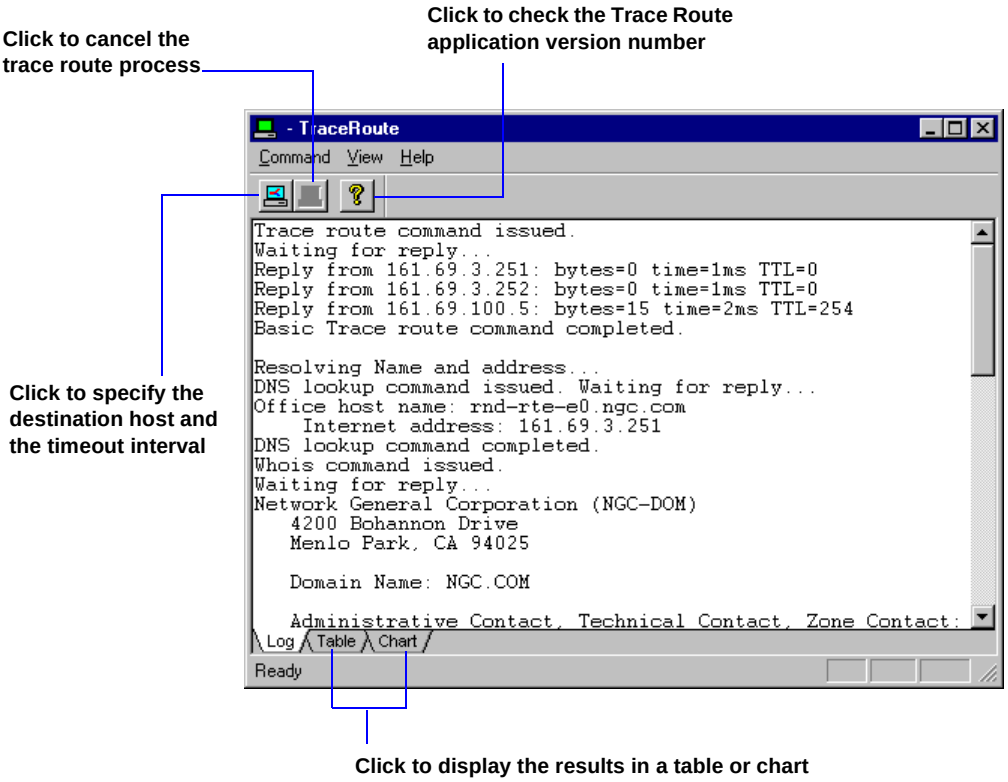


Figure 8–2. The Trace Route Log Window

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

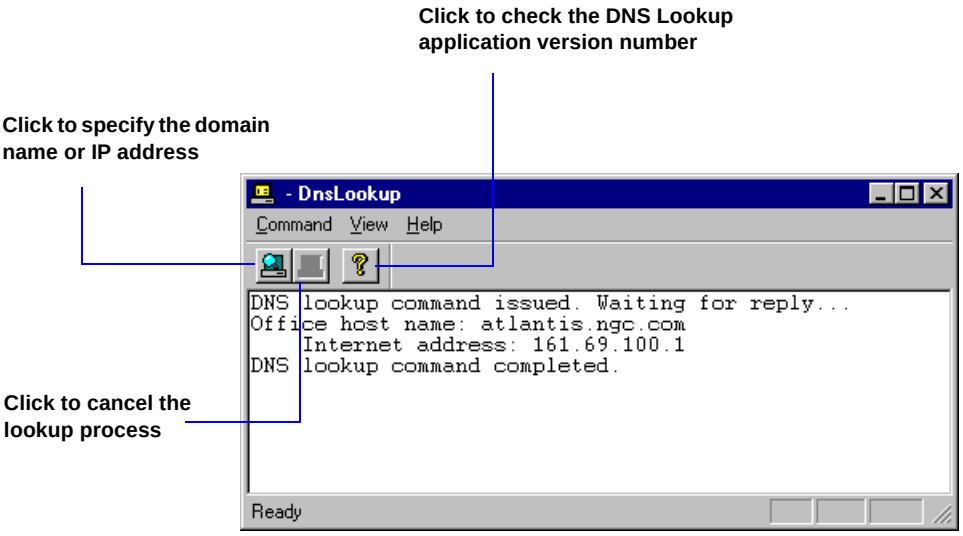


Figure 8–3. The DnsLookup Log Window

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*.

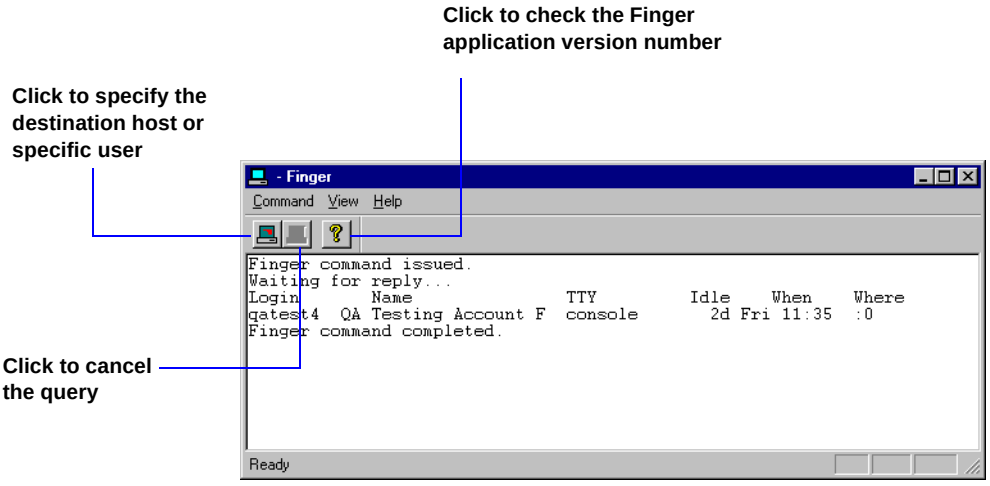


Figure 8–4. The Finger Log Window

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*.

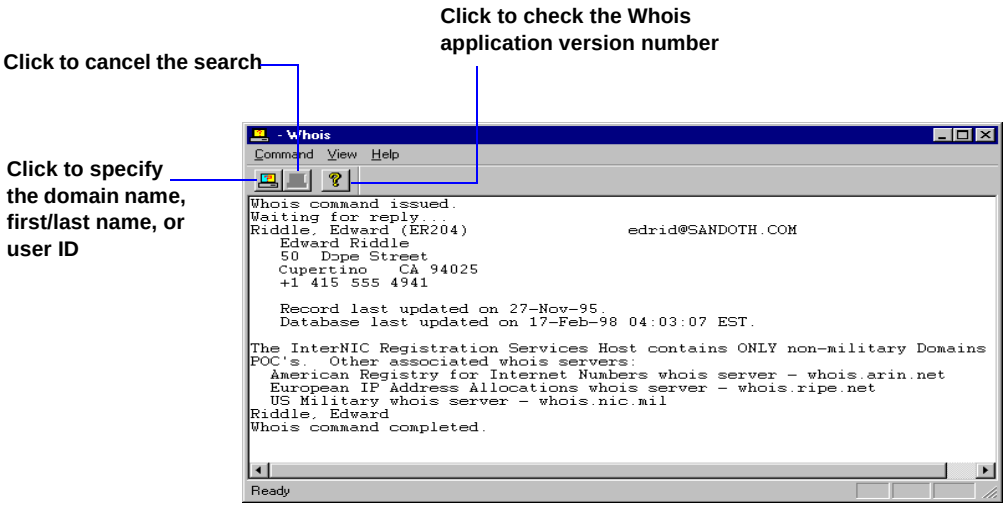


Figure 8–5. The Whois Log Window

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**.

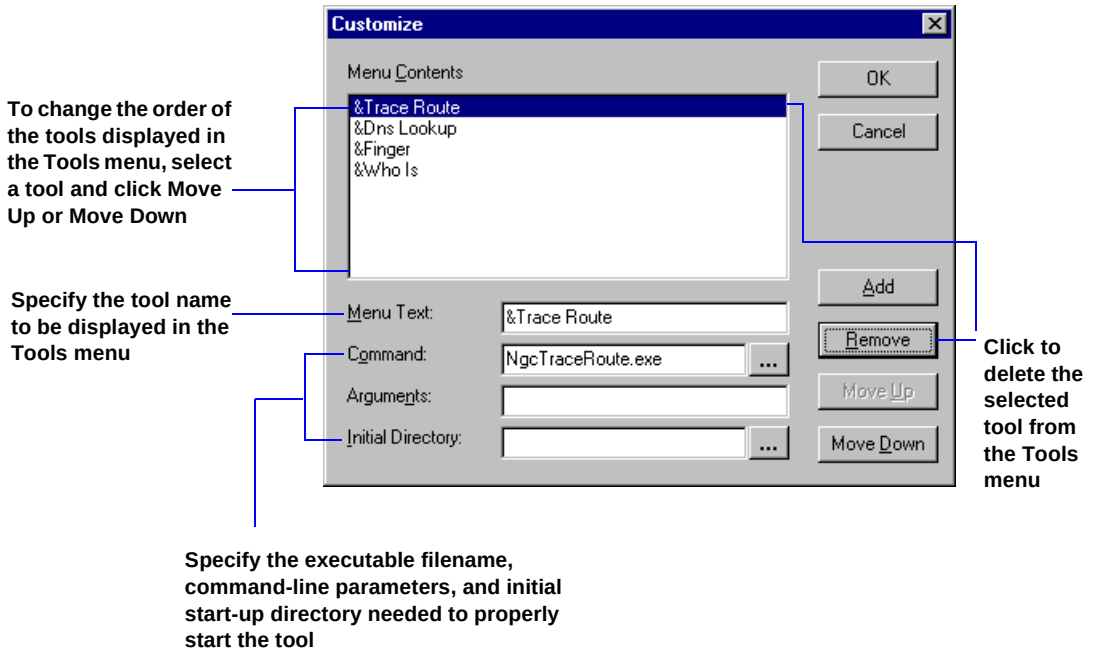


Figure 8–6. Adding Tools to the Tools Menu

Using the Packet Generator 9

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.

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.

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

Sending a Single Packet

Editing Packet Contents

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.

- 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).

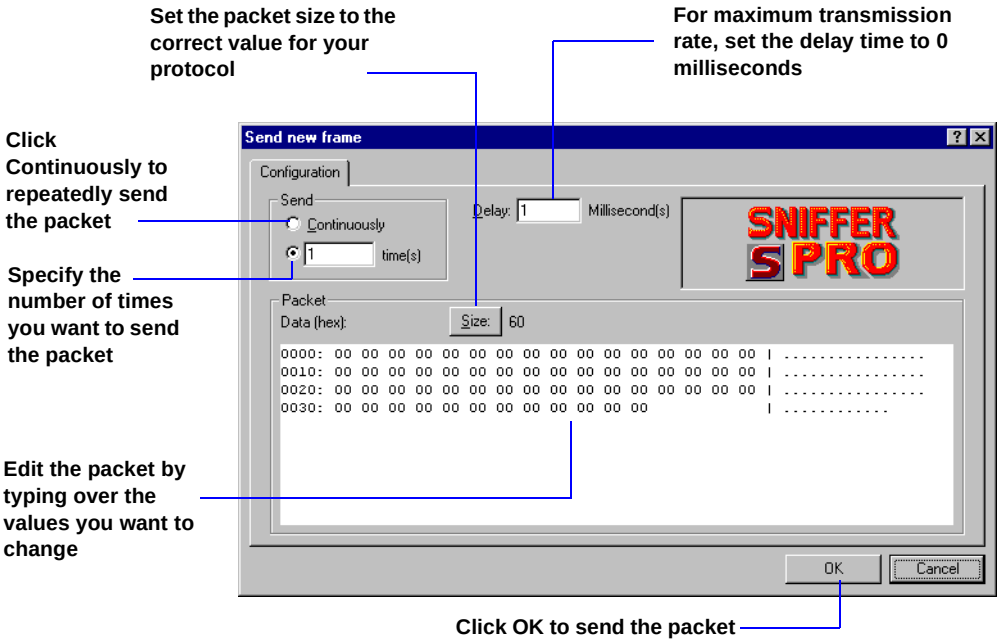


Figure 9–1. Transmitting a Single Packet

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.

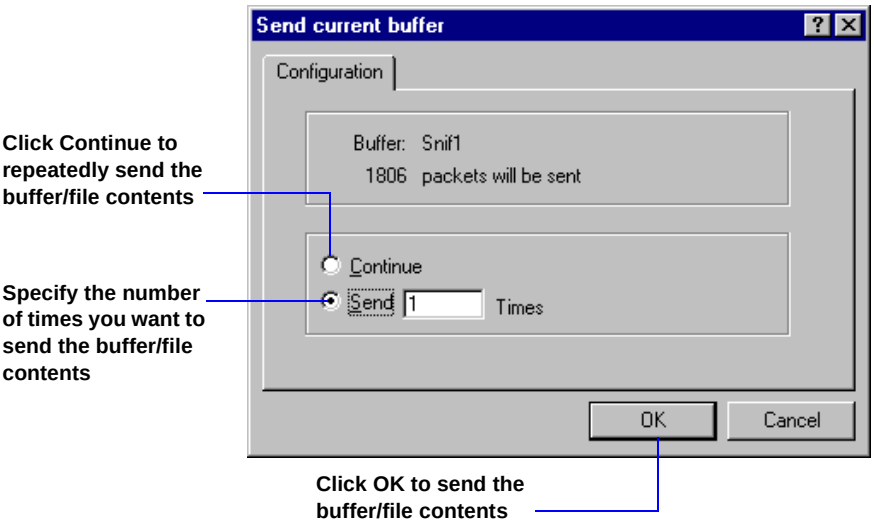


Figure 9–2. Transmitting the Current Buffer Contents

Network Adapters and Settings

10

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 10–1*). 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.

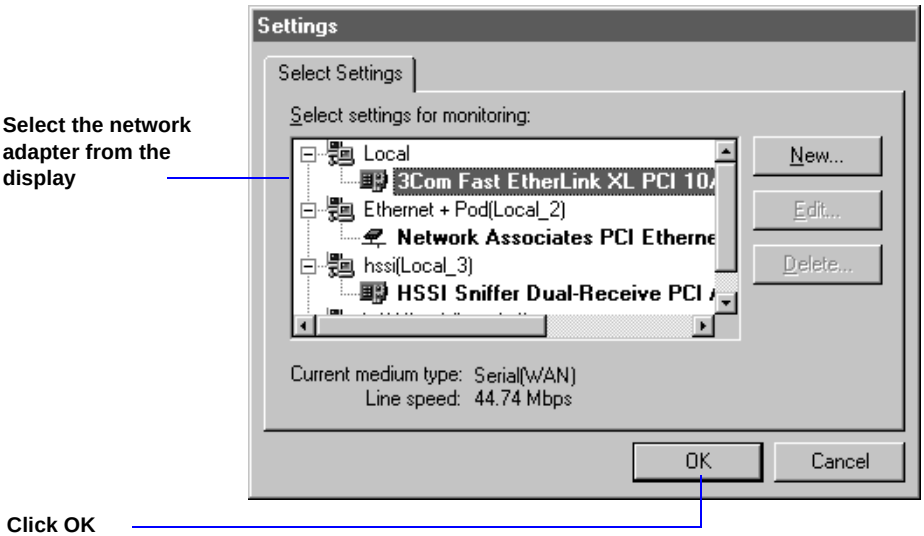


Figure 10–1. Selecting a Network Adapter

Creating Sniffer Local Agents

Monitoring Two or More Network Adapters Concurrently

Maintaining Multiple Sniffer Pro Settings Files

Defining a New Probe Using the WANBook

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 10–2 shows the New Settings dialog box.

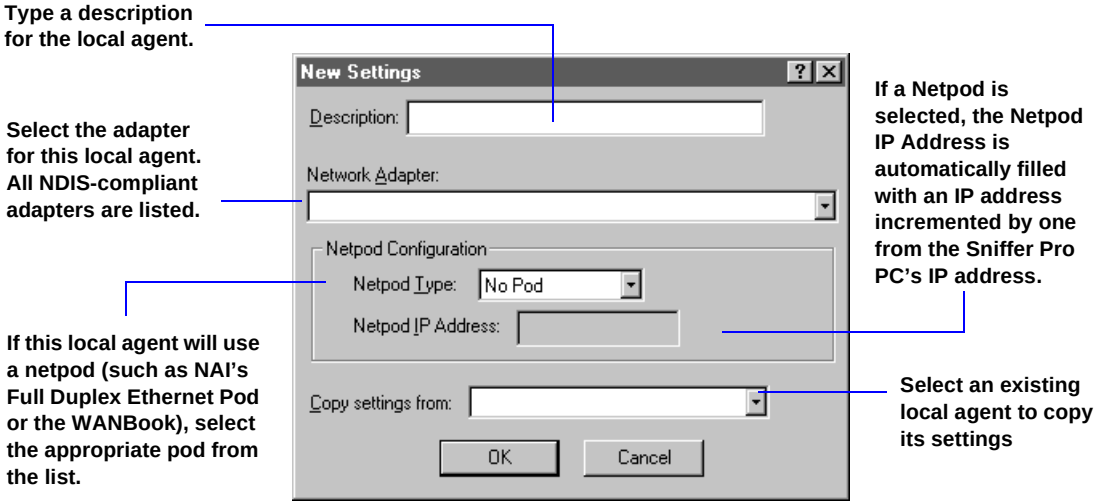


Figure 10–2. Creating a Probe