

NetXRay® Protocol Analyzer and Network Monitor User's Guide

Release 3.0

Network General, Sniffer, Distributed Sniffer System, SniffMaster and NetXRay are registered trademarks of Network General Corporation and/or its wholly owned subsidiaries. All other registered and unregistered trademarks in this document are the sole property of their respective owners. All specifications may be changed without notice.

© 1997 Network General Technology Corporation. All rights reserved.

September 1997

Part Number: 3037801

List of Figures

Figure		Page
1-1	<i>NetXRay Tool bar</i>	1-2
1-2	<i>NetXRay Status Bar</i>	1-3
1-3	<i>Dashboard View</i>	1-4
1-4	<i>Packet Capture Window</i>	1-5
1-5	<i>Packet Viewer Window</i>	1-6
1-6	<i>Traffic Map</i>	1-9
1-7	<i>IP Conversation Traffic in the Matrix Window</i>	1-10
1-8	<i>Packet Generator Window</i>	1-11
1-9	<i>Host Table Window</i>	1-12
1-10	<i>History Window</i>	1-14
1-11	<i>The Protocol Distribution Window</i>	1-15
1-12	<i>The Matrix Window Showing a Complete Traffic Map</i>	1-16
1-13	<i>Options Window</i>	1-17
1-14	<i>Discovery Option Dialog Box</i>	1-18
1-15	<i>Example of How to Arrange a Docking Window</i>	1-23
1-16	<i>Workspace Tab in the Options Window</i>	1-23
1-17	<i>General Dialog Page in the Options Window</i>	1-24
1-18	<i>Help Topic Window</i>	1-25
2-1	<i>Packet Capture Window</i>	2-2
2-2	<i>Capture Window</i>	2-3
2-3	<i>Capture Profiles Dialog Box</i>	2-8
2-4	<i>New Capture Profile Dialog Box</i>	2-8
2-5	<i>Address Filter Settings Window</i>	2-9
2-6	<i>Capture Setting Data Pattern Filter Page</i>	2-12
2-7	<i>Edit Pattern Dialog Box</i>	2-15
2-8	<i>Edit Pattern Dialog Box</i>	2-16
2-9	<i>Data Pattern Filter Page</i>	2-17
2-10	<i>The Advance Filter Page in the Settings Dialog Box</i>	2-18
2-11	<i>The Advance Filter Page in the Filter Settings Dialog Box</i>	2-20
2-12	<i>The Capture Setting Buffer Option Page</i>	2-21

2-13	<i>A Buffer Dialog Page</i>	2-23
2-14	<i>The Capture Dialog Box</i>	2-23
2-15	<i>The Open dialog Box</i>	2-24
2-16	<i>Detailed File Listing in the Open Dialog Box</i>	2-24
2-17	<i>The Apply Capture Trigger Dialog Box</i>	2-26
2-18	<i>The Start Trigger Dialog Box</i>	2-26
2-19	<i>The New Trigger Dialog Box</i>	2-27
2-20	<i>The Start Trigger Dialog Box</i>	2-27
2-21	<i>The Apply Capture Trigger Dialog Box</i>	2-28
2-22	<i>The Apply Capture Trigger Dialog Box</i>	2-28
2-23	<i>The Stop Trigger Dialog Box</i>	2-29
2-24	<i>The Apply Capture Trigger Dialog Box</i>	2-29
2-25	<i>The Trigger Operation in Repeat Mode</i>	2-30
2-26	<i>The General Page in the Options Dialog Box</i>	2-31
3-1	<i>The Packet Viewer Window</i>	3-1
3-2	<i>Packet Display Option Dialog Box</i>	3-3
3-3	<i>Packet View Summary Window</i>	3-4
3-4	<i>Packet Display Options Window</i>	3-5
3-5	<i>The Packet Decode Summary Window</i>	3-6
3-6	<i>The Summary Display Page</i>	3-7
3-7	<i>Summary Display Page, HTTP and HTTPS Selected</i>	3-7
3-8	<i>Packet Decode Summary Window, TCP Displayed</i>	3-8
3-9	<i>Packet Viewer Detail Pane</i>	3-9
3-10	<i>Protocol Display Tab Dialog Box</i>	3-10
3-11	<i>Anchored Field in the Detail Pane</i>	3-12
3-12	<i>Search Packet Dialog Box – Data Page</i>	3-13
3-13	<i>Detail Decode View of a Packet</i>	3-13
3-14	<i>Search Packet Dialog Box – Status Page</i>	3-14
3-15	<i>The Go To Packet Dialog Box</i>	3-15
3-16	<i>Marking Packets in the Summary Pane</i>	3-15
3-17	<i>Marking All Packets</i>	3-16
3-18	<i>Post Filter Dialog Box</i>	3-17
3-19	<i>Print Dialog Box</i>	3-19
3-20	<i>Print to File Dialog Box</i>	3-20
3-21	<i>Save As Dialog Box</i>	3-21

3-22	<i>File Open Dialog Box</i>	3-21
4-1	<i>Matrix Summary in Outline Table Format</i>	4-5
4-2	<i>View of Matrix Higher-Layer Protocol Traffic</i>	4-6
4-3	<i>Display of the Detail Table</i>	4-7
4-4	<i>Detail Table Generating Protocol Types for a Particular Node Address</i>	4-7
4-5	<i>Bar Chart of Detail Table View</i>	4-8
4-6	<i>Pie Chart of Detail Table View</i>	4-9
4-7	<i>Pie Slicing in the Detail Table View</i>	4-9
4-8	<i>Traffic Map Window</i>	4-10
4-9	<i>Display of IP-Layer Traffic Map</i>	4-11
4-10	<i>Display of Selected Node from the Context Menu</i>	4-12
4-11	<i>Display of Visual Filter Selected Network Nodes</i>	4-13
4-12	<i>Display of the Packet Viewer Window</i>	4-13
4-13	<i>Display of Protocols with only the “Others” Box Checked</i>	4-14
4-14	<i>Display of New Packet Viewer Window with “Others” Checked</i>	4-15
4-15	<i>Metrix Summary in Outline Table Format</i>	4-18
4-16	<i>Host Table Outline</i>	4-19
4-17	<i>Traffic Loads Segregated by Protocol Types in Detail View</i>	4-20
4-18	<i>Node Addresses Grouped by Traffic Load in Detail Table View</i>	4-21
4-19	<i>IPX Selected in Bar Chart View</i>	4-22
4-20	<i>Top-N Pie Chart View</i>	4-23
4-21	<i>IP-Layer Protocol Distribution in Bar Chart View</i>	4-25
4-22	<i>IP-Layer Protocol Distribution in Pie Chart View</i>	4-26
4-23	<i>Display of Summary Information</i>	4-27
5-1	<i>The Packet Generator Window</i>	5-1
5-2	<i>The Packet Generator—Detail View</i>	5-2
5-3	<i>The Current Packet Window</i>	5-3
5-4	<i>The Decode Page in the Send Packet Dialog Box</i>	5-3
5-5	<i>Editing Packet Contents on The Decode Page</i>	5-4
5-6	<i>The Send Current Buffer Dialog Box</i>	5-5
6-1	<i>The Dashboard Window</i>	6-2
6-2	<i>The Dashboard—Detail Tab Display</i>	6-3
6-3	<i>The Dashboard—Mac Tab Display</i>	6-5

6-4	<i>Bar Chart of Network Utilization Distribution</i>	6-11
6-5	<i>Bar Chart of Packet Size Distribution</i>	6-11
6-6	<i>A History Samples Window</i>	6-12
6-7	<i>The Start Sample Menu</i>	6-13
6-8	<i>The General Page in the History Dialog Box</i>	6-13
6-9	<i>Sample History Graph</i>	6-16
6-10	<i>A Host Table in Ethernet LAN</i>	6-22
6-11	<i>A Host Table in Token Ring LAN</i>	6-23
6-12	<i>Display of the IP Host Detail Table</i>	6-27
6-13	<i>Bar Chart View of Top-N Host Nodes in Real Time</i>	6-28
6-14	<i>Host Table Properties Dialog Box, Top-N Chart Selected</i>	6-29
6-15	<i>Pie Chart View of Top-N Host Nodes in Relative Percentage (%) Load</i>	6-30
6-16	<i>Display of the Complete Traffic Map</i>	6-34
6-17	<i>Display of the IP Conversation Traffic Map</i>	6-34
6-18	<i>Display of Matrix Traffic Map Showing the Selected Nodes</i>	6-35
6-19	<i>Display of the MAC Matrix Outline Table View</i>	6-36
6-20	<i>Display of the IPX Matrix Detail Table View</i>	6-38
6-21	<i>Bar Chart View of the Top-N Busiest Node Pairs</i>	6-39
6-22	<i>Display of the Matrix Properties Dialog Box</i>	6-40
6-23	<i>Display of the Pie Chart View of Top-N Node pairs</i>	6-41
6-24	<i>Pie Chart View of Small Percentage (%)</i>	6-41
6-25	<i>Protocol Distribution Window</i>	6-43
6-26	<i>IP Protocol Distribution Window</i>	6-43
6-27	<i>Protocol Distribution in Table Form</i>	6-44
6-28	<i>The Protocols Page in the Options Dialog Box</i>	6-45
7-1	<i>The Alarm Page in the Options Dialog Box</i>	7-2
7-2	<i>The Alarm Actions Dialog Box</i>	7-2
7-3	<i>The New Alarm Action Dialog Box</i>	7-3
7-4	<i>Mail Information Dialog Box</i>	7-3
7-5	<i>The Schedule Dialog Box</i>	7-4
7-6	<i>The Test Dialog Box</i>	7-5
7-7	<i>The Pager Information Dialog Box</i>	7-6
7-8	<i>The Communication Setup Dialog Box</i>	7-6
7-9	<i>The Beeper Information Dialog Box</i>	7-7
7-10	<i>The Communication Setup Dialog Box</i>	7-8

7-11	<i>The Setup Information Dialog Box</i>	7-9
7-12	<i>The Select File Dialog Box</i>	7-10
7-13	<i>Display of Options Menu with Alarm Selected</i>	7-11
7-14	<i>Alarm Actions Dialog Box</i>	7-12
7-15	<i>New Alarm Action Dialog Box</i>	7-12
7-16	<i>Script Information Dialog Box</i>	7-13
7-17	<i>Select File Dialog Box</i>	7-13
7-18	<i>Test Dialog Box</i>	7-14
7-19	<i>The Alarm Page in the Options Dialog Box</i>	7-16
7-20	<i>The Alarm Page in the Options Dialog Box</i>	7-17
7-21	<i>The Define Alarm Severity Dialog Box</i>	7-18
7-22	<i>The Threshold Page in the Options Dialog Box</i>	7-19
7-23	<i>The Alarm Log</i>	7-20
8-1	<i>The Address Book</i>	8-2
8-2	<i>The New/Edit Address Dialog Box</i>	8-2
8-3	<i>The Address Book Context Menu</i>	8-3
8-4	<i>The Discovery Option Dialog Box</i>	8-5
8-5	<i>The Network Address Dialog Box</i>	8-5
8-6	<i>The Discovery Option Dialog Box</i>	8-7
8-7	<i>The Network Address Dialog Box</i>	8-7
8-8	<i>The Discovery Option Dialog Box</i>	8-8
9-1	<i>The Adapter Dialog Box</i>	9-1
9-2	<i>The New Probe Dialog Box</i>	9-2

List of Tables

Table		Page
<i>i</i>	<i>Scope of Each Chapter in this Manual</i>	<i>xix</i>
<i>ii</i>	<i>Network General Technical Support Department</i>	<i>xx</i>
1-1	<i>Tool bar Command Buttons and Their Usage</i>	1-2
2-1	<i>Capture Window Button List</i>	2-2
2-2	<i>Capture Gauge Windows Field Definitions</i>	2-3
2-3	<i>Capture Detail Window Field Definitions</i>	2-3
2-4	<i>Capture Window Context Menu Commands</i>	2-5
2-5	<i>Capture Menu Commands</i>	2-7
2-6	<i>Data Pattern Filter Button Definitions</i>	2-12
2-7	<i>Edit Pattern Dialog Box Field Definitions</i>	2-17
2-8	<i>Capture Buffer Setting Options</i>	2-21
3-1	<i>Description of the Summary Pane</i>	3-2
3-2	<i>Summary Address Field Display Format</i>	3-5
3-3	<i>Packet Window Shortcut Key Definitions</i>	3-11
3-4	<i>Packet Decode Printer Output Format</i>	3-18
4-1	<i>Information Displayed in Each View of the Matrix Summary</i>	4-2
4-2	<i>Three Additional Help Buttons for the Matrix Summary</i>	4-4
4-3	<i>Four Different Views of the Host Summary</i>	4-16
4-4	<i>Two Additional Help Buttons for the Host Summary</i>	4-17
4-5	<i>Three Different Views of the Protocol Distribution Summary</i>	4-24
4-6	<i>Three Additional Help Buttons for Protocol Distribution</i>	4-25
6-1	<i>Ethernet Global Statistics Network Field Definitions</i>	6-3
6-2	<i>Ethernet Global Statistics Error Field Definitions</i>	6-4
6-3	<i>Ethernet Global Statistics Packet Size Distribution Field Definitions</i>	6-4
6-4	<i>Token Ring Global Statistics LLC Field Definitions</i>	6-6
6-5	<i>Token Ring Global Statistics MAC Error Definitions</i>	6-7
6-6	<i>Context Menu Item Descriptions</i>	6-9

6-7	<i>History Dialog Box Parameters</i>	6-14
6-8	<i>Sample Interval and Sample Period Relationship</i>	6-15
6-9	<i>Display of the Four Different Views of the Host Table</i>	6-19
6-10	<i>Seven Additional Help Buttons for the Host Table</i>	6-20
6-11	<i>Ethernet Host Table Field Definitions</i>	6-22
6-12	<i>Token Ring Host Table Field Definitions</i>	6-24
6-13	<i>Context Menu Options</i>	6-26
6-14	<i>Display of Five Views of the Matrix Statistics</i>	6-30
6-15	<i>Seven Additional Help Buttons for the Matrix Statistics</i>	6-32
6-16	<i>The Context Menu Commands</i>	6-35
6-17	<i>Context Menu Commands</i>	6-37
8-1	<i>Script Names and File Formats</i>	8-10

Preface

About This Manual

This manual introduces the NetXRay[®] Protocol Analyzer and Network Monitor, a powerful network management and trouble shooting tool specifically designed for the Windows 95 and Windows NT environments.

Table i describes the organization of this manual.

Table i. Scope of Each Chapter in this Manual (1 of 2)

Chapter	Contents
<i>Chapter 1, Getting Started</i>	Describes the NetXRay operating environment, and gives you a quick tour of NetXRay..
<i>Chapter 2, Packet Capture</i>	Describes the Packet Capture operations, and various filter and trigger setting options.
<i>Chapter 3, Packet Decode</i>	Describes the contents of the Packet Viewer. It lists various methods to assist you in searching, viewing, filtering and saving the captured packets.
<i>Chapter 4, Packet Post Analysis</i>	Describes the Post Analysis of the Packet Viewer function.
<i>Chapter 5, Packet Generator</i>	Provides detailed steps to generate packets from the Packet Generator.
<i>Chapter 6, Network Monitor</i>	Describes the tools; Dashboard, History, Host Table, Matrix Table and Protocol Distribution for monitoring the real time statistical performance and long term trend analysis of your network.

Table i. Scope of Each Chapter in this Manual (2 of 2)

Chapter	Contents
<i>Chapter 7, Alarm Manager</i>	Shows how you can set up the alarm actions, statistics threshold, and work with the alarm log.
<i>Chapter 8, Address Data Base</i>	Explains the address book and data base files used in NetXRay.
<i>Chapter 9, Network Adapter Selection</i>	Shows you how to select a network adapter to run.
<i>Appendix A, Decode SNMP MIBs</i>	Shows you how to improve your SNMP MIB decoding.
<i>Appendix B, NetXRay Specifications</i>	Lists NetXRay protocol decode specifications.
<i>Appendix C, Configuration File NETXRAY.INI</i>	Lists NETXRAY.INI configuration options.

Technical Support

Network General[®] Technical Support is available from 6 a.m. to 6 p.m. Pacific time, weekdays. Technical Support is available via telephone, FAX, FAX-on-Demand, TDD for the hearing impaired, Internet mail, electronic bulletin board, and the World Wide Web home page. Outside of support hours, you may leave a voice message. Our Technical Assistance Centers are located in California and the United Kingdom.

If you purchased your Network General Corporation product from one of our International Distributors, you must contact that distributor for support assistance. Please review our World Wide Web site at <http://www.ngc.com> for information about contacting our International Distributors.

Table ii describes the various ways to access Technical Support.

Table ii. Network General Technical Support Department (1 of 2)

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

Telephone Number (North America only)	+1-800-395-3151
---------------------------------------	-----------------

Table ii. Network General Technical Support Department (2 of 2)

Telephone Number (other International)	+1-650-473-2090
FAX	+1-650-473-2540
FAX-on-Demand (North America)	+1-800-764-3329
FAX-on-Demand (other International)	+1-650-473-2690

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

Telephone - France (toll-free)	0800 90 72 91
Telephone - Germany (toll-free)	0130 81 92 37
Telephone - Switzerland (toll-free)	0800 55 00 29
Telephone - Europe - Voice	+44 1753 827590
FAX	+44 1753 827520
e-mail	uk_support@ngc.com

Worldwide

TDD for the hearing impaired	650-473-2444
SniffNet BBS (300 to 28,800 bps)	650-327-3875
Internet Address	support@ngc.com
World Wide Web (Internet) information	http://www.ngc.com


World Wide Web

You can obtain additional information about Network General and its products and services from the World Wide Web at <http://www.ngc.com>.

Training

Network General offers a comprehensive set of training courses focused on hands-on network analysis, monitoring, and troubleshooting using Network General products. Courses can be conducted at your site, at central locations throughout the globe, or at training centers in Menlo Park and Anaheim, California; Chicago, Illinois; and Atlanta, Georgia. For more information

about these courses, contact your sales representative or call
Network General Corporation.



Chapter 1

Getting Started

This chapter describes the steps to start NetXRay, and gives you a quick tour of the basic NetXRay functionality.

Starting NetXRay

To start NetXRay:

1. In Windows 95 or Windows NT 4.0, click the **Start** button, and then point to Programs. Click the NetXRay program to start it.
2. In Windows NT 3.51, open the NetXRay program group, and double-click the **NetXRay** icon to start.
3. If you have more than one NDIS 3.1 compliant adapters installed in the system, an Adapter dialog box may be displayed. You must select a network adapter as the target network for NetXRay to monitor.

NOTE: If you previously selected the **NDIS Dial-Up Network** option during Windows 95 setup, a **Dial-Up Adapter** icon will be shown in the Adapter list box. Choose the Dial-Up Adapter to allow you to monitor traffic between your computer and the remote host or server.

Using the Tool Bar

The NetXRay Tool bar shown in [Figure 1-1](#) gives you access to frequently used menu commands without going to the Menu Bar. You can reveal the Tool tips by placing the mouse pointer over the Tool bar icon. A small pop-up box with the name of the tool will be displayed. The Tool bar is a standard docking window. You can follow the tips outlined in [Arranging Docking Windows on page 1-22](#) to place the Tool bar at the location of your choice.



Figure 1-1. NetXRay Tool bar

The Tool bar commands are listed in [Table 1-1](#).

Table 1-1. Tool bar Command Buttons and Their Usage (1 of 2)



















Button	Usage
	Invoke the File Open dialog box.
	Save the active document to a file.
	Invoke the Print dialog box.
	Stop and abort the current printer output.
	Go to the first packet in the Packet Viewer.
	Go to the previous packet in the Packet Viewer.
	Go to the next packet in the Packet Viewer.
	Go to the last packet in the Packet Viewer.
	Toggle to open or close Dashboard.
	Toggle to open or close Packet Capture.
	Toggle to open or close Packet Generator.
	Start Host Table.

Table 1–1. Tool bar Command Buttons and Their Usage (2 of 2)

Button	Usage
	Start Matrix Statistics.
	Open History folder.
	Start Protocol Distribution.
	Display chart size and utilization.
	Display Alarm Log.
	Display Address Book.

NOTE: Tool bar can be removed from the Windows space. To remove, go to Tools and select **Options...** click the Workspace tab. Uncheck **Tool bar**.

Viewing the Status Bar

The NetXRay Status bar as shown in [Figure 1–2](#) shows:

- The current packet # being printed.
- Number (#) of packets transmitted in progress.
- Number (#) of packets captured in progress.
- Capture trigger armed.
- Number (#) of unacknowledged alarm events.




Figure 1–2. NetXRay Status Bar

NOTE: The Status bar can be removed from the Windows space. To remove, go to **Tools** and select **Options....** Click the **Workspace** tab. Uncheck **Status bar**.

Opening the Dashboard

The Dashboard, as shown in [Figure 1–3](#), lets you view the network statistics in real time.

To start the Dashboard:

1. Go to the Tools menu, and select the **Dashboard** button, or click the  icon on the Tool bar. A Dashboard window is displayed.
2. The network traffic, packets per second, utilization, and errors per second is updated every second on the left side of each small box under the odometer. The number shown on the right side is the highest number recorded since the last reset.
3. Click the **Detail** tab to view the total network traffic statistics cumulated since NetXRay is started.

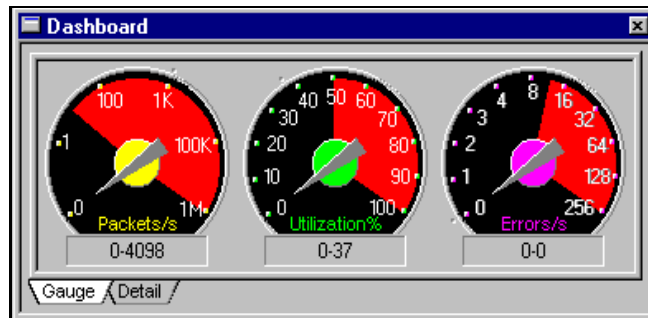


Figure 1–3. Dashboard View

Capturing Unique Protocol Packets

NetXRay has a unique ability to set up an Advanced Filter to capture packets that match one or more protocol types. [Figure 1–4](#) shows the packet capture window.

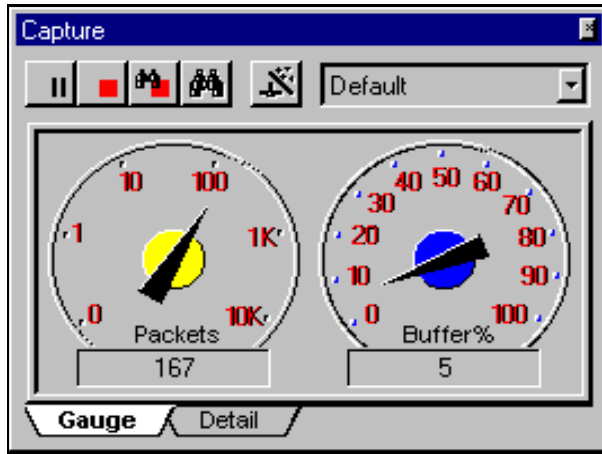






Figure 1–4. Packet Capture Window

To capture IPX packets:

1. Go to Tools menu, and select **Capture**, or click the  icon on the Tool bar. A Dashboard window is displayed.
2. From the Capture window, click  to bring up the Capture Setting property dialog box.
3. Click the **Profiles...** button to bring up the Capture Profiles dialog box.
4. Click the **New...** button. Enter the new profile name, for example, my IPX filter. Click **OK**.
5. Click the **Done** button to close the Profile dialog box.
6. Click the **Advance Filter** property page tab.
7. Click the check box in front of the IPX from the protocol tree list.
8. Click **OK**.
9. Click  to start capture.
10. Wait until you see packet counter showing packets being captured.
11. Click  button to stop the capture and bring up the Packet Viewer window, [Figure 1–5](#). The Packet Viewer shows only IPX packets captured.

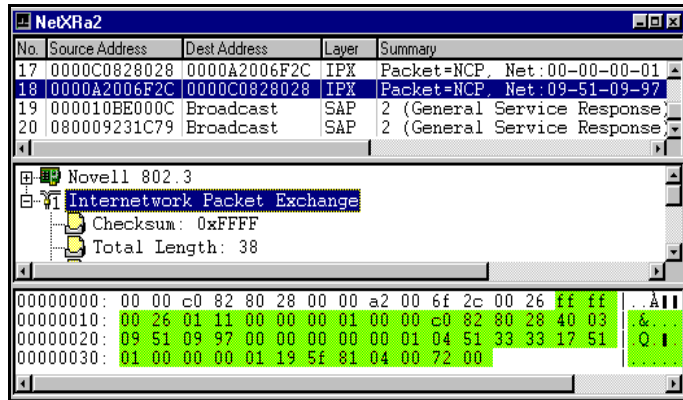


Figure 1–5. Packet Viewer Window

Captured packets can only be saved from the Packet Viewer window.


To save a capture file:



1. Select **File** from the Menu bar, click on **Save As....** A Save As dialog box will be displayed.
2. Enter the file name for your capture file. You have the option of choosing a file folder or location in which to put it.
3. Click **OK**.

Capturing Conversations Over IP Routers

NetXRay provides you with the ability to set IP address filters. This enables easy capturing of IP conversations over routers.

To set up to capture IP conversations:

1. From the Capture window, click  to bring up the Capture Setting property dialog box.
2. Click the **Profiles...** button to bring up the Capture Profiles dialog box.
3. Click the **New...** button. Enter the new profile name, for example, **my IP filter**. Click **OK**.


4. Click the **Done** button to close the Capture Profiles dialog box.
5. Select **IP** from the Address Type list box.
6. Click the **Include** radio button.
7. Enter the first IP address (for example, 192.44.81.128) under Station 1.
8. Enter the second IP address (for example, 192.55.90.133) under Station 2.
9. Select  (both directions).
10. Click **OK**. You have just set up a capture filter profile for **my IP filter** to capture conversation between a pair of IP stations.
11. Click  to start capture.

NOTE: Using Address Book facility, you can pre-assign a logical name and an IP address for each host or server in your network. Then you can simply find the host name you want to use from the address book list box, and drag it to the station cell in the address filter.

Capturing Packets Matching a Certain Data Pattern

NetXRay lets you set up Data Pattern Filter to capture packets that match predefined data patterns.

To capture IPX RIP packets.

1. From the Capture window, click  to bring up the Capture Setting property dialog box.
2. Click the **Profiles....** button to bring up the Capture Profiles dialog box.
3. Click the **New...** button. Enter the new profile name, for example, IPX/RIP (PATTERN). Click **OK**.
4. Click the **Done** button to close the Capture Profiles dialog box.
5. Click the **Advance Filter** property page tab.
6. Select IPX from the protocol tree list box.

7. Click the **Data Pattern** property page tab. A default AND operator is shown.
8. Click the **Toggle AND/OR** button to change the operator to OR.
9. Click the **Add Pattern** button to invoke Edit Pattern dialog box.
10. Click the **From** list box down arrow button. Select **Protocol**. Enter 16 in the Offset field.

TIP: 16 bytes offset from beginning of IPX packet is the Destination Socket field.

11. Enter 2 in the **Len** field. Select **Hex** from the **Format** field. Enter hex number 04 at column 0 row 1, then 53 at column 1 row 1.

TIP: 0453 hex is the socket number for IPX/RIP.


12. Enter a symbolic name in the Name field, for example, Dest Socket.
13. Click **OK**. A new data pattern Dest Socket is created and connected to the OR operator.
14. Click the OR operator again to select it.
15. Click the **Add Pattern** button to invoke another Edit Pattern dialog box.
16. Click the **From** list box down arrow button. Select **Protocol**. Enter 28 in the Offset field.

TIP: 28 bytes offset from the beginning of an IPX packet is the Source Socket field.

17. Enter 2 in the **Len** field. Select **Hex** from the **Format** field. Enter hex number 04 at column 0 row 1, then 53 at column 1 row 1.

TIP: 0453 hex is the socket number for IPX/RIP.

18. Enter a symbolic name in the **Name** field, for example, Src Socket.
19. Click **OK**. A new data pattern Src Socket is created and connected to the OR operator just below the Dest Socket data pattern.
20. Click the **Evaluate** button. The resulting OR operation (Dest Socket OR Src Socket) is shown after the OR operator.
21. Click **OK** to save the filter.



22. Click  to start capture.

NOTE: Using capture filter requires additional CPU processing time to examine each packet for matching criteria. In a network with heavy traffic loads, you may miss packets. To avoid losing packets in capture, you can capture all traffic and assign the largest buffer size. After capture is stopped, apply a display filter to select the packets you want to see. Alternatively, you can use high performance PCI network adapter cards.

Using A Hot Link to Start Capture

NetXRay supports hot link in the Matrix traffic map, Matrix outline table, and Host outline table which allows you to launch packet capture with address filter for network nodes directly. The following procedure shows the steps to launch capture with multiple IP address filters.

To launch capture with multiple IP address filters:

1. Select Matrix from the Tools menu, or click  on the Tool bar.
2. Click the traffic map button  on the side of the Matrix window to show a birds-eye view of the network traffic pattern in real time (*Figure 1–6*).

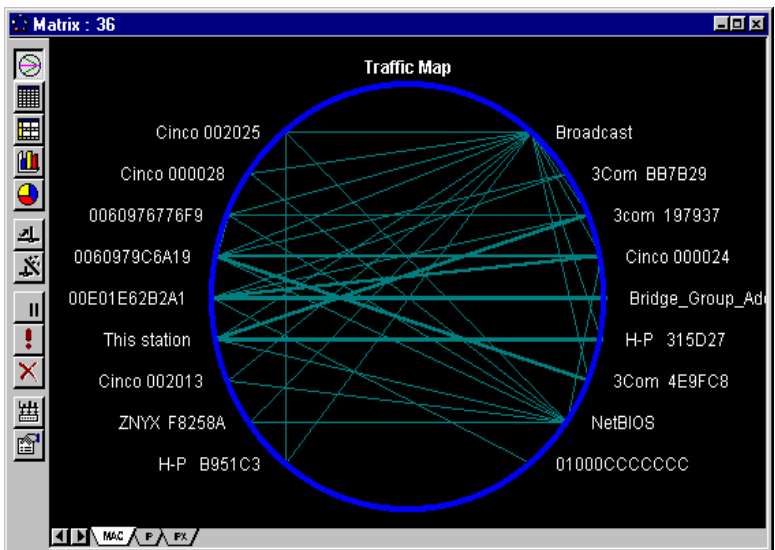


Figure 1–6. Traffic Map

3. To view IP conversation traffic, click the IP tab on the bottom of the Matrix window. The traffic map is showing all IP conversation (*Figure 1–7*).

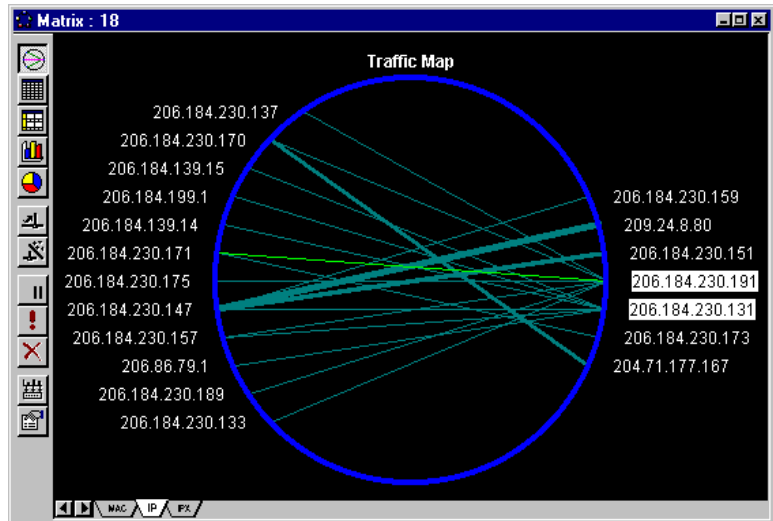





Figure 1–7. IP Conversation Traffic in the Matrix Window

4. To filter traffic for the network node, click and select the node of your choice. To select more than one node, hold the **Control** key down, then click additional nodes. If the network node address is not legible on the traffic mode, you can use Zoom command from the context menu to enlarge the map, or point the cursor on the address object until a small pop-up window displays the address of the node.
5. Click the right mouse button to invoke the Matrix context menu.
6. Select Capture to launch packet capture with address filter.

Playing Back a Captured File

Once you have an active Packet Viewer displayed, you can playback (retransmit) the entire contents onto the network.

To playback the contents on the network:

1. Choose **Packet Generator** from the Tools menu, or click the  icon on the Tool bar. A Packet Generator window as shown in *Figure 1–8* is displayed.
2. Select **File** from the Menu bar, click on **Open....** A File Open dialog box is displayed.
3. Enter the file name for your capture file. You have the option of choosing a file folder or location in which to put it.
4. Click **OK**. A Packet Viewer window is displayed.
5. Click the  **Send Current Buffer** button. A Send current buffer... dialog page is displayed.
6. Choose between send continuously, or send a number of times.
7. Click **OK** to start packet generation.
8. Click the **Anim** tab to view the packet generator progress in animated graphic mode. Note that the rate of the small ball going through the network link does not reflect the true speed of transmission. You can also click the **Detail** tab to see the actual transmission rate.
9. Click the  button, if you want to stop the transmission of packets.

NOTE: If you want to transmit only certain type of packets, for example, IPX packets, you can apply Display Filter to the packets in the Packet Viewer first, then playback the filtered IPX packets.

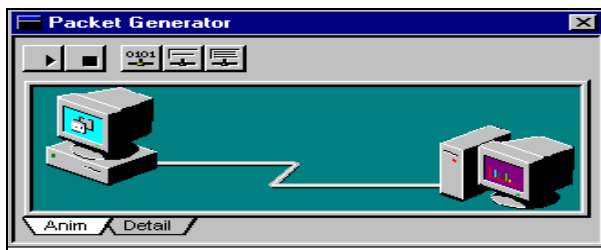




Figure 1–8. Packet Generator Window

Displaying the Most Active Sending Nodes

The host statistics provides a quick analysis of the traffic statistics collected for each host node in real time. You can view host traffic at the MAC layer, or selectively view only network layer traffic in the IP or IPX layers.

To view the most active nodes in the network:

1. Go to Tools menu, and select Host Table, or click  on the Tool bar. A host table window is displayed ([Figure 1-9](#)).
2. Click  then select the MAC tab in the window.

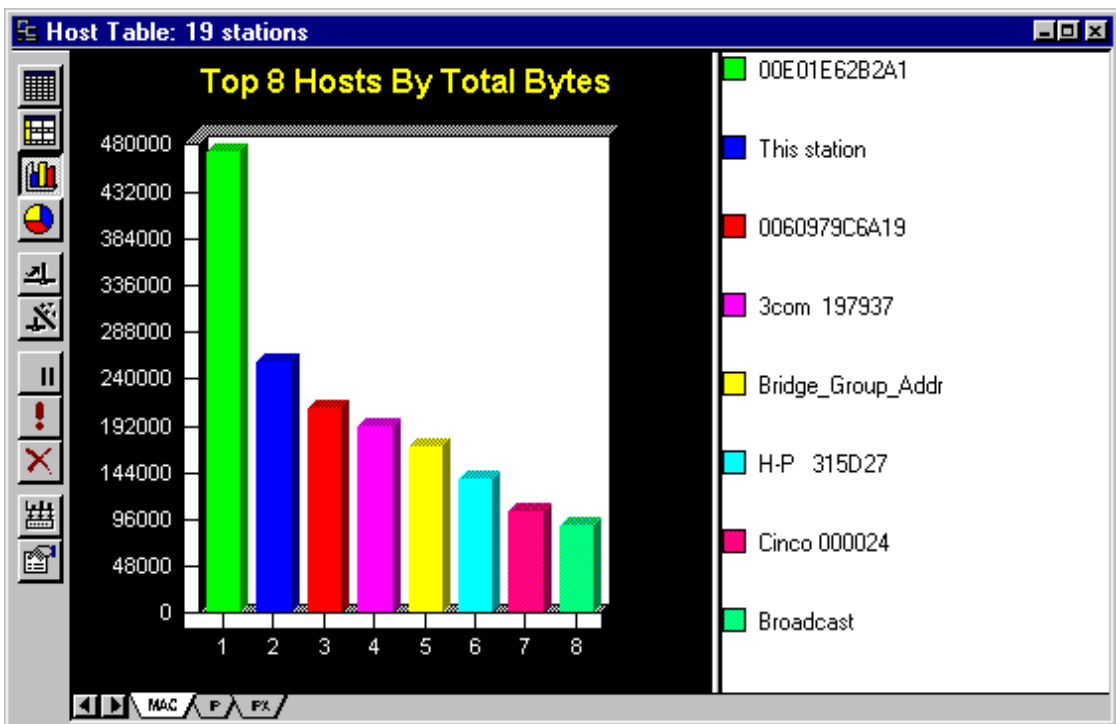




Figure 1-9. Host Table Window

Using Network Monitor: History

History allows you to collect network statistics for a particular variable over a period of time.

To start monitoring:

1. Select **History** from the Tools menu or click the  icon on the Tool bar. A History folder, as shown in *Figure 1-10* is displayed.
2. Click and select a network variable icon of your choice to be monitored from the History folder.
3. Click the right button to invoke the context menu.
4. Select **Property....** A History dialog box is displayed.
5. Enter the sampling interval (up to 3,600 seconds). NetXRay maintains a maximum of 3,600 samples in the system. For example, if you enter 60 seconds, History graph will plot a maximum of 3,600 minutes (60 hours) of statistical samples.
6. Enter high and low threshold values for the network statistics you want to monitor. If the sampled value exceeds the high threshold value, the above normal color will be shown in the bar graph. Any values that fall outside of the thresholds will be recorded in the Alarm Log.
7. Optionally, select a graph type to display.
8. Click the **Color** tab to show the color setting page. You can customize various color combinations for the graph display.
9. Click **OK** to save the property setting.
10. To start the History trend, double-click the icon of your choice. A history graph will be displayed.
11. You can adjust the scaling factor, or change the graph into a line chart or an area chart. If you want to freeze the graph from updating, click the **Pause**  button.
12. The history graph will stop when the maximum number of samples are collected or when the history window is closed.

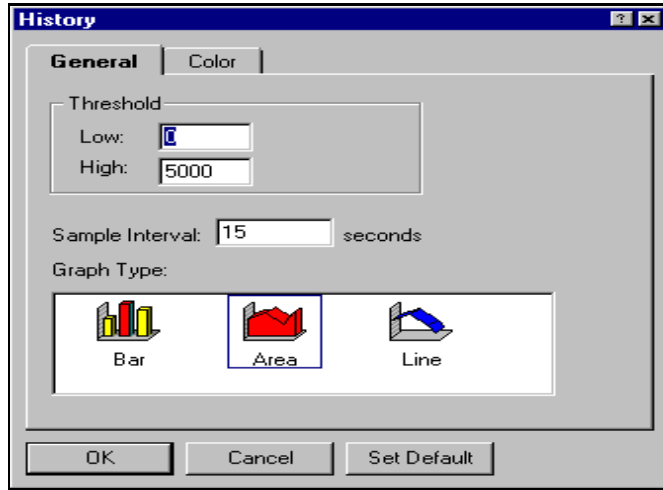



Figure 1–10. History Window

Monitoring Network Protocol Distribution

The NetXRay Protocol Distribution function allows the reporting of network usage based on the network-layer protocols, that is, IPX/SPX, TCP/IP, NetBIOS, AppleTalk, DECnet, SNA, Banyan and others in real time. It also supports the “TCP/IP Application Distribution” function, which reports on the percentage or cumulated load of each TCP/IP application as part of TCP/IP traffic. NetXRay monitors popular applications, such as NFS, FTP, Telnet, SMTP, POP, HTTP (WWW), Gopher, NNTP, SNMP, X-Window, and others.

It also monitors IPX transport-layer protocols; NCP, SAP, RIP, NetBIOS, Diagnostic, Serialization, NMPI, NLSP, SNMP, and SPX. Protocols not listed are grouped into the **Others** category.

To start protocol distribution monitoring,

1. Select **Protocol Distribution** from the Tools menu, or click the  button
2. Click the IP tab to view IP protocol distribution ([Figure 1–11](#)).

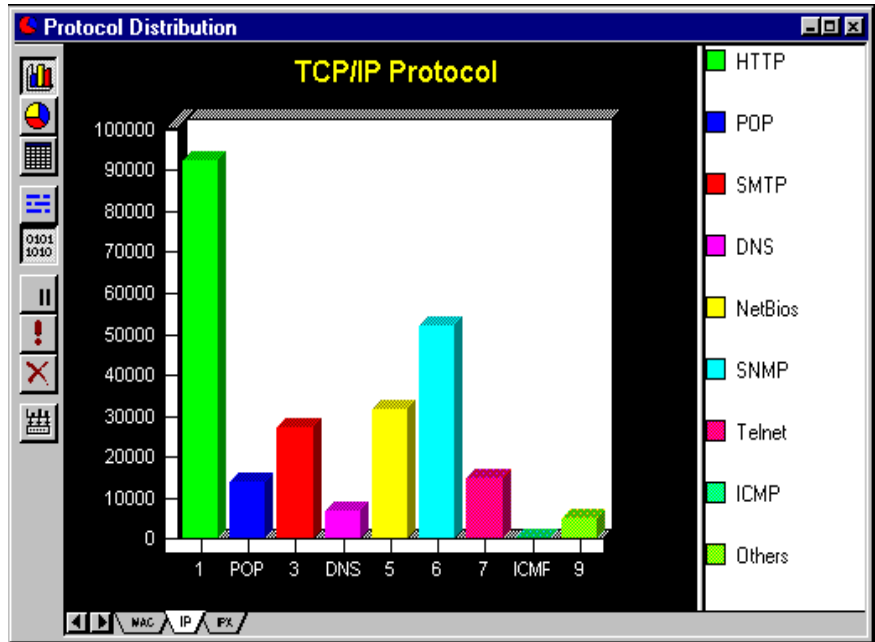


Figure 1-11. The Protocol Distribution Window

3. To exit, simply close the window.

Monitoring Traffic Between Nodes: Matrix

The matrix traffic map provides you with a birds-eye view of the network traffic patterns in real time. It gives a complete graphical presentation of the traffic pattern between network nodes.

To show the traffic map, simply click the **Traffic Map** button



on the left side of the Matrix Window [Figure 1-12](#).

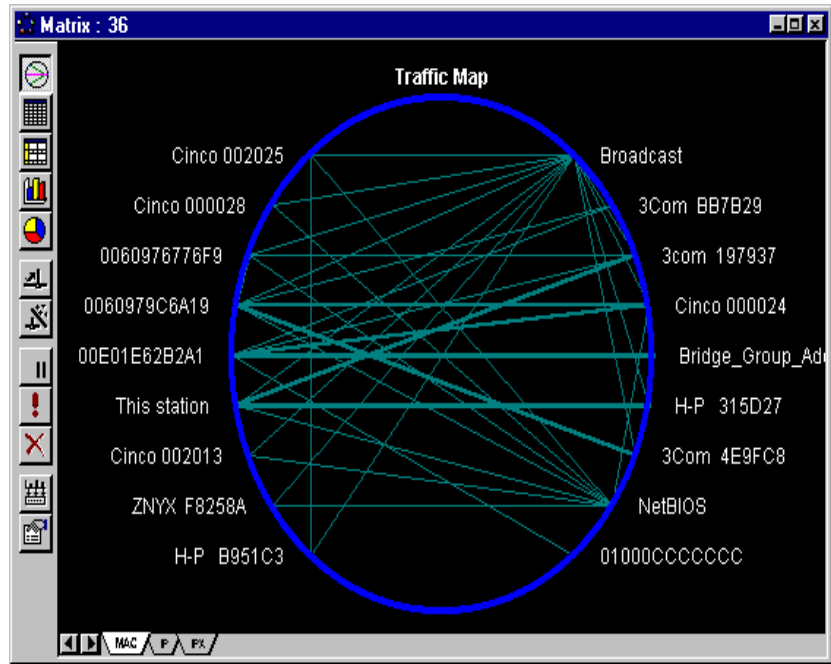


Figure 1–12. The Matrix Window Showing a Complete Traffic Map

Applying Pre-filter to Statistics Gathering

NetXRay lets you apply a pre-filter to network statistics gathering in real time. The same filter profile you defined for packet capture can be applied to statistics gathering as well.

To set up a filter, refer to [Packet Capture Setting on page 2–7](#). The filter you set for the statistics is applied to Dashboard, Host Table, Matrix Table, History, and Protocol Distribution equally.

Using the real time pre-filter on statistics, you can now look at your network loads in many different views. For example, by creating a hardware address filter to and from a router, you can easily tally the conversation traffic load to and from that router only. The Matrix Table can easily show who is talking to the router, and how often. If you open the Protocol Distribution window, it will show the % traffic load passing through the router by protocol types. The history graph will plot traffic load at the router over time.

Perhaps you want to examine who is running TCP/IP applications and how much IP traffic each host node is generating. In this example, you can create and apply the IP protocol filter to statistics, then start the Matrix and Host table statistics.

The same can be done to other protocol types, for example, IPX, AppleTalk, SNA, NetBEUI, and so on.

To apply a pre-filter to statistics gathering:

1. Select Tools/Options. The Options window opens as shown in [Figure 1-13](#).
2. Check **Apply Filter** for Statistics.
3. Select a filter of your choice from the drop-down list, and click **OK**.

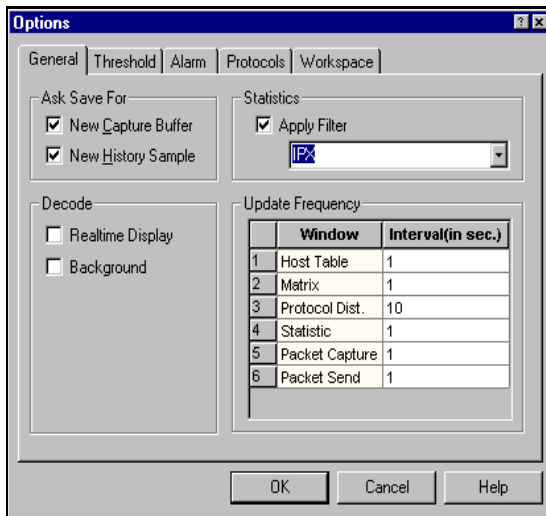



Figure 1-13. Options Window

Detecting Duplicated IP Addresses

The NetXRay IP Address and domain name auto-discovery function lets you create and maintain an address book of the recognized network nodes in your network. See [Chapter 8, Address Data Base](#) for instructions about how to use NetXRay to auto-learn addresses and names, and place them into your address book.

Once you have created the address book, you can follow the following steps to monitor your network for duplicated IP addresses.

To monitor your network for duplicated IP addresses:

1. Click the **Auto Discovery** button  on the Address Book window to bring up the Discovery Option dialog box ([Figure 1-14](#)).
2. Click the **Any IP address on the network** radio button. Click **OK** to start monitoring.

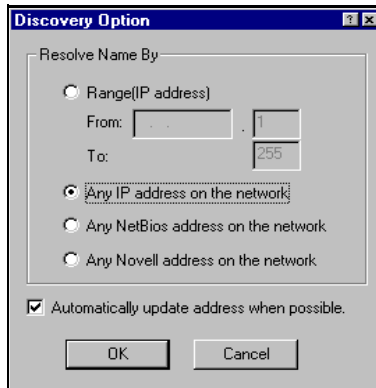


Figure 1-14. Discovery Option Dialog Box

3. A small modeless dialog box will show you the discovery in process. Every time NetXRay sees a new IP address, it will attempt to learn the IP's domain name. If a name is not found, the IP address is dropped, and not entered into the address book.
4. If a duplicated IP address is discovered with a hardware address different from the one previously saved in the address book, an alarm will be sounded and an entry is entered into the Alarm log.
5. To stop monitoring, click the **Cancel** button on the modeless dialog box.

Maintaining Multiple NetXRay Configuration Files

If you are a network support specialist maintaining multiple sites, the NetXRay multiple work space feature lets you create separate address books and other configuration settings for each separate site conveniently.

Every time you create a new probe, NetXRay sets up a separate directory to maintain another copy of the address book, capture filter setting, packet display options, update frequency, and alarm thresholds. By naming a new local probe after each site that you manage, you can easily select and invoke configuration information for each site.

To create a new site:

1. Go to Tools, and click the **Select Network Probe/Adapter** to bring up the Adapter dialog box.
2. Click **New Probe** button to bring up a New Probe dialog box.
3. Enter the description, select the **Local Probe** radio button, then click **OK**.
4. Optionally, you can copy a workspace setting for the new probe from the existing probes. Click the drop-down box and select an existing probe as the source from which to copy. A probe's workspace setting including the address book, capture filter setting, packet display options, update frequency, and alarm thresholds will be copied to the new probe space.


To use the particular setting for a site:

1. Go to Tools, and click the **Select Network Probe/Adapter** to bring up the Adapter dialog box.
2. Open the Local Probe (Site) of your choice by clicking the plus (+) sign in front of the probe (Site) name.
3. Select an adapter, and click **OK**.

Now NetXRay will switch to the configuration settings that were previously defined for this site.

Printing Files

NetXRay supports printing the packet decode from the Packet Viewer, table and graphic picture in Matrix, Host and Protocol windows.

To print, simply click on the desired window to make it the active window. Then select the **Print from File** menu, or select the  icon from the Tool Bar.


NetXRay performs printing in background. You do not have to pause to wait for capture printing completion.

Exporting to Files

NetXRay lets you save the statistics gathered during the monitoring session in a comma-separated-values (CSV) format file. The CSV file gives you the ability to import the statistical data into other applications, such as a database or a spreadsheet.

NetXRay supports exporting History, Host Table, Matrix, Address Book, and Alarm Log.

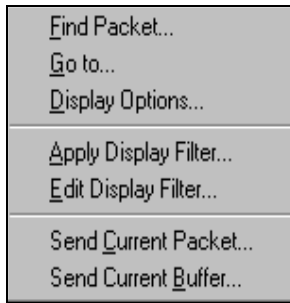
To export data to a file, simply click on the right mouse button to invoke the context menu. Then select **Export**.

Or you can click  on the side of the active window.

Using Context Menu

The Context menu is invoked when you position your mouse over an object and press the right mouse button. The menu displays a list of commands that you can use to perform an operation on this object (window).

Select your choice by clicking on the context menu command line.



Organizing Tables

Host Outline Table, **Matrix Outline Table**, **Address Book**, and **Alarm Log** are displayed in table format with column headings. You can reorganize these tables by adjusting the size of the column, and sorting the table entries.

The Summary pane column in the Packet Viewer can be resized and moved.

Resizing the Column

To resize the column width:

1. Place the mouse pointer over the right edge of the column you want to resize. A two-way arrow is displayed.
2. Click the mouse button, and drag the edge to the desired position.
3. Release the mouse button.

Sorting Column Data

Data contained in the table can be sorted.

To sort the column data in descending order, click the column heading.

To sort data in ascending order, hold down the Control key and click the column heading.

Moving a Column

Only the summary pane column in the Packet Viewer can be moved.

To move a column:

1. Click the column heading, and move the mouse. A dashed box with left arrow is shown.
2. Move the dashed box to the new column position.
3. Release the mouse button to place the column.

Using Drag and Drop

NetXRay supports drag and drop in the Address Filter setting, and also in creating a new Address Book entry.

To use drag and drop, simply click the item of your choice, and drag it to the desired location or field. Then drop it there. A new entry is created.

Arranging Docking Windows

The Packet Viewer, Dashboard, and Packet Generator may each be displayed either as a docking window or a normal MDI window.

Docking windows are new in Windows 95; their display characteristics are very similar to those of the Tool Bar. They always stay on top of other MDI windows, and will be visible at all times. When one is dragged and attached to the border of the main window, it docks (merges) with the border. To undock the window from the border, click on the small stripe between the border of the inside box and the border of the docking window; a black rectangular box will be visible. Hold the mouse button, and press the Control key down; you can drag the window out of its docking position. [Figure 1-15](#) shows where to place mouse pointer to drag the window.

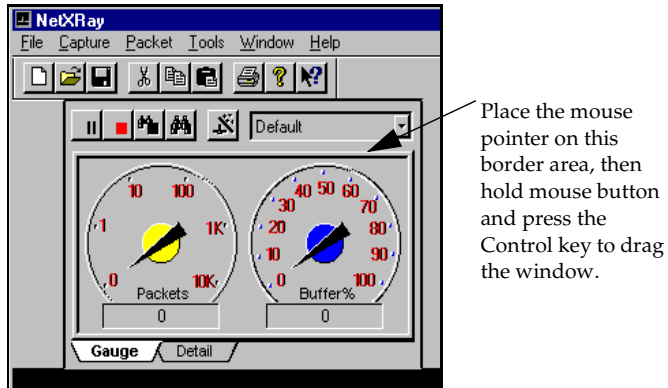


Figure 1-15. Example of How to Arrange a Docking Window

Unless you have a large windows space, and want to view these windows at all times, you can configure them into normal MDI windows. To change a docking window back to a normal MDI window, click the right button of your mouse to bring up a context menu. Uncheck the **Docking View** in the context menu.

Alternatively, go to **Tools/Options...** and click the **Workspace** tab (Figure 1-16). Uncheck the ones you want to turn into MDI windows.

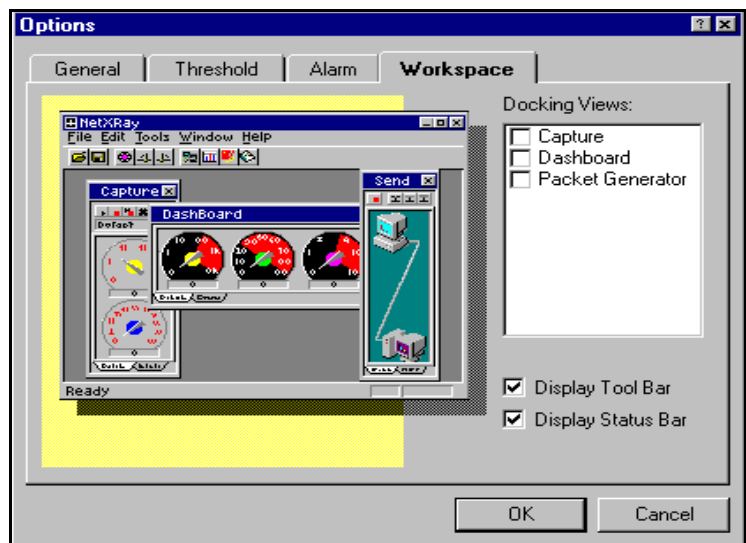


Figure 1-16. Workspace Tab in the Options Window

Removing Prompting

When you close a capture buffer decode viewing window, or a history trend graph, NetXRay will invoke a dialog box prompting you to save the data.

To disable the prompt, you can uncheck the items desired in the **Options/General** dialog page ([Figure 1-17](#)).

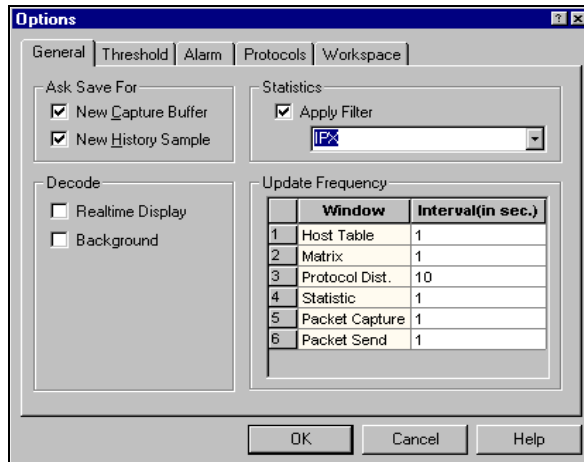


Figure 1-17. General Dialog Page in the Options Window

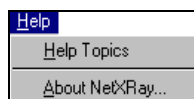
Changing Update Frequency

You can change how frequently each monitor window display is updated with the latest data.

To change the update frequency, click **Tools/Options...**, select the **General** page, then make necessary changes.

Using the Help Menu

NetXRay Help is fully compliant with Windows 95. To access Help, click **Help** from the Menu bar and select **Help Topics**.



A Help Topic window is displayed (See [Figure 1-18](#)).

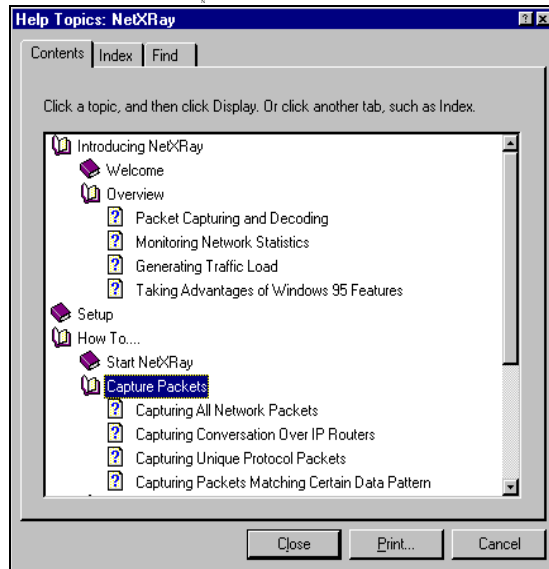


Figure 1-18. Help Topic Window

The **Contents** tab displays a list of topics in the Help system; it is organized by category. The **Contents** tab is like a table of contents in a book — it helps you to navigate through the Help hierarchy to find a desired category or subject.

The **Index** tab is similar to a traditional book index, listing keywords alphabetically. The **Index** tab is particularly useful if you are looking for Help on a specific topic.

The **Find** provides functionality of a full text search for any word or phrase in the Help system.

Using Context Sensitive Help

You can access context-sensitive Help for a dialog box object by several means:

- Click the right mouse button on the object to display a What is this message.
- Click the ? icon in the dialog box title bar to display a Help cursor, then click the object.
- Press the **F1** key to get Help on the selected object.



Chapter 2

Packet Capture

This chapter describes the packet capture operations, and various setting options.

Packet Capture allows you to capture packets and store them in memory for as long as you like. Captured packets can be saved in a file from the Packet Viewer. Later, you can display these packets and examine their contents to help you analyze your network operation and locate the source of problems. If the memory buffer is not large enough, you may spool the captured packets to files in real time.

The trigger option adds the ability to start and stop capture based on predefined trigger events; that is, data/time, alarms, or event filter.

You may capture all the data on your LAN, or you may set up filters to capture only the specified data in which you are interested. Filters may be set up to capture data which:

- Is transmitted between specific network nodes (or address pairs)
- Belongs to one or more protocol groups
- Matches a defined data pattern
- Has size within a defined range
- Has a combination of the above specifications

Packet Capture Window

To bring up the Packet Capture window, select **Capture** from the **Tools** menu, or click the **Capture** icon, directly on the Tool Bar. A Packet Capture window is shown in [Figure 2-1](#).

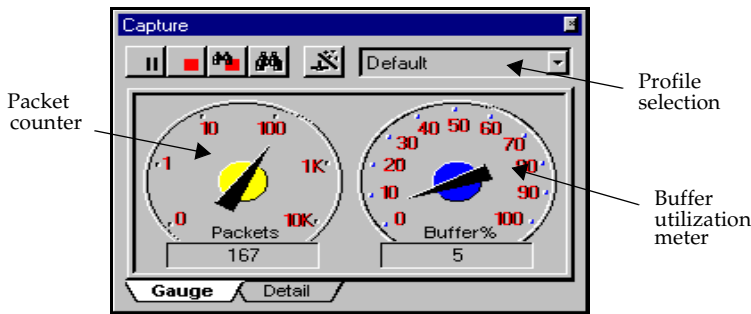








Figure 2-1. Packet Capture Window

Buttons shown in [Figure 2-1](#) are defined in [Table 2-1](#).

Table 2-1. Capture Window Button List

Button	Usage
	Start Packet Capture.
	Pause capture temporarily. To resume, click the Start button again.
	Stop capture.
	Stop and view the capture buffer.
	View the capture buffer
	Invoke the Capture Setting property page.

The remaining objects in the packet Capture windows are explained in [Table 2-2](#).

Table 2–2. Capture Gauge Windows Field Definitions

Object	Usage
Profile Selection	Allows you to select and apply capture criteria from a list of previously defined and saved capture settings.
Packet Counter	Displays the number of packets collected according to the capture criteria.
Buffer Utilization Meter	Displays the percent of capture buffer used.
Gauge Tab	Shows the capture gauge.
Detail Tab	Shows capture progress in table format.

Packet Capture Detail Window

To view the capture progress in detail, click the **Detail** tab. A Capture window ([Figure 2–2](#)) will be shown in table format.

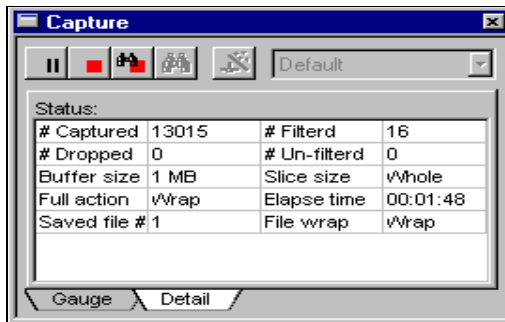


Figure 2–2. Capture Window

The meaning of each detail field of the Capture window is explained in [Table 2–3](#).

Table 2–3. Capture Detail Window Field Definitions (1 of 2)

Field	Description
# Captured	Total # of packets seen by NetXRay.
# Dropped	Total # of packets dropped by NetXRay due to network traffic loads that exceed NetXRay's ability to capture all of them. This setting will normally be zero.

Table 2–3. Capture Detail Window Field Definitions (2 of 2)

Field	Description
# Filtered	Total # of packets passed through the filter and saved in the capture buffer.
# Unfiltered	Total # of packets rejected by the filter criteria.
Buffer size	Size of the current memory buffer selected.
Slice size	Size of the packet being saved.
Full action	Current selected capture action when buffer is full.
Elapse time	Time since the capture started.
Saved File	The file number currently being saved.
File Wrap	File wrapping status.

NOTE: Due to the multithread nature of Windows 95 and Windows NT, Capture performance greatly varies depending on your computer's overall performance. To maximize NetXRay's ability to capture all packets, Network General recommends you close all other Windows applications, and invoke only the capture function in NetXRay.

Additional monitoring functions, such as Host Table and History, consume CPU time, and reduce NetXRay's ability to achieve a high capture rate.

To capture packets at wire speed, Network General recommends that you use a Pentium-based computer with a PCI network interface card.

Context Menu

The Capture context menu gives you access to additional functions and short-cut commands. [Table 2–4](#) describes the Context menu commands and usage.

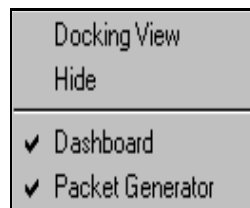





Table 2–4. Capture Window Context Menu Commands


Command	Usage
Docking View	Click to toggle between Docking View and normal view. If Docking view is checked (✓), the Packet Capture will stay on top all the time.
Hide	Close the Packet Capture.
Dashboard	Launch or hide the Dashboard window depending on whether the Dashboard is previously activated or not. If a check (✓) symbol is shown, clicking this command will hide the Dashboard window.
Packet Generator	Launch or hide the Packet Generator window depending on whether the Packet Generator is previously activated or not. If a check (✓) symbol is shown, clicking this command will hide the Packet Generator window.

Starting Packet Capture

To start a packet capture:

1. Select a capture profile from the profile list box.
2. Click  to start capture. The capture gauge shows the capture status in progress.
3. If you want to pause the capture, click  to pause temporarily. To resume capture again, Click .

Stopping Packet Capture


Unless you have selected **Stop when buffer is full**, the capture will continue. To stop capture manually, click  to stop the Capture.

If you restart Capture without saving the captured packet buffer, all previously captured data will be lost.

Saving Captured Packets

Captured packets can only be saved from the Packet Viewer window.

To save a captured packet:

1. Click  (the **View** button) to bring up the Packet Viewer window.
2. Select **File** from the Menu bar, and click **Save As....** A Save As dialog box is displayed.
3. Enter the filename for your capture file. You will have the option of choosing a file folder or location in which to put it. Click **OK**.

Using the Capture Menu

Alternatively, you can control the complete Capture operation from the Capture menu without invoking the Packet Capture window.

Clicking **Capture** from the menu bar will show the following drop- down command list. Select and click the command of your choice to activate. [Table 2-5](#) describes the Capture menu commands and usage.

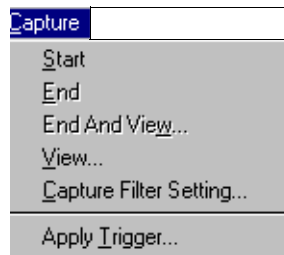


Table 2–5. Capture Menu Commands

Command	Usage
Start	Start Capture
End	Stop Capture
End And View...	Stop Capture, and invoke Packet View
View...	Invoke Packet Viewer to view captured packet in capture buffer
Capture Filter Setting...	Invoke Capture Setting property page
Applied Triggers...	Invokes Applied Capture Trigger dialog box.

Packet Capture Setting


The Capture Setting property page lets you define:

- Address filter
- Protocol filter
- Boolean data pattern filter
- Buffer option
- Profile selection

Working with Capture Setting Profiles

Each capture setting can be saved in a profile. NetXRay supports and saves multiple profiles. You can easily retrieve and apply previously defined capture profiles before you activate capture. You can also create a new profile by copying from existing or sample profiles supplied by NetXRay.

To create a new profile:

1. From the Capture window, click  to bring up the Capture Setting property dialog box.
2. Click the **Profiles...** button to bring up the Capture Profiles dialog box ([Figure 2–3](#)).

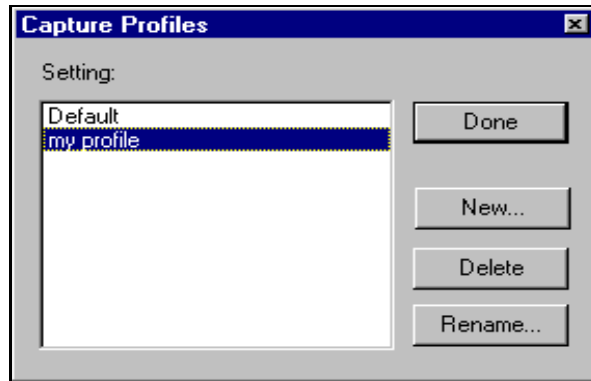


Figure 2–3. Capture Profiles Dialog Box

3. Click the **New...** button. A New Capture Profile dialog box is displayed ([Figure 2–4](#)). Enter a new profile name, for example, **my profile**. Click **OK**.

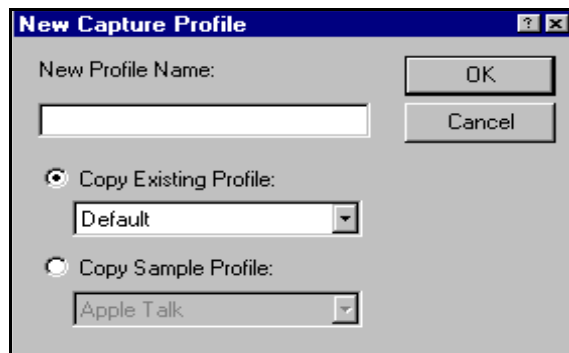


Figure 2–4. New Capture Profile Dialog Box

4. Click the appropriate radio button depending on whether you want to copy from existing profiles or from sample profiles.
5. Click on the drop-down list. Scroll the list to pick a filter to copy. Click **OK**.
6. Click the **Done** button to close the Profile dialog box.
7. Now you can define the capture setting.


From the Capture Profiles dialog box, you can also delete or rename an existing profile.

NetXRay provides many useful filters in the Sample Profiles, such as, token ring MAC frame, ethernet broadcast and multicast frames, and FDDI SMT and NIF frames.

NOTE: The Default profile shipped with NetXRay has no capture filter criteria set, and the capture buffer is set at 256 K bytes. The buffer full action is set to Stop capture.

Setting the Address Filter

The Address Filter page allows you to set up an address filter to capture packets between a pair or up to ten pairs of network addresses. Using the Host Table to pre-learn the network node addresses first saves you from typing in the hardware addresses. See [Known Addresses on page 2-10](#).

To bring up the Address Filter setting shown in [Figure 2-5](#), click  on the Packet Capture window.

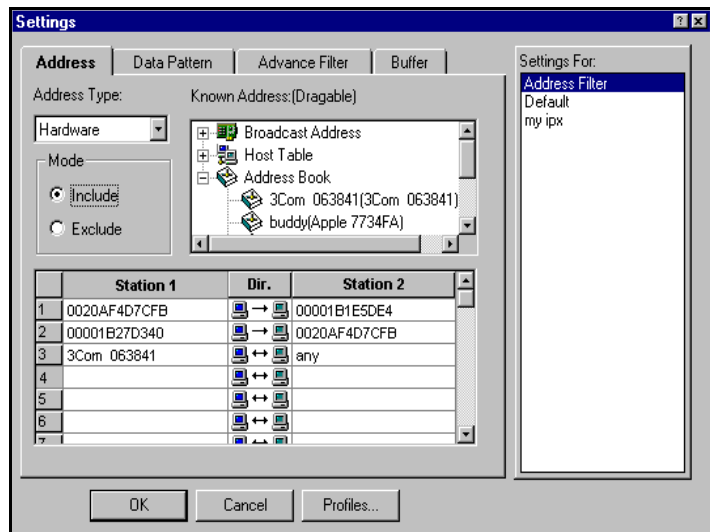


Figure 2-5. Address Filter Settings Window

The address filter options are defined below.

Address Type

This option lets you define the address monitored as either a network hardware address (6 bytes in hexadecimal value) or a network IP address (4 octets).

Selection of either address type is mutually exclusive.

Filter Mode


The following describes the filter modes.

- **Include** lets you capture packets that match the address specification.
- **Exclude** captures packets that do not match the address specification.

Known Addresses

Displays known addresses from three sources:

- | | |
|---------------------|---|
| • Broadcast Address | Predefined broadcast, multicast, and functional addresses |
| • Host Table | Current learned station hardware addresses |
| • Address Book | Addresses that you have defined |

You can open and examine the detail list by clicking on the address icon  .

The Known Address list is used to simplify the definition of address filter pair. You can drag and drop the symbolic address of your choice into either the **Station 1** or **Station 2** field.

Station 1

Enters the address of the 1st station in the address pair. You can drag a symbolic name from the known address list and drop it here, or type in the proper network address format. The address format is listed below:

- | | |
|--------------------|--|
| • Hardware Address | 6 bytes in hexadecimal value, for example, 100889ACD908. |
| • IP Address | 4 decimal octets separated by . (dot), for example, 198.90.123.98. |

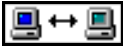
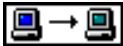
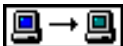
You can also enter 'Any' as a valid station address.

Station 2

Enters the address of the 2nd station in the address pair. The same address criteria in Station 1 applies here also.

Dir.

Selects the direction of the data traffic to be filtered.

	For both directions.
	From Station 1 to Station 2.
	From Station 2 to Station 1.

NOTE: The Default profile shipped with NetXRay has no capture filter set, and the capture buffer is set at 1 MB. The buffer full action is set to Stop capture.

Setting Data Pattern Filter

The Capture Setting Data Pattern Filter page can be invoked by first clicking the **Setting** button, then the **Data Pattern** tab (*Figure 2-6*). You can define a data pattern filter to capture only those packets that match the data pattern criteria you specify. *Table 2-6* describes the **Data Pattern** Filter button definitions.

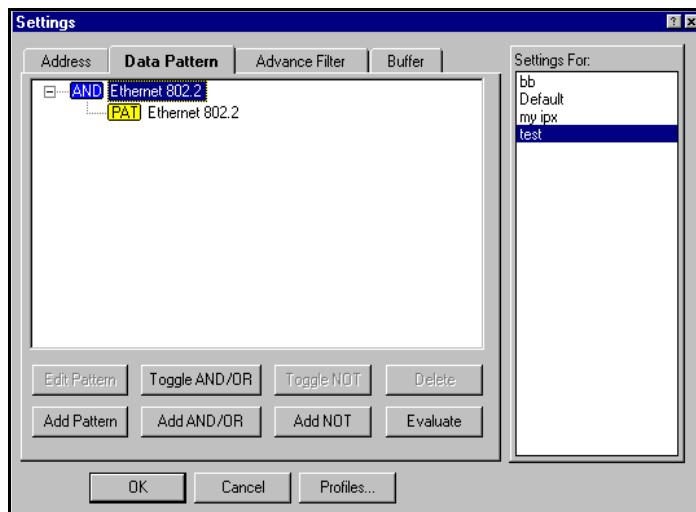


Figure 2–6. Capture Setting Data Pattern Filter Page

Table 2–6. Data Pattern Filter Button Definitions

Button	Usage
Edit Pattern	Invokes the Edit Pattern dialog box. Allows you to modify the data pattern field contents.
Add Pattern	Invokes the Edit Pattern dialog box. Allows you to create a new data pattern.
Toggle AND/OR	Toggles Boolean operator between AND and OR.
Add AND/OR	Creates a new Boolean Operator AND.
Toggle NOT	Turns on or off the NOT operator.
Add NOT	Creates a NOT operator.
Delete	Deletes the selected Operator or Pattern. If the Operator has other child operators or patterns, they will all be deleted.
Evaluate	Evaluates the Boolean equation immediately. If the equation is incomplete, an error message will be prompted.

A data pattern filter can be a simple data pattern filter, or a very sophisticated filter which involves multiple data pattern definitions connected together by AND/OR/NOT Boolean

operators. A complex filter can contain no more than 20 Boolean operators and data patterns.

A data pattern is defined by a particular sequence of bits, the length of these bits, and its offset position within the packet. You have the option of specifying the offset from the beginning of the full packet, or from the first level protocol boundary. The maximum data pattern length is 32 octets.

The beginning octet location of a protocol boundary from the packet may vary depending upon the media type, (Ethernet, Token Ring), or the DLC format (Ethernet II, 802.2, 802.2 SNAP) it uses. For example, suppose an IPX protocol starts from offset byte 14 in Ethernet II type packet, but from byte 17 in an 802.2 type packet. Since NetXRay recognizes various DLC format types, and is able to mark the protocol boundary correctly, using the protocol layer boundary as a starting location for calculating the offset allows you to capture protocol packets with a matching data pattern across different network media or using different DLC formats.

To facilitate the definition of a data pattern, NetXRay allows you to 'copy' the data pattern of your choice from a known packet. To do this, you must be in the packet decode viewer and have selected that particular packet before you invoke the capture filter profile. In the Data Pattern Filter page, there is a built-in **Set Data** button to allow you to copy a known data field from the decoded packet into the data pattern fields including calculating the offset and length, filling the data pattern, and suggesting a default field name automatically.

The construction of a complex data pattern filter will require you to build the linkage of the data patterns using AND/OR/NOT Boolean operators. The result is displayed in treelike diagram to show logical relationship.

The best way to learn the construction of a Boolean Data Pattern filter is to start from a simple data pattern filter. The first step is writing down the logical relationships in Boolean equation on a piece of paper. The next is to clarify the Boolean operation's precedence by using parenthesis liberally, so that the final equation can be constructed using a binary tree diagram.

The following example demonstrates the construction of the sample filter, My Subnet, step by step. (My Subnet is also listed in the sample Boolean Data Pattern filters supplied in the NetXRay capture profiles.)


Suppose that you want to capture all IP traffic except ones to and from subnet 36.56.0. First, write a data pattern Boolean equation that represents this operation:

Not (Src Subnet 36.56.0 OR Dest Subnet 36.56.0)

Then go to **File/Open...**, select the sample capture file **TCPIP.CAP**. Click **Open** to bring up the Packet Decode Viewer. Select packet #5 which contains the source subnet address 36.56.0.

Now, you should start defining the data pattern filter.

To define the data pattern filter:

1. From the Capture window, click  to bring up the Capture Setting property dialog box.
2. Click the **Profile...** button to bring up the Profile dialog box.
3. Click the **New...** button. Enter a new profile name, for example, **My Subnet**. Click **OK**.
4. Click the **Done** button to close the Profile dialog box.
5. Click the **Advance Filter** property page tab.
6. Select **IP** from the Available Protocols list box. This will preclude any non-IP packets that might have the same data pattern as the subnet 35.56.0.
7. Click the **Data Pattern** property page tab. A default AND operator is shown on the top of the dialog space.
8. Click the **Add NOT** button to create a NOT operator.
9. From the newly created NOT line, Click **Add AND/OR** to create a new child operator AND that is linked to the NOT operator.
10. Click the **Toggle AND/OR** button to change the AND to OR.
11. From the OR line, Click the **Add Pattern** button to invoke the Edit Pattern dialog box.
12. Scroll the detail decode window to locate the IP source address that contains subnet 35.56.0. Highlight the field.
13. Select **Protocol** in the **From:** combo box. This will tell NetXRay to calculate the source IP address offset from the beginning of the IP protocol data packet.
14. Click the **Set Data** button to tell NetXRay to fill in the field for source IP address. The Edit Pattern dialog box will look like the one shown in [Figure 2-7](#).

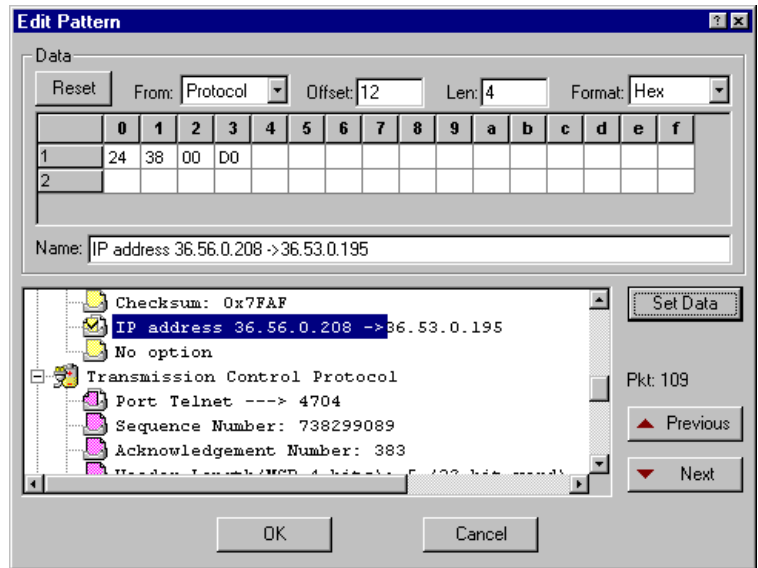


Figure 2-7. Edit Pattern Dialog Box

The Edit Pattern dialog fields are defined in [Table 2-7 on page 2-17](#).

15. Change **Len:** from 4 to 3 for the length of subnet of 3 bytes. Delete the 4th octet from the data pattern field.
16. Edit the **Name:** field, so it shows Src Subnet 36.56.0.
17. Click **OK**. A new data pattern Src Subnet 36.56.0 is created and connected to the OR operator.
18. Click the OR operator again to select it.
19. Click the **Add Pattern** button to invoke another Edit Pattern dialog box.
20. Click the **Next** button to display the next packet decode. Scroll the detail window to look for IP destination address with subnet 36.56.0. Repeat this step until it is found. Highlight the IP destination address field.
21. Select **Protocol** in the **From:** drop-down list. This will tell NetXRay to calculate the destination IP address offset from the beginning of the IP protocol data packet.
22. Click the **Set Data** button to tell NetXRay to fill in the field for the source IP address.
23. Change **Len:** from 4 to 3 for the length of subnet of 3 bytes. Delete the 4th octet from the data pattern field.

24. Edit the **Name** field so that it shows Dest Subnet 36.56.0. The Edit Pattern dialog box will look like the one shown in [Figure 2–8](#).

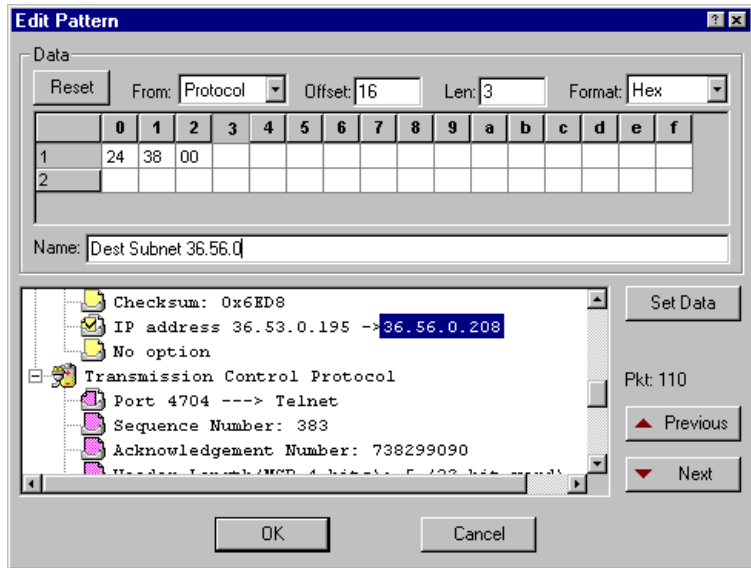


Figure 2–8. Edit Pattern Dialog Box

25. Click **OK**. A second data pattern Dest Subnet 36.56.0 is created and connected to the OR operator.
26. The resulting operation **Not (Src Subnet 36.56.0 OR Dest Subnet 36.56.0)** is shown on the top line. The **Data Pattern Filter** page will look like the one shown in [Figure 2–9](#).

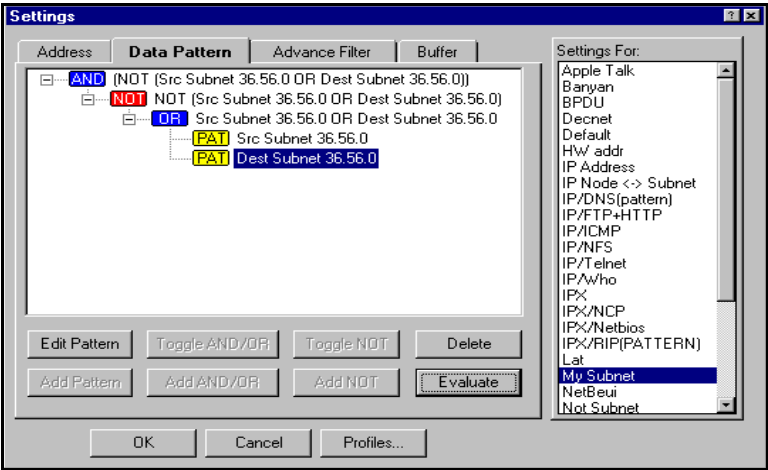


Figure 2–9. Data Pattern Filter Page

27. Click **OK** to save the filter.

Table 2–7. Edit Pattern Dialog Box Field Definitions


Field	Usage
From	Select data pattern's offset from either the beginning of the packet, or the beginning of the protocol layer.
Offset	Specify the data pattern offset in decimal value.
Len	Length of the data pattern up to 32 octets.
Format	Select the data pattern type in Hex, ASCII, or EBCDIC.
Name	Symbolic name for the data pattern. It is used in the Boolean equation to identify the operand.

Setting Packet Size Filter

The **Advance Filter** page lets you specify a packet size filter. It lets you capture packets based on packet size, that is, Equal to, Greater than, Less than, in Between, Not in Between certain ranges.

Setting Protocol Filter

The **Advance Filter** page lets you select one or more protocols or subprotocols to filter. If the packet matches one of the selected protocol types, it will be captured in the memory buffer. If no protocol is selected, NetXRay defaults to capture all protocol types.

To view the **Advance Filter** page (see [Figure 2–10](#)), click the  button on the Packet Capture window, then click the **Advance Filter** tab.

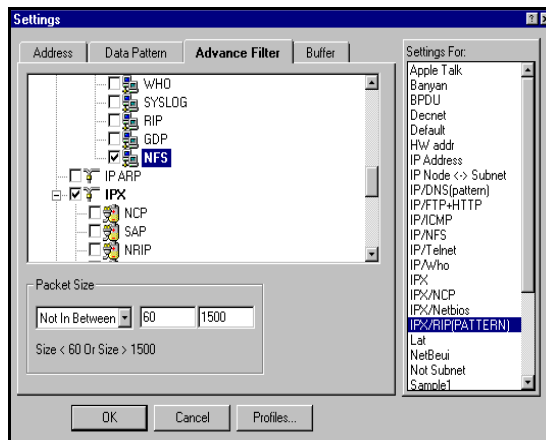


Figure 2–10. The Advance Filter Page in the Settings Dialog Box

The Packet Capture Protocol filter for IP has been expanded to include transport-layer protocols, that is, TCP, UDP, ICMP, IGMP, ISO-TP4, Hello, IP-VINES, OSPF, GGP, EGP, and IGRP, as well as TCP and UDP application-layer subprotocols, (FTP, REXEC, RLOGIN, RSH, PRINTER, SMTP, Telnet, DNS, GOPHER, POP, HTTP, NNTP, NetBIOS, NFS, RPC, X-Window, BOOTP, TFTP, SNMP, BIFF, WHO, SYSLOG, RIP and GDP).

The protocol filter for IPX is also expanded to filter on various subprotocols, such as RIP, SAP, NCP, SPX, NBIOS, Diagnostic, Serialization, NMPI, NLSP and SNMP.

NOTE: If you specify more than one type of filter, for example, address and data pattern, a packet must match all the criteria before NetXRay will save it in the memory buffer.


NOTE: If the specific protocol filter type is not defined in the standard list, you can define your own protocol filter using a boolean data pattern, or select one from the sample profiles described earlier.

Setting Ethernet Error Filter

With a special NDIS driver written and supported by Network General, NetXRay is capable of capture a full range of Ethernet error packets; that is, CRC, runt, fragment, oversize, and jabber. You can also set pre- and post-filters to capture and view one or more error packet types.

The current supported NIC cards are NE2000 compatible ISA and PCMCIA cards. Contact Network General, or visit www.ngc.com for the latest list of NIC card supported.

To define Error Packet filter:

1. Click  on the Packet Capture window, then click the **Advance Filter** tab, a Buffer dialog page is displayed as shown in [Figure 2-11](#).

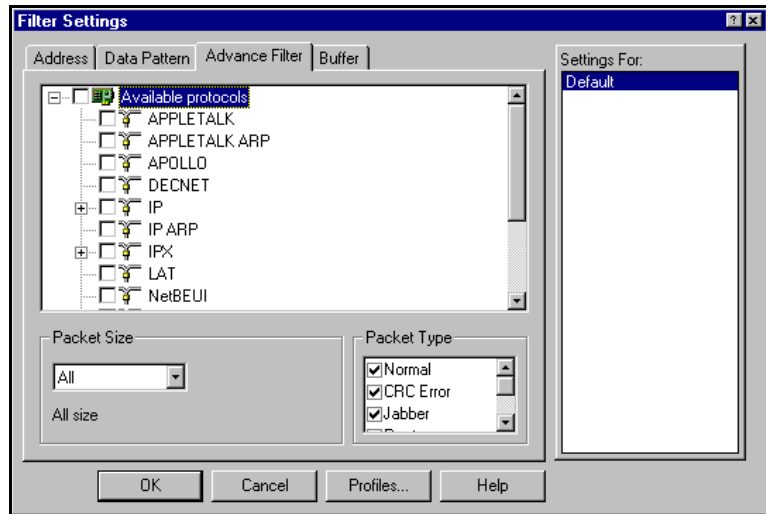


Figure 2-11. The Advance Filter Page in the Filter Settings Dialog Box

2. Uncheck the **Normal** packet type, or other error packet types. Do not uncheck packets on which you want to filter.
3. Click **OK**.

Defining Capture Buffer Options

You can invoke the **Capture Setting Buffer Option** page (see [Figure 2-12](#)) by clicking the **Setting** button, then the **Buffer** tab. From that dialog page you can select a capture data buffer in memory to accommodate the amount of network traffic you want to capture. Selecting a smaller packet size saves buffer space by ignoring unnecessary data. You can also define the action when the buffer is full.

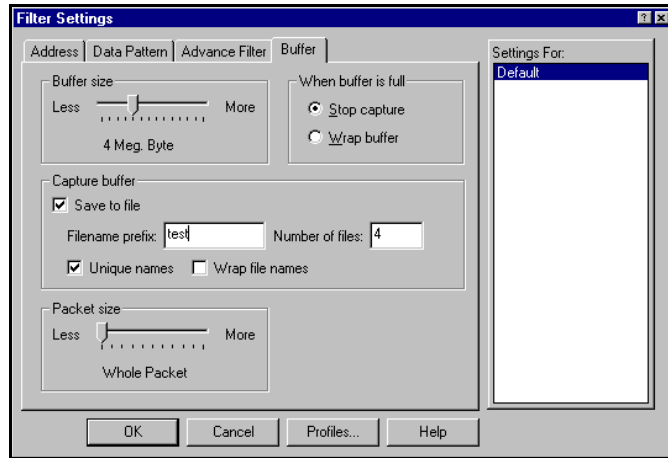


Figure 2–12. The Capture Setting Buffer Option Page

Table 2–8 defines various options for capture buffer.

Table 2–8. Capture Buffer Setting Options

Option	Usage
Buffer Size	Move the slider to select the memory size for the capture buffer. You can select 256K, 512K, 1M, 2M, 4M, 8M, 12M, 16M, 24M, 32M, 63M, 96M, 128M or 192M Bytes. NT system is limited at 63M bytes.
Buffer Full Action	Selects the capture action when the memory buffer is full. You can choose to stop capture, or let the capture wrap the memory buffer. The Wrap buffer mode will cause new packets to overwrite the oldest packets in the memory buffer.
Capture Buffer Save to File	Check to enable
Filename prefix	Enter Windows long filename
Number of files	Enter 1 to 99,999
Unique names	Check to let NetXRay create unique filename
Wrap file names	Check to let capture save to restart from the first file after the last one is full.

Table 2–8. Capture Buffer Setting Options

Option	Usage
Packet size	Move the slider to select the size of the packet to be captured and saved in memory. Any network data packet size greater than the selected size will be truncated. You can select Whole Packet, 32, 64, 128, 256, 512, 1024, 4096, 8192, or 16384 octets.

Capturing Packet and Real Time Spooling to Files

NetXRay has an option to spool captured packets from capture buffer to files in real time. Packet capture performance is dependent on the network load, the CPU speed, and the hard disk through-put.

The file spooling is defined in Capture Buffer setting. You can set the filename prefix, and the number of files to be spooled. The maximum number of files allowed is 99,999. Each file size is defined as the same as the capture buffer size. For example, if you select 4 M buffer size, then each file created will be 4 MB. The last file size may be smaller than 4 MB. Setting the buffer size between 8 to 12 M bytes will yield the best capture performance.

You may select the **unique names** option to guarantee that the filename created by packet capture is unique in the same directory. This is a useful option when you use packet capture spooling in conjunction with the capture trigger repeat mode, so that several packet capture sequences can be saved in separate unique files.

By selecting **Wrap file names** option, the capture will continue to spool and overwrite the first file if the last file is full. Otherwise, the capture will stop once it reaches the end of the last file.

To define packet capture to a file:

1. Click  on the Packet Capture window, then click the **Buffer** tab. A Buffer dialog page is displayed as shown in [Figure 2–13](#).

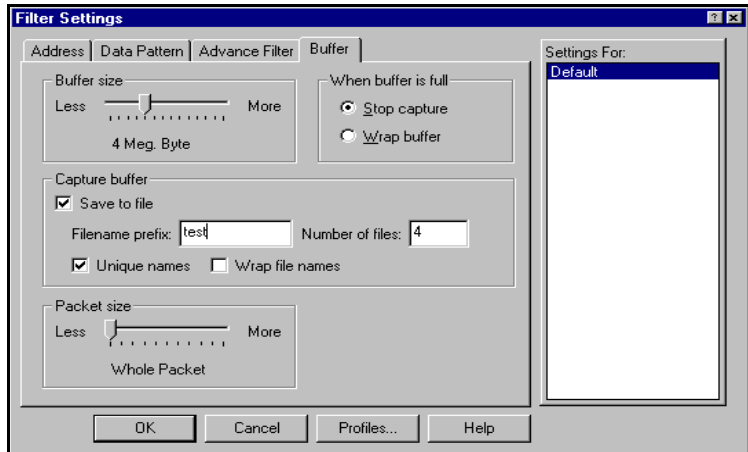


Figure 2-13. A Buffer Dialog Page

2. Check the **Save to file** check box, and set the appropriate field as described previously.
3. Optionally, set other filter parameters.
4. Click **OK**.

To start capture and view the capture results:

1. To start capture, click the **Start Capture** button. If you want to view the file spooling in progress, click the **Detail** tab in the Capture window. A summary capture status is displayed showing you to which file the captured packets are currently being spooled, and whether the files are wrapped.

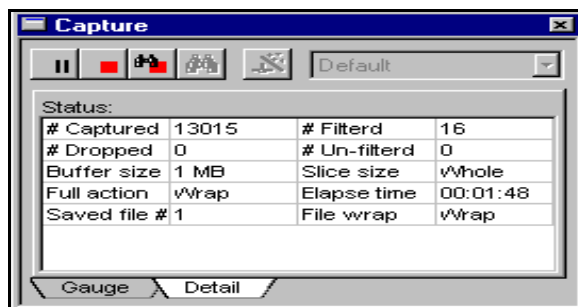


Figure 2-14. The Capture Dialog Box

2. To stop and view the packet capture file, click the **Stop/View** button. A dialog box is displayed to let you select a packet capture file to open (*Figure 2–14*).

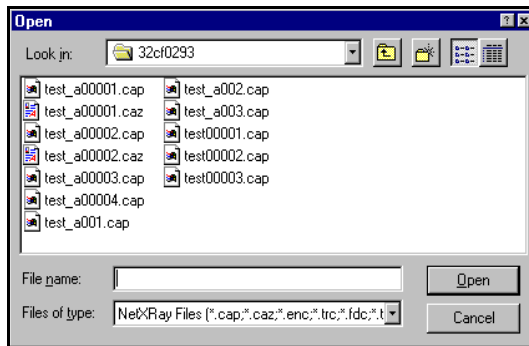



Figure 2–15. The Open dialog Box

3. To see the file listing in detail, click the  button. A detail file listing is displayed (*Figure 2–16*).

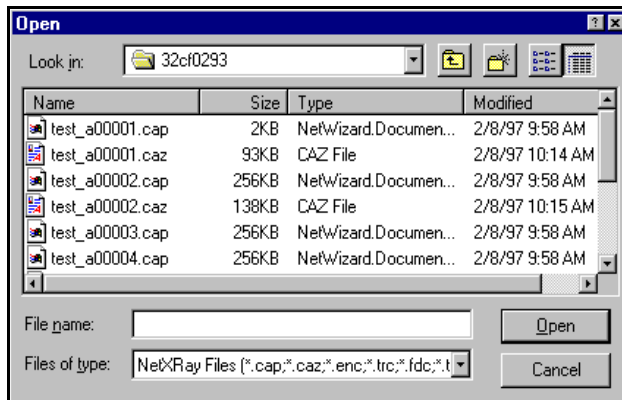


Figure 2–16. Detailed File Listing in the Open Dialog Box

4. Select a file, and click the **Open** button. A Packet Viewer window is displayed.

Setting Start and Stop Triggers for Packet Capture

The trigger function adds a new dimension to your ability to start and stop capture packets based on a trigger event. The trigger events supported are **Date/Time**, **Alarms** (those caused by network traffic loads) exceeding threshold levels, and **Event Filter**. Event filter is defined the same way as capture filter and is always given a profile name. For example, if you want to start capture only after seeing a known IP address, you can accomplish this by defining an IP address filter to/from 'any' in the capture filter and use it as the event filter for the start trigger.

You can select all three trigger events. If any one of the events occur, the trigger will activate.

The **Stop Trigger** delay option determines whether packet capture stops immediately when the Stop trigger is detected or after a number of packets are captured. By setting a delay, you can capture and examine the packets that precede or follow the stop trigger.

The trigger function can also be re-armed automatically. When it is used in conjunction with the Packet Capture spooled to file function, you can capture multiple instances of the network traffic packet streams that match the trigger conditions without manual intervention.

If you want to use event filter as a trigger, it must be defined first from the **Capture Filter** setting.

Setting packet capture trigger consists of the following:

- Define how you want the trigger to control the packet capture; use start trigger, stop trigger, delay after trigger, repeat (loop) mode, or a combination of them.
- Decide which event(s), (that is, **Date/Time**, **Alarms**, or **Event filter**) to use as trigger.
- If the **Event filter** is chosen, use the capture filter setting to define the event filter profile.
- Finally, invoke the trigger panel, and set the trigger selection according to your definition. Then apply the trigger.

It is strongly recommended that you experiment with the capture trigger function to gain proficiency on how to use it before applying a trigger to real world troubleshooting.

The following example shows an event filter of looking for any Telnet packet is used to trigger the start of a packet capture. After either 60 minutes has lapsed or a predefined IP address is detected, the packet capture continues for 3,000 packets, then the capture stops. This example assumes that the event filters for Telnet packets, and a known IP address has been defined.

1. Select **Capture/Apply Trigger** to invoke the Apply Capture Trigger dialog box ([Figure 2-17](#)).

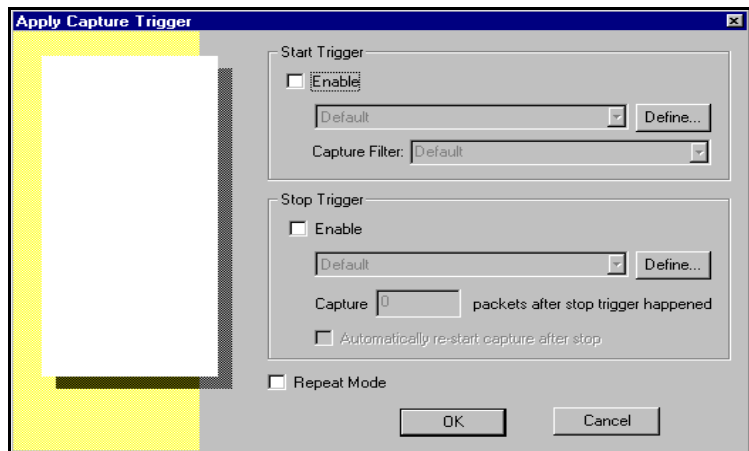


Figure 2-17. The Apply Capture Trigger Dialog Box

2. Check the **Enable** check box of the **Start Trigger** section, and Click the **Define...** button. A Start Trigger dialog box is shown ([Figure 2-18](#)).

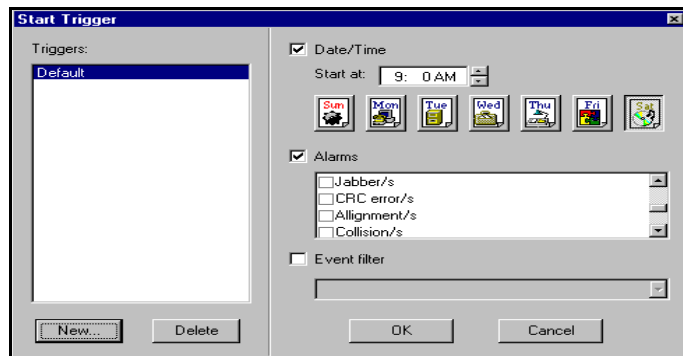


Figure 2-18. The Start Trigger Dialog Box

- Click the **New...** button to invoke a New Trigger dialog box. Enter the name of the Start Trigger. Click **OK**.

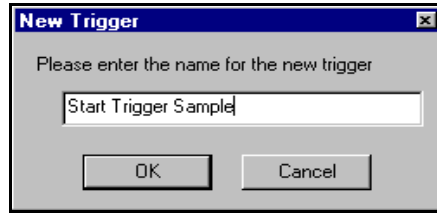


Figure 2-19. The New Trigger Dialog Box

- Check the **Event filter** check box, and select **Telnet Packet** as the event filter (see [Figure 2-20](#)). Click **OK**. Optionally, you may use **Date/Time** or **Alarms** as the trigger. Enter the time, and select each weekday of your choice by clicking on the button to toggle its ON/OFF state. A floating button means OFF, while a sinking button means ON. If you are interested in network traffic load to trigger capture, select **Alarms** and one or more network variables as the trigger.

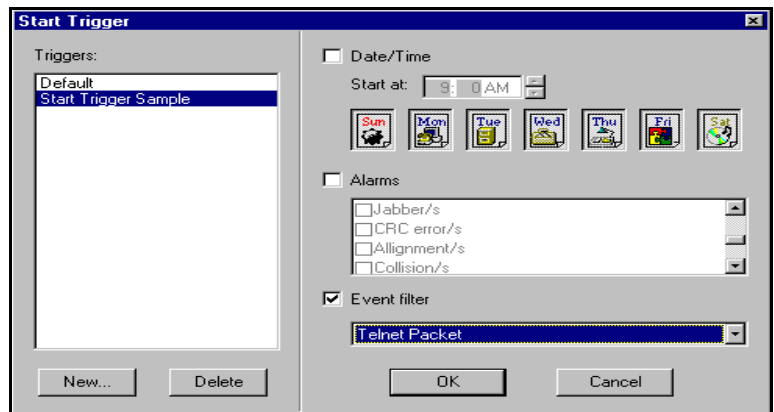


Figure 2-20. The Start Trigger Dialog Box

- Select a capture filter profile from the **Capture Filter** drop-down list (see [Figure 2-21](#)). The capture filter selected here will be used as the packet capture pre-filter when the start trigger activates the capture.

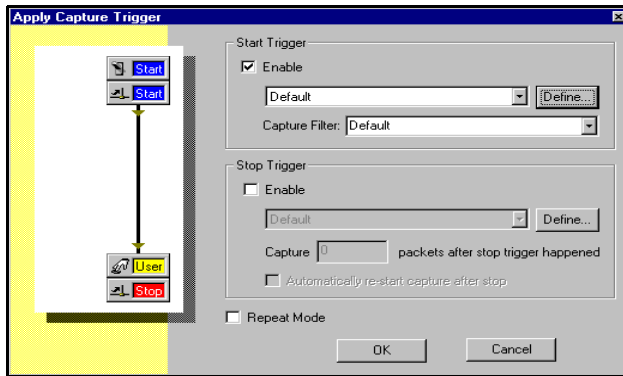


Figure 2–21. The Apply Capture Trigger Dialog Box

6. Check the **Enable** check box in the **Stop Trigger** section, and click the **Define...** button (see [Figure 2–22](#)).

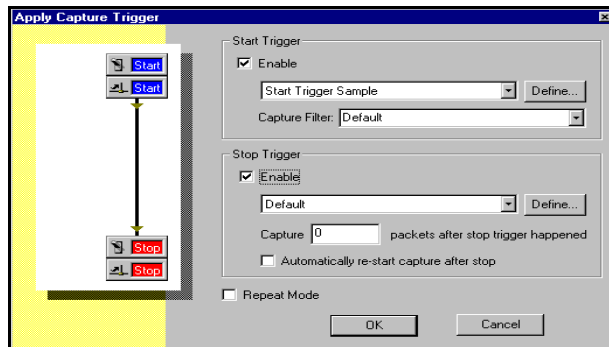


Figure 2–22. The Apply Capture Trigger Dialog Box

7. Click the **New...** button, and a new stop trigger “Stop Trigger Sample”. Check the **Time** check box, and select **Stop after 3600 seconds from start** as first stop trigger. Check the **Event filter** check box, and select **IP Address Sample 1** as the second stop trigger. Click **OK**. The Stop Trigger dialog box opens ([Figure 2–23](#)).

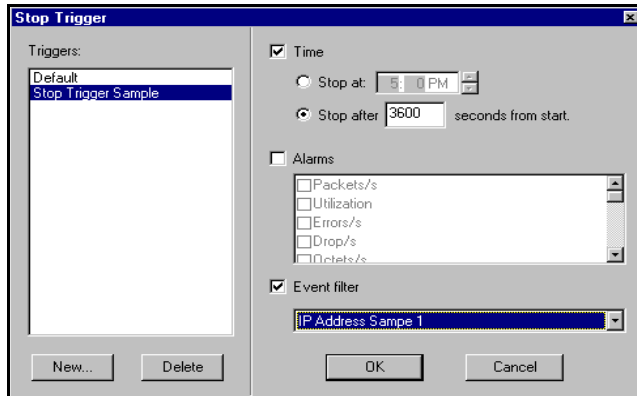


Figure 2-23. The Stop Trigger Dialog Box

8. Enter 3000 to capture 3000 packets after stop trigger happened. Click OK. The Apply Capture Trigger dialog box opens (Figure 2-24).

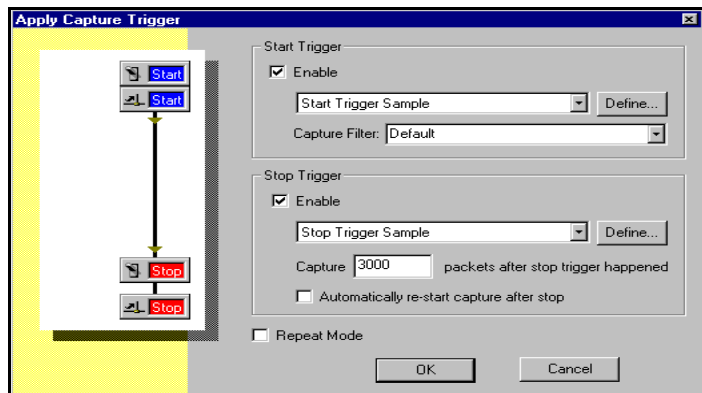


Figure 2-24. The Apply Capture Trigger Dialog Box

Re-starting and Re-arming Triggers

There are two options that you may select to restart the trigger function automatically to capture packet streams without manual intervention. Since the auto restart Repeat mode will most likely be used in unattended situations, it is recommended you also set the packet capture profile to use File Spooling mode as described earlier in this chapter.

If you check the **Repeat Mode** check box, the Start Trigger will be re-armed immediately after the **Stop Trigger** action is completed. [Figure 2–25](#) shows the trigger operation in Repeat mode.

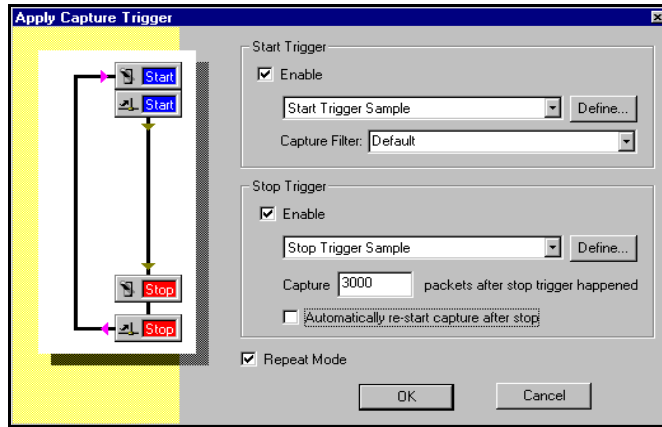


Figure 2–25. The Trigger Operation in Repeat Mode

If you check **Repeat Mode**, and also check the **Automatically re-start capture after stop**, then the capture will start immediately after Stop trigger is matched without waiting for the Start trigger to be tripped.

Showing Packet Decode during Capture

NetXRay lets you set the option to display the packet decode summary while capturing packets.

To enable real time decode, go to **Tools/Options** and check **Realtime Display** in the **Decode** option (see [Figure 2–26](#)). Click **OK** to close the dialog box.

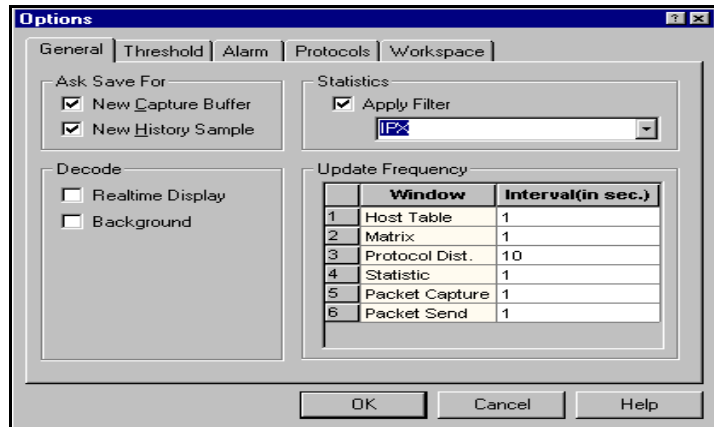


Figure 2–26. The General Page in the Options Dialog Box

When you start the packet capture, a separate window will pop up to show the packet summary in real time. This window can be closed without affecting the packet captured in the buffer.

WARNING: Real time decode can not keep up with a high rate of traffic on the network. The rate by which it can display the packet summary decode entirely depends on the type of NIC card and driver used and the CPU speed. Network General strongly recommends that the capture filter be set to reduce the actual packet rate.

Chapter 3

Packet Decode

This chapter describes the decode function of the Packet Viewer. It lists various methods to assist you in searching, viewing, and filtering the captured packets.

The Packet Viewer is invoked when you stop and view a captured buffer, or when you open a previously captured file by going to the File/Open... menu.

You can invoke as many Packet Viewer windows as you want, as long as your Windows 95 or Windows NT virtual memory is set up to handle them. However, opening too many viewing windows may severely impact your computer's performance.

Packet Viewer Window

The Packet Viewer contains three separate panes to show Summary, Detail, and Hex ([Figure 3-1](#)).

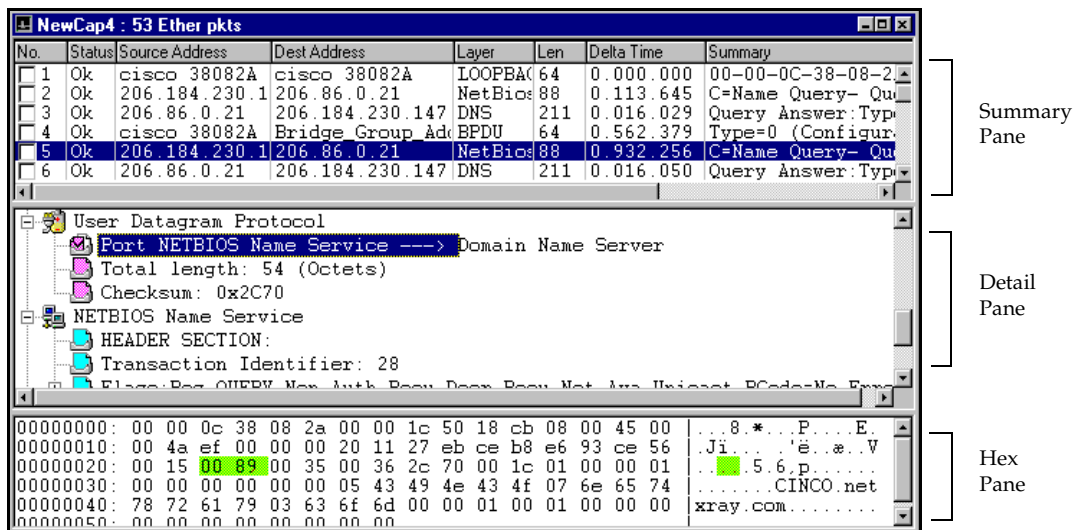


Figure 3-1. The Packet Viewer Window

Summary Pane

The Summary pane shows an overview of the conversation between stations in line-by-line summarized format. The position and size of the column can be adjusted to fit your viewing need.

[Table 3–1](#) shows Summary pane information.

Table 3–1. Description of the Summary Pane

Field	Description
Number	The order number in which the packets were received. The small check box in front of the number lets you select and mark the packet.
Status	Packet Error or Trigger status. If the frame is an event filter trigger, a [T] is shown. In Ethernet, it also shows the frame's error status; that is, OK (good valid frame), CRC, runt, fragment, jabber, oversize, or alignment, provided you are using one of the NGC supplied NDIS drivers.
Source Address	The address of the node that sent the packet. It is displayed in symbolic name, hardware (MAC) address, MAC address with manufacturer ID, or IP address.
Dest Address	The address of the node that received the packet. It is displayed in symbolic format, hardware (MAC) address, MAC address with manufacturer ID, or IP address.
Layer	The highest protocol layer interpreted
Len	The total number of octets in the packets except the last 4 bytes of CRC. For NGC supplied NDIS driver, it is the actual packet size including 4 bytes of CRC.
Rel. Time	The elapsed time since the first packet in hh:mm:ss.msec format.
Delta Time	The elapsed time between the end of the previous packet and the end of the current packet in ss.msec.usec format
Summary	A brief summary of the highest protocol layer interpreted
Abs. Time	The computer's date/time when the packet arrived.

Customizing Color-Coded Summary Pane

The packets in Summary pane can be color-coded based on their protocol type. This feature allows you to group packets with the same protocol or subprotocol reference, and assists you in visually identifying the packets of your choice.

To set up protocol color highlighting,

1. Choose **Display Options...** from the Packet menu or from context menu. An Options property dialog box is displayed as shown in [Figure 3-2](#).
2. Click the **Summary Color** tab.
3. Click on the protocol type for which you want to change color display.
4. Select the **Text** and the **Background** color of your choice. The protocol type color will change to reflect your selection.
5. When you are satisfied with the color selection, click **OK**.

The default color is based on windows setup text and background color. The **Reset** button sets the current selected protocol to default color. The **Reset All** button sets all protocols back to the default color.

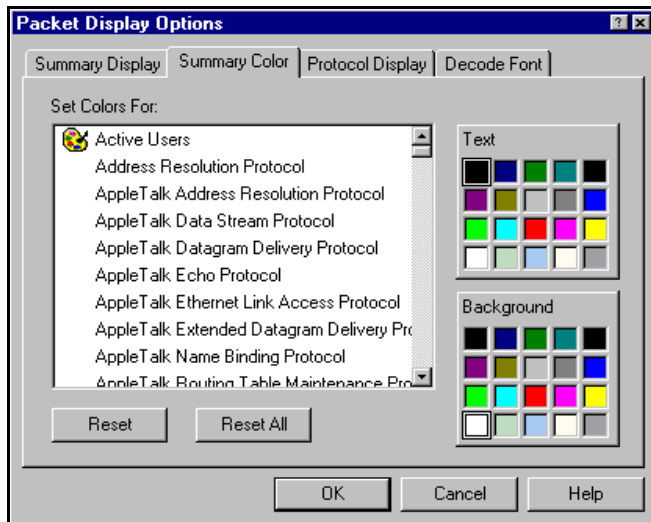


Figure 3-2. Packet Display Option Dialog Box

Showing Ethernet Packet Error Status

With a special NDIS driver written and supported by Network General, NetXRay is capable of capturing a full range of Ethernet error packets, that is, CRC, runt, fragment, oversize, alignment, and jabber. You can also set pre- and post-filters to capture and view one or more error packet types.

The current supported NIC cards are NE2000 compatible ISA and PCMCIA cards. Contact NGC Networks, or visit www.ngc.com for the latest list of NIC card supported.

The packet viewer summary window in [Figure 3-3](#) shows an example of captured Ethernet error packets.

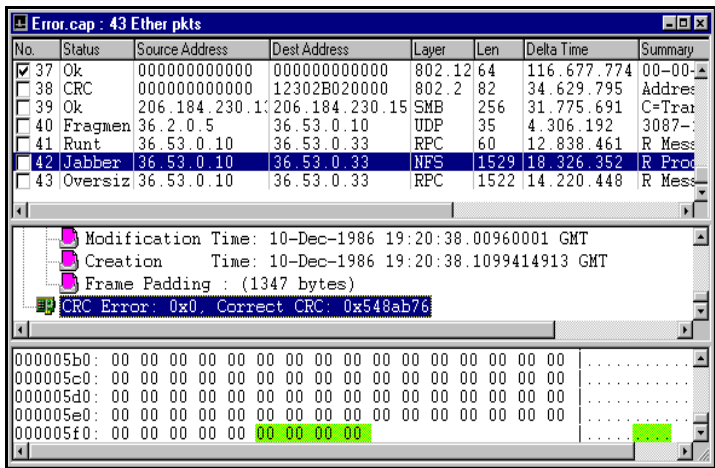


Figure 3-3. Packet View Summary Window

Changing Summary Address Field Display Format

In the Packet Viewer Summary window, you can customize the source and destination addresses field to display in hardware (MAC), network address, or node name format.

- To set the option:**
1. Select **Packet/Display Options....** The Packet Display Options window opens as shown in [Figure 3-4](#).
 2. Click the **Summary Display** page.

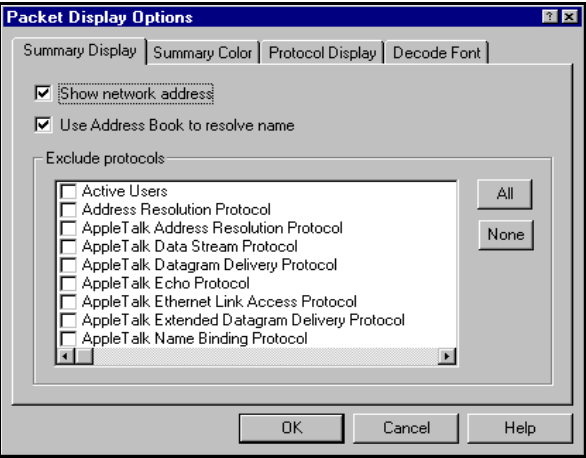


Figure 3–4. Packet Display Options Window

3. Select the appropriate check box(s) as listed in [Table 3–2](#) to set the address field format.
4. Click **OK**.

Table 3–2. Summary Address Field Display Format

Show Network Address	Use Address Book to Resolve Name	Address Format Displayed
<input type="checkbox"/>	<input type="checkbox"/>	Hardware address (MAC).
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Show IP address if IP packets; otherwise, show hardware address
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Show node name if defined, otherwise show hardware address with manufacturer ID.
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Show node name if defined, or else show IP address if IP packet; otherwise, show hardware address with manufacturer ID.

Overriding Protocol Field Display in the Summary Window

As a default, the protocol field in the Packet Viewer Summary window shows the highest level of the OSI protocols decoded by NetXRay. You can override the default choice to display only a particular protocol level of the OSI protocol for a given type of packet. For example, a HTTP packet will be shown as HTTP in the summary protocol field. If you want to show only a TCP protocol type being displayed in the summary window, you can use the packet display option to exclude HTTP from the summary selection.

The packet decode summary window (Figure 3–5) shows HTTP is displayed as the default choice.

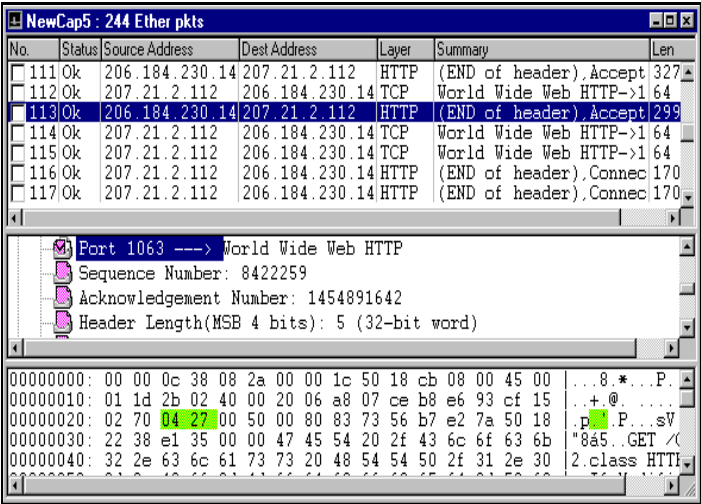


Figure 3–5. The Packet Decode Summary Window

To change the default:

1. Select **Packet/Display Options...**, then select the **Summary Display** page to show the list of decode protocols supported. The **Summary Display** page in the Packet Display Option window is shown in Figure 3–6.

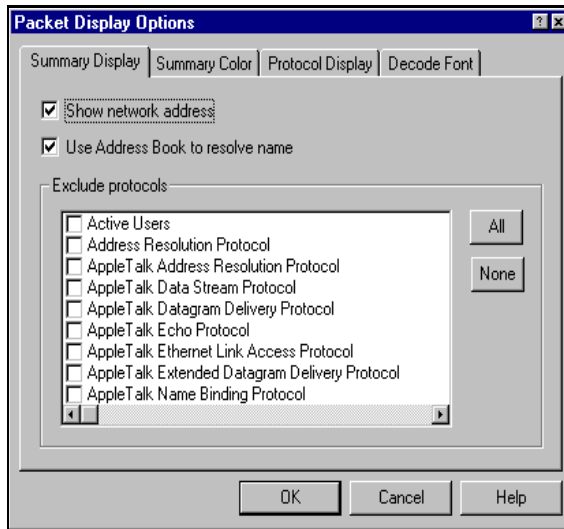


Figure 3-6. The Summary Display Page

2. In the summary window, select the protocols that will be excluded. In [Figure 3-7](#), HTTP and HTTPS are selected. Click **OK**.

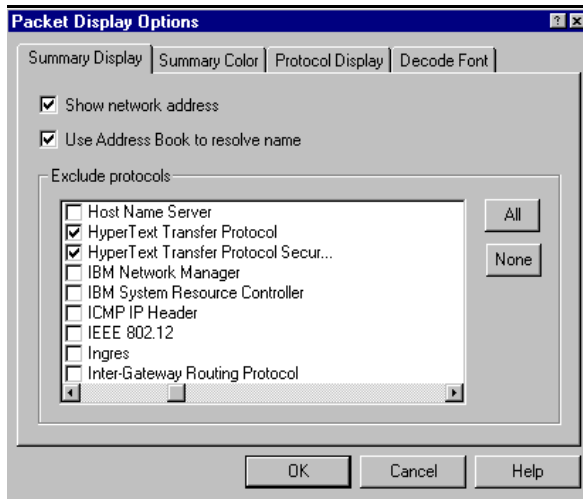


Figure 3-7. Summary Display Page, HTTP and HTTPS Selected

When you open a new packet decode window, HTTP will no longer be shown in the summary field. Instead, the next level protocol, TCP, is displayed as shown in [Figure 3-8](#).

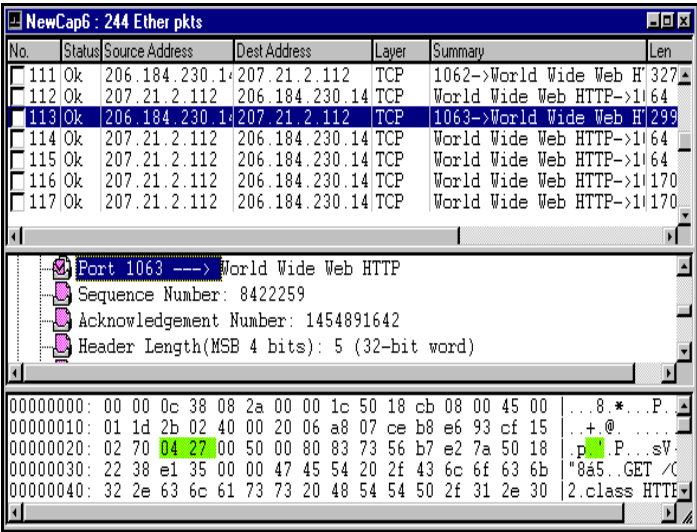


Figure 3–8. Packet Decode Summary Window, TCP Displayed

Detail Pane

The Detail pane, shown in [Figure 3–9](#), displays the detailed contents of the current selected packet. Each layer of the protocol is interpreted and displayed by protocol fields.

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, NetXRay expands protocol layer details in the Detail pane. You can save viewing space by clicking the minus (-) sign in front of the protocol sublayer line. The detail fields of that protocol layer will be contracted into a single line display with only the summary information. To expand the protocol display again, click the plus (+) sign.

NOTE: Contracting the protocol layer saves viewing space. This is useful when you want to print in WYSIWYG format. For more information, see [Printing Decoded Packets on page 3–18](#).

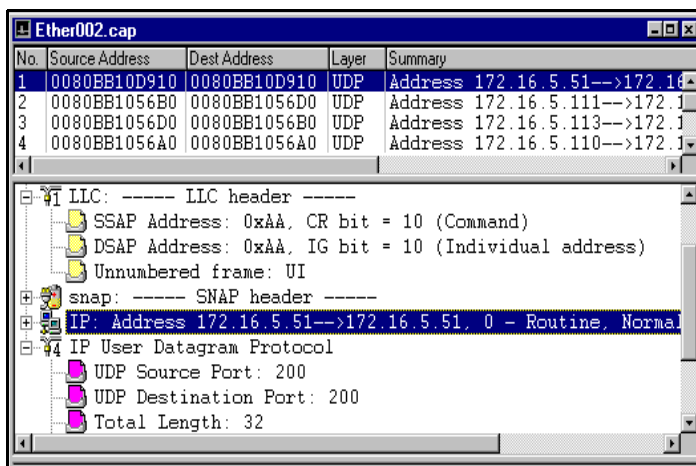


Figure 3–9. Packet Viewer Detail Pane

The expand or contract state of each subprotocol field is “memorized” by the packet viewer. The same state for that subprotocol is maintained, when you view the next or the previous packet. For example, when you contract the RIP protocol layer in IPX decode, subsequent viewing of other IPX RIP packets will show RIP protocol displayed in one-line summary mode.

The default viewing mode of the Detail pane can be customized.

To change the initial contracted or expanded view of each individual subprotocol:

1. Choose **Display Options...** from the Packet menu. A Packet Display Options property dialog box is displayed.
2. Click the **Protocol Display** tab (*Figure 3–10*).
3. Click on the check box to change that protocol type’s initial viewing state. A check mark indicates expanded view, otherwise, it is contracted view.
4. You can also click the **Open All** button to set all protocol layers in full expanded view. Click the **Close All** button to set all protocol layers in contracted view.
5. When you are satisfied with the selection, click **OK**.

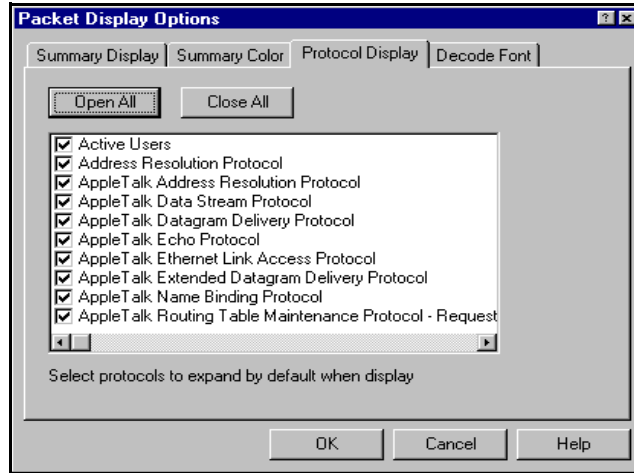


Figure 3-10. Protocol Display Tab Dialog Box

Hex Pane

The Hex pane shows the selected packet in hexadecimal and either ASCII, or EBCDIC format. The ASCII or EBCDIC section of the display shows a dot (.) for every octet that does not have an equivalent character representation.

To select either the ASCII or EBCDIC view, position the mouse anywhere on the Hex pane and click the right mouse button to bring up the context menu. Select either ASCII, or EBCDIC.

When you click on a one-line protocol summary, or a detailed protocol field in the Detail pane, the equivalent hexadecimal octets in the packet are highlighted in the Hex pane. This is helpful if you want to associate and understand the protocol field and its equivalent bytes in the packet.

Special Viewing Tips

Each pane can be resized by clicking and dragging the separator bar between the panes. Each pane contains scroll bars which may be manipulated using the mouse to change the viewing position in the pane. Cursor, Page Up, and Page Down keys also provide similar functions for the pane window that has the focus.

Keyboard Shortcuts

Aside from supporting full mouse action to allow easier viewing of the packets, the Packet Viewer supports the keys shown in [Table 3-3](#) to enhance your ability to advance packets quickly.

Table 3-3. Packet Window Shortcut Key Definitions

Key	Usage
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
F7	View the previous packet in the Summary pane
F8	View the next packet in the Summary pane
Alt +F3	Invoke the Find Packet dialog box
F2	Find the next marked packet
F3	Find next

To maximize the efficiency in scanning packets for details, Network General recommends that you follow the steps below:

- Adjust the packet viewer size and individual pane to maximize the viewing area for your particular interests.
- Select the starting packet of your interest in the Summary pane by clicking on it.
- Click the Detail pane to gain focus. The cursor movement and Page Up/Page Down keys will now apply to the Detail pane.
- Use the F7 key to move to the previous packet, and F8 to move to the next packet.
- If you want to move the viewing area in the Detail pane, use the cursor and Page Up/Page Down keys.

Anchoring a Field in the Detail Pane

By simply clicking on a selected field or protocol summary line to highlight it, you have anchored the field to be displayed in the Detail pane. NetXRay “remembers” the highlighted field in each packet, and will always place that field in the viewing windows of the Detail pane.

Anchoring a field in the Detail pane allows you to go back and forth between several packets without having to reposition the Detail pane by using the scroll bar *Figure 3-11*.

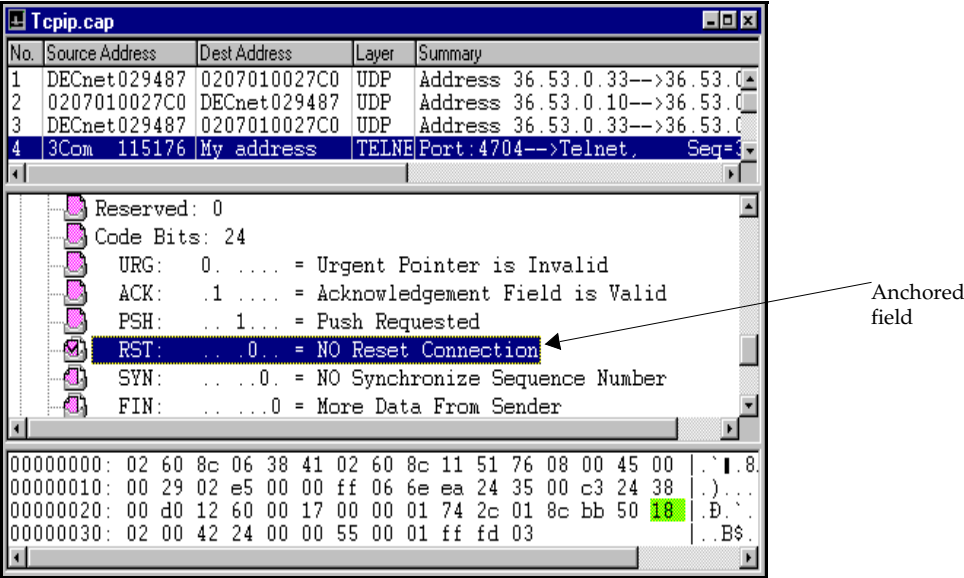


Figure 3-11. Anchored Field in the Detail Pane

Searching Packets

NetXRay gives you the ability to search and locate packets that match a protocol field, a data pattern, or packet status in the packets.

NetXRay can also help you to advance to a particular packet number.

To search and locate a packet that matches a data field in a known packet:

1. Locate and highlight a protocol field or a data pattern in the Detail pane of the packet viewer.
2. Select **Find Packet...** from the Packet menu, or from the context menu in Packet Viewer to invoke the Search Packet dialog box (*Figure 3–12*).

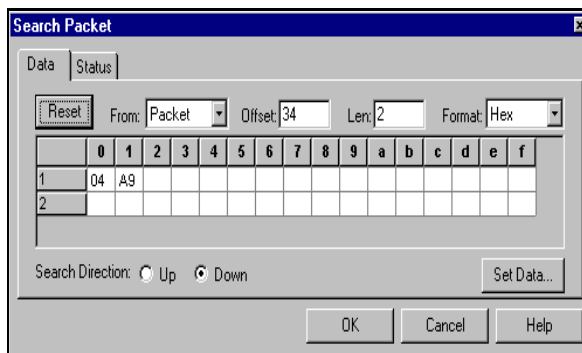


Figure 3–12. Search Packet Dialog Box – Data Page

3. Open the drop-down list **From** and select **Don't Care**. Click **Set Data...** button to open the Detail Decode view of the packet (*Figure 3–13*).

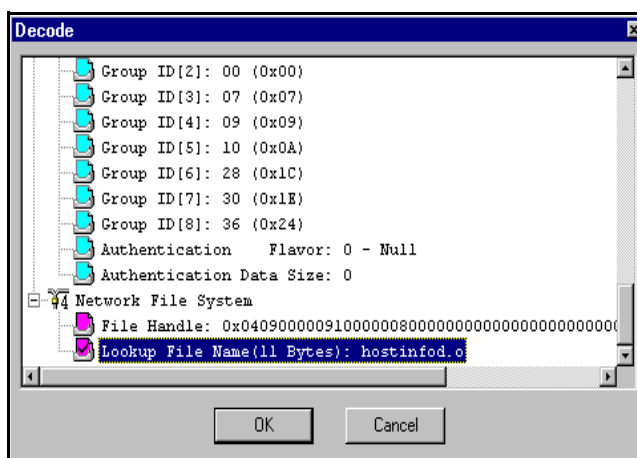


Figure 3–13. Detail Decode View of a Packet

4. Select and highlight the data pattern or field of your choice, and click **OK**. The new data is placed in the data pattern area. Adjust the data and the length if necessary, and click **OK** to start the search.

If a pattern match is found, the packet containing the pattern is displayed in the Packet Viewer. Press F3 to search for the next packet.

To search a packet with a known data pattern without locating the packet first:

1. Select **Find Packet...** from the Packet menu, or from the context menu in the Packet Viewer to invoke the Search Packet dialog box.
2. Change the offset, size, or the contents of the data field if necessary, and click **OK** to start the search.

To search a trigger frame or an Ethernet error packet:

1. Select **Find Packet...** from the Packet menu, or from the context menu in the Packet Viewer to invoke the Search Packet dialog box. Click the **Status** page ([Figure 3-14](#)).

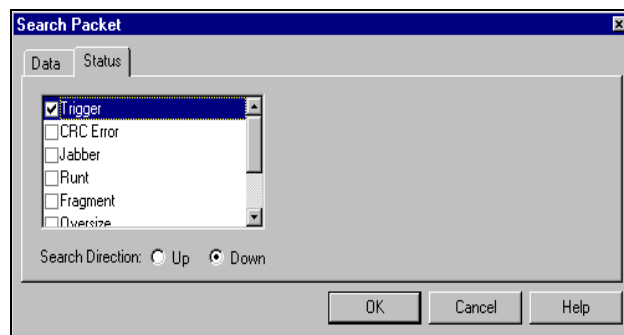


Figure 3-14. Search Packet Dialog Box – Status Page

1. Check **Trigger** or the appropriate Ethernet errors, and click **OK** to start the search.

Alternatively, if you know the packet number, you can advance to the packet by selecting **Go To...** from the Packet menu, or from the context menu in the Packet Viewer. Enter the packet number, then click **OK** ([Figure 3-15](#)).

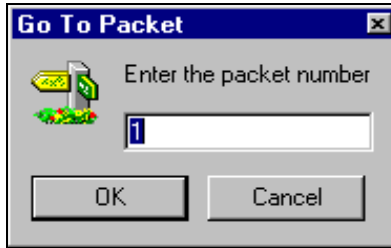


Figure 3-15. The Go To Packet Dialog Box

Marking Packets

NetXRay lets you mark individual packets or a group of packets in the Summary pane of the packet viewer window. You can save the marked packets into separate packet viewer windows for viewing or you can save them to a file. You can also treat the marked packets as bookmarks. Use F2 to advance the packets in the Summary pane from packet to packet.

Marking packets allows you to pick out only those packets that are of interest to you, so that they can be saved for troubleshooting or as a source of packet playback to re-create the same network conversation scenario.

Figure 3-16 shows marked packets in the Summary Pane. The procedures following *Figure 3-16* describe several ways to mark the packets.

To mark individual packets, click the check box in front of the packet's index number.

No.	Source Address	Dest Address	Layer	Len	Summary	Rel. Time
<input type="checkbox"/> 1	139.87.84.20	139.87.84.70	NFS	138	Port NFS -> 0:00:0	
<input type="checkbox"/> 2	139.87.84.70	139.87.84.20	NFS	1514	Port 1022 -> 0:00:0	
<input type="checkbox"/> 3	139.87.84.70	139.87.84.20	UDP	734	Port 34438 -> 0:00:0	
<input checked="" type="checkbox"/> 4	129.213.240.25	139.87.84.54	NFS	182	Port 1019 -> 0:00:0	
<input checked="" type="checkbox"/> 5	139.87.84.54	129.213.240.25	NFS	1514	Port NFS -> 0:00:0	
<input checked="" type="checkbox"/> 6	139.87.84.54	129.213.240.25	UDP	1514	Port 32029 -> 0:00:0	
<input checked="" type="checkbox"/> 7	139.87.84.2	139.87.84.54	ICMP	98	Type=Redirect 0:00:0	
<input type="checkbox"/> 8	139.87.84.54	129.213.240.25	NetBios	1514	Type - 0x66 0:00:0	
<input type="checkbox"/> 9	139.87.84.54	129.213.240.25	UDP	1514	Port 36497 -> 0:00:0	

Figure 3-16. Marking Packets in the Summary Pane

To mark a group of packets:

1. Click the right mouse button, and select **Mark Range....**
2. Click the **Range** radio button, and enter the packet range of your choice.
3. Click the **Mark** button.

To clear all marked packets:

1. Click the right mouse button, and select **Mark Range....**
2. Click the **All *nnn* Packets** radio button ([Figure 3-17](#)).
3. Click **Unmark**.

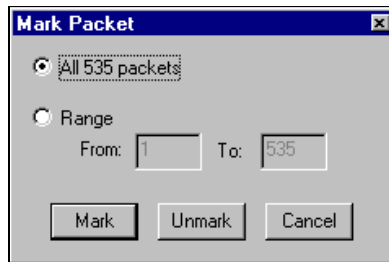


Figure 3-17. Marking All Packets

To mark all packets except a few undesired packets:

1. Click the right mouse button, and select **Mark Range....**
2. Click the **All *nnn* Packets** radio button.
3. Click the **Mark** button.
4. Scroll the Summary pane to locate the undesired packets. Click the check box in front of the undesired packet to deselect it. Once you have marked the packets you can save them.

To save the marked packets:

1. Click the right mouse button, and select **Save Marked**.
2. A new packet viewer is created showing only the marked packets.

NOTE: When you mark and save packets into a separate window, the relative time from packet to packet is properly maintained.

Using The Display Filter

The Display filter feature allows you to filter out unwanted packets after you have captured them. You can use the display filter to only view:

- 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

The Display filter shares the same profile database used by the capture filter. Once a filter is defined, it can be used interchangeably by Packet Viewer and Packet Capture.

To apply a filter:

1. Select **Apply Display Filters...** from the Packet menu.
2. Pick a predefined filter of your choice from the Post Filter dialog box ([Figure 3-18](#)), then click **OK**.

A new Packet Viewer window is displayed showing all the packets that matched and passed through the filter criteria.

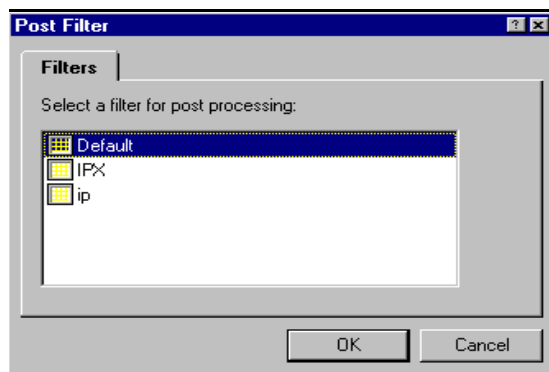


Figure 3-18. Post Filter Dialog Box

To create a new filter, select **Edit Display Filters...** from the Packet menu or from the context menu. For further information, refer to the [Packet Capture Setting on page 2-7](#).


Printing Decoded Packets

The decoded data packets in the Packet Viewer can be printed on hardcopy. You can select from four different decode views to print out. [Table 3-4](#) shows the Packet Decode printer output formats.

Table 3-4. Packet Decode Printer Output Format

Format	Information
Full Decode	Complete expanded list of protocol fields in Detail pane
Hex	Hex data and ASCII or EBCDIC characters in Hex pane
Summary	Line-by-line list of the packets in Summary pane
WYSIWYG Decode	Output the Detail pane as is displayed to the printer

To print from the Packet Viewer:

1. Select **Print...** from the File menu, or click the **Printer** icon on the Tool Bar.
2. From the printer dialog box ([Figure 3-19](#)), enter a range of packets and type of decode format.
3. Click **OK**.
4. If you want to abort the printing, click **Abort Printing**  on the Tool Bar.

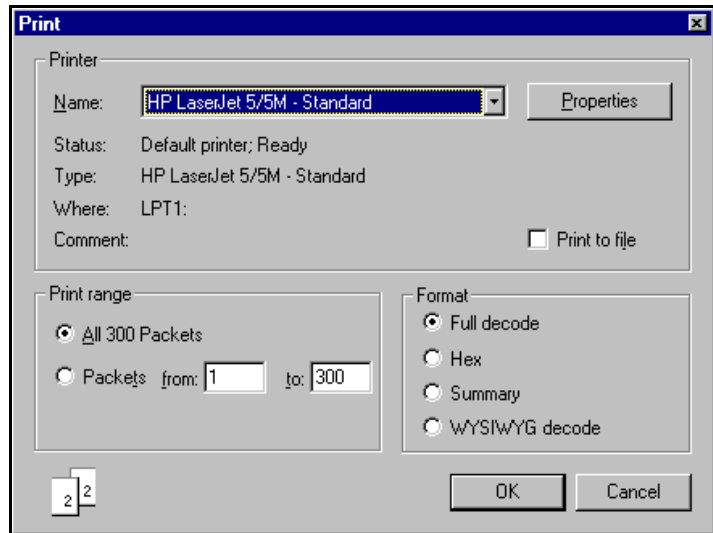



Figure 3-19. Print Dialog Box

NOTE: Some of the decode summary lines may be longer than 80 columns. Make sure your printer has been configured to handle long print lines. Alternatively, you can use print-to-a-file in the next section to output full width summary decode reports.

Printing Decoded Packets to a File

You can also output the decoded packets to an ASCII text file, so that viewing can be done separately by using a text editor or a word processor.

To print to a text file in NetXRay:

1. Select **Print...** from the File menu, or click the **Printer** icon on the Tool Bar.
2. From the printer dialog box, enter a range of packets and type of decode format. Then check the **Print to file** check box.
3. Click **OK**. A Print to File dialog box is displayed ([Figure 3-20](#)).
4. Enter an output filename, then click **Save**.
5. If you want to abort the print to a file, click **Abort Printing**  on the Tool Bar.

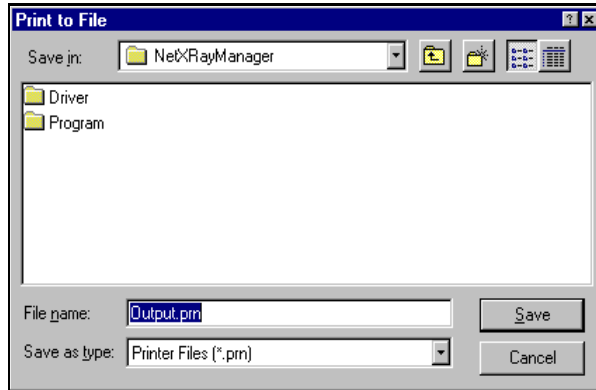


Figure 3-20. Print to File Dialog Box

Saving Captured Packets to a File

You can save captured packets to a file so that later, you can open the saved capture file for viewing or printing.

To save captured packets to a file:

1. Select **File** from the Menu bar, click on **Save As....** A Save As dialog box ([Figure 3-21](#)) is displayed.
2. Enter the filename for your capture file. You have the option of choosing a file folder or location in which to put this file. Click **OK**.
3. Optionally, you can save in compressed file format to conserve disk space. Enter the file extension, *CAZ*, to specify compression.

NOTE: Captured packets can only be saved from the Packet Viewer window.

NOTE: If you do not specify a filename extension or if you specify an extension as CAP, NetXRay will save the file in NetXRay file format. However, if the extension name is ENC, TRC or FDC, the captured file will be saved in Sniffer analyzer Ethernet, Token Ring, or FDDI data format respectively. Files saved in Sniffer analyzer format can be viewed by the Expert Sniffer Network Analyzer or other network analyzers that support this format.

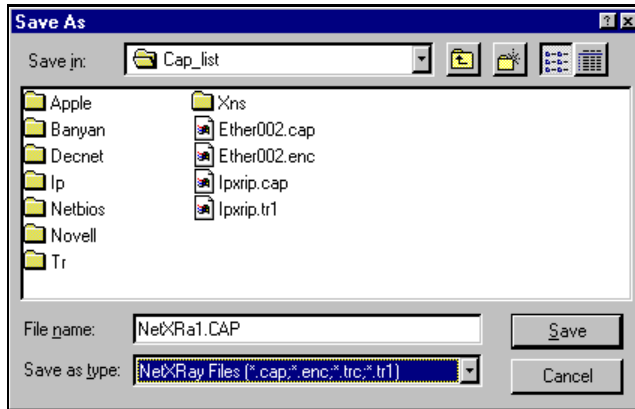



Figure 3-21. Save As Dialog Box

Displaying Packets from a Capture File

To review a saved capture file:

1. Select **File** from the Menu bar. Click on **Open...** or click the  icon on the Tool bar. A File Open dialog box (Figure 3-22) is displayed.
2. Enter the filename for your capture file. You have the option of choosing a file folder or location in which to put this file. Click **OK**.
3. The selected file is displayed in a new Packet Viewer window.

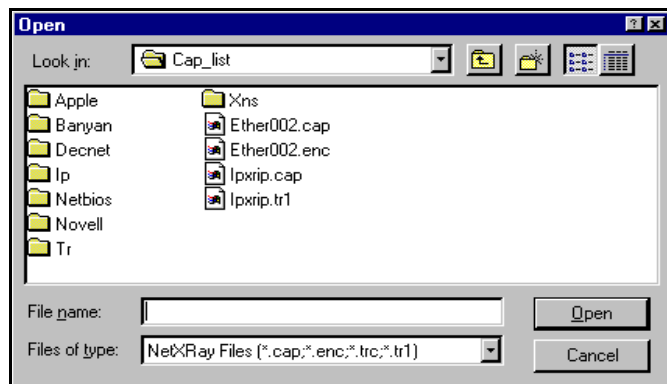


Figure 3-22. File Open Dialog Box

In addition to retrieving files previously saved in its internal (.CAP, .CAZ) format, NetXRay also recognizes Ethernet (.ENC), Token Ring (.TRC) and FDDI (.FDC) capture files created by Network General's Expert Sniffer Network Analyzer. Files created using Versions 4.1 and earlier are supported; files created by later versions must be saved in an encompassed format. A compressed Sniffer capture file cannot be viewed by NetXRay.

Novell LANalyzer for Windows capture files (.TR1) can also be displayed by NetXRay.

Packet Post Analysis

This chapter describes the Post Analysis of the Packet Viewer function.

The Post Analysis gives you the ability to perform network statistical analysis on the packet capture buffer. These functions are summarized below:

- Matrix statistics in MAC, IP, and IPX levels. The summary is viewed in a traffic map, outline table, detail table, bar chart, or pie chart format.
- Matrix traffic map provides a birds-eye view of the network conversation in traffic load and protocol type.
- Visual filter in the matrix provides a powerful method to allow you to filter out unwanted traffic quickly.
- Host statistics in MAC, IP, and IPX levels. The summary is viewed in an outline table, detail table, bar chart, or pie chart format.
- Protocol distribution statistics in MAC, IP, and IPX levels. The summary is viewed in a table, bar chart, or pie chart format.
- Summary statistics information.

Showing Matrix Summary in Packet Decode

The matrix summary provides a quick analysis of the conversation traffic statistics collected in the packet capture buffer. You can view all traffic at the MAC layer, or selectively view only network layer traffic in IP or IPX.

The matrix has five different views: traffic map, outline table, detail table, bar chart, or pie chart, giving a flexible set of choices to show statistics in different ways. [Table 4-1](#) shows the information displayed for each type of view.

*Table 4–1. Information Displayed in Each View of the Matrix
Summary (1 of 3)*


Type of View	OSI Layer	Information Displayed
Traffic map 	MAC	Graphical presentation of conversation relationship between MAC-layer nodes, their network load, and the type of network protocols used (that is, IP, IPX, NetBIOS, DecNET, and so on). If more than one protocol is recorded between two nodes, the connecting line will be shown with multiple color segments representing multiple protocols. The length of each color segment will be proportionally set to the number (#) of bytes recorded for that protocol.
	IP	Graphical presentation of conversation relationship between IP-layer nodes, their network load, and the type of application protocols used (that is, FTP, Telnet, HTTP, Gopher, NFS, and so on).
	IPX	Graphical presentation of conversation relationship between IPX-layer nodes, their network load, and the type of transport protocol used (that is, NCP, SAP, RIP, NetBIOS, and so on).

Table 4–1. Information Displayed in Each View of the Matrix Summary (2 of 3)








Type of View	OSI Layer	Information Displayed
Outline table 	MAC	Total bytes and packets transmitted between pairs of MAC-layer nodes. They are listed in unidirection and bidirection totals. The expanded view shows traffic breakdown by network protocols (that is, IP, IPX, NetBIOS, DecNET, and so on).
	IP	Total bytes and packets transmitted between pairs of IP-layer nodes. They are listed in unidirection and bidirection totals. The expanded view shows traffic breakdown by application protocols (that is, FTP, Telnet, HTTP, Gopher, NFS, and so on).
	IPX	Total bytes and packets transmitted between pairs of IPX-layer nodes. They are listed in unidirection and bidirection totals. The expanded view shows traffic breakdown by transport protocols (that is, NCP, SAP, RIP, NetBIOS, and so on).
Detail table 	MAC, IP, IPX	Same as Outline table, except the entries are grouped by protocol types.

Table 4–1. Information Displayed in Each View of the Matrix Summary (3 of 3)

Type of View	OSI Layer	Information Displayed
Bar chart 	MAC, IP, IPX	Top-N conversation pairs based on the selected statistics recorded for each respective protocol layer; MAC, IP, or IPX.
Pie chart 	MAC, IP, IPX	Top-N conversation pairs based on the percentage of the selected statistics load recorded for each respective protocol layer; MAC, IP, or IPX.

In addition to the view buttons, there are three buttons to help you operate each view more efficiently. They are defined in [Table 4–2](#).

Table 4–2. Three Additional Help Buttons for the Matrix Summary


Button	Usage
	Visual Filter. Activated only in traffic map view. Use it to apply a post filter from the traffic map.
	Export. Activated when in outline or detail table view. It lets you export the table contents to a CSV file.
	Sort. Activated when in bar or pie view. It lets you display the top-N chart based on different statistical criteria, for example, total packets versus total bytes.

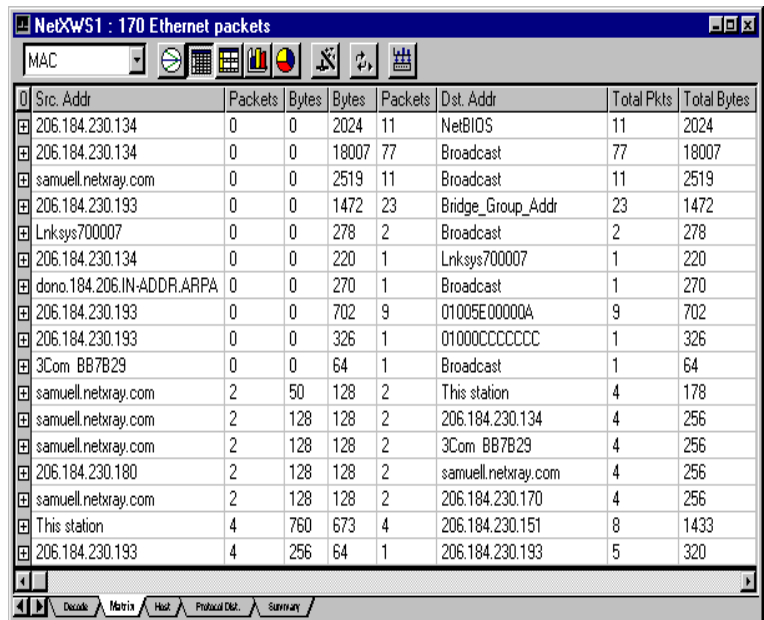
Traffic Map View

For information on the traffic map view, refer to [Using Matrix Traffic Map in Packet Decode on page 4–10](#).

Outline Table View

The outline table view ([Figure 4-1](#)) provides a quick summary of total bytes and packets transmitted between pairs of MAC layer nodes captured in the packet buffer. By selecting the MAC, IP, or IPX layer, you can view the traffic summary in each network layer instantaneously.

To view a matrix summary in outline table format, click 



0	Src. Addr	Packets	Bytes	Bytes	Packets	Dst. Addr	Total Pkts	Total Bytes
+	206.184.230.134	0	0	2024	11	NetBIOS	11	2024
+	206.184.230.134	0	0	18007	77	Broadcast	77	18007
+	samuell.netxray.com	0	0	2519	11	Broadcast	11	2519
+	206.184.230.193	0	0	1472	23	Bridge_Group_Addr	23	1472
+	Lnksys700007	0	0	278	2	Broadcast	2	278
+	206.184.230.134	0	0	220	1	Lnksys700007	1	220
+	dono.184.206.IN-ADDR.ARPA	0	0	270	1	Broadcast	1	270
+	206.184.230.193	0	0	702	9	01005E00000A	9	702
+	206.184.230.193	0	0	326	1	01000CCCCCCC	1	326
+	3Com BB7B29	0	0	64	1	Broadcast	1	64
+	samuell.netxray.com	2	50	128	2	This station	4	178
+	samuell.netxray.com	2	128	128	2	206.184.230.134	4	256
+	samuell.netxray.com	2	128	128	2	3Com BB7B29	4	256
+	206.184.230.180	2	128	128	2	samuell.netxray.com	4	256
+	samuell.netxray.com	2	128	128	2	206.184.230.170	4	256
+	This station	4	760	673	4	206.184.230.151	8	1433
+	206.184.230.193	4	256	64	1	206.184.230.193	5	320

Figure 4-1. Matrix Summary in Outline Table Format

The matrix table also tracks higher-layer protocol traffic totals for individual conversation pairs (see [Figure 4-2](#)). You can view the higher-layer traffic summary by clicking the + (plus) sign in front of individual node selectively, or by selecting the Expand All command from the context menu (invoked by clicking the right hand mouse button) or clicking the **o** symbol next to the **Src. Addr** column.

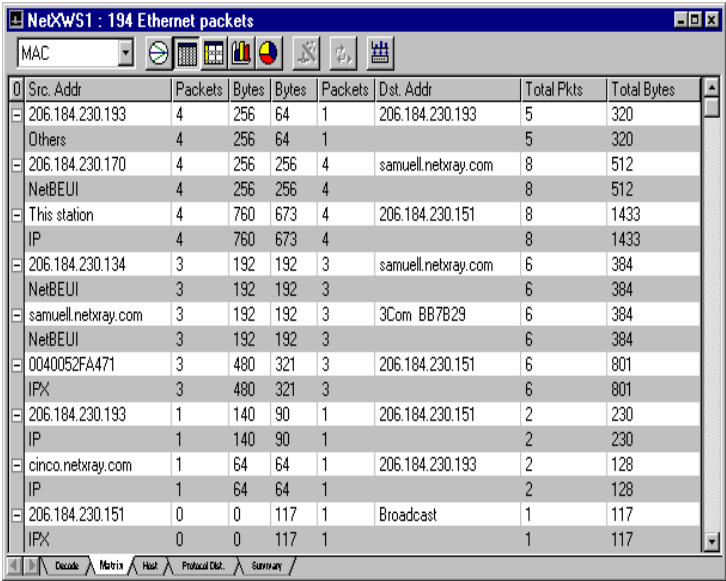



Figure 4-2. View of Matrix Higher-Layer Protocol Traffic

Detail Table View

The detail table shows a different summary view from the outline table. You can group the entries by the protocol type or by the node addresses. To group entries by protocol, click the  and click the **Protocol** column header.

The traffic loads segregated by protocol types appears (see [Figure 4-3](#)).

Protocol	Src. Addr	Packets	Bytes	Bytes	Packets	Dst. Addr
IP	3com 197937	10	580	863	11	This station
	Cinco 000024	4	326	326	4	ZNYX F8258A
	00400514E446	0	0	247	1	Broadcast
	0060979C6A19	0	0	247	1	
	Cinco 000027	1	108	64	1	H-P B951C3
	cisco 38082A	0	0	192	3	Broadcast
	This station	12	2280	2019	12	H-P 315D27
	ZNYX F8258A	0	0	64	1	
	H-P B951C3	0	0	1769	8	Broadcast
	cisco 38082A	0	0	2730	35	01005E0000QA
IPX	Cinco 000027	0	0	1978	9	
	This station	0	0	300	2	Broadcast
	H-P 315D27	0	0	234	2	
NetBEUI	Intel B64B86	0	0	192	3	
	Cinco 002022	12	840	840	12	Cinco 000027
	This station	0	0	195	1	NetBIOS
	0060979C6A19	10	640	640	10	0060976776F9
	H-P B951C3	0	0	736	4	NetBIOS


Figure 4-3. Display of the Detail Table

Clicking the node address column header will group all conversation pairs into node address order, which reveals the traffic load generated by protocol types for a particular node address (see Figure 4-4).

Protocol	Src. Addr	Packets	Bytes	Bytes	Packets	Dst. Addr
IP	ZNYX F8258A	0	0	64	1	Broadcast
NetBEUI		12	768	768	12	0060979C6A19
IP	This station	0	0	300	2	Broadcast
NetBEUI		12	2280	2019	12	H-P 315D27
NetBEUI	Intel B64B86	0	0	195	1	NetBIOS
IPX		0	0	192	3	Broadcast
NetBEUI	H-P B951C3	0	0	184	1	NetBIOS
IP		0	0	1769	8	Broadcast
NetBEUI	H-P 315D27	0	0	736	4	NetBIOS
IPX		0	0	234	2	Broadcast
Others	cisco FFF4AF	17	2074	122	1	cisco FFF4AF
		0	0	5632	88	Bridge_Group_Addr
IP	cisco 38082A	16	1024	64	1	cisco 38082A
		0	0	2730	35	01005E0000QA
Others	Cinco 002022	0	0	192	3	Broadcast
		0	0	984	3	01000CCCCCCC
NetBEUI	Cinco 002022	16	1168	1168	16	0060979C6A19
IPX		12	840	840	12	Cinco 000027

Figure 4-4. Detail Table Generating Protocol Types for a Particular Node Address

Bar Chart View

The bar chart reveals the top-N busiest conversation node pairs in captured packet buffer. You can view top-N conversation in MAC, IP, or IPX-layer traffic. For example, to view top-N conversations, click  then select IP from the drop-down list on the upper left corner of the window (see [Figure 4-5](#)).

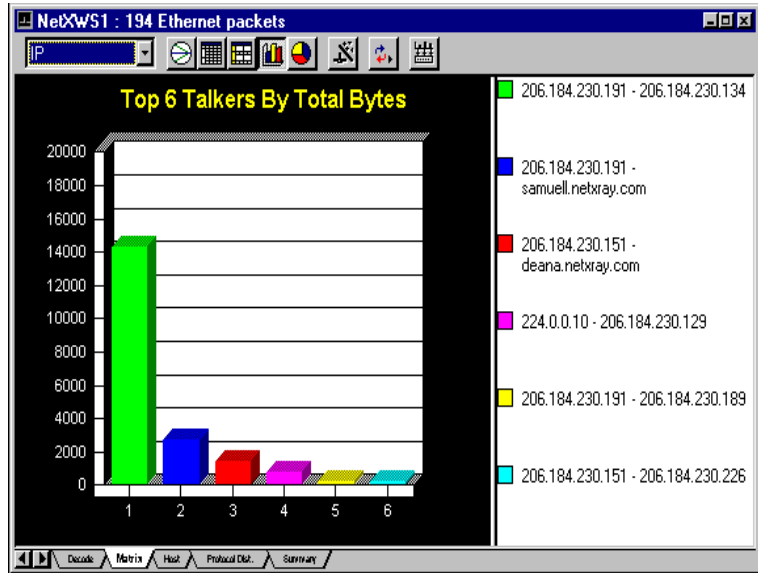



Figure 4-5. Bar Chart of Detail Table View

Pie Chart View

The pie chart reveals the top-N busiest conversation node pairs in their relative percentage (%) load of the total top-N traffic. To view the top-N pie chart, click the  icon (see [Figure 4-6](#)).

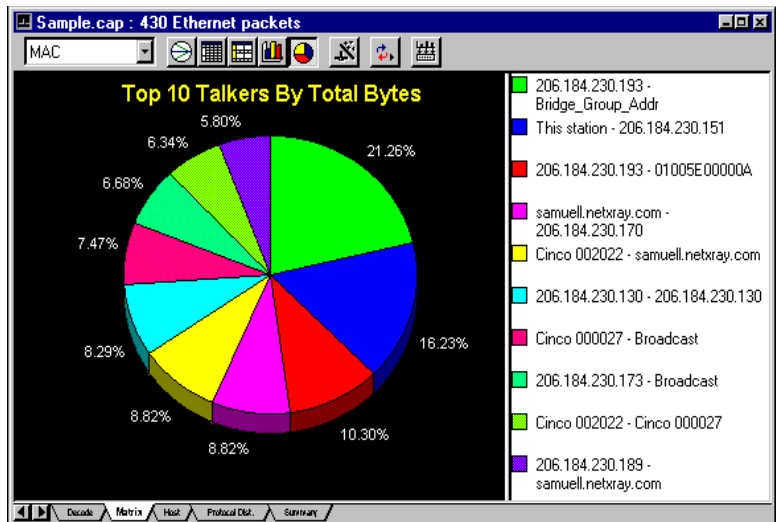


Figure 4-6. Pie Chart of Detail Table View

Sometimes, if the percentage load is not evenly distributed, the small percentage (%) numbers shown on the pie chart will overlap each other, making the percentage numbers illegible. You can click and drag the slice of pie outward to make room for the numbers as shown in [Figure 4-7](#).

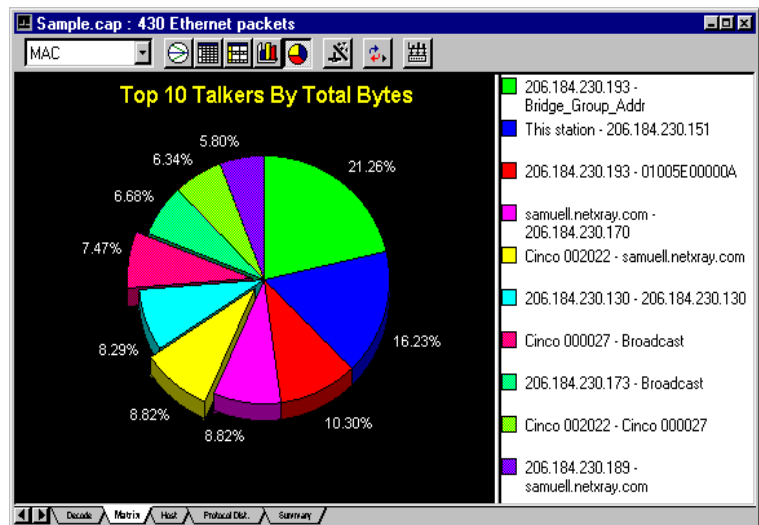


Figure 4-7. Pie Slicing in the Detail Table View

Using Matrix Traffic Map in Packet Decode

The traffic map in packet decode is a powerful tool that provides you with a birds-eye view of the network traffic patterns captured in the packet buffer. It gives a complete graphical presentation of the traffic pattern between network nodes, as well as the type of protocol used for communications.

In addition, you can filter out unwanted traffic by unchecking certain protocols, or by selecting network nodes of interest for display. The ability to step-by-step analyze and filter traffic helps you to isolate and identify problems quickly.

Figure 4–8 shows how you can display the complete traffic map, then shows the IP level traffic, and finally isolates traffic transmitted to and from one particular IP node.

To display the traffic map, simply select the Matrix tab on the bottom of the packet viewer window, and click the traffic map button.

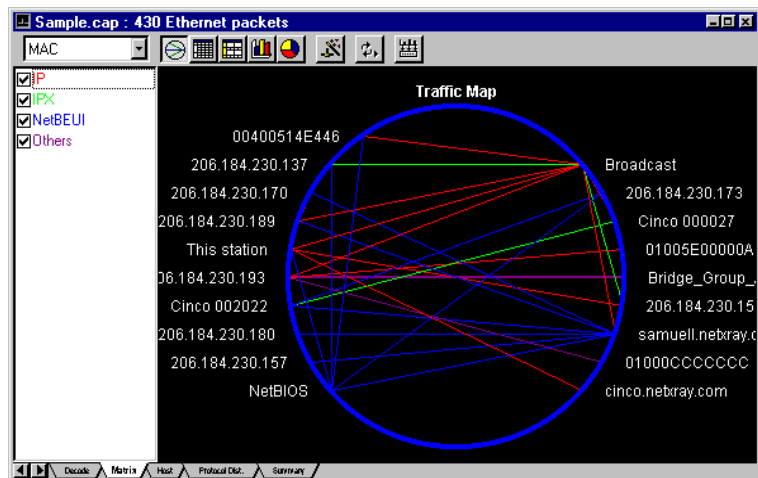


Figure 4–8. Traffic Map Window

The drop-down list on the upper left corner of the traffic map window lets you view the traffic map from the MAC, IP, or IPX layer. The protocol checklist on the left side of the window will change depending on the layer you choose. For example, if you

select IP from the drop-down list, the traffic map will display only IP-layer conversation as shown in [Figure 4-9](#). Notice the protocol checklist on the left now shows IP application-layer protocols of NetBIOS, Others, POP, and SNMP.

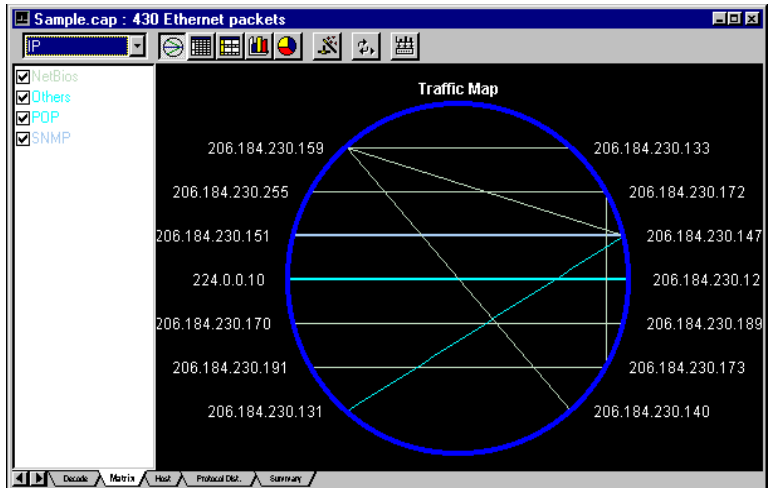


Figure 4-9. Display of IP-Layer Traffic Map

Each connection line between two network nodes is colored with protocol(s) that are communicated between them. If more than one protocol is recorded between two nodes, the connecting line will be broken into color segments with each color representing a different protocol. The length of each color segment is proportionally set to the # of bytes recorded for that protocol.

To further isolate traffic to and from one node, you can highlight the node of your choice, then click **Show Selected Nodes** from the Context menu. The IP node 206.184.230.147 is selected in [Figure 4-10](#), where the resulting traffic map is shown.

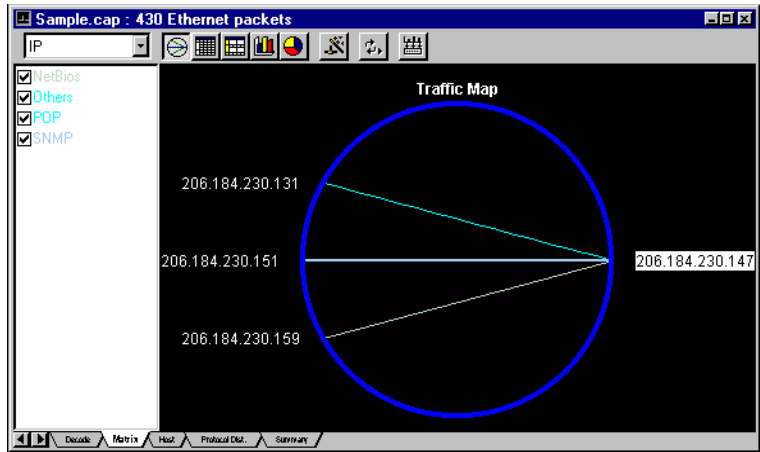


Figure 4–10. Display of Selected Node from the Context Menu

Using Visual Filter in the Matrix Traffic Map

The traffic map can also be used as a “visual post filter” to filter the packets in the packet buffer to match the current traffic map address and protocol criteria. To use the visual filter, simply click and highlight the network node(s) on the traffic map as shown in [Figure 4–11](#). To select more than one node, hold the **Control** key down, then click additional nodes.

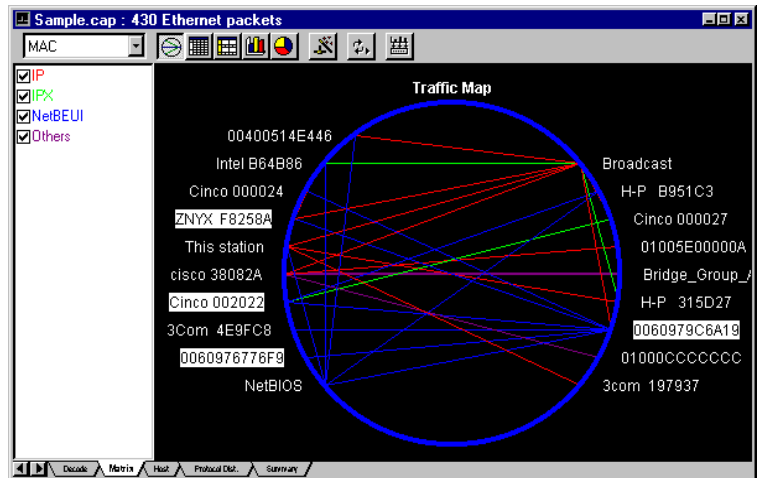



Figure 4-11. Display of Visual Filter Selected Network Nodes

To apply the visual filter, click  and a new packet viewer window is shown with only packets which match the node addresses selected (see Figure 4-12).

No.	Status	Source Address	Dest Address	Layer	Len	Delta Time	Summary
26	Ok	ZNYX F8258A	0060979C6A19	LLC	64	0.000.000	Sap 0xF0 ---
27	Ok	0060979C6A19	ZNYX F8258A	LLC	64	0.000.156	Sap 0xF0 ---
28	Ok	Cinco 002022	0060979C6A19	LLC	64	0.924.807	Sap 0xF0 ---
30	Ok	0060979C6A19	Cinco 002022	LLC	64	0.000.244	Sap 0xF0 ---
35	Ok	0060979C6A19	Cinco 002022	LLC	64	1.399.105	Sap 0xF0 ---
36	Ok	0060979C6A19	ZNYX F8258A	LLC	64	0.000.132	Sap 0xF0 ---
37	Ok	ZNYX F8258A	0060979C6A19	LLC	64	0.000.109	Sap 0xF0 ---
38	Ok	Cinco 002022	0060979C6A19	LLC	64	0.000.109	Sap 0xF0 ---
58	Ok	0060979C6A19	0060976776F9	LLC	64	12.019.436	Sap 0xF0 ---
59	Ok	0060976776F9	0060979C6A19	LLC	64	0.000.138	Sap 0xF0 ---
61	Ok	Cinco 002022	0060979C6A19	SMB	100	1.045.758	C=Echo, Repea

Logical Link Control	
SSAP Address:	0xF0, CR bit = 0 (Command)
DSAP Address:	0xF0, IG bit = 0 (Individual address)
Supervisor frame:	RR, POLL, N(R) = 5
Frame Padding:	(16 bytes)

Hex	ASCII
00000000: 00 60 97 9c 6a 19 00 c0 95 f8 25 8a 00 04 f0 f0	...j..A...%
00000010: 01 0b 00 00 00 00 00 00 00 00 00 00 00 00 00
00000020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000030: 00 00 00 00 00 00 00 00 00 00 00 00 4e 2f de 6aN/b

Figure 4-12. Display of the Packet Viewer Window

NOTE: The sequence number of each packet in the original capture buffer has been retained. It is useful to reference the filtered packets against the original buffer. However, if the filtered packets are saved to a file then reopened again, all packets will be resequenced from number one.

Using Visual Filter to Identify “Others” Protocol Type

The traffic map’s powerful “visual post filter” provides an ideal way to find out “Other” protocol types in the capture buffer that do not fall in the protocol categories predefined by NetXRay.

To use the traffic map to filter “Other” protocol packets, simply uncheck all protocols listed in the traffic map except the Others box (see [Figure 4-13](#)).

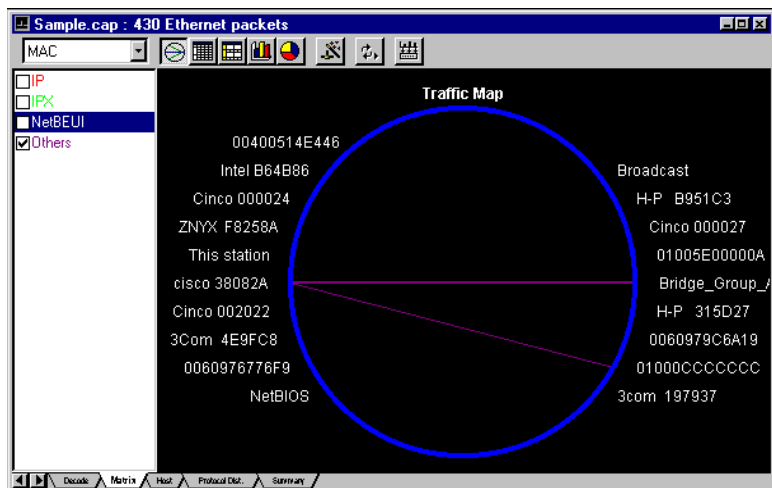



Figure 4-13. Display of Protocols with only the “Others” Box Checked

Click  and a new packet viewer window is shown with only packets in the “Others” category (see [Figure 4-14](#)).

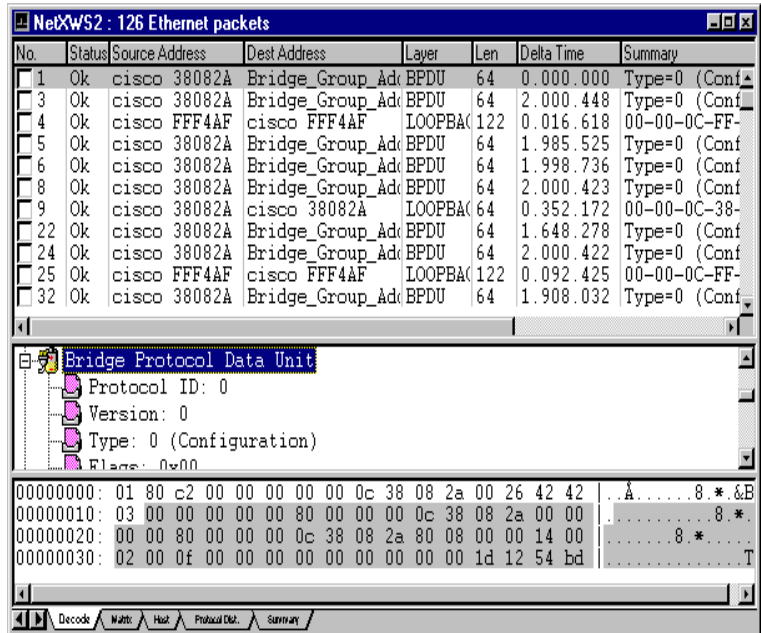


Figure 4-14. Display of New Packet Viewer Window with “Others” Checked

Showing Host Summary in Packet Decode

The host summary provides a quick analysis of the traffic statistics collected for each host node in the packet capture buffer. You can view host traffic at the MAC layer, or selectively view only network traffic at the IP or IPX layer.

Similar to the matrix summary, the host summary has four different views: outline table, detail table, bar chart, or pie chart. [Table 4-3](#) shows the information displayed for each type of view.

Table 4-3. Four Different Views of the Host Summary (1 of 2)







Type of View	OSI Layer	Information Displayed
Outline table 	MAC	Total bytes and packets transmitted by the MAC-layer host nodes. The number of packets and bytes transmitted in, out, and total in/out for each host node are listed. The expanded view shows traffic breakdown by network protocols (that is, IP, IPX, NetBIOS, DecNET, and so on).
	IP	Total bytes and packets transmitted by IP-layer host nodes. The number of packets and bytes transmitted in, out, and total in/out for each host node are listed. The expanded view shows traffic breakdown by application protocols (that is, FTP, Telnet, HTTP, Gopher, NFS, and so on).
	IPX	Total bytes and packets by IPX-layer host nodes. The number of packets and bytes transmitted in, out, and total in/out for each host node are listed. The expanded view shows traffic breakdown by transport protocols (that is, NCP, SAP, RIP, NetBIOS, and so on).
Detail table 	MAC, IP, IPX	Same as Outline table, except the entries are grouped by protocol types.
Bar chart 	MAC, IP, IPX	Top-N talkers based on the selected statistics recorded for each respective protocol layer; MAC, IP, or IPX.

Table 4–3. Four Different Views of the Host Summary (2 of 2)


Type of View	OSI Layer	Information Displayed
Pie chart 	MAC, IP, IPX	Top-N talkers based on the percentage of the selected statistics load recorded for each respective protocol layer; MAC, IP, or IPX.

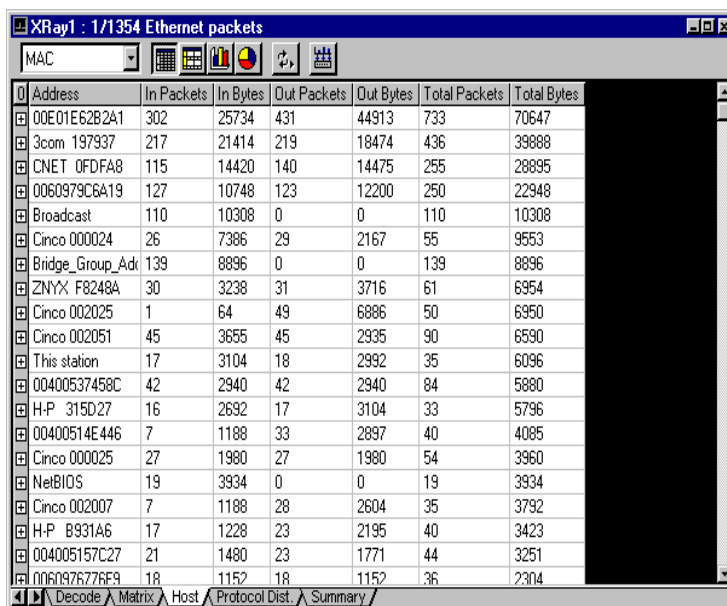
In addition to the view buttons, there are two buttons to help you operate each view more efficiently. They are defined in [Table 4–4](#).

Table 4–4. Two Additional Help Buttons for the Host Summary

Button	Usage
	Sort. Activated when in bar or pie view. It lets you display top-N chart based on different statistical criteria, for example, total packets versus total bytes.
	Export. Activated when in outline or detail table view. It lets you export the table content to a CSV file.

Outline Table View

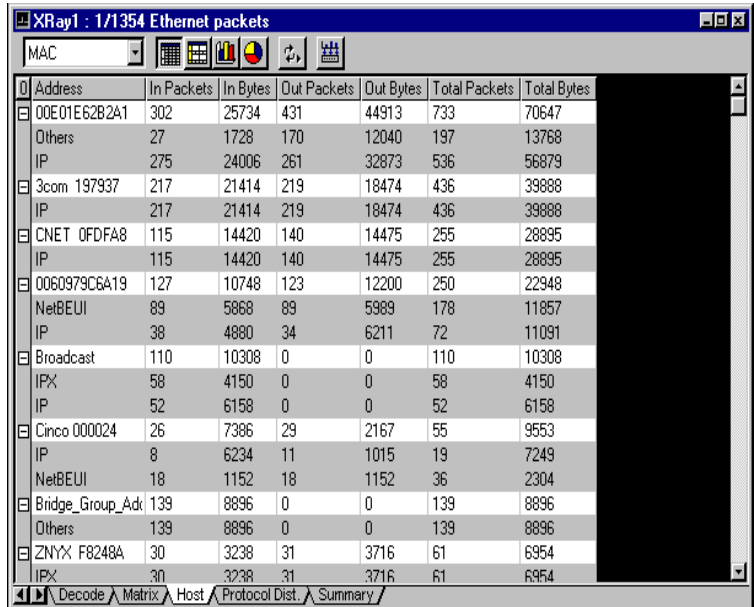
The outline table view provides a quick summary of total bytes and packets transmitted by each network node captured in the packet buffer. By selecting MAC, IP, or IPX layer, you can view traffic summary in each network layer instantaneously. To view matrix summary in outline table format, click on the  icon. [Figure 4–15](#) is displayed.



Address	In Packets	In Bytes	Out Packets	Out Bytes	Total Packets	Total Bytes
00E01E62B2A1	302	25734	431	44913	733	70647
3com 197937	217	21414	219	18474	436	39888
CNET 0FDFA8	115	14420	140	14475	255	28895
0060979C6A19	127	10748	123	12200	250	22948
Broadcast	110	10308	0	0	110	10308
Cinco 000024	26	7386	29	2167	55	9553
Bridge_Group_Adr	139	8896	0	0	139	8896
ZNYX F8248A	30	3238	31	3716	61	6954
Cinco 002025	1	64	49	6886	50	6950
Cinco 002051	45	3655	45	2935	90	6590
This station	17	3104	18	2992	35	6096
00400537458C	42	2940	42	2940	84	5880
H-P 315D27	16	2692	17	3104	33	5796
00400514E446	7	1188	33	2897	40	4085
Cinco 000025	27	1980	27	1980	54	3960
NetBIDS	19	3934	0	0	19	3934
Cinco 002007	7	1188	28	2604	35	3792
H-P B931A6	17	1228	23	2195	40	3423
004005157C27	21	1480	23	1771	44	3251
0060976776F9	18	1152	18	1152	36	2304

Figure 4-15. Metrix Summary in Outline Table Format

The host outline table also tracks higher layer protocol traffic totals for each network node. You can view the higher layer traffic summary by clicking the + (plus) sign in front of individual node selectively, or by selecting the **Expand All** command from the Context menu (invoked by clicking the right mouse button) or clicking the **o** symbol next to the **Src Addr** column. [Figure 4-16](#) is displayed.



XRay1 : 1/1354 Ethernet packets


MAC

Address	In Packets	In Bytes	Out Packets	Out Bytes	Total Packets	Total Bytes
00E01E62B2A1	302	25734	431	44913	733	70647
Others	27	1728	170	12040	197	13768
IP	275	24006	261	32873	536	56879
3com 197937	217	21414	219	18474	436	39888
IP	217	21414	219	18474	436	39888
CNET 0FDFA8	115	14420	140	14475	255	28895
IP	115	14420	140	14475	255	28895
0060979C6A19	127	10748	123	12200	250	22948
NetBEUI	89	5868	89	5989	178	11857
IP	38	4880	34	6211	72	11091
Broadcast	110	10308	0	0	110	10308
IPX	58	4150	0	0	58	4150
IP	52	6158	0	0	52	6158
Cinco 000024	26	7386	29	2167	55	9553
IP	8	6234	11	1015	19	7249
NetBEUI	18	1152	18	1152	36	2304
Bridge_Group_Adr	139	8896	0	0	139	8896
Others	139	8896	0	0	139	8896
ZNYX F8248A	30	3238	31	3716	61	6954
IPX	30	3238	31	3716	61	6954

Decode Matrix Host Protocol Dist Summary

Figure 4-16. Host Table Outline

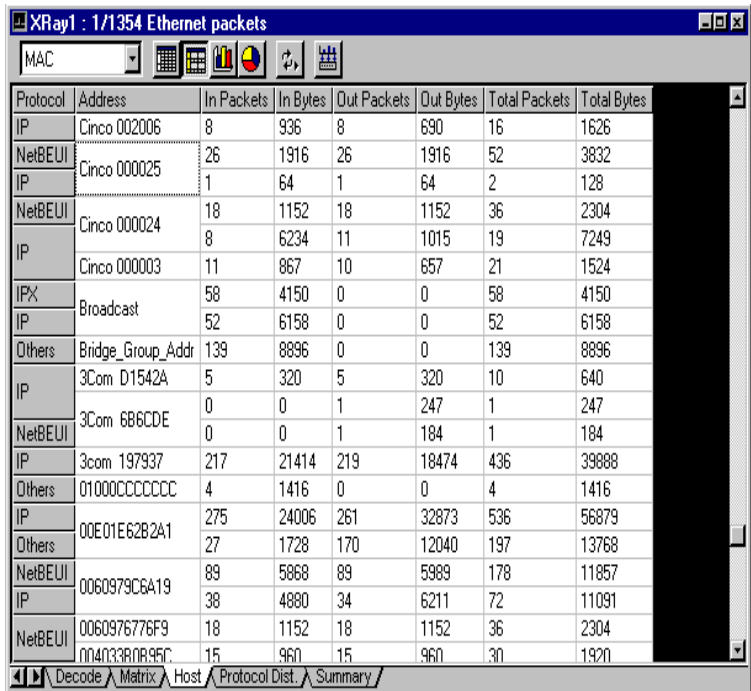
Detail Table View

The detail table shows a different summary view from the outline table. You can group the entries by the protocol type or by the node addresses. To group entries by protocol, click the  button and click the **Protocol** column header. You can see the traffic loads segregated by protocol types in [Figure 4-17](#).

Protocol	Address	In Packets	In Bytes	Out Packets	Out Bytes	Total Packets	Total Bytes
IPX	Cinco 002013	0	0	4	256	4	256
	Broadcast	58	4150	0	0	58	4150
	00400514E446	7	1188	33	2897	40	4085
	Lnksys700007	1	220	5	470	6	690
	Cinco 002007	7	1188	27	2339	34	3527
	H-P B931A6	16	1120	19	1426	35	2546
NetBEUI	ZNYX F8248A	30	3238	31	3716	61	6954
	3Com 6B6CDE	0	0	1	184	1	184
	0060979C6A19	89	5868	89	5989	178	11857
	00400537458C	42	2940	42	2940	84	5880
	NetBIOS	19	3934	0	0	19	3934
	Cinco 000025	26	1916	26	1916	52	3832
	0060976776F9	18	1152	18	1152	36	2304
	004005157C27	21	1480	23	1771	44	3251
	Cinco 000024	18	1152	18	1152	36	2304
	Cinco 002025	0	0	14	2870	14	2870
	004033B0B95C	15	960	15	960	30	1920
	H-P B931A6	0	0	1	273	1	273
	Xircom251BBA	0	0	1	195	1	195
	010000000000	4	1416	0	0	4	1416

Figure 4-17. Traffic Loads Segregated by Protocol Types in Detail View

Clicking the node address column header will group nodes into node address order, which reveals the traffic load generated by protocol types for a particular node address ([Figure 4-18](#)).



XRay1 : 1/1354 Ethernet packets


MAC

Protocol	Address	In Packets	In Bytes	Out Packets	Out Bytes	Total Packets	Total Bytes
IP	Cinco 002006	8	936	8	690	16	1626
NetBEUI	Cinco 000025	26	1916	26	1916	52	3832
IP	Cinco 000025	1	64	1	64	2	128
NetBEUI	Cinco 000024	18	1152	18	1152	36	2304
IP	Cinco 000003	8	6234	11	1015	19	7249
IP	Cinco 000003	11	867	10	657	21	1524
IPX	Broadcast	58	4150	0	0	58	4150
IP	Broadcast	52	6158	0	0	52	6158
Others	Bridge_Group_Addr	139	8896	0	0	139	8896
IP	3Com D1542A	5	320	5	320	10	640
NetBEUI	3Com 686CDE	0	0	1	247	1	247
IP	3com 197937	0	0	1	184	1	184
IP	3com 197937	217	21414	219	18474	436	39888
Others	01000CCCCC	4	1416	0	0	4	1416
IP	00E01E62B2A1	275	24006	261	32873	536	56879
Others	00E01E62B2A1	27	1728	170	12040	197	13768
NetBEUI	0060979C6A19	89	5868	89	5989	178	11857
IP	0060979C6A19	38	4880	34	6211	72	11091
NetBEUI	0060976776F9	18	1152	18	1152	36	2304
NetBEUI	004033B0B95C	15	960	15	960	30	1920

Decode Matrix Host Protocol Dist. Summary

Figure 4-18. Node Addresses Grouped by Traffic Load in Detail Table View

Bar Chart View

The bar chart reveals the top-N busiest host nodes in the captured packet buffer. You can view top-N hosts in MAC, IP or IPX layer traffic. For example, to view top-N IPX conversation, click the  button, then select IPX from the drop-down menu. [Figure 4-19](#) is displayed.

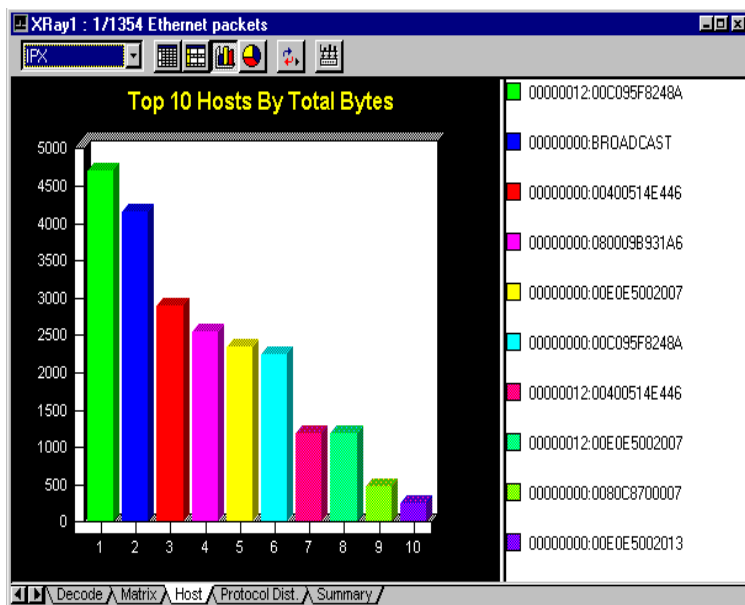



Figure 4-19. IPX Selected in Bar Chart View

Pie Chart View

The pie chart reveals the top-N busiest hosts in their relative % load of the total top-N traffic. To view top-N pie chart, click the  icon. [Figure 4-20](#) is displayed.

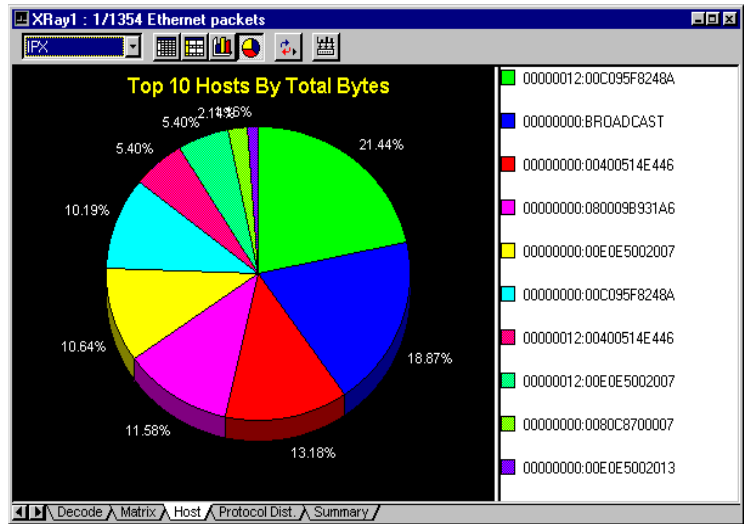





Figure 4–20. Top-N Pie Chart View

Showing Protocol Distribution Summary in Packet Decode

The protocol summary provides a quick analysis of the protocol distribution statistics collected in the packet capture buffer. You can view protocol distribution at the MAC layer, or selectively view only protocol distribution in the IP or IPX layers.




The protocol distribution summary has only three views: detail table, bar chart, or pie chart. [Table 4–5](#) shows the information displayed for each type of view.

Table 4–5. Three Different Views of the Protocol Distribution Summary

Type of View	OSI Layer	Information Displayed
Table 	MAC	Total bytes and packets transmitted in each MAC-layer protocol (that is, IP, IPX, NetBIOS, DecNET, and so on).
	IP	Total bytes and packets transmitted in each IP-layer application protocol (that is, FTP, Telnet, HTTP, Gopher, NFS, and so on).
	IPX	Total bytes and packets transmitted in each IPX-layer transport protocol (that is, NCP, SAP, RIP, NetBIOS, and so on).
Bar chart 	MAC, IP, IPX	Protocol distribution displayed in bar chart.
Pie chart 	MAC, IP, IPX	Protocol distribution displayed in percentage (%) pie chart.

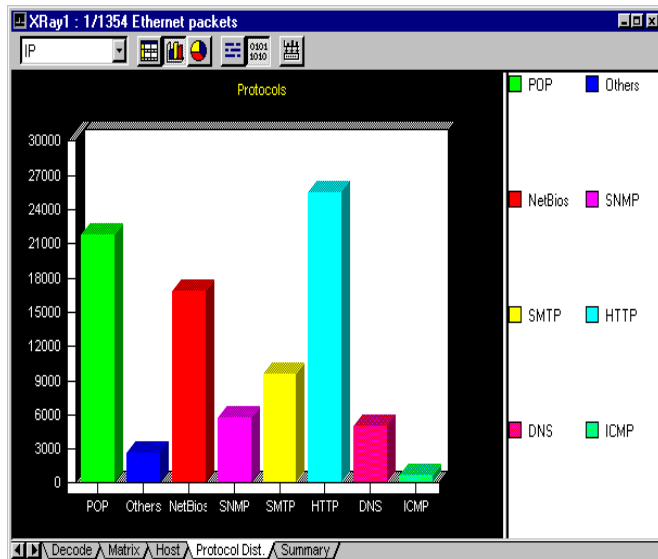
In addition to the view buttons, there are three buttons to help you operate each view more efficiently. They are defined in [Table 4–6](#).

Table 4–6. Three Additional Help Buttons for Protocol Distribution

Button	Usage
	Packets. Activated when in bar or pie chart view. It lets you display the protocol distribution chart based on total packets captured.
	Bytes. Activated when in bar or pie chart view. It lets you display the protocol distribution chart based on total bytes captured.
	Export. Activated only in table view. It lets you export the table content to a CSV file.

Bar Chart View

Figure 4–21 shows the IP-layer protocol distribution post analysis in bar chart view.

*Figure 4–21. IP-Layer Protocol Distribution in Bar Chart View*

Pie Chart View

Figure 4-22 shows the IP-layer protocol distribution post analysis in pie chart view.

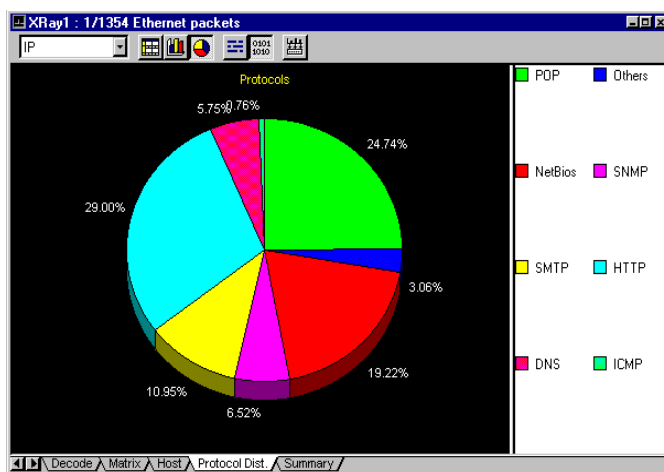
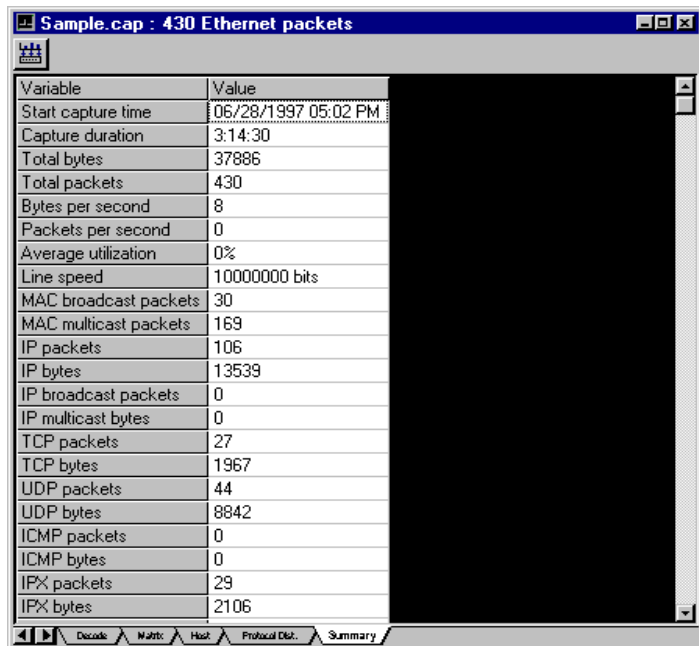


Figure 4-22. IP-Layer Protocol Distribution in Pie Chart View

Showing Summary Statistics Information in Packet Decode

For each capture buffer, NetXRay accumulates statistics information to assist you in analyzing the traffic load of a capture session. It shows MAC, IP, and IPX-layer traffic total counts.

To display summary information, click the Summary tab at the bottom of the packet viewer window (see [Figure 4-23](#)).



Variable	Value
Start capture time	06/26/1997 05:02 PM
Capture duration	3:14:30
Total bytes	37886
Total packets	430
Bytes per second	8
Packets per second	0
Average utilization	0%
Line speed	10000000 bits
MAC broadcast packets	30
MAC multicast packets	169
IP packets	106
IP bytes	13539
IP broadcast packets	0
IP multicast bytes	0
TCP packets	27
TCP bytes	1967
UDP packets	44
UDP bytes	8842
ICMP packets	0
ICMP bytes	0
IPX packets	29
IPX bytes	2106

Figure 4-23. Display of Summary Information

Chapter 5


Packet Generator

This chapter describes the steps for generating packets from the Packet Generator.

Transmitting packets onto the network gives you the ability to:

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

The Packet Generator is designed to share the CPU processing with other NetXRay operations and other Windows 95 applications. In fact, you can generate traffic, capture packets, and monitor the network load at the same time.

To invoke the Packet Generator, choose **Packet Generator** from the **Tools** menu or click the  icon on the Tool bar. A packet generator window is displayed (see [Figure 5-1](#)).

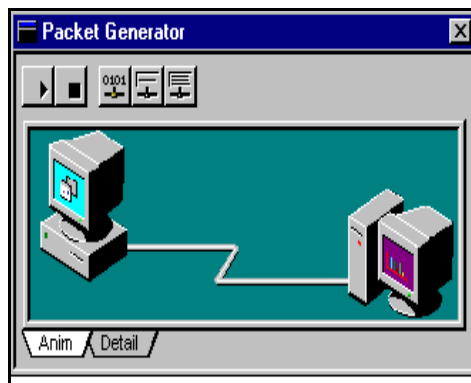


Figure 5-1. The Packet Generator Window

The Packet Generator has two views; one in animation view, and the other in detail view. To see a packet transmitting progress in detail, click the **Detail** tab (see [Figure 5-2](#)).

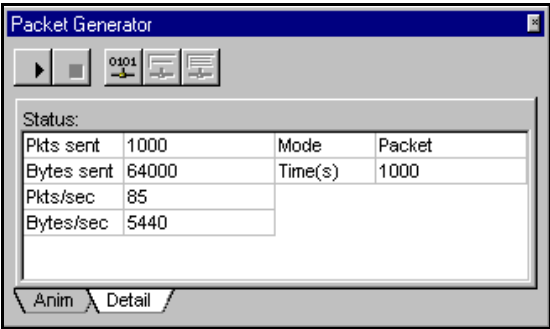



Figure 5–2. The Packet Generator—Detail View

The status details of the transmission are listed below:

Pkts sent	Total # of packets sent during this transmission.
Bytes sent	Total # of bytes sent during this transmission.
Pkts/sec	Rate of transmission in packets/second.
Bytes/sec	Rate of transmission in bytes/second.
Mode	Packet (single) or Buffer (file) mode.
Time(s)	# of times selected in Send dialog box.

WARNING: Transmitting packets to a real network may produce unexpected results which may cause difficulties in your operation. Make sure you have isolated your test network from the production network before proceeding with network load testing.

Transmitting a Single Packet

Transmitting a single packet can be invoked by clicking the **Send New Packet** button, or clicking the  **Send Current Packet** button when a captured file or buffer is displayed in Packet Viewer (Figure 5–3).

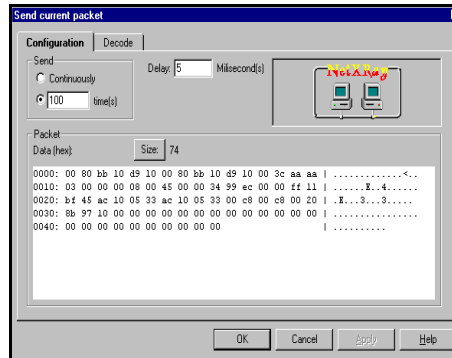


Figure 5-3. The Current Packet Window

You can change the following packet send parameters:

- Send # of times, or continuously
- Delay Time in milliseconds between packet send
- Packet size
- Packet contents

The **Decode** page in the Send Packet dialog box (see [Figure 5-4](#)) gives you instant analysis of the hex data pattern you just entered in decoded form.

Setting the delay time to zero milliseconds produces the maximum # of packets transmitted per second. The rate of transmission is dependent on the size of the packet, the NIC card NDIS driver's performance, and your computer's CPU speed. To achieve maximum transmission rate, use a PCI NIC adapter.

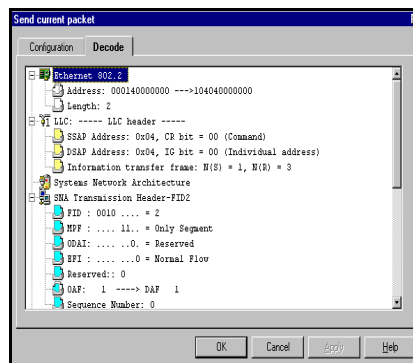


Figure 5-4. The Decode Page in the Send Packet Dialog Box

NOTE: Since NetXRay is designed to run in Windows 95's multitasking environment, the delay time used in packet transmission cannot be accurately controlled. It may vary depending on the number of and type of applications you are running on your computer.

Editing the Packet Contents

Packet contents can be modified from the hex field or directly from each decoded field in the **Decode** page.

To edit packet contents for the Packet Generator:

1. Click the **Decode** page.
2. Select a field (highlight) of your choice, then click the mouse button once.
3. A small edit box is displayed over the field with the content shown in hex value.
4. Enter a new hex value, then press **Enter**.
5. The new value and its new meaning are displayed instantly. If the field changed is a subprotocol field, the subsequent field may change as well to reflect the newly defined packet type.

Figure 5–5 shows the Ethernet II Protocol Type field is being edited.

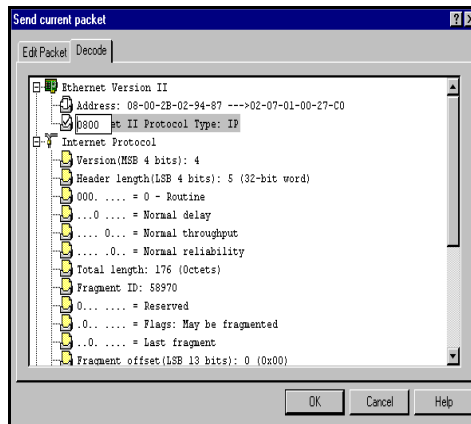



Figure 5–5. Editing Packet Contents on The Decode Page

Transmitting an Entire Capture

Click  to invoke the **Send Current Buffer** button when a captured file or buffer is displayed in Packet Viewer (see [Figure 5-6](#)).

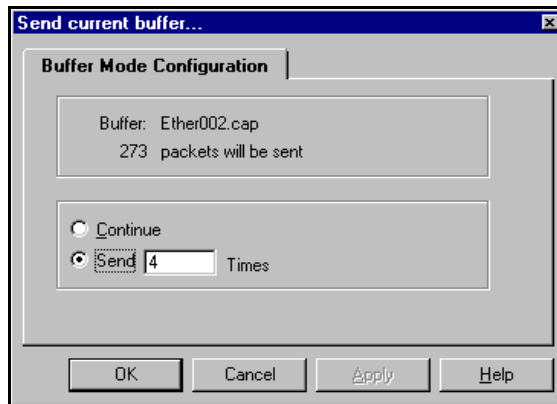
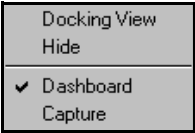


Figure 5-6. The Send Current Buffer Dialog Box

You can either send the entire buffer a specific number of times or continuously. The time delay between each packet send is calculated from the original delay time stored in the captured buffer. Again the delay time may not be reproduced exactly because Windows 95 system timer's smallest resolution is one millisecond, and the delay time may vary depending on the type of applications running concurrently with NetXRay.

Context Menu

The Packet Generator context menu gives you access to additional functions and short cut commands.



Docking View	Click to toggle between docking view and normal window. If Docking View is checked, the Packet Generator will stay on top all the time.
Hide	Close the Packet Generator.
Dashboard	Launch or hide the Dashboard window depending on whether the Dashboard is previously activated or not. If a check mark is shown, clicking this command will hide the Dashboard window.
Capture	Launch or hide the Capture window depending on whether the Capture is previously activated or not. If a check mark is shown, clicking this command will hide the Capture window.

Network Monitor

NetXRay provides tools for you to monitor real time statistical performance and long-term trend analysis of your network. You can collect the following information:


- Real time statistics
- Both short- and long-term history trends
- Host (station) statistics
- Station conversation statistics (Matrix)
- Protocol distribution

In addition, the network statistics collected in NetXRay includes network and application-layer statistics commonly found in IP and IPX networks. They are summarized below:

- IP and IPX-layer matrices are supported. The views are now provided in traffic map, outline table, detail table, bar chart, or pie chart format.
- Matrix traffic map provides a birds-eye view of the real time network conversation traffic load.
- IP and IPX-layer hosts are supported. The views are now provided in outline table, detail table, bar chart, or pie chart format.
- IPX protocol distribution has been added.
- Segment statistics packet size distribution can now be viewed in bar and pie chart formats.
- A new network bandwidth utilization distribution chart is added in either bar or pie format.

Since Ethernet and Token Ring are collecting different physical-layer information, the statistical variables displayed will be listed in a separate table for each media type.

Segment Statistics

NetXRay collects the network segment's statistics immediately upon starting up. To view the network statistics in real time, go to the **Tools** menu and select **Dashboard**, or click the  icon on the Tool bar. A Dashboard window is displayed (see [Figure 6–1](#)).

The Dashboard Window displays the network performance in real time. It includes:

- The Number of Packets per Second
- The Percent Utilization rate
- The Number of Errors per Second

The Dashboard numeric window shows a pair of numbers; the left is the real time value, and the right is the highest value recorded since the past reset.

The red zone defines the area of the network activity which exceeds the high threshold you set. To set high thresholds for these three variables, see [Reassigning Severity Level to Alarms on page 7–16](#).

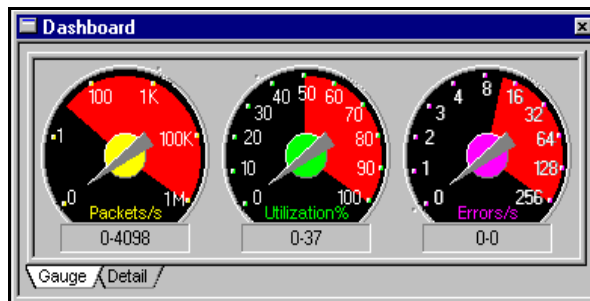


Figure 6–1. The Dashboard Window

To view the Ethernet Network detail total summary, click the **Detail** tab. The Detail Tab display appears ([Figure 6–2](#)).

Network:		Detail errors:		Size distribution:	
Packets	129182	CRCs	0	64s	27583
Dropped	7	Runt	0	65-127s	24320
Broadcasts	1549	Oversize	0	128-255s	6531
Multicasts	1710	Fragment	120	256-511s	1660
Bytes	102552719	Jabber	0	512-1023s	10249
Utilization	0	Alignment	43	1024-1518s	58839
Errors	163	Collision	2056		

Figure 6–2. The Dashboard—Detail Tab Display

The Ethernet Network statistics details are displayed in three groups: Network, Error, and Size Distribution.

The Ethernet Global Statistics Network field definitions are shown in [Table 6–1](#).

Table 6–1. Ethernet Global Statistics Network Field Definitions

Field	Description
# Packets	Total # of all packets seen
# Dropped	Total # of packets dropped
# Broadcasts	Total # of broadcast packets seen
# Multicasts	Total # of multicast packets seen
# Bytes	Total # of octets seen
# Utilization	Current % network utilization

Errors

The Ethernet global statistics error field definitions are shown in [Table 6–2](#).

Table 6–2. Ethernet Global Statistics Error Field Definitions

Field	Description
# Packets	Total # of error packets.
# CRCs	Total # of CRC error packets. The packet size is legal, but contains a bad (frame check sequence) FCS.
# Runt	Total # of undersize packets (packets less than 64 bytes in length).
# Oversize	Total # of oversize packets (packets greater than 1518 bytes in length).
# Fragment	Total # of fragment packets. Fragment packets are undersized and contains bad FCS.
# Jabber	Total # of jabber packets. Jabber packets are oversized and contains bad FCS.
# Alignment	Total # of alignment packets. Alignment packets do not end on an 8-bit boundary.
# of Collision	Total # of collision packets

Packet Size Distribution

The Ethernet global statistics packet size distribution field definitions are shown in [Table 6–3](#).

Table 6–3. Ethernet Global Statistics Packet Size Distribution Field Definitions (1 of 2)

Field	Description
# 64s	Total # of packets in 64-byte size
# 65-127s	Total # of packets in size from 65 to 127 bytes
# 128-255s	Total # of packets in size from 128 to 255 bytes

Table 6–3. Ethernet Global Statistics Packet Size Distribution Field Definitions (2 of 2)

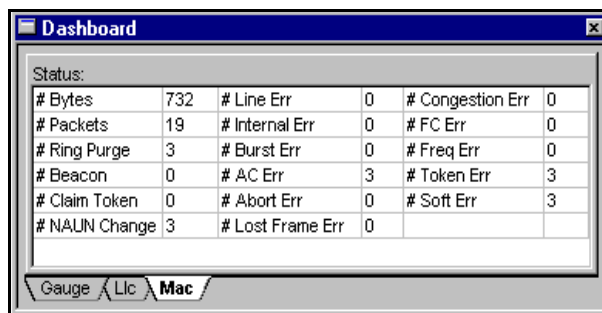
Field	Description
# 256-511s	Total # of packets in size from 256 to 511 bytes
# 512-1023s	Total # of packets in size from 512 to 1023 bytes
# 1024-1518s	Total # of packets in size from 1024 to 1518 bytes

NOTE: The packet size defined here includes four bytes of CRC. However, CRC is not displayed in the Packet Viewer window.

If the numbers displayed are truncated, you can place the mouse on the vertical divider between the item description and the numbers, then click and drag the divider line to the left to make room for the numbers.

Most of the NIC card manufacturers do not support counting of Ethernet errors. Network General supplies an NE2000-compatible NDIS driver which will count and report Ethernet errors listed above. Contact Network General, or visit www.ngc.com for the latest list of NIC cards supported.

To view the Token Ring Network detail total summary, click the **Llc** or **Mac** tab. The Mac tab display is shown in [Figure 6–3](#).



Status:					
# Bytes	732	# Line Err	0	# Congestion Err	0
# Packets	19	# Internal Err	0	# FC Err	0
# Ring Purge	3	# Burst Err	0	# Freq Err	0
# Beacon	0	# AC Err	3	# Token Err	3
# Claim Token	0	# Abort Err	0	# Soft Err	3
# NAUN Change	3	# Lost Frame Err	0		

Figure 6–3. The Dashboard—Mac Tab Display

The Token Ring Network statistics details are displayed in two groups: LLC and MAC.

LLC

Token Ring global statistics LLC field definitions are shown in [Table 6-4](#).

Table 6-4. Token Ring Global Statistics LLC Field Definitions

Field	Description
# Packets	Total # of all packets seen (including MAC layer)
# Dropped	Total # of packets dropped
# Broadcasts	Total # of broadcast packets seen
# Multicasts	Total # of multicast packets seen
# Bytes	Total # of octets seen
# Utilization	Current % network utilization
# Error	Total # of errors seen
# 18-63s	Total # of packets in size from 18 to 64 bytes
# 64-127s	Total # of packets in size from 65 to 127 bytes
# 128-255s	Total # of packets in size from 128 to 255 bytes
# 256-511s	Total # of packets in size from 256 to 511 bytes
# 512-1023s	Total # of packets in size from 512 to 1023 bytes
# 1024-2047s	Total # of packets in size from 1024 to 2047 bytes
# 2048-4095s	Total # of packets in size from 2048 to 4095 bytes
# 4096-8191s	Total # of packets in size from 4096 to 8191 bytes
# 8192-18000s	Total # of packets in size from 8192 to 18000 bytes
# > 18000s	Total # of packets in size greater than 18000 bytes

Mac

The Token Ring global statistics MAC error definitions are shown in [Table 6-5](#).

Table 6-5. Token Ring Global Statistics MAC Error Definitions (1 of 3)

Field	Description
# Bytes	Total # of MAC octets seen.
# Packets	Total # of MAC packets seen.
# Ring Purge	Total # of ring purge MAC packets detected.
# Beacon	Total # of beacon MAC packets detected. Beacon packets are generated when a network station detects faulty cable or hardware.
# Claim Token	Total # of claim token MAC packets detected.
# NAUN Change	Total # of NAUN changes detected.
# Line Err	Total # of line errors detected in error reporting packets. This error occurs when an FCS or Manchester code violation is detected by an adapter as it repeats or copies a packet.
# Internal Err	Total # of internal errors detected in error reporting packets. These errors occur when a network adapter card experiences a hardware problem but is able to remain on the network.
# Burst Err	Total # of burst errors detected in error reporting packets. Burst error is caused by a brief disconnection in the cable, or a station entering or exiting the ring as its lobe attaches or removes itself from the ring. It will cause the active monitor function to execute its ring purge function.

Table 6–5. Token Ring Global Statistics MAC Error Definitions (2 of 3)

Field	Description
# AC Err	Total # of AC errors detected in error reporting packets. The AC error is incremented when an adapter receives more than one AMP or SMP MAC packet with ARI/FCI equal to zero, without first receiving an intervening AMP AMC packet. This error counter indicates that the upstream adapter is unable to set its ARI/FCI bits in the packet that it has copied.
# Abort Err	Total # of abort errors detected in error reporting packets. This error occurs during packet transmission when a board is forced to abort the transmission by sending a special abort delimiter sequence.
# Lost Frame Err	Total # of lost frame errors detected in error reporting packets. This error occurs when an adapter is in transmit (stripping) mode and fails to receive the end of the frame it transmitted.
# Congestion Err	Total # of congestion errors detected in error reporting packets. This error occurs when an adapter recognizes a packet addressed to its specific address, but has no buffer space available to copy the packet.
# FC Err	Total # of FC errors detected in error reporting packets. This error occurs when an adapter recognizes a packet addressed to its specific address, but finds the ARI bits not equal to 00. It may be caused by a line hit or duplicate address.
# Freq Err	Total # of frequency errors detected in error reporting packets. It is a condition in which the ring clock and the crystal clock frequency of the adapter differ by more than 0.6%.

Table 6–5. Token Ring Global Statistics MAC Error Definitions (3 of 3)

Field	Description
# Token Err	Total # of token errors detected in error reporting packets. This error occurs when the Active Monitor function detects an error with the token protocol.
# Soft Err	Total # of soft errors detected in error reporting packets. A soft error is an error condition that temporarily degrades system performance; however, the ring recovers by using the protocols of the adapter.

Dashboard Context Menu

The Dashboard context menu gives you access to additional functions and short-cut commands. [Table 6–6](#) describes the Dashboard Context menu items.



Table 6–6. Context Menu Item Descriptions (1 of 2)

Menu	Description
Docking View	Click to toggle between docking view and normal view. If Docking View is checked, the Dashboard will stay on top all the time.
Hide	Close the Dashboard.
Reset	Clear the statistical counters in the Dashboard.
Show Total	Click to show cumulated statistics total value.
Show Average	Click to show current average statistics value per second.

Table 6–6. Context Menu Item Descriptions (2 of 2)

Set Threshold...	Invoke the Option dialog page for setting Threshold.
Capture	Launch or hide the Capture window depending on whether the Capture is previously activated or not. If a check symbol is shown, clicking this command will hide the Capture window.
Packet Generator	Launch or hide the Packet Generator window depending on whether the Packet Generator is previously activated or not. If a check symbol is shown, clicking this command will hide the Packet Generator window.

Network Utilization and Packet Size Distribution

NetXRay displays in both bar and pie charts for network utilization distribution (see [Figure 6–4](#)) and for packet size distribution (see [Figure 6–5](#)). These new statistics enable the network manager to better understand the overall activity levels in the network and to pin-point large and small size packet traffic loads, each of which can have a different effect on overall network performance and availability.

Network utilization distribution shows network bandwidth consumption distributed among each 10% grouping, that is, 0-10%, 11%-20%, ..., 91%-100%. To display the utilization distribution screen, select **Tools/Global Statistics**, and click the Utilization Dist. tab.

The red dotted line shown in the graph is the average network utilization rate since the start of the monitor.

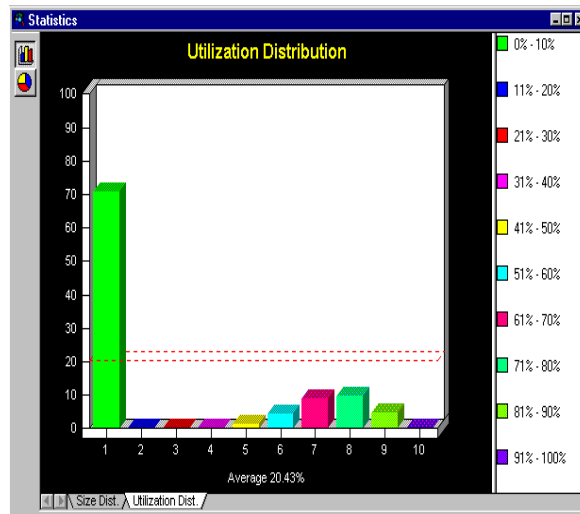


Figure 6-4. Bar Chart of Network Utilization Distribution

To display the packet size distribution screen (see [Figure 6-5](#)), click the Size Dist. tab.

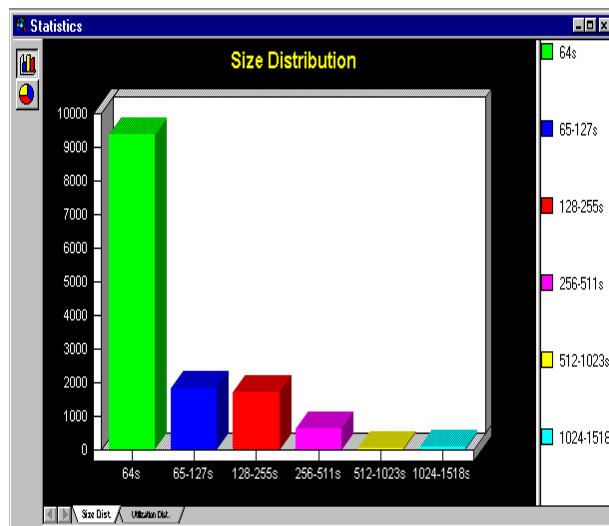


Figure 6-5. Bar Chart of Packet Size Distribution


History Statistics

History Statistics records network activities over a period of time. You can use the recorded data to establish the network performance base-line so that thresholds can be set to trigger alarms when above normal network activities occur. The history statistics are also useful for determining the network loading over the long term so that future network expansion can be planned.

NetXRay supports the monitoring of up to ten network activities concurrently. Multiple history statistics can be started for the same network variable so that both short-term and long-term trends can be recorded simultaneously.

Before you launch the history statistics gathering, you may want to adjust the settings first.

To change the history statistics setting:

1. Go to the **Tools** menu and select **History**, or click the  icon on the Tool bar. A History sample window ([Figure 6-6](#)) is displayed.

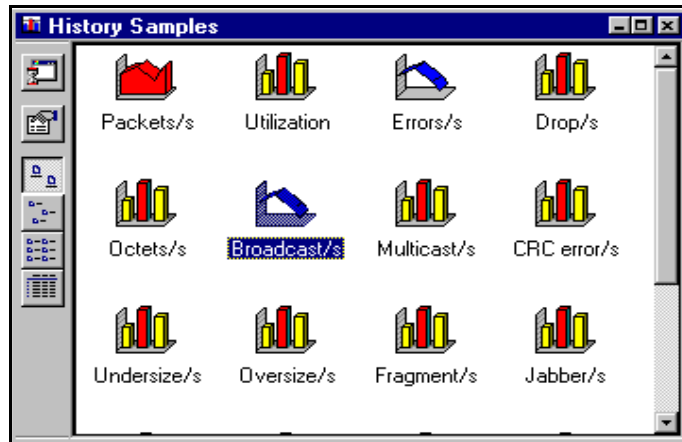


Figure 6-6. A History Samples Window

2. Click a network variable icon of your choice to be monitored from the History folder.
3. Click the right mouse button to invoke the start sample menu ([Figure 6-7](#)).

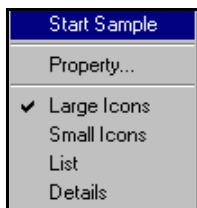


Figure 6–7. The Start Sample Menu

4. Select **Property....** A History dialog box is displayed (Figure 6–8).

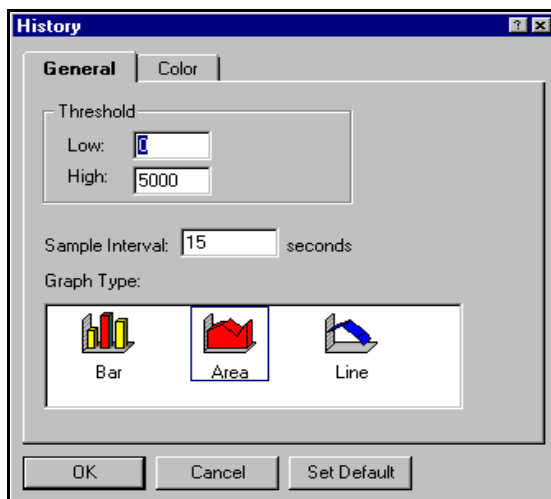


Figure 6–8. The General Page in the History Dialog Box

5. Enter the high and low threshold levels, and the sampling interval.
6. Select the initial graph type for the history sample.
7. Optionally, click the **Color** tab to view the color selection for the History graph.
8. Choose color for Above Normal (threshold), Normal, Foreground, and Background colors.
9. Click **OK** to complete the history setting.

The History dialog box parameters are listed in [Table 6–7](#).

Table 6–7. History Dialog Box Parameters

Parameters	Description
High Threshold	Enter a high threshold level for the sampled data. Any sampled data value which exceeds the high threshold level will be displayed in the above normal color in the history statistics bar graph.
Low Threshold	Enter a low threshold level for the sampled data.
Sampling Interval	Enter the sampling interval in # of seconds. The maximum sample interval is 3,600 seconds (1 hour).
Set Default	Reset the threshold, and the sampling interval back to default values defined by NetXRay.
OK	Accept the history setting changes.
Cancel	Cancel history setting changes.

Since NetXRay collects a maximum of 3,600 samples, by changing the sample interval you can adjust the total amount of time over which the History data are sampled.


When baselining a network segment, you are generally more interested in obtaining an overview of network performance over a longer period of time than specific per-second details. If you were to chart a 1-second sample over an 8-hour day, you would have 28,800 data points. The resulting graph would be unreadable, and analysis would be very difficult.

A more practical sample interval of 1-minute would yield only 480 samples in an 8-hour day, or 1,440 data points over a 24-hour period. The smaller samples make reviewing the history trend over a day more manageable.

[Table 6–8](#) lists the relationship between the sample interval and the recommended sample period.

Table 6–8. Sample Interval and Sample Period Relationship

Sample Interval	Recommended Sample Period	Maximum Sample Period
1 second	up to 1 hour	1 hour
10 seconds	30 minutes to 8 hours	10 hours
20 seconds	1 hour to 16 hours	20 hours
30 seconds	2 hours to 24 hours	30 hours
1 minute	4 hours to 2 days	2 days, 12 hours
3 minute	12 hours to 6 days	7 days, 12 hours
10 minute	2 days to 20 days	25 days
30 minute	5 days to 2 months	2 months, 15 days
1 hour	1 week to 4 months	5 months

To start history statistical sampling, double-click the statistical icon of your choice. A history window is displayed showing the on-going sampling of the network data. When a total of 3,600 samples are recorded, the statistics monitoring stops automatically. You can also stop the monitor by closing the History window. The slider allows you to adjust the vertical scale of the graph chart. If you want to view the history graph without being interrupted by the periodic updating of the new data points, click the Pause  button on the side of the History window to stop the graph from moving. To see other data points, use the horizontal scroll bar to move the history graph back and forth in time.

Clicking on a sample in the History graph will pop up a small window to show the sample's data value and the time stamp ([Figure 6–9](#)).

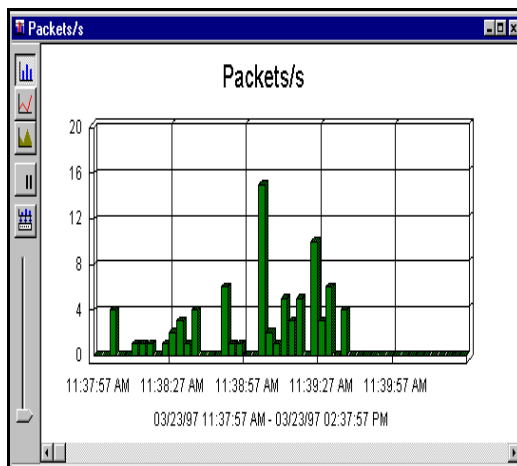





Figure 6–9. Sample History Graph

When you close the History monitoring window, you will be given an option to save the recorded sampling data to a file. The default history file extension is .HST.

NOTE: When the history is viewed in Bar chart mode, the sampled data will be displayed in Above Normal color if it exceeds the set history threshold.

Customizing the History Statistics View

The History Statistics graph can be viewed in three different graph modes: bar, line, and area. There are three buttons on the side of the graph chart for you to select the appropriate graph mode. They are:

	Bar chart
	Line chart
	Area chart

Viewing Saved History Statistics Data

To view saved history statistics:

1. Go to the **File** menu and select **Open....**
2. From the Open dialog box, select a saved history statistics file and click **OK**.

Exporting History Data

NetXRay lets you save history data in comma-separated value (CSV) file format. The CSV file gives you the ability to import the history data into other applications such as database or spreadsheet.

To export data to a file:

1. Click the right mouse button to invoke the context menu.
2. Select **Export**. A Save As dialog box is displayed.
3. Enter the filename, and click **Save**.

Exporting History Data Directly to Excel

NetXRay comes with a built-in Visual Basic interpreter. One of the Basic scripts supplied by NetXRay lets you save history data onto an Excel spreadsheet directly.

To export sample data to Excel:

1. Select the History data you want to export by clicking anywhere inside the window.
2. Select **Run Script...** from the **File** menu.
3. Select **hi2excel.bas** from the dialog box, then click **Open**.
4. Excel program will be spawned with a new spreadsheet showing the History sample data being imported one by one. When the importing is complete, a small dialog box that says **Done** appears. Click **OK**.

Printing a History Statistics Snapshot

To print a snapshot of the history statistics graph shown in the window:

1. Go to the **File** menu and select **Print....**
2. Click **OK**.

WARNING: hi2excel.bas contains Basic script used by NetXRay to perform the exporting function. *Do not* attempt to make any modifications to it or unpredictable results may occur.

WARNING: You must have at least one History graph running to perform data exporting to Excel.

Host Statistics

The host statistics provide a quick analysis of the traffic statistics collected for each host node in real time. You can view host traffic

at the MAC layer, or selectively view only network-layer traffic in the IP or IPX layers.

The Host statistics table is extremely useful for transferring hardware address into the address filter and address book. If you do not have an inventory of all the network hosts and nodes in your network, the hardware (MAC) address shown in the host statistics table may not reveal the true identity of the network node. See [Chapter 8, Address Data Base](#) about locating and adding symbolic node names to network nodes.

The host table has four different views: outline table, detail table, bar chart, or pie chart. [Table 6–9](#) shows the information displayed for each type of view.

Table 6–9. Display of the Four Different Views of the Host Table (1 of 2)





Type of View	OSI Layer	Information Displayed
Outline table 	MAC	Total bytes and packets transmitted in, out, plus additional breakdown into broadcast and error packets for each host node in MAC-layer are listed.
	IP	Total bytes and packets transmitted in, out, plus additional breakdown into broadcast packets for each host node in IP-layer are listed.
	IPX	Total bytes and packets transmitted in, out, plus additional breakdown into broadcast packets for each host node in IPX-layer are listed.
Detail table 	MAC, IP, IPX	Same as Outline table, except the entries are grouped by protocol types.

Table 6–9. Display of the Four Different Views of the Host Table (2 of 2)

Type of View	OSI Layer	Information Displayed
Bar chart 	MAC, IP, IPX	Top 10 talkers based on the selected statistics recorded for each respective protocol layer: MAC, IP, or IPX.
Pie chart 	MAC, IP, IPX	Top 10 talkers based on percentage of the selected statistics load recorded for each respective protocol layer: MAC, IP, or IPX.

In addition to the view buttons, there are seven more buttons to help you operate each view more efficiently. They are defined in [Table 6–10](#).

Table 6–10. Seven Additional Help Buttons for the Host Table (1 of 2)









Button	Usage
	Capture. Activated in outline table view only, and at least one node address is selected. Use it to launch the packet capture.
	Create filter. Activated in outline table view only, and at least one node address is selected. Use it to launch the filter setting dialog box.
	Pause. Activated all the time. Use it to suspend the real time update of the host display temporarily.

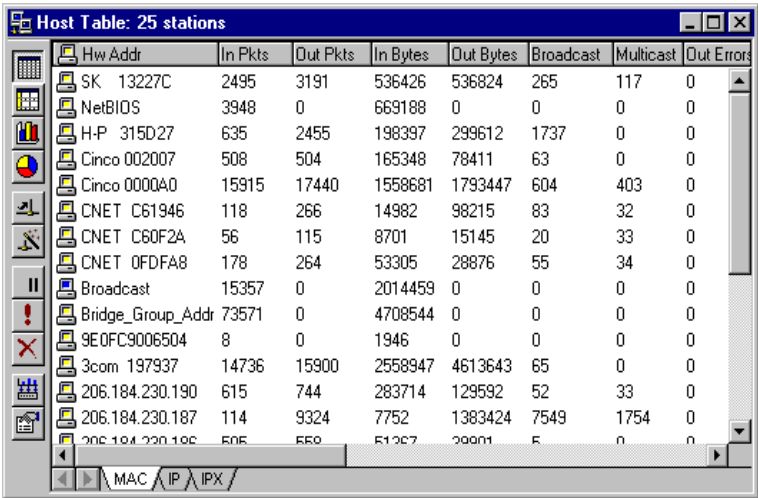
Table 6–10. Seven Additional Help Buttons for the Host Table (2 of 2)

Button	Usage
	Refresh. Activated all the time. Use it to obtain a real time update of the host display immediately.
	Reset. Activated all the time. Use it to clear the host statistical counter immediately.
	Export. Activated when in outline or detail table view. Use it to export the table contents to a CSV file.
	Properties. Activated all the time. Use it to toggle address mode, change display update rate, or change Top-N display criteria.

Outline Table View

The outline table view provides a quick summary of total bytes and packets transmitted in and out of each network node in real time. By selecting the MAC, IP, or IPX-layer, you can view the traffic summary in each network layer instantaneously.

To bring up Host Table and start collecting statistics, go to the Tools menu and select **Host Table**, or click the  icon on the Tool bar. In Ethernet LAN, an outline view is displayed in the format shown in [Figure 6–10](#).



Hw Addr	In Pkts	Out Pkts	In Bytes	Out Bytes	Broadcast	Multicast	Out Errors
SK 13227C	2495	3191	536426	536824	265	117	0
NetBIOS	3948	0	669188	0	0	0	0
H-P 315D27	635	2455	198397	299612	1737	0	0
Cinco 002007	508	504	165348	78411	63	0	0
Cinco 0000A0	15915	17440	1558681	1793447	604	403	0
CNET C61946	118	266	14982	98215	83	32	0
CNET C60F2A	56	115	8701	15145	20	33	0
CNET 0FDFA8	178	264	53305	28876	55	34	0
Broadcast	15357	0	2014459	0	0	0	0
Bridge_Group_Addr	73571	0	4708544	0	0	0	0
9E0FC9006504	8	0	1946	0	0	0	0
3com 197937	14736	15900	2558947	4613643	65	0	0
206.184.230.190	615	744	283714	129592	52	33	0
206.184.230.187	114	9324	7752	1383424	7549	1754	0
206.184.230.186	505	559	51267	39901	5	0	0

Figure 6–10. A Host Table in Ethernet LAN

Ethernet Host Table

The fields in the Ethernet host table are listed in [Table 6–11](#).

Table 6–11. Ethernet Host Table Field Definitions (1 of 2)

Field	Description
HW Addr	Station's symbolic name or Hex address
In Pkts	Total # of packets received by the station
Out Pkts	Total # of packets transmitted by the station
In Octets	Total # of octets received by the station
Out Octets	Total # of octets transmitted by the station
Out Errors	Total # of all errors generated by the station
Broadcast	Total # of broadcast packets transmitted by the station
Multicast	Total # of multicast packets transmitted by the station
CRC	Total # of CRC errors transmitted by the station
Jabber	Total # of oversize packets with CRC errors transmitted by the station

Table 6–11. Ethernet Host Table Field Definitions (2 of 2)

Field	Description
Runt	Total # of undersize (less than 64 bytes) packet errors transmitted by the station
Fragment	Total # of undersize packets with CRC errors transmitted by the station
Oversize	Total # of oversize (greater than 1518 bytes) packet errors transmitted by the station
Alignment	Total # of alignment errors transmitted by the station
Update Time	The last time the station has any incoming or outgoing traffic
Create Time	The time station is created in the table

Token Ring Host Table

In a Token Ring LAN, a host table view is displayed in the format shown in [Figure 6–11](#).

Hw Addr	Order	Broadcast	Multicast	In Pkts	Out Pkts	In Bytes	Out Bytes
NwkGnID0215F	Active Mon.	0	34	0	34	0	1276
This station	2	0	33	0	33	0	1317
0001DDBAF481	Inactive	0	0	2	2	518	157
Intel 70313C	Inactive	0	0	2	2	157	518
400003026882	Inactive	0	0	10	10	1092	1679
400007028276	Inactive	0	0	10	10	1679	1092
LAN Manager	Group	0	0	7	0	433	0
TR_Broadcast	Group	0	0	60	0	2160	0

Figure 6–11. A Host Table in Token Ring LAN

The fields in Token Ring host table are listed in [Table 6–12](#).

Table 6–12. Token Ring Host Table Field Definitions (1 of 2)

Field	Description
HW Addr	Station's symbolic name or Hex address
Order	Stations' polling order in this ring with respect to the Active Monitor (AM). Stations labeled as Group are broadcast or functional addresses. Stations labeled as Inactive are either local stations removed from the ring or non-local stations.
Broadcast	Total # of broadcast packets transmitted by the station.
Multicast	Total # of multicast packets transmitted by the station.
In Pkts	Total # of packets received by the station.
Out Pkts	Total # of packets transmitted by the station.
In Octets	Total # of octets received by the station.
Out Octets	Total # of octets transmitted by the station.
Out Errors	Total # of all errors generated by the station.
Line Errors	Total # of line errors generated by the station.
Burst Errors	Total # of burst errors generated by the station.
A/C Errors	Total # of A/C errors generated by the station.
Internal Errors	Total # of internal errors generated by the station.
Abort Errors	Total # of abort errors generated by the station.
Congestion Errors	Total # of congestion errors generated by the station.
Lost Frame Errors	Total # of lost frame errors generated by the station.

Table 6–12. Token Ring Host Table Field Definitions (2 of 2)

Field	Description
F/C Errors	Total # of F/C errors generated by the station.
Frequency Errors	Total # of frequency errors generated by the station.
Token Errors	Total # of token errors generated by the station.
Beacon Errors	Total # of beacon packets generated by the station.
Update Time	The last time the station has any incoming or outgoing traffic.
Create Time	The time the station was created in the table.

The detailed definitions of all Token Ring errors are listed in [Segment Statistics on page 6–2](#).

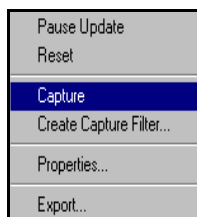
Sorting the Host Table

A sorted Host Table view gives you the ability to find stations that are the most or the least active in a specific category of network statistics.

Clicking a column heading selects that variable as the sort key, and will cause the sorting of the host table entries in descending order. Holding the Control key down and clicking a column heading will sort the table in ascending order.

Context Menu

To access additional commands, press the right mouse button on the Host Table view to bring up the context menu shown below.




[Table 6–13](#) shows the context menu options.

Table 6–13. Context Menu Options

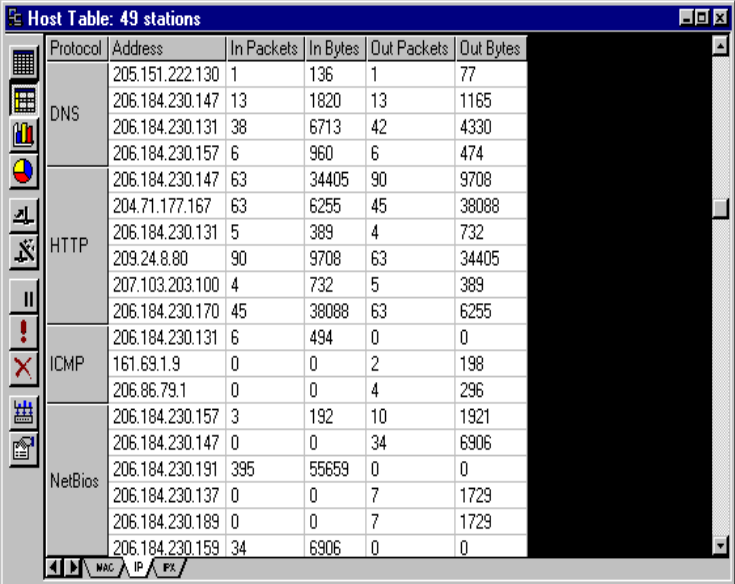
Menu Items	Description
Pause Update	Suspend the host table counter update temporarily.
Reset	Clear all statistics counters in the host table.
Capture	Hot link to launch a capture session with the selected hardware address to and from any as the filter criterion.
Create Capture Filter...	Hot link to launch a capture filter setting dialog box with the selected hardware address to and from any as the filter criterion.
Properties....	Launch a Host table property dialog box. Check Show Hardware Address to display hex hardware address format, otherwise a symbolic name is displayed as defined in the Address Book.
Export...	Save the Host Table data to a CSV format file.

Detail Table View

The detail table shows a different summary view from the outline table. You can group the entries by the protocol type or by the node address. To group entries by protocol, click  and click the Protocol column header.

You can see the traffic loads segregated by protocol types.


[Figure 6–12](#) shows an IP host detail table view.



Protocol	Address	In Packets	In Bytes	Out Packets	Out Bytes
DNS	205.151.222.130	1	136	1	77
	206.184.230.147	13	1820	13	1165
	206.184.230.131	38	6713	42	4330
	206.184.230.157	6	960	6	474
HTTP	206.184.230.147	63	34405	90	9708
	204.71.177.167	63	6255	45	38088
	206.184.230.131	5	389	4	732
	209.24.8.80	90	9708	63	34405
	207.103.203.100	4	732	5	389
	206.184.230.170	45	38088	63	6255
ICMP	206.184.230.131	6	494	0	0
	161.69.1.9	0	0	2	198
	206.86.79.1	0	0	4	296
NetBios	206.184.230.157	3	192	10	1921
	206.184.230.147	0	0	34	6906
	206.184.230.191	395	55659	0	0
	206.184.230.137	0	0	7	1729
	206.184.230.189	0	0	7	1729
	206.184.230.159	34	6906	0	0

Figure 6–12. Display of the IP Host Detail Table

Bar Chart View

The bar chart reveals the top-N busiest host nodes in real time (see [Figure 6–13](#)). You can view top-N host traffic in MAC, IP, or IPX-layer traffic. For example, to view top-N MAC-layer traffic, click  then select the MAC tab in the window.

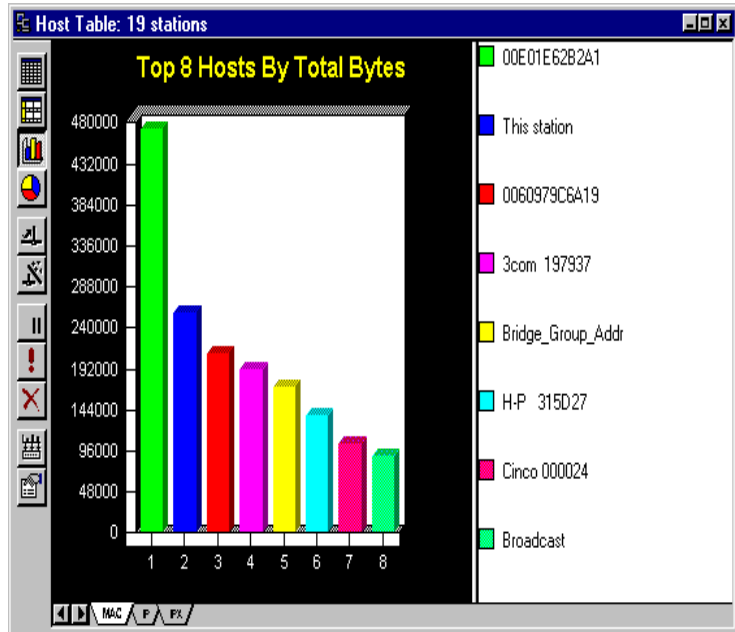


Figure 6–13. Bar Chart View of Top-N Host Nodes in Real Time

By default, the Top-N display is sorted by total bytes in traffic load counted and displayed with the top 10 nodes.

To change this setting, click  to invoke the Host Table.

Properties dialog box, and select the TopN Chart page (see [Figure 6–14](#)).

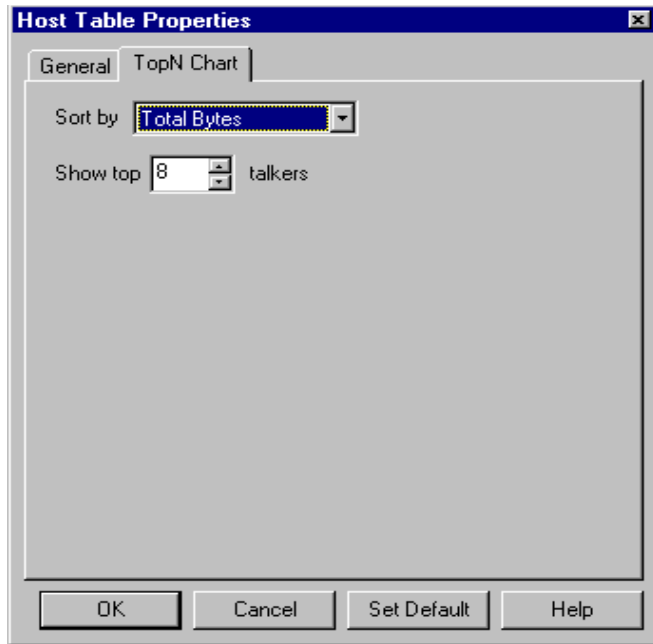



Figure 6–14. Host Table Properties Dialog Box, Top-N Chart Selected

You can change the sorting criteria to sort by **In packets**, **In bytes**, **Out packets**, **Out bytes**, **Total packets**, or **Total bytes**. In addition, you can change the top-N node displayed.

Pie Chart View

The pie chart reveals the top-N busiest host nodes in their relative percentage load of the total top-N traffic (see [Figure 6–15](#)). To view the top-N pie chart, click  .

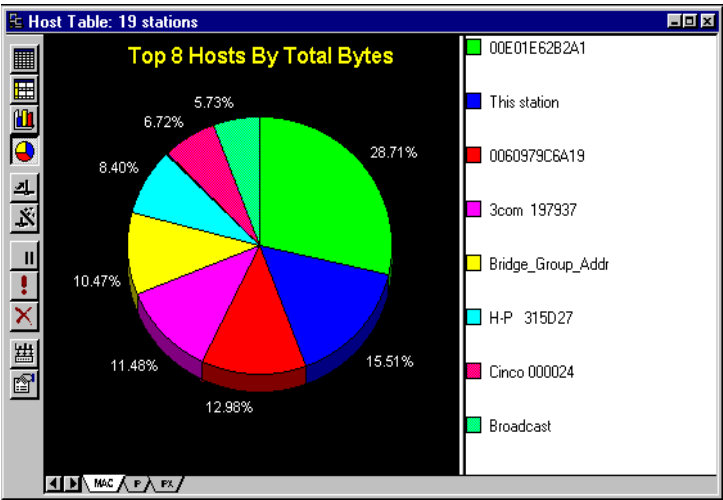


Figure 6–15. Pie Chart View of Top-N Host Nodes in Relative Percentage (%) Load

Matrix Statistics

The matrix statistics provide a quick analysis of the conversation traffic statistics collected in real time. You can view conversation traffic at the MAC layer, or selectively view only network traffic in the IP or IPX layers.

The matrix statistics have five different views: traffic map, outline table, detail table, bar chart, or pie chart. [Table 6–14](#) shows the information displayed in each type of view.

Table 6–14. Display of Five Views of the Matrix Statistics (1 of 3)


Type of View	OSI Layer	Information Displayed
Traffic map 	MAC	Graphical presentation of conversation relationship between MAC-layer nodes and their network load. The thickness of the connecting line represents the relative traffic load in total number of bytes transmitted.

Table 6–14. Display of Five Views of the Matrix Statistics (2 of 3)





Type of View	OSI Layer	Information Displayed
	IP	Graphical presentation of conversation relationship between IP-layer nodes and their network load. The thickness of the connecting line represents the relative traffic load in total number of bytes transmitted.
	IPX	Graphical presentation of conversation relationship between IP-layer nodes and their network load. The thickness of the connecting line represents the relative traffic load in total number of bytes transmitted.
Outline table 	MAC	Total bytes and packets transmitted in each direction between pairs of MAC-layer nodes.
	IP	Total bytes and packets transmitted in each direction between pairs of IP-layer nodes.
	IPX	Total bytes and packets transmitted in each direction between pairs of IP-layer nodes.
Detail table 	MAC, IP, IPX	Same as Outline table, except the entries are grouped by protocol types.

Table 6–14. Display of Five Views of the Matrix Statistics (3 of 3)

Type of View	OSI Layer	Information Displayed
Bar chart 	MAC, IP, IPX	Top-N conversation pairs based on the total number of bytes recorded for each respective protocol layer; MAC, IP, or IPX.
Pie chart 	MAC, IP, IPX	Top-N conversation pairs based on % of load recorded for each respective protocol layer: MAC, IP, or IPX.

In addition to the view buttons, there are seven more buttons to help you operate each view more efficiently. They are defined in [Table 6–15](#).

Table 6–15. Seven Additional Help Buttons for the Matrix Statistics (1 of 2)








Button	Usage
	Capture. Activated when in traffic map or outline table view, and at least one node address is selected. Use it to launch packet capture.
	Create filter. Activated when in traffic map or outline table view, and at least one node address is selected. Use it to launch filter setting dialog box.
	Pause. Activated all the time. Use it to suspend the real time update of the matrix display temporarily.

Table 6–15. Seven Additional Help Buttons for the Matrix Statistics (2 of 2)


Button	Usage
	Refresh. Activated all the time. Use it to update the real time update of the matrix display immediately.
	Reset. Activated all the time. Use it to clear the matrix statistical counter immediately.
	Export. Activated when in outline or detail table view. Use it to export the table contents to a CSV file.
	Properties. Activated all the time. Use it to toggle address mode, change display update rate, configure display color, or change Top-N display criteria.

Traffic Map View

The traffic map provides you with a birds-eye view of the network traffic patterns in real time. It gives a complete graphical presentation of the traffic pattern between network nodes.

In addition, you can filter out unwanted traffic by selecting network nodes of interest.

Figure 6–16 shows how you can display the complete traffic map, then isolate traffic transmitted to and from several network nodes.

To show the traffic map, simply click the traffic map button  on the left side of the matrix window.

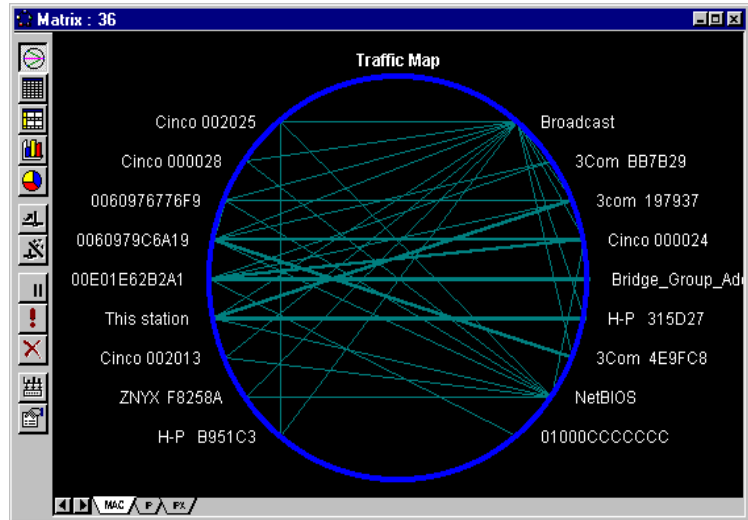


Figure 6-16. Display of the Complete Traffic Map

If you are interested in viewing real time traffic conversation only related to IP or IPX networks, select the appropriate tab in the matrix window. An example of the IP conversation traffic map is shown in [Figure 6-17](#).

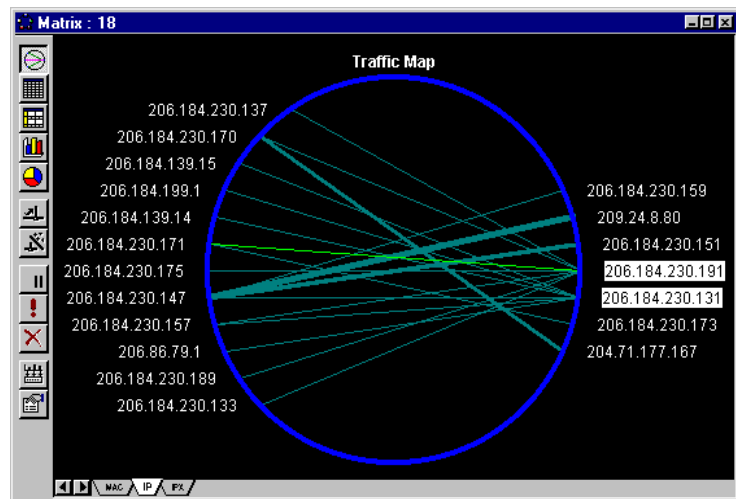


Figure 6-17. Display of the IP Conversation Traffic Map

To view conversation traffic between certain nodes, click and highlight the network node on the traffic map as shown in [Figure 6-17](#). To select more than one node, hold the **Control** key

down, then click additional nodes. Click the right mouse button to invoke the matrix context menu, and select the **Show Select Node** command. The matrix traffic map in [Figure 6-18](#) shows only those selected nodes, and their conversation peer nodes.

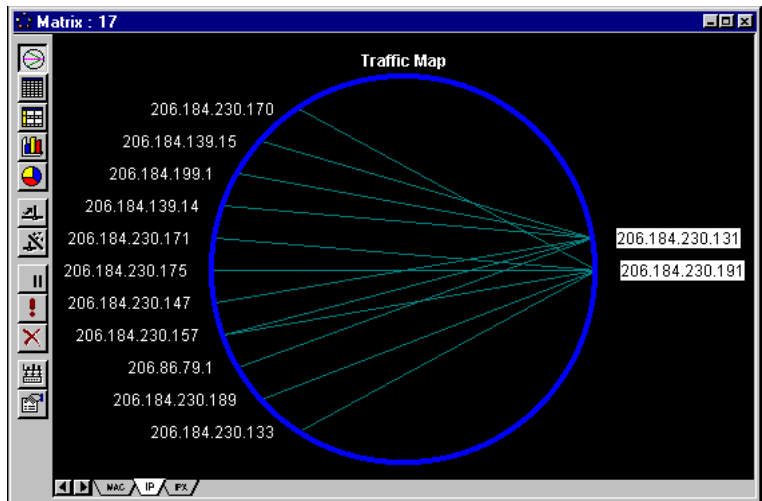


Figure 6-18. Display of Matrix Traffic Map Showing the Selected Nodes

To access additional commands, press right mouse button to invoke the context menu. The commands are listed in [Table 6-16](#).


Table 6-16. The Context Menu Commands (1 of 2)

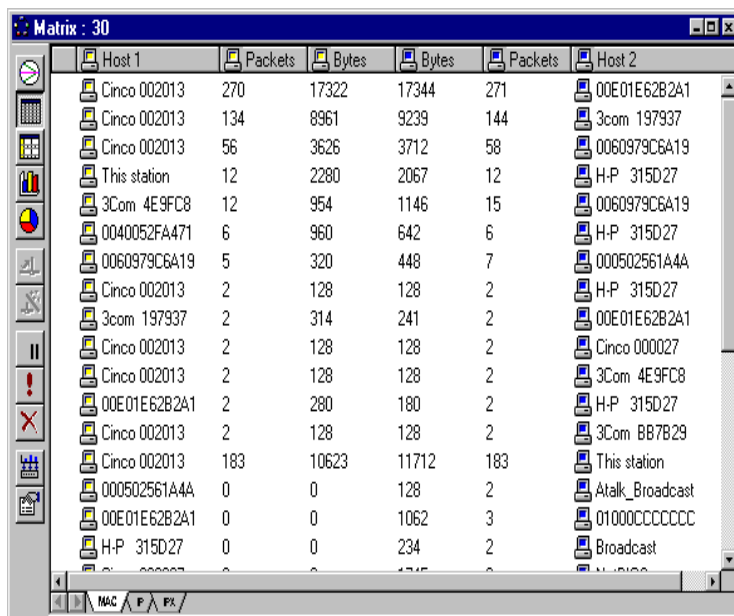
Menu	Function
Show all	Show all network nodes
Show Selected Nodes	Show only selected nodes and their conversation peers.
Hide Selected Nodes	Hide only selected nodes and their conversation peers.
Zoom	Enlarge the traffic map
Reset	Clear the traffic map
Refresh	Update the traffic map immediately
Pause Update	Freeze the traffic map update
Capture	Launch packet capture with selected network address(es) set as address filter

Table 6–16. The Context Menu Commands (2 of 2)

Menu	Function
Create Capture Filter...	Launch capture filter setting dialog box with selected network address(es) set as the address filter(s)
Properties	Launch the matrix configuration dialog box

Outline Table View

The outline table view provides a quick summary of total bytes and packets transmitted between pairs network nodes in real time. By selecting the MAC, IP, or IPX layer, you can view the traffic summary in each network layer instantaneously. To view the matrix in outline table format, click  *Figure 6–19* shows a MACmatrix outline table view.



Host 1	Packets	Bytes	Bytes	Packets	Host 2
Cinco 002013	270	17322	17344	271	00E01E62B2A1
Cinco 002013	134	8961	9239	144	3com 197937
Cinco 002013	56	3626	3712	58	0060979C6A19
This station	12	2280	2067	12	H-P 315D27
3Com 4E9FC8	12	954	1146	15	0060979C6A19
0040052FA471	6	960	642	6	H-P 315D27
0060979C6A19	5	320	448	7	000502561A4A
Cinco 002013	2	128	128	2	H-P 315D27
3com 197937	2	314	241	2	00E01E62B2A1
Cinco 002013	2	128	128	2	Cinco 000027
Cinco 002013	2	128	128	2	3Com 4E9FC8
00E01E62B2A1	2	280	180	2	H-P 315D27
Cinco 002013	2	128	128	2	3Com BB7B29
Cinco 002013	183	10623	11712	183	This station
000502561A4A	0	0	128	2	Atalk_Broadcast
00E01E62B2A1	0	0	1062	3	01000CCCCCCC
H-P 315D27	0	0	234	2	Broadcast

Figure 6–19. Display of the MAC Matrix Outline Table View

To view your top talkers, simply click the table's **Packets** column heading. The **Packets** and **Bytes** columns on the left of the table


show the total traffic sent from Host 1 to Host 2, while the columns on the right show the traffic volume flow from the Host 2 to Host 1.

To access additional commands, press the right mouse button on the Host Table view to bring up the context menu. The commands are listed in [Table 6–17](#).

Table 6–17. Context Menu Commands

Menu	Function
Reset	Clear all statistics counters in the matrix table.
Refresh	Update counter Immediately.
Pause Update	Suspend the matrix table counter update temporarily.
Capture	Hot link to launch a capture session with the selected hardware address pair as the filter criterion.
Create Capture Filter...	Hot link to launch a capture filter setting dialog box with the selected hardware address pair as the filter criterion.
Export...	Save the Matrix table data to a CSV format file.
Properties...	Invoke Matrix properties dialog box.

Detail Table View

The detail table shows a different summary view from the outline table. You can group the entries by the protocol type or by the node address. To group entries by protocol, click  and then click the **Protocol** column header. You can see the traffic loads segregated by protocol types. [Figure 6–20](#) shows an IPX matrix detail table view.

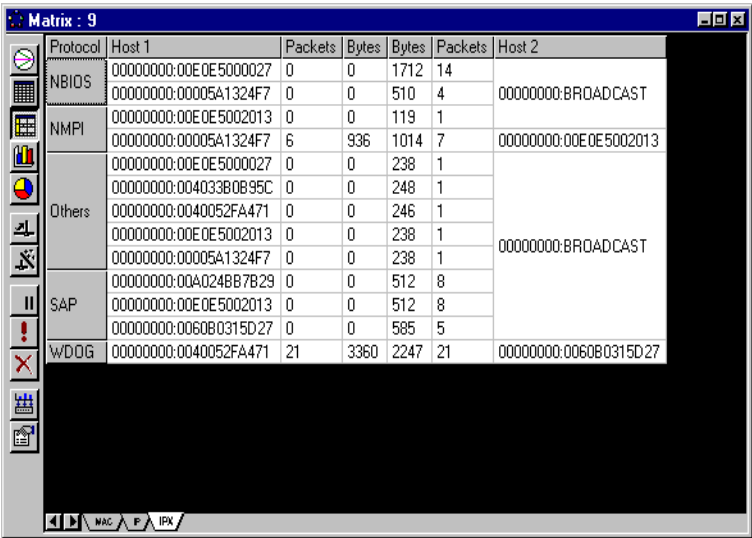



Figure 6–20. Display of the IPX Matrix Detail Table View

Bar Chart View

The bar chart reveals the top-N busiest conversation node pairs in real time. You can view top-N conversations in MAC, IP, or IPX-layer traffic. For example, to view top-N MAC-layer traffic conversation, click  and then select the MAC tab in the window (see [Figure 6–21](#)).

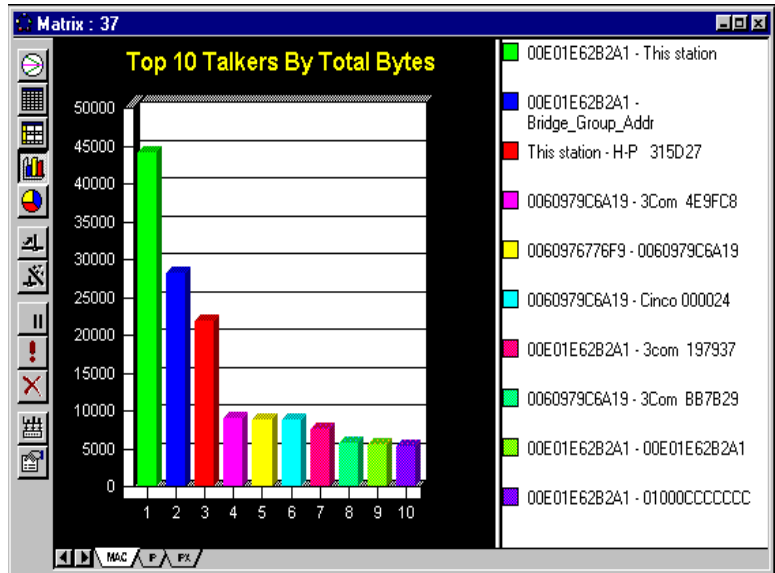


Figure 6-21. Bar Chart View of the Top-N Busiest Node Pairs

By default, the Top-N display is sorted by total bytes in traffic load counted and displayed with the top 10 nodes.

To change these setting, click  to invoke the MatrixProperties dialog box and select the TopN Chart page (see [Figure 6-22](#)).

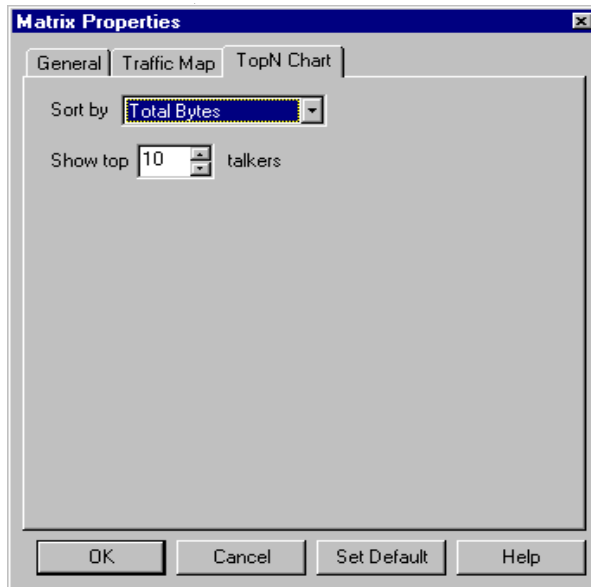


Figure 6–22. Display of the Matrix Properties Dialog Box

You can change the sorting criteria by source packets, source bytes, destination packets, destination bytes, total packets, or total bytes. In addition, you can change the top-N node displayed.

Pie Chart View

The pie chart reveals the top-N busiest conversation node pairs in their relative % load of the total top-N traffic (see [Figure 6–23](#)). To view the top-N pie chart, click



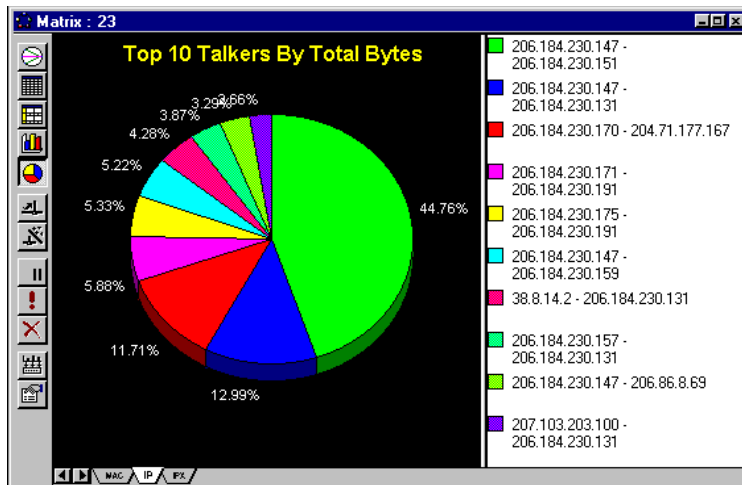


Figure 6-23. Display of the Pie Chart View of Top-N Node pairs

Sometimes, if the percentage load is not evenly distributed, the small percentage (%) numbers shown on the pie chart will overlap each other, making the percentage numbers illegible. You can click and drag the slice of pie outward to make room for the numbers as shown in [Figure 6-24](#).

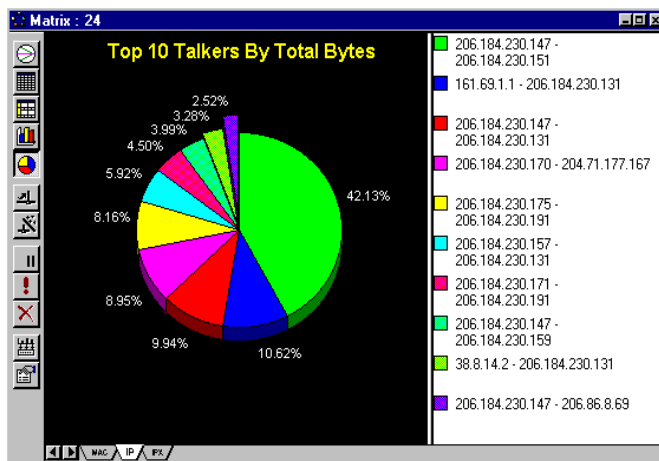




Figure 6-24. Pie Chart View of Small Percentage (%)

Using Matrix Traffic Map to Launch Packet Capture

The traffic map provides you with a birds-eye view of the network traffic patterns, and a powerful packet capture hot link to set up address filters and launch the capture engine by a simple “point and click” operation.

To capture packets generated by network nodes of your interest, click and select the node address first. Hold the **Control** key if you want to select more than one address. Then click Capture  to launch packet capture.

Similarly, you can click Capture setting  to build the address filter automatically.


Protocol Distribution

Protocol Distribution allows the reporting of network usage based on each protocol discovered in MAC, IPX, or IPX-layer.

Network-layer protocols monitored are IPX/SPX, TCP/IP, NetBIOS, AppleTalk, DECnet, LAT, OSI, SNA, Banyan Vines, Apollo, and XNS. Protocols not listed are grouped into **Others**.

Optionally, NetXRay can also monitor TCP/IP Application distribution, which reports on the percentage of each TCP/IP application as part of TCP/IP traffic. TCP/IP applications monitored are NFS, FTP, Telnet, SMTP, POP, HTTP (WWW), Gopher, NNTP, SNMP, X-Window, IMAP, IRC, LPD, and NetBIOS. Applications not listed are grouped into **Others**.

The IPX protocols monitored are NCP, SAP, RIP, NetBIOS, Diagnostic, Serialization, NMPI, NLSP, SNMP, and SPX. Protocols not listed are grouped in the Others category.

To start the Protocol Distribution monitoring, select **Protocol Distribution** from the **Tools** menu or click the  icon. A Protocol Distribution window is displayed ([Table 6–25](#)).

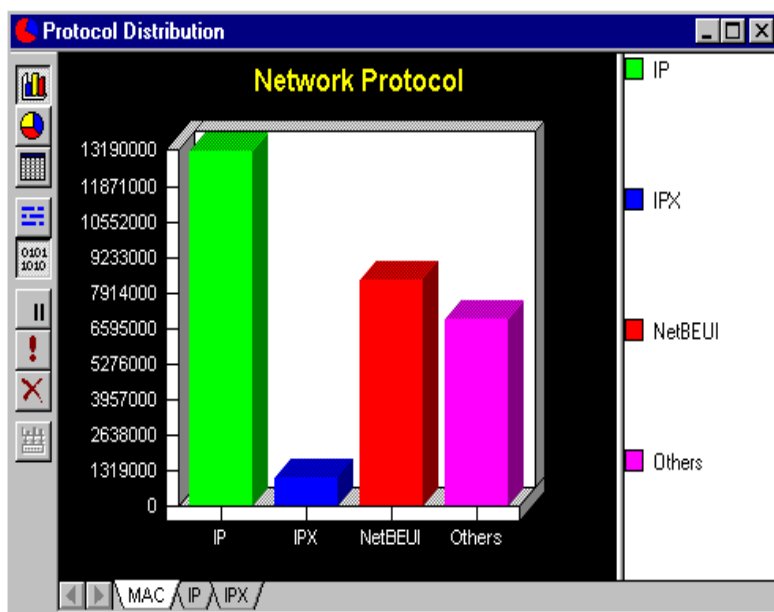


Figure 6-25. Protocol Distribution Window

To view IP-layer protocol distribution, click the IP tab on the bottom of the window ([Figure 6-26](#)).

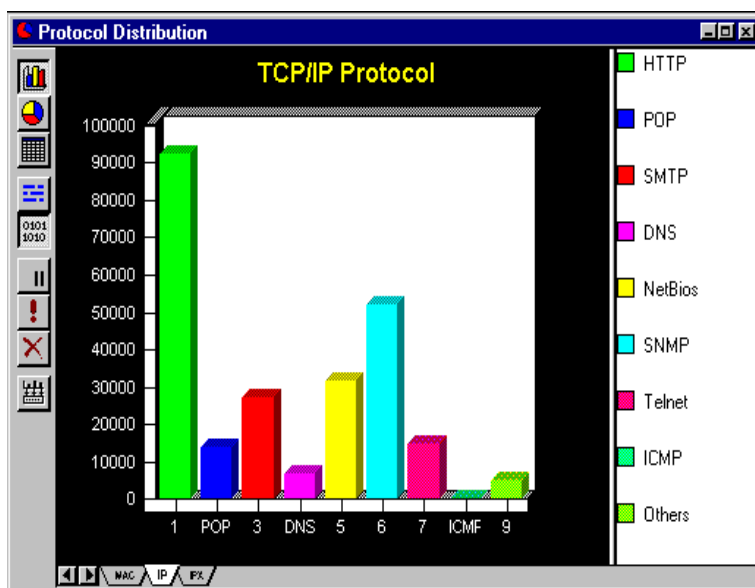



Figure 6-26. IP Protocol Distribution Window

To review total types, packets, and their relative percentage usage in table form, click  on the side of the window ([Figure 6–27](#)).

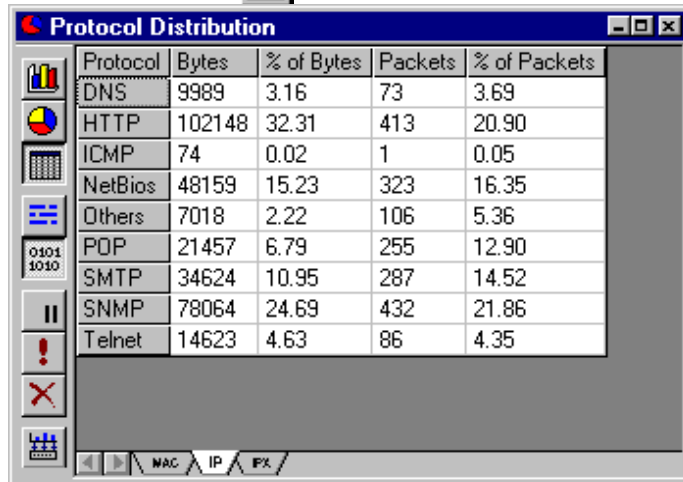


Figure 6–27. Protocol Distribution in Table Form

Customizing TCP Protocol Distribution

TCP/UDP application packets with port numbers not listed in the default protocol list are lumped together and counted in the **Others** category. You may add application-specific port numbers in the protocol list, so that they will be displayed as separate items.

To assign TCP/UDP application port numbers in a protocol list, follow these steps:

1. Go to the **Tools/Options** menu, select the **Protocols** page ([Figure 6–28](#)).

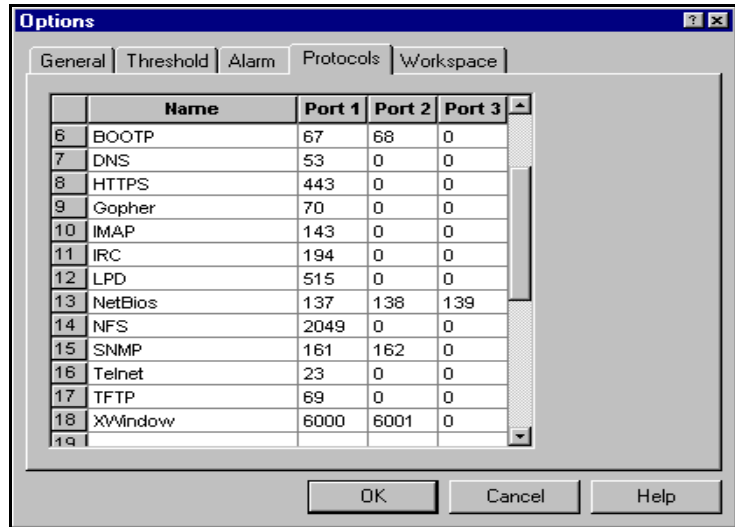


Figure 6–28. The Protocols Page in the Options Dialog Box

2. Enter the desired name and the port number you want to monitor as a separate item on the chart, then click **OK**. You may enter up to 3 port numbers for each application name. Enter 0 in the unused port location. Click **OK**.
3. Now, the protocol distribution chart will show the newly added item in the graph.

NOTE: NetXRay can only track protocol loads that are based on well-known and fixed port numbers. If you have an application that assigns and uses TCP/UDP port numbers dynamically, they will be grouped into the **Others** category.

Printing Protocol Distribution Graph

To print the protocol distribution graph:

1. Go to the **File** menu and select **Print....**
2. Click **OK**.



Chapter 7

Alarm Manager

NetXRay provides a comprehensive method of detecting, logging, and notifying you of unusual network events that occur during the course of monitoring your network activities. The alarm manager always logs the events in the alarm log. It will optionally sound audible alarms and notify you by:

- Sending email
- Calling a beeper number
- Calling a pager number with alarm text attached
- Invoking a NetXRay built-in Visual Basic script which in turn can launch other programs
- Sending NetXRay Alarm as SNMP trap to an SNMP console.

Abnormal network events, such as network load exceeding threshold level or detecting duplicating IP addresses, can be assigned to one of five different levels of severity; Critical, Major, Minor, Warning, and Informational. In addition, each severity level can be associated with up to four alarm notification actions activated during certain time periods within a day, as well as certain days during a week.

To support beeper or alpha pager, you must first install a working modem to a phone line. Refer to a Windows 95 or Windows NT user's guide about installing modems for your PC.

Defining SMTP Mail Alarm Notification

This section describes the step-by-step procedures to define SMTP mail alarm action.

To define alarm notification via SMTP mail:

1. Go to **Tools/Options**, and select the **Alarm** page ([Figure 7-1](#)).

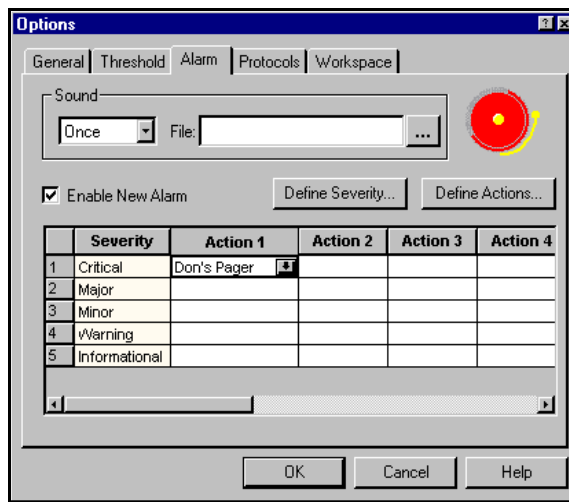


Figure 7-1. The Alarm Page in the Options Dialog Box

2. Click **Define Actions...** to invoke the Alarm Action dialog box (Figure 7-2).

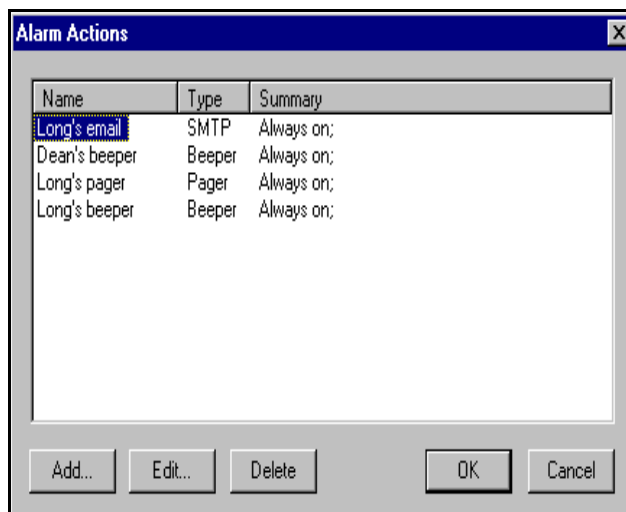


Figure 7-2. The Alarm Actions Dialog Box

3. Click **Add...** to invoke the New Alarm Action dialog box (Figure 7-3).

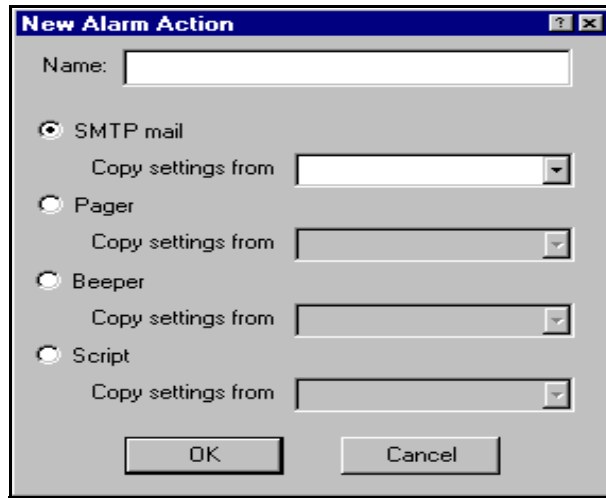


Figure 7-3. The New Alarm Action Dialog Box

4. Enter the new Alarm Action name, and select the **SMTP Mail** radio button. Optionally, you can copy from an predefined action. Click **OK**. The Mail Information dialog box appears (Figure 7-4).

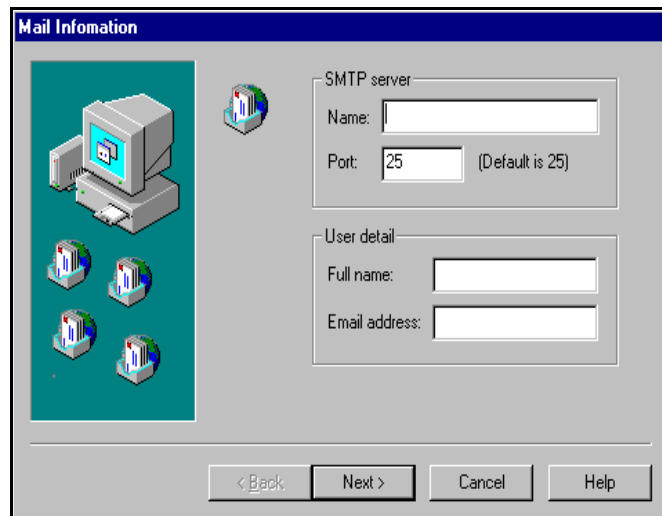


Figure 7-4. Mail Information Dialog Box

5. Enter the SMTP server name, and its port number. The default port number is 25.

6. Enter the mail recipient's full name and email address, then click the **Next** button. The Schedule dialog box appears (*Figure 7-5*).

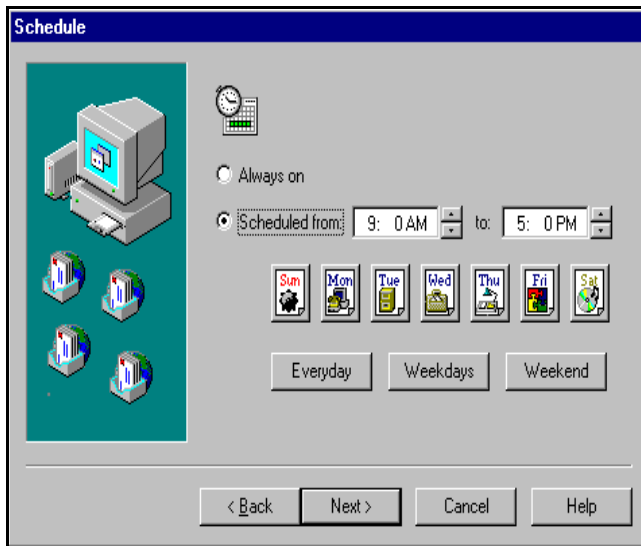


Figure 7-5. The Schedule Dialog Box

7. Select **Always on** if you want the Alarm action to be enabled at all times, or select **Scheduled from** if you want to enable the Alarm action during certain time periods.
8. Enter the time period, and select each weekday of your choice by clicking on the button to toggle its ON/OFF state. A floating button means OFF, while a sinking button means ON. You can optionally click **Everyday**, **Weekdays**, or **Weekend** to turn ON those days appropriately.
9. Click **Next** to advance to the Test dialog box (*Figure 7-6*).

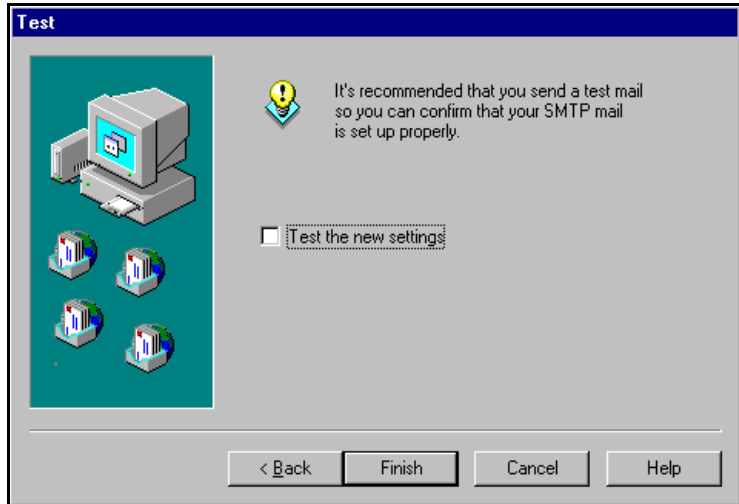


Figure 7–6. The Test Dialog Box

10. Check **Test the new settings** to make sure your email is being sent to the right person. Click **Finish**.
11. Click **OK** to complete the Alarm action definition.

Defining Alpha Pager Alarm Notification

This section describes the step-by-step procedures to define the Alpha Pager alarm action. The procedure is identical to the one in Defining SMTP Mail alarm except when selecting a new alarm, you will check the **Pager** radio button instead.

To define alarm notification via Alpha Pager:

1. Follow the procedure in [Defining SMTP Mail Alarm Notification on page 7–1](#).
2. Enter the new Alarm Action name, and select the **Pager** radio button. Optionally, you may copy from a predefined action. Click **OK**. The Pager Information dialog box opens ([Figure 7–7](#)).

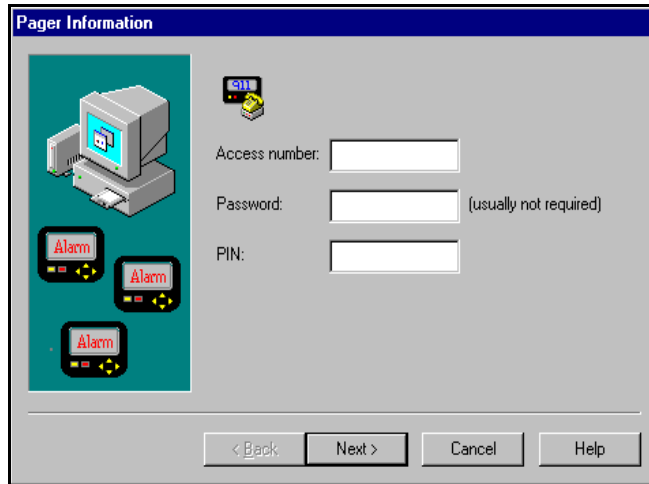


Figure 7-7. The Pager Information Dialog Box

3. Enter the telephone access number, an optional password and your PIN number for the pager. Click the **Next** button. The Communication Setup dialog box opens ([Figure 7-8](#)).

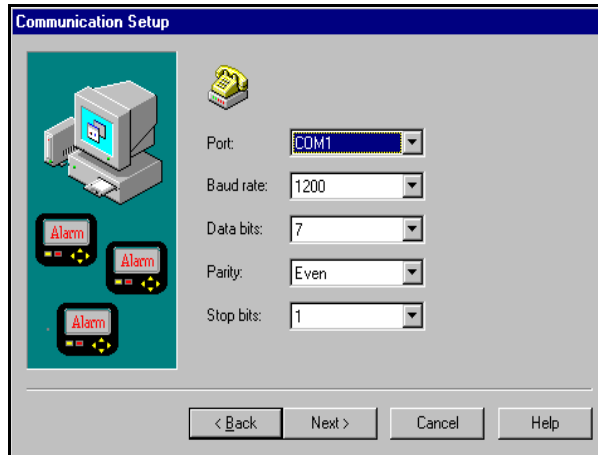


Figure 7-8. The Communication Setup Dialog Box

4. Enter the communication port setup information where you have the modem connected, then click the **Next** button.
5. Follow [Steps 7 thru 11](#) in [Defining SMTP Mail Alarm Notification on page 7-1](#).

Defining Beeper Alarm Notification

This section describes the step-by-step procedures to define Beeper alarm action. The procedure is identical to the one in [Defining SMTP Mail Alarm Notification on page 7-1](#) except when selecting a new alarm, you will check the **Beeper** radio button instead.

To define alarm notification via Beeper:

1. Follow the procedure as defined in [Defining SMTP Mail Alarm Notification on page 7-1](#).
2. Enter the new Alarm Action name, and select the **Beeper** radio button. Optionally, you may copy from a predefined action. Click **OK**. The Beeper Information dialog box opens ([Figure 7-9](#)).



Figure 7-9. The Beeper Information Dialog Box

3. Enter the telephone access number and a numeric message, which is usually the telephone number of the modem. It may also be any number which represent your message coding scheme. Optionally, adjust the delay periods for your particular beeper. Click the **Next** button. The Communication Setup dialog box appears ([Figure 7-10](#)).

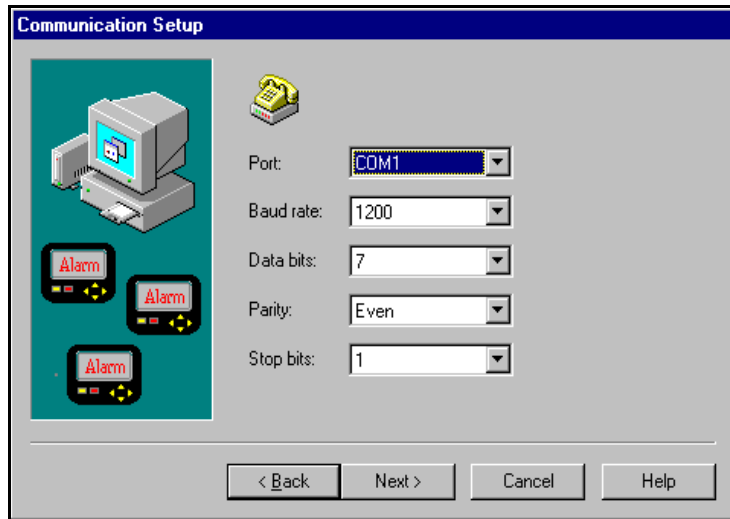


Figure 7-10. The Communication Setup Dialog Box

4. Enter the communication port setup information where you have the modem connected, then click the **Next** button.
5. Follow [Steps 7 thru 11 in Defining SMTP Mail Alarm Notification on page 7-1](#).

Defining Script Alarm Notification

A script is a Visual Basic program that the built-in NetXRay Basic interpreter is capable of understanding and executing to perform a specific defined task. NetXRay includes a sample ALARM.BAS that shows how to invoke an external program with the alarm message as the input parameter. By following the sample program, you can write a program to perform other tasks to handle the incoming alarm notification.

This section describes the step-by-step procedures to define the Script alarm action. The procedure is identical to the one in [Defining SMTP Mail Alarm Notification on page 7-1](#) except when selecting new alarm, you will check the **Script** radio button instead.

To define alarm notification via Script:

1. Follow the procedure in [Defining SMTP Mail Alarm Notification on page 7-1](#).
2. Enter the new Alarm Action name, and select the **Script** radio button. Optionally, you may copy from a predefined action. Click **OK**. The Script Information dialog box appears ([Figure 7-11](#)).

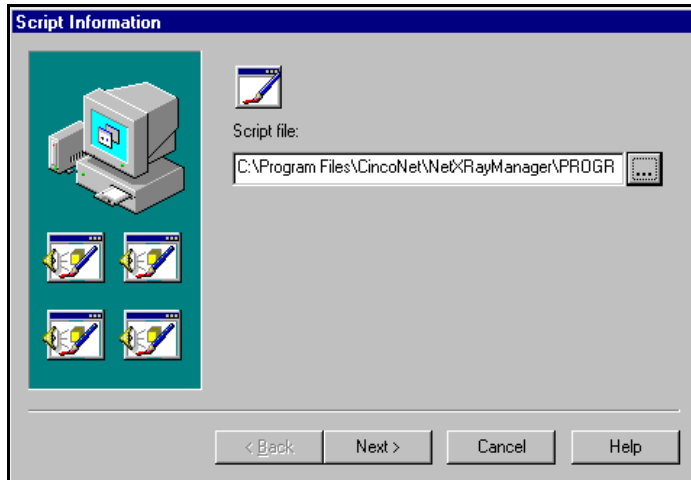


Figure 7-11. The Setup Information Dialog Box


3. Click the  button to invoke a Select file dialog box ([Figure 7-12](#)).



Figure 7–12. The Select File Dialog Box

4. Select a Basic Script file through the Select File dialog box, and click **OK**. Then click the **Next** button.
5. Follow [Steps 7](#) thru [11](#) in [Defining SMTP Mail Alarm Notification on page 7–1](#).

Defining Script Alarm to Forward an SNMP Trap

A script is a Visual Basic program that the built-in NetXRay Basic interpreter is capable of understanding and executing to perform a specific defined task. NetXRay includes a script XRAYALRM.BAS which will invoke the program XRAYALRM.EXE to convert NetXRay alarm messages into SNMP trap format and forward them to a remote SNMP management console.

The IP address of the SNMP management console must be defined in the XRAYALRM.BAS for NetXRay to forward the SNMP trap correctly. To change the SNMP management console IP address, open the XRAYALRM.BAS script file with a text editor. Locate the text line containing `Command = Command` as shown below:

```
Command = Command & " 206.184.230.178"
```

The IP address shown in the text line is for the remote SNMP management console. Substitute it for the IP address of your SNMP management console and save the change in the script file.

Note that a space character is required between the quote (") and the first character of the IP address 206.184.230.178.

This section describes the step-by-step procedures to define the Script alarm to forward SNMP traps.

To define alarm notification via Script:

1. Go to **Tools/Options...**, and select the **Alarm** page (see [Figure 7-13](#)).

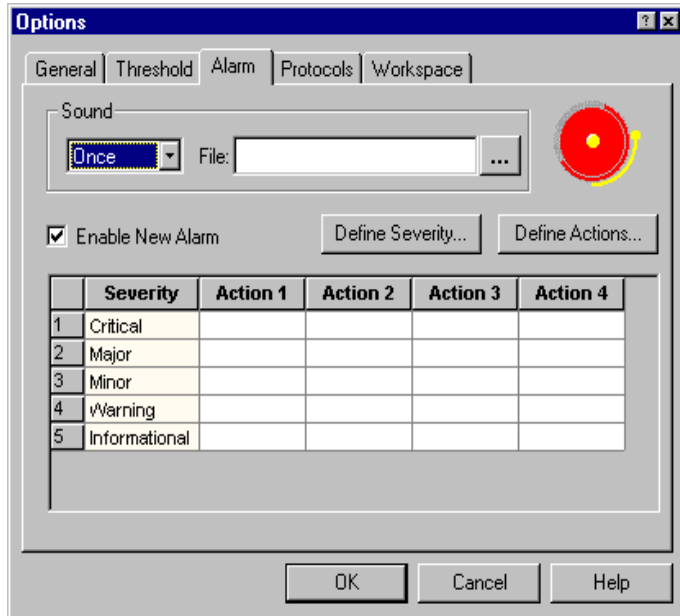


Figure 7-13. Display of Options Menu with Alarm Selected

2. Click **Define Actions...** to invoke the Alarm Actions dialog box (see [Figure 7-14](#)).

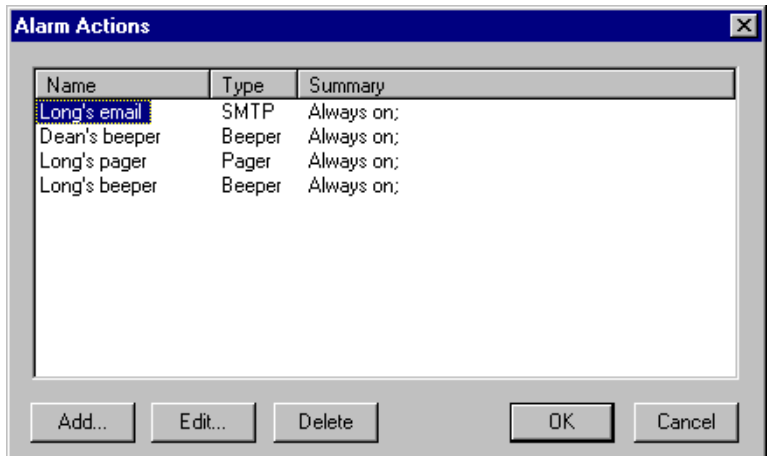


Figure 7–14. Alarm Actions Dialog Box

3. Click **Add...** to invoke the New Alarm Action dialog box (see [Figure 7–15](#)).

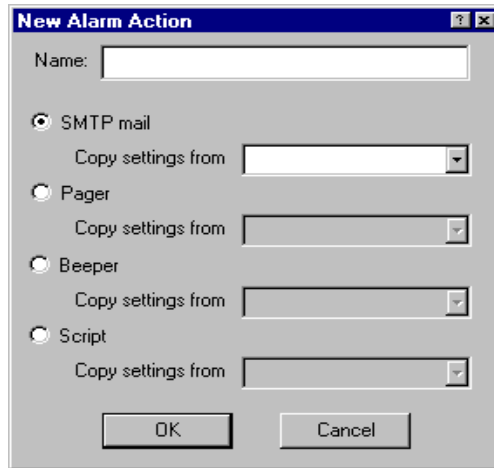


Figure 7–15. New Alarm Action Dialog Box

4. Enter the new Alarm Action name (for example SNMP Trap) and select the **Script** radio button. Optionally, you may copy from a predefined action. Then click **OK**.
5. Enter the Script file by doing one of the following:
 - a. Enter the full path of the script file as follows:
 C:\Program Files\CincoNet\NetXRay\Program\XRayAlrm.bas.
 Then click **Next** (see [Figure 7–16](#)).

OR

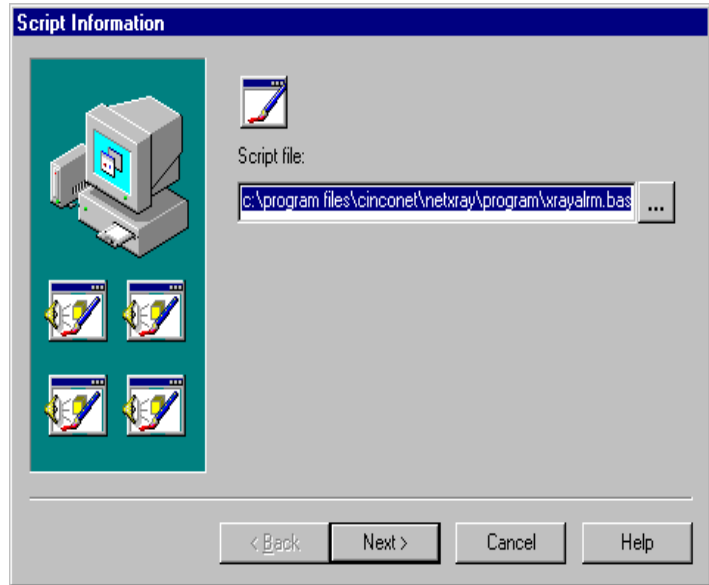


Figure 7-16. Script Information Dialog Box


- b. Select the script file through the Select file dialog box by clicking . Then click the **Next** button (see [Figure 7-17](#)).



Figure 7-17. Select File Dialog Box

6. Select **Always on** if you want the Alarm action to be enabled at all times, or Select **Scheduled from** if you want to enable the Alarm action during certain time periods.

7. Enter the time period, and select each weekday of your choice by clicking on the button to toggle its ON/OFF state. A floating button means OFF, while a sinking button means ON. Or you can click the **Everyday**, **Weekdays**, or **Weekend** buttons to turn ON those days appropriately.
8. Click **Next** to advance to the next page.
9. Check **Test the new settings** to make sure a test SNMP trap is sent to the SNMP management console. Click **Finish** (Figure 7-18).

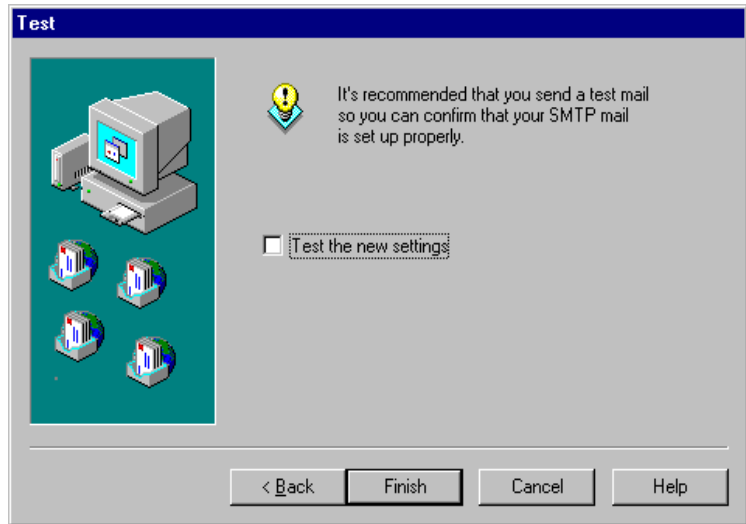


Figure 7-18. Test Dialog Box

10. Click **OK** to complete the Alarm action definition.

After you complete the definition of the alarm action, you must assign a severity level of your choice to the SNMP Trap alarm to take effect.

Configuring HP OpenView for Windows 1.2 SNMP Console

In order for HP OpenView to display the NetXRay trap appropriately, you must compile the XRAYALRM.MIB located in directory C:\Program Files\CincoNet\NetXRay\Program by using the SNMP management console MIB compiler. Refer to the appropriate user's guide for the instructions to compile the MIB file.

Next, you must follow the steps below to add the NetXRay Alarm device to the HP OpenView Device List and to define the Customize Trap Alarm.

To add a new Device Class to the list:


1. Open the device list file name **DEVICE** under the subdirectory **OVFILES** with a text editor.
2. Add the following line to the end of file:
 "NetXRay Alarm" 1.3.6.1.4.1.3051.1 0x1338 ANALYZER 0
3. Save the change.

To customize alarm responses to NetXRay Trap:

1. Go to **Monitor\Customize Traps...** and click **Add Devices Class...** to invoke the Add Device class dialog box.
2. Select the **NetXRay Alarm** device class, then click **OK**.
3. Click **Add Trap...** to invoke the Add Trap dialog box.
4. Select **Specific** in the Generic text box, then enter **1** in the **Specific** text box, and click **OK**.
5. Enter the following line into the **Description** text box:
 Trap Type: \$1
6. Enter the following line into the **Extended Description** text box:
 Severity level: \$2\nDescription: \$3\nTime Occurred: \$4
7. Click **OK** to complete the customized alarm.

Enabling Alarm Actions

After you complete the definition of the alarm actions, you must assign each a severity level of your choice with at least one alarm action to take effect. Otherwise, NetXRay may detect abnormal network conditions, but will not be able to forward notifications.

The alarm will make a beep sound once by default. If you prefer another sound for your alarm, you can replace the standard beep by choosing the **.wav** file. To do this, click the  button and select a wave file through the Select File dialog box, and click **OK**.

To assign Alarm actions to severity level:

1. Go to **Tools/Options...**, and select the **Alarm** page to display a table of assigned alarm actions ([Figure 7-19](#)).

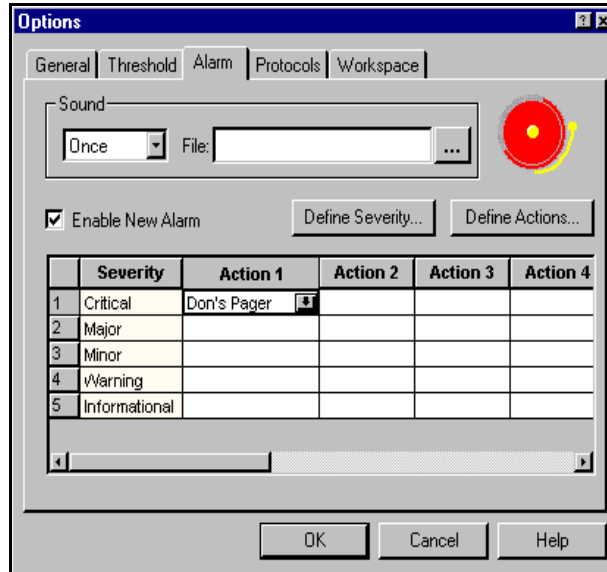


Figure 7-19. The Alarm Page in the Options Dialog Box

2. Click on the cell in the table where you want to assign a new alarm action. A drop-down list appears.
3. Click the down arrow to display a list of defined actions. Choose one.
4. Repeat [Steps 2](#) and [3](#) to assign more alarm actions.
5. Check **Enable New Alarm** to enable alarm notification.
6. Click **OK**.

Reassigning Severity Level to Alarms

NetXRay monitors the network traffic and network node availability. When the following events occur, it will generate the alarm actions that are associated with the severity level assigned for the event.

- Threshold: Over Upper Limit
- Address: Duplicated IP Address

- Address: Duplicated Data in Address Book

The default severity level assigned to each event may be changed to suit the specific network operating environment in your area.

To reassign the severity level:

1. Go to **Tools/Options...**, and select the **Alarm** page to display a table of assigned alarm actions. The **Alarm** page in the Options dialog box appears (*Figure 7–20*).

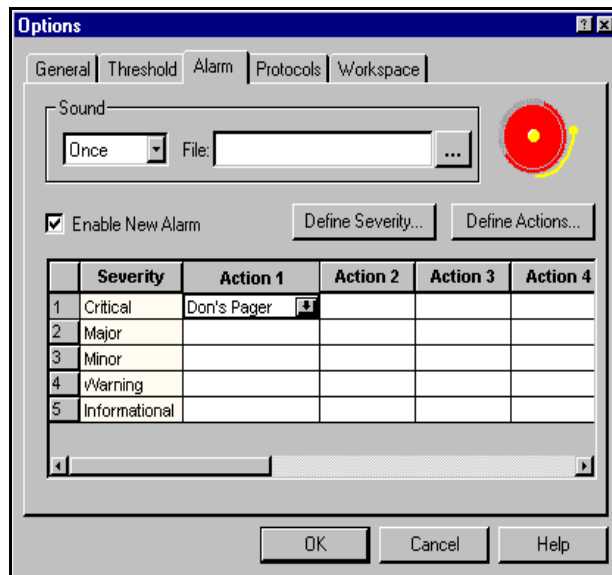


Figure 7–20. The Alarm Page in the Options Dialog Box

2. Click **Define Severity** to invoke the Define Alarm Severity dialog box. The Define Alarm Severity dialog box appears (*Figure 7–21*).

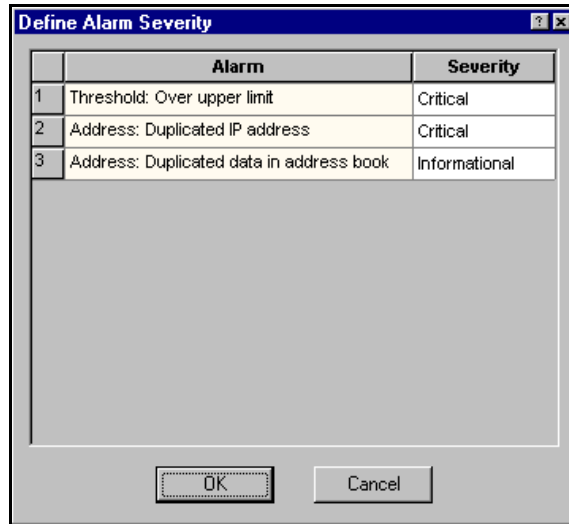


Figure 7-21. The Define Alarm Severity Dialog Box

3. Click on the severity cell where you want to make a change to display a list of severity levels. Choose one.
4. Click **OK** to complete the change.

NOTE: If you do not want a particular alarm event to generate an alarm or log entry, select **None** in the severity level.

Modifying the Statistics Threshold Level

NetXRay monitors the network's packet rate and utilization in real time. Alarms are generated anytime when the preset threshold parameters are exceeded, informing you of network exception conditions requiring immediate attention.

To set threshold levels:

1. Go to **Tools/Options..** to invoke the Options dialog box. Click the **Threshold** page. The Threshold Page in the Options dialog box opens ([Figure 7-22](#)).

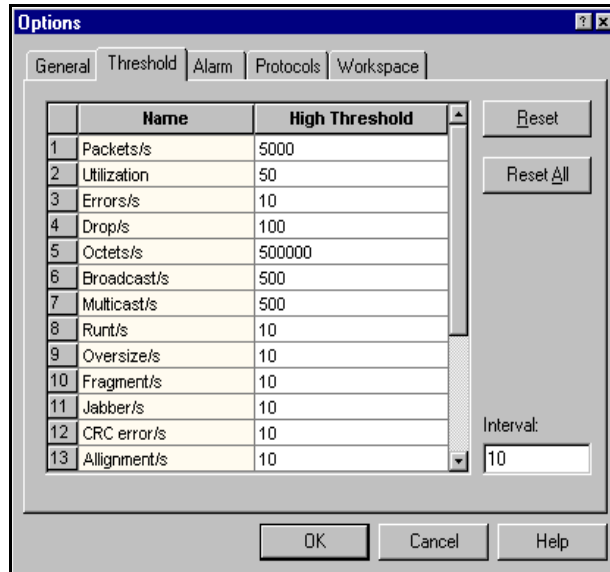





Figure 7–22. The Threshold Page in the Options Dialog Box

2. Change the threshold level and the monitoring interval, if necessary. Click **OK**. The monitoring interval defines how often the network data rate is sampled against the threshold level.

Working with Alarm Log

NetXRay monitors and detects abnormal network events, and saves them in the alarm log.

To view the Alarm Log, go to the **Tools** menu and select **Alarm Log**, or click the  icon on the Tool bar. An Alarm Log view is displayed. Each field in the Alarm Log is described below.

Status	Acknowledged  , or Unacknowledged  .
Type	Alarm cause type. Reserved.
Log Time	Date/Time when the entry is recorded
Severity	The severity of the alarm. It is always 1.
Description	Description of the cause of the alarm.

The Alarm Log shows all the recorded entries with the most recent entry first. You can sort the alarm entries by their column headings. To sort in ascending order, simply click the desired column heading. To sort in descending order, hold the Control key down and click the column heading.

The Alarm Log in [Figure 7–23](#) shows the entries sorted by description in ascending order.

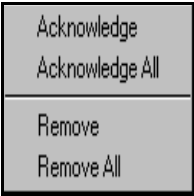
Alarm Log



Status	Type	Log Time	Severity	Description
	Event	09/15/95 11:45:40 PM	1	Under 64 Bytes/s: current value = 133, High Threshold = 5
	Event	09/15/95 06:52:10 PM	1	Octets/s: current value = 281575, High Threshold = 12800
	Event	09/15/95 06:52:10 PM	1	Broadcast/s: current value = 53, High Threshold = 10
	Event	09/15/95 06:52:10 PM	1	Under 64 Bytes/s: current value = 3458, High Threshold = 5
	Event	09/15/95 06:52:10 PM	1	Packets/s: current value = 4343, High Threshold = 200
	Event	09/15/95 06:52:10 PM	1	65 - 127 Bytes/s: current value = 832, High Threshold = 200
	Event	09/15/95 06:52:00 PM	1	Octets/s: current value = 281312, High Threshold = 12800
	Event	09/15/95 06:52:00 PM	1	Broadcast/s: current value = 52, High Threshold = 10
	Event	09/15/95 06:52:00 PM	1	65 - 127 Bytes/s: current value = 832, High Threshold = 200
	Event	09/15/95 06:52:00 PM	1	Packets/s: current value = 4341, High Threshold = 200
	Event	09/15/95 06:52:00 PM	1	Under 64 Bytes/s: current value = 3457, High Threshold = 5
	Event	09/15/95 06:51:50 PM	1	Octets/s: current value = 270550, High Threshold = 12800
	Event	09/15/95 06:51:50 PM	1	Broadcast/s: current value = 50, High Threshold = 10
	Event	09/15/95 06:51:50 PM	1	65 - 127 Bytes/s: current value = 800, High Threshold = 200
	Event	09/15/95 06:51:50 PM	1	Under 64 Bytes/s: current value = 3325, High Threshold = 5
	Event	09/15/95 06:51:50 PM	1	Packets/s: current value = 4175, High Threshold = 200
	Event	09/15/95 06:51:40 PM	1	Broadcast/s: current value = 52, High Threshold = 10

Figure 7–23. The Alarm Log

Context Menu

To acknowledge or remove alarm entries, select an entry by clicking it. Press the right mouse button on the Alarm Log view to bring up the context menu. Choose the appropriate command.



Acknowledge	Acknowledge the entry. The status  will change to  .
Acknowledge All	Acknowledge all entries.
Remove	Delete the selected entries.
Remove All	Remove all entries.

Exporting Alarm Log

NetXRay lets you save the Alarm Log in comma-separated values (CSV) file format. The CSV file gives you the ability to import the Alarm Log into other applications, such as a database or spreadsheet.

To export data to a file:

1. Click the right mouse button to invoke the context menu.
2. Select **Export**. A Save As dialog box is displayed.
3. Enter the filename, and click **Save**.

Address Data Base


NetXRay is shipped with predefined Manufacturer's ID codes, and Multicast address tables. You can create an Address Book to manage your own symbolic name table or import an external address/name file into the Address Book. Additionally, NetXRay learns IP network addresses and its associated domain names dynamically in real time and saves them in the Address Book.

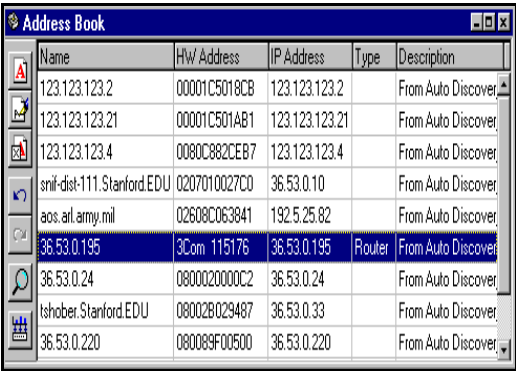
Address Book

The Address Book (see [Figure 8-1](#)) lets you predefine your network nodes in readable symbolic names. NetXRay uses the address book in Filter definition, Packet Viewer, Matrix Table, and Host Table to replace the 6-byte hardware address of the network node with its respective symbolic name.

The most convenient way to build your own address book is to get the hardware address from the Host Table.

To obtain the hardware address from the host table:

1. Invoke the Host Table. Allow several minutes for NetXRay to learn the hardware addresses of the most active nodes.
2. Invoke the Address Book by clicking on the **Address Book** in the **Tools** menu or  on the Tool Bar. The Address Book is displayed.
3. Click the right mouse button to bring up a context menu.
4. Select **Open Host Table as Drag Source** if the Host Table is not in the window view.
5. Click and drag an entry of your choice from the Host Table, then drop it in the Address Book. A new entry is created automatically with the manufacturer ID address format as its default name. You need to modify the name field to a symbolic name to help you identify the node later — for example, John's Pentium PC.




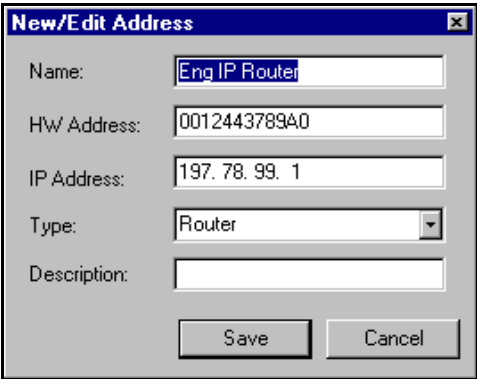
The screenshot shows the 'Address Book' window with a table of network entries. The table has five columns: Name, HW Address, IP Address, Type, and Description. The entries are as follows:

Name	HW Address	IP Address	Type	Description
123.123.123.2	00001C5018CB	123.123.123.2		From Auto Discover
123.123.123.21	00001C501AB1	123.123.123.21		From Auto Discover
123.123.123.4	0080C882CEB7	123.123.123.4		From Auto Discover
snik-dist-111.Stanford.EDU	0207010027C0	36.53.0.10		From Auto Discover
aos.art.army.mil	02608C063841	192.5.25.82		From Auto Discover
36.53.0.195	3Com 115176	36.53.0.195	Router	From Auto Discover
36.53.0.24	0800020000C2	36.53.0.24		From Auto Discover
tshober.Stanford.EDU	08002B029487	36.53.0.33		From Auto Discover
36.53.0.220	080089F00500	36.53.0.220		From Auto Discover

Figure 8–1. The Address Book

To edit an entry:

- 1. Double click an entry, or select and highlight an entry, then click the  button.
- A New/Edit Address dialog box is displayed (Figure 8–2).
- 2. Modify the fields, then press **Save**.



The screenshot shows the 'New/Edit Address' dialog box with the following fields:

- Name: Eng IP Router
- HW Address: 0012443789A0
- IP Address: 197. 78. 99. 1
- Type: Router
- Description: (empty)

Buttons: Save, Cancel

Figure 8–2. The New/Edit Address Dialog Box

An address book entry contains the following fields.

Name	Station’s symbolic name, or domain name.
------	--

HW Address	Station or node's hardware (MAC) address. This field may be blank if this entry is created by autodiscovery and the node's hardware address cannot be resolved.
IP Address	Station or node's IP address. Enter this address only if you are interested in IP filtering.
Type	The Node Type selections are Workstation, Host Computer, Server, File Server, Printer Server, Router, Bridge, and Hub. The Router host type is used in the IP address autodiscovery process, so that the router's own hardware address will not be associated with any IP address that is located outside of the current network segment.
Description	Used as reference information.

The context menu gives you additional commands to manipulate the address book. To invoke the context menu, click the right mouse button. An address book context menu is displayed (*Figure 8–3*).

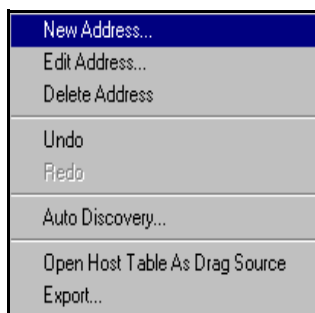


Figure 8–3. The Address Book Context Menu

The address book context menu includes the following selections:

New Address...	Create a new address book entry.
Edit Address...	Edit the selected entry.
Delete Address	Delete the selected entry.


Undo	Undo the last change.
Redo	Reapply the last Undo.
Auto Discovery...	Start IP address autolearning.
Open Host Table as Drag Source	Launch Host Table.
Export...	Export Address Table to a CSV file.

Autodiscovering IP Address and Domain Name

NetXRay supports auto-learning of a network node's IP address, its associated hardware address, and domain name. The learned addresses and domain name are added to the address book. If a duplicated IP address is found to be associated with a different hardware address, an entry is entered in the alarm log, and an audible alarm is sounded.

To properly learn IP addresses and domain names in your network, you must understand the role of IP routers and gateways. Since a router carries traffic between other subnets and your local segment where NetXRay resides, its hardware address will be associated with any IP node address that is outside of the local segment and has passed through the router. These router characteristics make the IP address autodiscovery process difficult if you have not manually identified the router in the address book first. You must enter your IP network routers' IP address, hardware address, and domain name in the address book first, and select the node type as Router.

Follow these steps to perform IP address and domain name discovery:

1. Click the **Auto Discovery** button  on the Address Book window to bring up the Discovery Option dialog box (*Figure 8-4*).

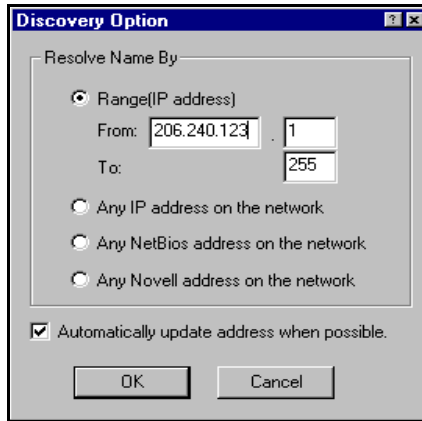


Figure 8-4. The Discovery Option Dialog Box

2. Click the **Range (IP address)** radio button, enter the local subnet address where NetXRay is monitoring. Click **OK**.
3. A small modeless dialog box will show you the discovery in process (Figure 8-5). When the search is finished, the dialog box will be removed.

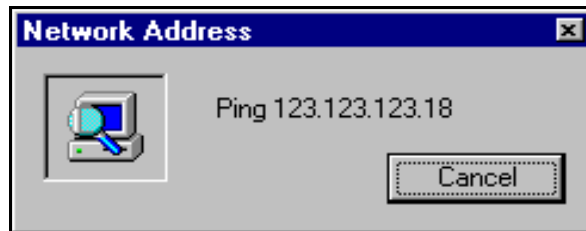


Figure 8-5. The Network Address Dialog Box


4. Next, identify the routers in your subnet. Double-click the router entry, select type as **Router**. Repeat this step for all the routers. This step must be performed, otherwise an IP node outside of your subnet will be entered into the address table with a duplicated router hardware address.

During the discovery process, NetXRay will first ping to an IP address to resolve the hardware address first. If the ping is successful, the resolved hardware address is entered in the address book. The IP address itself will be entered into the name field. It then sends a DNS request to the Domain Name Server to obtain the name entry for this IP address. If one is found, the domain name will be entered in the name field to replace the IP address.

The **Automatically update address when possible** check box is used to permit NetXRay to replace the name field with the newly discovered domain name automatically without warning. If the box is unchecked, a warning will be entered into the Alarm log when the name is replaced.

Once you have identified the local nodes and the routers, you can optionally use NetXRay to monitor and attempt to resolve the domain name of any IP node that has traffic present in the local subnet.

Follow these steps to identify additional domain names:

1. Click the **Auto Discovery** button  on the Address Book window to bring up the Discovery Option dialog box.
2. Click the **Any IP address on the network** radio button. Click **OK**.
3. A small modeless dialog box will show you the discovery in process. Every time NetXRay sees a new IP address, it will attempt to learn the IP's domain name. If a name is not found, the IP address is dropped, and not entered into the address book.
4. To stop the discovery, click the **Cancel** button on the modeless dialog box.


NOTE: The Autodiscovery function requires the use of the Microsoft TCP/IP ICMP.DLL. If you have not installed Microsoft TCP/IP, autodiscovery will fail with an error message displayed.

Some network systems use Dynamic IP address assignment. In that case, autodiscovery will not be useful, since the IP address for a network node can change from time to time. An unnecessary alarm will be generated.

Autodiscovering a NetBIOS Name and Hardware Address

NetXRay supports the process of auto-learning a network node's NetBIOS name and hardware (MAC) address, and saving them to the address book.

Follow these steps to perform NetBIOS name discovery:

1. Click the **Auto Discovery** button  on the Address Book window to bring up the Discovery Option dialog box (*Figure 8-6*).

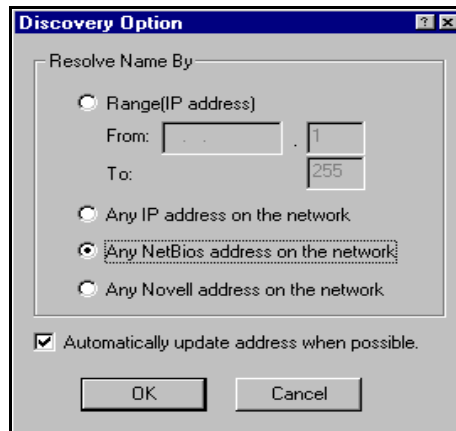


Figure 8-6. The Discovery Option Dialog Box

2. Click the **Any NetBIOS address on the network** radio button, then click **OK**.
3. A small modeless dialog box (*Figure 8-7*) will show you the discovery in process. NetXRay watches for node broadcast messages to learn its identity. You may need to leave the discovery on for 20 to 30 minutes to learn all the active node names. Click **Cancel** to stop the learning process.

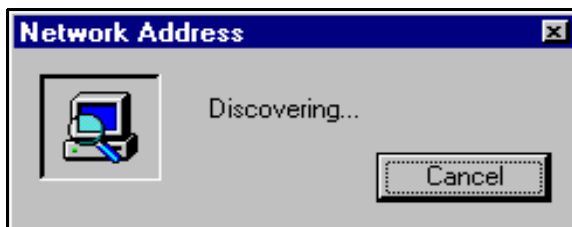



Figure 8-7. The Network Address Dialog Box

Discovering a NetWare User Name and Hardware Address

NetXRay supports a semiautomatic way of learning IPX network nodes' NetWare user name and hardware (MAC) address, and saving them to the address book.

Follow these steps to perform NetWare 3.X name discovery:

1. Click the **Auto Discovery** button  on the Address Book window to bring up the Discovery Option dialog box (*Figure 8-7*).

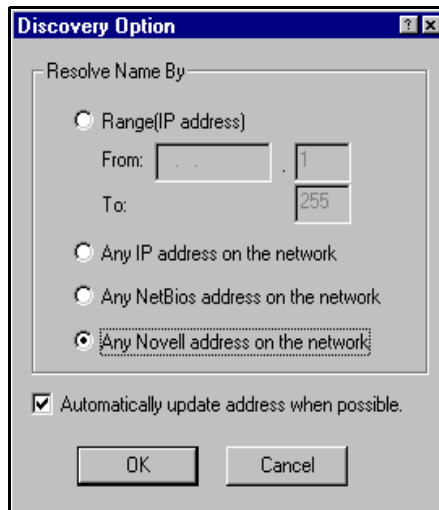


Figure 8-8. The Discovery Option Dialog Box

2. Click the **Any Novell address on the network** radio button. Click **OK**.
3. A small modeless dialog box will show you the discovery in process. Every time NetXRay sees a Get Nearest Server request, NetXRay will attempt to capture the server name and its hardware address and save it in the address book.
4. Next, log on to a Netware Server from your PC's DOS window. Enter the command:

USERLIST /A

NetXRay will extract the login user names and hardware addresses, and save them into the address book.

5. If you want to add additional user names from another server, repeat [Step 4](#).
6. To stop the discovery, click the **Cancel** button on the modeless dialog box.

If you are using NetWare 4.x, you must use the NetXRay Visual Basic script NOV2XRAY.BAS to import a user name file captured by using the NLIST USER /A command in a DOS window.

It is assumed that you have NetXRay installed on a workstation that can also log into a NetWare 4.x server.

To import user names:

1. Open a DOS window and log on to the NetWare 4.x server. Then type:

```
NLIST USER /A > \Program Files\CincoNet\NetXRay\Program \Novell.txt
```

This will retrieve the complete User list from the server and save it in NOVELL.TXT.

NOTE: The directory name assumes you have used the default path name during setup. Use your own directory path if they are different.

2. Go to NetXRay and select **Files/Run Macro...**
3. Locate NOV2XRAY.BAS (which is in the PROGRAM directory) and open the file.
4. A dialog box will query you to open a .TXT file. Select NOVELL.TXT that was created in [Step 1](#).
5. At this point, your Address Book should be updated with a list of NetWare login names and their hardware addresses from your NetWare server.

NOTE: Only users logged into the NetWare 4.x server will be displayed in this list.

Importing an External Address/Name File

NetXRay provides sample Visual Basic scripts to let you import an external address/name file in CSV format containing entries of IP address, hardware address, and corresponding host name into the NetXRay Address Book without having to enter them one-by-one.

The sample Basic script `Ripcsv.bas` and the sample external address/name file `lpdbsamp.csv` are located in NetXRay program directory.

The sample external address/name file is a CSV file and has the following format:

"Hostname", "TCP/IP Address", "Location", "LAN Type",
 "Full Name", "LAN Address", "Phone", "Serial Number",
 "Application", "Model"

The sample Basic script takes the contents in fields 1, 2, 3, 4, and 6, and creates entries in the NetXRay Address Book until the end of the file is reached. NetXRay has a capacity of 5,000 entries in the Address Book.

To import the sample external address/name file:

1. Select **Run Script...** from the **File** menu.
2. Select **Ripcsv.bas** from the dialog box, then click **Open**.
3. From the Open dialog box, Select **lpdbsamp.csv**, click **Open**.
4. The IP address and the associated fields will be added to the Address Book.

If you are an experienced Basic programmer, you can modify the sample Basic script to suit your need. However, the built-in Basic interpreter does not contain a debugging facility. Troubleshooting any mistakes you made will be difficult.

NetXRay is shipped with several Visual Basic scripts to help you import different user name file formats into the address book. The script names and file formats supported are listed in [Table 8–1](#).

Table 8–1. Script Names and File Formats

Macro Name	File format Supported
XRAY2XRAY	Exported XRAY format file, from either NetXRay or WebXRay.
LAN2NETX	Lanalyzer for Windows exported address format.
RIPCSV.BAS	Special format defined by NetXRay. See the comments in the Basic script.

Editing The Manufacturer's ID File

The network hardware address on Ethernet, Token Ring, and FDDI consists of six bytes. The first 3 bytes represent the manufacturer's ID, which is administered and assigned by the Institute of Electrical and Electronic Engineers (IEEE).

NetXRay maintains several manufacturer's ID files, each of which contains a table of manufacturer's names abbreviated in 6 bytes, and the corresponding 3 bytes of ID in hexadecimal format.

NETXRAY.BET contains manufacturer's IDs for Ethernet nodes.

NETXRAY.BTR contains names for Token Ring nodes.

NETXRAY.BFD contains names for FDDI nodes.

During NetXRay startup, NetXRay reads in the ID files and saves them in memory. NetXRay automatically substitutes known IDs with the abbreviated names when the hardware address is displayed.

If you want to add additional manufacturer name/ID entries which are not already included, you can use any text editor and follow the examples in the file to create new entries.

NOTE: Make sure you have backed up and saved the original files, in case you want to restore them to their original contents.

Multicast/Functional Address Files

NetXRay also maintains multicast and functional address files, each of which contains a table of predefined addresses and their corresponding symbolic names. NETXRAY.ETM contains multicast addresses for Ethernet. NETXRAY.TRM contains functional addresses for Token Ring. NETXRAY.FDM contains functional addresses for FDDI.

During NetXRay startup, NetXRay reads in these files and saves them into memory. NetXRay automatically replaces known multicast or functional addresses with their symbolic names when the hardware address is displayed.

Chapter 9

Network Adapter Selection

Select Network Adapter

If you have more than one NDIS 3.1 compliant adapter installed in your system, NetXRay lets you attach to the adapter of your choice.

To select an adapter:

1. Close all active windows.
2. Go to the **Tools** menu and click **Select Network Probe/Adapter**. An Adapter dialog box is displayed ([Figure 9-1](#)).

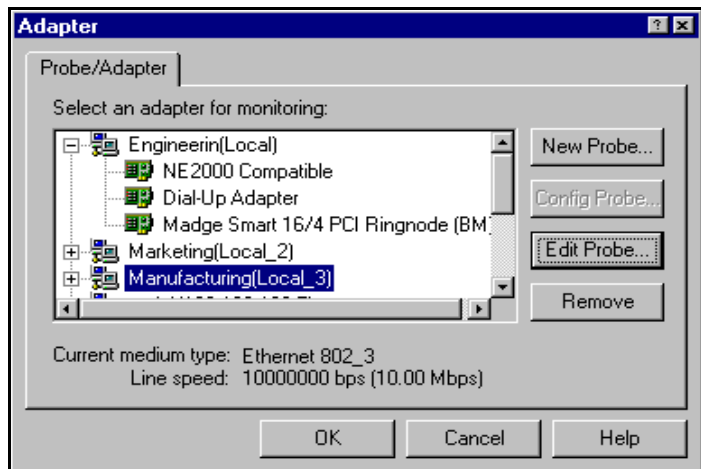


Figure 9-1. The Adapter Dialog Box

3. Select a network adapter as the target network for NetXRay to monitor.
4. Click **OK**.

TIP: If you select the **Dial-Up Network** option during Windows 95 setup, a **Dial-Up Adapter** icon will be shown in the list box. You can choose the Dial-Up Adapter if you want to monitor traffic between your computer and the remote host or server.

Monitor More Than One Network Adapters Concurrently

NetXRay allows you to launch multiple copies of NetXRay with each one monitoring a separate adapter. In order to run multiple NetXRay sessions, you must create a separate entity called “probe” for NetXRay to hold session information, such as address book, capture filter setting, and so on. pertinent to that adapter.

To launch a new NetXRay session:

1. Go to **Programs**, then click the **NetXRay** icon to launch a new session. An Adapter dialog box opens.
2. Click the **New Probe** button to bring up a New Probe dialog box([Figure 9–2](#)).

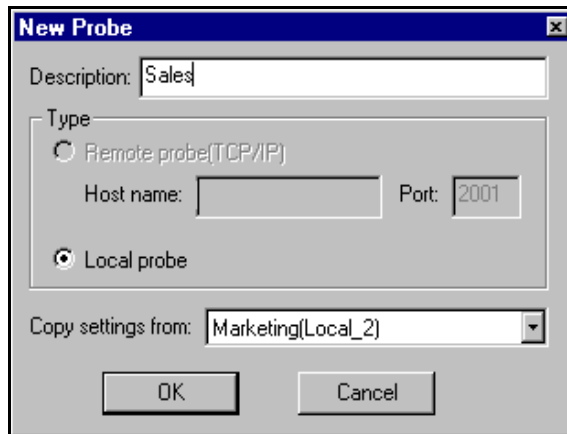


Figure 9–2. The New Probe Dialog Box

3. Enter the description, select the **Local probe** radio button, then click **OK**. Optionally, you can copy a workspace setting for the new probe from the existing probes. Open the drop-down list and select an existing probe as the source to copy from. A probe's workspace setting includes the address book, capture filter setting, packet display options, update frequency, and alarm thresholds.
4. Select an adapter which is not being monitored by another NetXRay session and click **OK**.
5. Wait a few seconds, and a new NetXRay session is created to monitor the selected adapter.



Appendix A

Decode SNMP MIBs

This appendix describes an advanced feature of NetXRay which should only be used by technical personnel who have a detailed understanding of SNMP concepts and who knows how SNMP has been implemented by various vendors.

NetXRay provides the ability to decode SNMP MIB OID in symbolic format to ease the viewing of the captured SNMP packets. It can also decode the enumerate values into their respective names. In order for NetXRay to display the symbolic names, you must parse the MIB file into a compressed dictionary-like output and place the output file in NetXRay's local directory before invoking NetXRay.

You can use any MIB compiler as long as the output format matches NetXRay's requirement. Alternatively, you can down-load a version of Bay Networks' SMIC SNMP MIB compiler from NGC's FTP server.

To download the MIB compiler:

1. Log on to ftp.ngc.com anonymously.
2. Change directory to `/pub/Share/NetXRay` (case sensitive).
3. Download the file `smic.EXE` in binary mode and save it in your local directory.
4. Rename `smic.EXE` to `smiczip.EXE`.
5. Run `smiczip.EXE` from your directory to unzip the files.

Compiling MIB File

`smic.EXE` (`smiczip.EXE`) contains the following files:

- SMIC compiler, `SMIC.EXE`
- SMIC User Guide, `SMICUG.TXT`
- Standard RFC MIB files

- Example Batch file to compile MIB II, MIBII.BAT
- Example MIB-II output file, SNMP.LST

You can follow the example MIBII.BAT to construct and compile your own proprietary MIB file. Refer to the SMIC User Guide for additional compiler related information.

NetXRay supports multiple SNMP dictionary files. NetXRay will search any filename with the prefix of snmp and the file extension lst, then stores the OID entries into its internal table. If NetXRay encounters duplicate OID entries, it will override the entry in the internal table with the latest entry from the .lst file.

To start compiling the MIB file:

1. Start MS-DOS from **Start/Programs** menu. An MS-DOS window is displayed.
2. Change directory to where you saved and unzipped the SMIC compiler.
3. Type in the Batch filename you just constructed to start compiling your MIB file.
4. An SMIC output window is displayed to list the results of the compilation.
5. Close the SMIC output window.
6. Repeat Steps 2 thru 4 until there is no error.
7. Copy the compiler output file SNMP*.LST to the NetXRay Program subdirectory.
8. Now you are ready to use NetXRay to decode your specific MIBs.

SNMP.LST Format

A sample SNMP.LST file format is listed below:

```
[NetWizrd]
```

```
Filename= snmp.lst
```

```
Version= 1.0
```

```
[OIDtree]
```

1.3= org
1.3.6= dod
1.3.6.1= internet
1.3.6.1.1= directory
1.3.6.1.2= mgmt
1.3.6.1.2.1= mib-2
1.3.6.1.2.1.1= system
1.3.6.1.2.1.1.1= sysDescr
1.3.6.1.2.1.1.2= sysObjectID
1.3.6.1.2.1.1.3= sysUpTime
1.3.6.1.2.1.1.4= sysContact
1.3.6.1.2.1.1.5= sysName
1.3.6.1.2.1.1.6= sysLocation
1.3.6.1.2.1.1.7= sysServices
...
....
1.3.6.1.3= experimental
1.3.6.1.4= private
1.3.6.1.4.1= enterprises

[Traps]

enterprise= 1.3.6.1.2.1.11
0= coldStart
1= warmStart
2= linkDown
3= linkUp
4= authenticationFailure
5= egpNeighborLoss

.....

.....

[ifAdminStatus.Allowable]

NumOfAllowable= 3

1= up

2= down

3= testing

[ifOperStatus.Allowable]

NumOfAllowable= 3

1= up

2= down

3= testing



Appendix B

NetXRay Specifications

Protocol Suites Supported (at time of publication).

NOTE: Protocols are being added constantly. If your protocol is not listed contact Network General to obtain an updated list. Support for proprietary or custom protocol decode is available upon request.

Ethernet	DIX V2, IEEE 802.3, 802.2 LLC, SNAP, SNMP, BPDU
Token Ring	IEEE 802.2 MAC, BPDU, LLC, SNAP
100VG-AnyLAN	IEEE 802.12
FDDI	SMT, 802.3 Raw
VLAN	IEEE 802.10, ISL, 802.1Q
Novell Netware	IPX, SPX, RIP, SAP, Echo, Error, NDIAG, NCP, NDS, LIP(Burst Mode), NWDOG, NBICAST, NLSP, Serialize, NetBIOS, SNMP
IP	IPv4, IPv6, TCP, UDP, ARP, RARP, ICMP, IGMP, SNMP, SNMPv2, TFTP, FTP, TELNET, HTTP, HTTPS, SMTP, POP3, NNTP, BOOTP, DHCP, OSPF, RIP, RIPv2, BGP, EGP, GDP, IGRP, NetBIOS over TCP, DNS, RPC, NFS, GRE, GREv2, IP-IN-IP, IPMOBIL, NWIP, LDAP
PPP	CBCP, IPCP, LCP, CCP, NBFCP, CHAP, LQM, IPXCP
AppleTalk	LAP, AARP, DDP, NBP, ATP, ZIP, RTMP, AEP, ADSP
IBM/Microsoft	NetBIOS, NetBUEI, SMB, NMPI

SNA	FID2, TH, RH, RU, DFC. SC, FMD/FMH, LU6.2
Banyan VINES	VLLC, VIP, VICP, VARP, VRTP, VIPC, VSPP, SMB
XNS	IDP, SPP, Error, RIP, Echo, PEP
DECnet	DRP, NSP, SCP, DAP, SMB, LAT



Appendix C

Configuration File NETXRAY.INI

NetXRay's configuration file, NETXRAY.INI, is located in Windows 95's or Windows NT's main directory.

User-alterable configuration entries are listed below. You may need to add or modify these entries to change NetXRay's operating characteristics.

[Network Adapter]

OverrideLinkSpeed=*n*

Specify *n* to override the speed detected from the NDIS driver.

n is defined as follows:

0 = Auto Detect (default)

1 = 10 Mbit

2 = 25 Mbit

3 = 100 Mbit

4 = 155 Mbit

5 = 4 Mbit

6 = 16 Mbit

7 = 56 Kbit

8 = 64 Kbit

9 = 1.54 Mbit

10 = 2.04 Mbit

11 = 45 Mbit

12 = 50 Mbit

13 = 45 Mbit

TRingMacFlag = 1

Specify **TRingMacFlag=1** to force an Olicom Token Ring Adapter to go into promiscuous mode.



IMPORTANT: DO NOT add this flag if you are using any other manufacturer's Token Ring network interface card.

[DecodeOptions]

EnableBackground=*n*

Specify *n* to enable or disable background packet decoding while viewing packets. When enabled, this flag lets NetXRay use spare CPU cycles to decode packets in the background so that viewing packet decodes can appear instantaneous.

n is defined as follows:

0 = Off (disabled)

1 = On (enabled, default)

EnableCache=*n*

When enabled, this flag allows the result of packet decodes to be cached in virtual memory so that, as the user scrolls through the Packet Viewer window, the detail decode can be seen without delay.

n is defined as follows:

0 = Off (do not cache)

1 = On (cache, default)

Caching is memory intensive. If you have a memory-limited PC, you must take care when viewing large capture files. For example, if you are running Windows 95 and your PC has only 16 Mbytes of RAM, you will have approximately 8 Mbytes of free memory. If you decode a large capture file, for example 16 Mbytes, NetXRay will not be able to place all of the decode results in RAM. Windows 95 will utilize virtual memory to put the decode output on the hard disk. Depending on how much this virtual memory is used, you may experience severe "disk thrashing" which will degrade the PC's performance.

To avoid disk thrashing, set **EnableBackground=0** and **EnableCache=0**.

[HostTableOptions]



IMPORTANT: The aging process, affected by the following NETXRAY.INI entries, can affect the performance of NetXRay monitoring. Make sure you always assign a table size greater than the number of entries you expect to monitor.

MaxNumNode=*nnnn*

The value *nnnn* specifies the maximum number of entries allowed in the Host Table. If a new entry is discovered which will increase the table size beyond the maximum size, the oldest entry in the table will be aged out.

nnnn is the number of nodes. It must be less than 10,000.

MaxNumIpNode=*nnnn*

The value *nnnn* specifies the maximum number of entries allowed in the IP Host Table. If a new entry is discovered which will increase the table size beyond the maximum size, the oldest entry in the table will be aged out.

nnnn is the number of nodes. It must be less than 10,000.

MaxNumIpxNode=*nnnn*

The value *nnnn* specifies the maximum number of entries allowed in the IPX Host Table. If a new entry is discovered which will increase the table size beyond the maximum size, the oldest entry in the table will be aged out.

nnnn is the number of nodes. It must be less than 10,000.

[MatrixTableOptions]



IMPORTANT: The aging process, affected by the following NETXRAY.INI entries, can affect the performance of NetXRay monitoring. Make sure you always assign a table size greater than the number of entries you expect to monitor.

MaxNumNode=*nnnn*

The value *nnnn* specifies the maximum number of entries allowed in the Matrix Table. If a new entry is discovered which will increase the table size beyond the maximum size, the oldest entry in the table will be aged out.

nnnn is the number of nodes. It must be less than 10,000.

MaxNumIpNode=*nnnn*

The value *nnnn* specifies the maximum number of entries allowed in the IP Matrix Table. If a new entry is discovered which will increase the table size beyond the maximum size, the oldest entry in the table will be aged out.

nnnn is the number of nodes. It must be less than 10,000.

MaxNumIpxNode=*nnnn*

The value *nnnn* specifies the maximum number of entries allowed in the IPX Matrix Table. If a new entry is discovered which will increase the table size beyond the maximum size, the oldest entry in the table will be aged out.

nnnn is the number of nodes. It must be less than 10,000.



Glossary

10 BASE5	IEEE 802.3 Physical Layer Specification for thick cable Ethernet using double-shielded RG11 coaxial cable. 10Base5 nomenclature stands for 10Mbits/s data rate, Baseband, at 500 meter maximum segment length.
10 BASE2	IEEE 802.3 Physical Layer Specification for thin cable Ethernet (also called Cheapernet) using RG-58 standard coaxial cable. 10Base2 is nomenclature for 10Mbit/s, Baseband, 185 meter maximum segment length
10 BASE-T	IEEE 802.3 Physical Layer Specification for Twisted-Pair Ethernet using Unshielded Twisted Pair wire at 10Mbit/s. (Rather than StarLAN's 1Mbit/s). 10Base-T is nomenclature for 10Mbit/s, Baseband, Twisted Pair cable.
1BASE5	IEEE 802.3 Physical Layer Specification for StarLAN Ethernet using twisted pair wire. 1Base5 is nomenclature for 1Mbit/s, Baseband, 500 meter maximum segment length.
4B/5B Encoding	The signal encoding method specified by the FDDI standard where each set of four bits is encoded as five bits as compared with the Manchester encoding method which requires eight bits of encoding for each four bits set.
802.3	See IEEE 802.3
802.5	See IEEE 802.5
Access Method	In Local Area Networks, the technique and/or program code used to arbitrate the use of the communications medium by granting access selectively to individual stations. Examples are CSMA/CD and Token Passing.
Adapter	An add-in board used to connect end-user nodes to the LAN network; each contains an interface to a specific type of workstation or system.

Adaptive Routing	A form of routing in which messages are forwarded through the network along the most cost-effective path currently available and are automatically rerouted if required by changes in the network topology (for example, if a circuit becomes disabled).
Address	A designator defining the unique ID of a terminal, peripheral device or any other nodal component in a network.
American National Standard Institute (ANSI)	An organization that coordinates, develops, and publishes standards for use in the United States. It also represents the United States in the International Standards Organization (ISO).
ANSI X3T9.5	A committee sponsored by ANSI, which sets system interconnection standards, including the specification for the Fiber Distributed Data interface (FDDI).
AppleTalk	Apple Computer's proprietary LAN protocol suite for linking Macintoshes and peripheral devices. AppleTalk is a CSMA/CA network with 115 Kbps data rate and allows connecting up to 32 devices.
Application	A software program designed to enable end users to carry out a specific task or function. Word processors, spreadsheets, graphics programs, and database managers are examples of applications.
Application Layer	The seventh and highest layer of the Open Systems Interconnection (OSI) data communications model. It supplies functions to applications or nodes allowing them to communicate with other applications or nodes. File transfer and electronic mail work at this layer. See OSI Model.
Application Program Interface (API)	A set of standardized interfaces to operating system functions available for use by applications programmers designed to ensure portability.
ARCnet	A token bus network architecture developed by Datapoint Corporation. It runs at between 2.5 and 4.0 Mbps over thin twisted pair RJ-62/U cable
Asynchronous/Asynchronous Transmission	A class of data transmission service whereby all requests for service contend for a pool of dynamically allocated ring bandwidth and response time.
Attenuation	Reduction or loss of signal strength, measured in decibels; opposite of gain. The difference between transmitted and received power.

Backbone	A LAN, a WAN, or combination of both dedicated to providing interconnectivity between 'subnetworks' in an enterprise-wide network. Subnetworks are connected to the backbone via bridges, routers and hubs/concentrators. The backbone serves as a data communications highway for LAN-to-LAN traffic.
Back End Network	A network term which often refers to the interconnection of mainframe computers to high performance mass storage devices, high speed controllers and file servers.
Bandwidth	A measure of the amount of traffic the media can handle at one time. In digital communications, describes the amount of data that can be transmitted over the line in bits-per-second.
Baseband	Transmission of digital signals without modulation. In a Baseband network, the entire spectrum of the cable is used by the signal; does not allow frequency - division multiplexing. IEEE 802.3 Ethernet uses baseband transmission.
Beacon Frame	A specialized frame in the Token Ring and FDDI protocol, sent during the Beacon process to indicate and recover from a break in the ring.
Bit	A single character of a language having just two characters, as either of the binary digits 0 or 1.
Bit Error Rate (BER)	The ratio of received bits that are in error relative to a specific number of bits received; measure of noise-induced distortion in digital communications links. Usually expressed as a number referenced to a power of 10; e.g., 1 error in 10 ⁵ bits is referred to as a BER of 10 ⁻⁵ .
Bits Per Second (bps)	Number of binary digits transmitted over a communications channel in one second.
Bit Rate	The number of bits of data transmitted over a communications line each second. To calculate the characters per second of a transmission in asynchronous communications, the bit rate is divided by ten.
Bits Per Second (bps)	Number of binary digits transmitted over a communications channel in one second.
Bit Rate	The number of bits of data transmitted over a communications line each second. To calculate the characters per second of a transmission in asynchronous communications, the bit rate is divided by ten.

BNC	A standardized 'T' shaped connector used with RG-58 coaxial cable.
Bridge	The simplest of the internetworking devices, the bridge connects two networks together. Bridges function at the data link layer of the OSI Model by selectively forwarding protocol independent data between two networks. Bridges can be used to connect or segment the traffic on networks.
Broadcast	The process of sending a signal or message from one station on a network to multiple stations on the network at the same time.
Brouter	In local area networking, a brouter is a device that combines the dynamic routing capability of an internetwork router with the ability of a bridge to interconnect local area networks. See Bridge, Router.
Bus Topology	A network topology in which nodes are connected to a single cable with terminators at each end.
Bypass	The ability of a station to be optically or electronically isolated from the network while maintaining the integrity of the ring.
Byte	A group of eight bits handled as a single logical unit.
Cable Plant	This term refers to the installed cabling, connectors, splices and patch panels within a given plant.
Campus Environment	An environment in which users (voice, video and data) are spread out over a broad geographic area, as in a university, hospital or medical center. There may be several LANS on a campus that are connected with bridges and/or routers communicating over telephone or fiber optic cable.
Carrier Sense Multiple Access/Collision Detection (CSMA/CD)	All nodes attached to the network contend for access and listen for transmissions in progress (carrier sense) before starting to transmit (multiple access). If two or more nodes transmit at the same time, a collision occurs (collision detection) and re-transmission occurs randomly.
Central Processing Unit (CPU)	The microprocessor that performs the central operations, commands and computations in a computer.
Circuit Switching	A switching technique in which an information path (circuit) between calling and called stations is physically established on demand for exclusive use by the two stations until the connection is released. Compare to Packet Switching.

Claim Frame	A specialized frame in the FDDI protocol sent during the claim process whereby one or more stations bid for the right to initialize the ring.
Client/Server Model of Computing	Computing in an environment where centralized computers called servers, support multiple distributed computers or clients. Part of the application runs on the server and part runs on the client computer.
Coax (Coaxial Cable)	A transmission medium consisting of one or more central wire conductors, surrounded by a dielectric insulator, and encased in either a woven wire mesh or extruded metal sheathing.
Code Bit	The smallest signaling element used by the Physical Layer for transmission on the medium.
Code Group	The specific sequence of five code bits representing an FDDI symbol.
Collision	Overlapping transmissions which occur when two or more nodes attempt to transmit at the same time, in which case the interference is termed a collision.
Common Management Information Protocol (CMIP)	A protocol formally adopted by the International Standards Organization (ISO), used for exchanging network management information over the OSI model. This network management information is exchanged between two management stations, or between an application and a management station. CMIP provides the protocol that network management systems use to request actions and report events. Other specification standards specify what actions can be requested or what events reported.
Communication Server	A LAN attached device offering communications to other nodes on the same network, or to other LANs.
Concentrator	FDDI- An FDDI concentrator has at least two Physical Layer entities and may or may not have one or more media access control entities. Token Ring- It provides a logical star topology while stations are physically connected as a ring. The concentrator (or center of the star topology) can actively bypass a station connect to it. Ethernet- See Multi-port Repeater.
Configuration Management (CFM)	That portion of Connection Management that provides for the configuration of PHY and MAC entities within a node in FDDI.

Connection Management (CMT)	In FDDI, the portion of the Station Management (SMT) function that controls network insertion, removal, and connection of PHY and MAC entities within a station.
Connector Plug	In FDDI, a device used to terminate an optical or copper cable. Plugs mate with receptacles.
Connector Receptacle	In FDDI, the fixed or stationary half of a connection that is mounted on a panel/bulkhead. Receptacles mate with plugs.
Counter-Rotation Ring	An arrangement where two signal paths, whose direction is opposite to each other, exist in a ring topology.
Crossconnect	Patch cable and passive hardware that is used to administer the connection of cables at a central or remote location
Cyclic Redundancy Check (CRC)	Error detection method, using a mathematical calculation on the data bits, that the transmitting and receiving nodes use to check the accuracy of transmitted packets.
Datagram	A transmission method used in packet-switching networks in which sections of a message are transmitted in scattered order and the correct order is reestablished by the receiving workstation.
Data Link Layer	The second layer of the Open Systems Interconnection (OSI) data communications model. It defines frame construction, addressing, error detection, and other services to higher layers.
Destination Address	The part of a message, usually a collection of characters or bits which indicate for whom the message is intended.
Destination Address Filtering	A feature of bridges where only messages intended for node on the extended LAN are forwarded.
Differential Manchester Encoding	A signaling method that encodes clock and data information into bit symbols. Each bit symbol is divided into two halves, where the second half is the inverse of the first half. A zero is represented by a polarity change at the start of the bit time; a one is represented by no polarity change at the start of the bit.
Diskless Workstation	A PC-like terminal for LANs, without disk drives, which must boot its operating system from the server and process client tasks in a client/server network environment.

Distributed Processing	LANs are used to link workstations and computer-servers that perform distributed processing. It can be an efficient use of processing power since each CPU can be devoted to a certain task. Processing done in multiple, separate networked computing systems where only mainframes are used to process.
DOS	The operating system for most IBM and compatible personal computers.
Downstream	A term that refers to the relative position of two stations in a LAN with a ring configuration. A station is downstream of its neighbor if it receives the token after its neighbor receives the token.
Dual Attachment Concentrator (DAC)	A concentrator that offers two attachments to the FDDI network which are capable of accommodating a dual (counter-rotating) ring, and additional ports for connection of other concentrators or FDDI stations.
Dual Attachment Station (DAS)	A FDDI station that offers two connections to the FDDI dual counter-rotating ring.
Dual-homing	A method of cabling concentrators and stations that permits an alternate or backup path to the ring in case the primary connection fails. Can be used in a tree or dual ring of trees configuration.
Dual Ring of Trees	A topology of concentrators and nodes that cascade from concentrators on a dual ring.
Early Token Release	This method of token passing allows for two tokens to exist on the network simultaneously. Early token release is especially helpful when traffic is heavy by taking advantage of the idle time created by regular token release. It is used primarily in 16Mbps Token-Ring and FDDI.
Electronic Industries Association (EIA)	A standards organization specializing in the electrical and functional characteristics of interface equipment.
E-Mail	Electronic Mail Program which allows messages to be exchanged among computers on a network.
Encapsulated Bridge	A proprietary hardware device that encapsulates data packets in specialized frames.
Encode	The act of changing data into a series of electrical or optical pulses that can travel efficiently over a medium reducing overhead and bandwidth requirements.

Enterprise Network	Also called an internetwork or a wide-area network. A network of networks that connects a corporation's or campus' local area networks (LANs). Local internetworks comprise networks within the same building or facility that are connected using bridges and routers. Internetworks that span distances typically connect remote facilities and rely on a public or leased data communications network. Bridges and routers typically connect networks to the long-distance data service, using an X.25 packet switched network, or a T1 line. See also Bridge and
Entity	An active element, or functional agent, within an Open System Interconnection (OSI) layer, sublayer, or SMT, in a specific station, including both operational and management functions.
Entity Coordination Management (ECM)	In FDDI, that portion of Connection Management that provides for controlling bypass relays and signaling to physical connection management (PCM) that the medium is available, and for coordinating trace functions.
Error Rate	In data transmission, the ratio of the number of incorrect elements transmitted to the total number of elements transmitted
Ethernet	Refers to the IEEE 802.3 CSMA/CD protocol which runs a 10Mbps transfer rate. CSMA/CD allows devices to transmit randomly with multiple access to the connecting medium. Ethernet is the most popular local area network used for connecting computers, printers, workstations and terminals. Ethernet 802.3 Physical Layer standards included 10BASE5, 10BASE2, 10BASE-T, and 10BASE-F.
EtherTalk	Apple's nomenclature for the Ethernet protocol that allows Apple Computer connectivity at 10Mbps. This standard replaces the earlier AppleTalk rate of 230.4 Kbps.
Extended LAN	A collection of local area networks interconnected by protocol independent store-and-forward devices (bridges).
Fault Tolerant	A method of making a computer or network system resistant to software errors and hardware problems. A fault tolerant LAN system tries to ensure that even in the event of a power failure, a disk crash or a major user error, data isn't lost and the system can keep running. Cabling systems can also be fault tolerant, using redundant wiring so that even if a cable is cut, the system can keep running.

Fiber Distributed Data Interface (FDDI)	FDDI is a set of ANSI/ISO standards for high speed (100 Mbps) LAN communications using fiber optic cable. It uses a dual ring or dual ring to trees topology and a token-passing media access method. It is compatible with the standards for the physical layer and the MAC portion of the data link layer of the OSI model. Up to 1000 stations can be connected with up to 3km b/w stations.
Fiber-Optic Cable	Network cabling that employs one or more optical fibers and carries information as light instead of electricity. Fiber-optic cable can carry more information over greater distances than copper cabling.
Fiber Optics	In data communications, the techniques of using fiber optic transmitters, receivers, and cables for the transmission of data.
File Server	A network device that can be accessed by several computers, through a local area network (LAN). It directs the movement of files and data on a multi-user communications network and "serves" files to nodes on a local area network. It typically is a combination of a computer, data management software, and large capacity hard &k drive.
File Transfer Protocol (FTP)	The file-sharing protocol operating at layers 5 through 7 of the Open Systems Interconnection (OSI) model that governs file sharing and file transfer capabilities.
Filtering	An operating parameter used in LAN bridges and routers that, when set, will cause these devices to block the transfer of packets or frames from one LAN to another. Filters can be set to prevent the internetworking of several types of messages. They may be set to block all packets originating from a specific destination, called source address filtering, or all packets heading for a particular destination, called destination address filtering.
Fragment	In FDDI, pieces of a frame left on the ring; caused by the normal operation of a station stripping a frame from the ring.
Fragmentation	A process in which large frames from one network are broken up into smaller frames that are compatible with the frame size requirements of the network to which they will be forwarded.
Frame	A group of bits sent serially (one after another) that includes the source address, destination address, data, frame check sequence, and control information. Generally a frame is a logical transmission unit. A frame usually contains its own control information for addressing and error checking. A frame is the basic data transmission unit employed in bit-oriented protocols.

Frame Check Sequence (FCS)	A 32-bit Cyclic Redundancy Check (CRC). Uses a matching calculation to determine validity of data packet or frame.
Front End Network	A network which interconnects workstations, word processors, personal computers, facsimiles, terminals, and printers.
Full Duplex	The capability of transmitting in two directions simultaneously.
Gateway	A gateway is an entrance into or exit out of a communications network. In data communications, a gateway connects two otherwise incompatible networks. Gateways perform protocol-conversion operations across a wide spectrum of communications functions or layers, and can handle protocols that do not correspond to the OSI model. Gateways are application specific such as NetWare to SNA, AppleTalk to DECnet, and NetWare to Banyan's VINES protocol.
Half Duplex	The capability to transmit in two directions, but not simultaneously.
Header	Control information attached to the front of a frame by an encapsulating bridge. The header, in conjunction with the trailer, surround the frame prior to the bridge forwarding it to another network.
Hub	See Multi-port Repeater.
IEEE 802.2	The IEEE standard for logical link control which defines a specific format for data and interface to a series of IEEE-specified physical layers.
IEEE 802.3	The IEEE standard specifying the 10Mbps Ethernet LAN. It has the largest installed base and supports Coaxial and Unshielded Twisted Pair (UTP) wiring.
IEEE 802.5	The IEEE standard specifying the MAC and physical sublayers for a star-wired topology with a token-passing access method.
IEEE 802.X	Institute of Electrical and Electronics Engineers, committee under the charter of ANSI to establish standards for the interconnection of LAN equipment, dealing with the Physical and Data Link Layers as defined by the OSI (Open Systems Interconnection) Reference Model.
Institute of Electrical and Electronic Engineers (IEEE)	Abbreviation for the Institute of Electrical and Electronic Engineers, a publishing and standards-making body responsible for many standards used in LANs, including the 802.X series.

Integrated Services Digital Network (ISDN)	A CCITT model for the eventual integration of voice, images, and data and a universal interface for networks.
Intermediate Crossconnect	An element in the EIA/TIA 568 Commercial Building Wiring standard. Consists of the active, passive, and support components that connect the inter-building cabling and the intra-building cabling for a building.
Intermediate System (IS)	An OSI term for a system that originates and terminates traffic, and that also forwards traffic to other systems. Also referred to as IS
International Standards Organization (ISO)	An international agency responsible for developing international standards for information exchange. The U.S. representative to the ISO is ANSI (American National Standards Institute).
Internetworking	Connecting two or more networks together by using devices such as bridges, routers, and gateways. See Enterprise Network.
Internetwork Protocol (IP)	An ISO standard defining a portion of the Layer 3 (network) OSI Model responsible for routing and delivery. As specified in RFC-791, IP provides for transmitting blocks of data (datagrams) between hosts identified by fixed-length addresses.
Interoperability	The ability to exchange information and operate multi-vendor networks interchangeably in heterogeneous environments.
Jitter/Timing Jitter	The deviation of clock recovery which can occur when a station's receiver recovers both clock and data from the received signal in a LAN using a ring configuration.
LAN Manager	The network operating system developed by Microsoft. It is an OS/2 application and is OEMed by a number of vendors including 3Com, IBM, DEC and AT&T, and is offered by Microsoft as a retained product.
LAN/Network Manager	A person within an organization who is responsible for managing the LAN. Duties can include adding new users, installing new hardware and software, diagnosing networking problems, helping users, performing backup and setting up the security system. Unlike MIS managers, LAN managers are rarely formally trained in LAN management.
LAN Server	IBM's proprietary implementation of Microsoft's LAN Manager.

Latency	The time interval between when a network station seeks access to a transmission channel and when access is granted or received. Same as waiting time. In a bridge or a router, it is the amount of time elapsed between receiving and retransmitting the LAN packet.
Layer	In the seven layered OSI model, it refers to a collection of network processing-functions that together comprise a set of rules and standards for successful data communication. See OSI Model.
Light Emitting Diode (LED)	A light emitting diode is an electrical component which produces light when stimulated by electricity. It is commonly used as a method for transmitting infra-red light along an optical fiber.
Load Balancing	The practice of splitting communication into two (or more) routes. By balancing the traffic on each route, the communication is made faster and more reliable. In remote internetworking, bridges and routers perform load balancing by splitting LAN-to-LAN traffic among two or more WAN links. This permits a combination of several lower speed lines to transmit LAN data simultaneously.
Local Area Network (LAN)	A short distance data communications network (typically within a building or campus) used to link together computers and peripherals under a standard protocol. The network provides high-bandwidth communication over coaxial cable twisted-pair, fiber, or microwave media. It is usually owned by the user. LANs have two main advantages: LAN users can typically access a centralized database and shared resources and LAN users can send messages to other LAN users.
LocalTalk	The cable and connector system used in Apple Computer's AppleTalk networks.
Logical Link Control (LLC)	A protocol subset developed by the IEEE 802.2 committee for data-link-level transmission control. It is the upper sublayer of the IEEE Layer 2 (OSI) protocol that complements the Media Access Control (MAC) protocol. IEEE standard 802.2 includes end-system addressing and error checking.
Logical Ring	The path a token follows in a FDDI or Token Ring network made up of all the connected MAC sublayers of each node. In FDDI, the physical topology can be a ring, a tree, or a dual ring of trees.

Look-Up Table	A set of addresses (source and destination) used by a bridge or router to determine what should be done with a packet. As the packet comes in, its address information is read and compared with the information in the look-up table. Depending on the information, the bridge may forward the packet, or discard it. Many bridges and routers can build their look-up tables as they operate.
Main Crossconnect (MCC)	An element in the EIA/TIA 568 commercial Building Wiring standard. Consists of the active, passive, and support components that connect the interbuilding backbone cables between intermediate crossconnects.
Manchester Encoding	A signaling method by which clock and data bit information can be combined into a single, self-synchronizable data stream. A transition takes place in the middle of each bit time. A low-to-high transition represents a one; a high-to-low transition represents a zero.
Media Access Control (MAC)	A media access control protocol within the OSI Model. It is the lower sublayer of the data link layer and complements the upper sublayer, the Logical Link Control (LLC).
Media Access Unit (MAU)	MAU is a physical device used in Ethernet to transmit signals from the MAC onto the medium. May be referred to as transceiver.
Media Interface Connector (MIC)	An optical fiber connector pair that links the fiber media to the FDDI node or another cable. The MIC consists of two halves. The MIC plug terminates an optical fiber cable. The MIC receptacle is associated with the FDDI node.
Metropolitan Area Network (MAN)	Usually public telecommunications networks that extend the reach of LANs, typically up to 50 kilometers. MANs operate at speeds from 1Mbit/s to 200Mbps, and some provide an integrated set of services for real-time data, voice and image transmission. New fiber optic-based MANs can extend the reach of a LAN up to 150 miles. Two standards bodies are involved with work on MANs: IEEE 802.3 and ANSI X3T9.5.
Mini Computer	A computer that is larger and more powerful than a typical personal computer, but smaller than a mainframe.
Multicast Packets	Multicast packets are addressed to a group of devices on a LAN. LAN stations use multicast packets to deliver information to a specific set of devices such as routers, file servers, and hosts.

Multimode	An optical fiber which allows the signal carrying light to travel along more than one path.
Multiple Access	The ability of several personal computers connected to a local area network to access one another through a common addressing scheme and protocol.
Multi-Port Repeater	The center of a star topology network, also called a hub, the multi-port repeater regenerates signals from port and retransmits to one or more other ports connected to it.
Multi-station Access Unit (MAU)	A concentrator used in Token-Ring networks. The Token-Ring MAU and an arrangement of relays that function as bypass switches. When only one MAU is used, its relays and internal wiring arrange themselves so that the MAU and the connected computers form a complete electrical ring. MAUs can be cascaded to create bigger rings.
Named Pipe	An API for OS/2 LAN Manager feature which allows application-to-application communications.
NetBIOS	Network Basic Input/Output System NetBIOS is an API originally designed as the interface to communication protocols for IBM PC networks. It has now been extended to allow programs written using the NetBIOS interface to operate on many popular networks.
NetView	IBM's family of network management products that allow centralized monitoring and management of enterprise level computing resources.
NetWare	The popular network operating system from Novell, Inc. NetWare supports both Ethernet, Token-Ring, and FDDI network interface cards.
Netware Loadable Module (NLM)	A software module that can be added to the NetWare 3.X operating system to add functionality to a network server. NLMs can be dynamically loaded on or unloaded from the NetWare 386 server without having to bring down the server.
Network	A set of communication channels interconnecting several or many locations.
Network File System (NFS)	A protocol for transparently sharing files across a computer network. Pioneered by Sun Microsystems, it is now a de facto standard in the UNIX world. It is built on TCP/IP and Ethernet protocols.

Network Interface Card (NIC)	Interface card required in the expansion bus of a personal computer to connect to the cabling of a PC LAN.
Network Layer	Layer 3 of the OSI model that permits communications between network nodes in an open network.
Network Management	Procedures, software, equipment and operations designed to keep a network operating near maximum efficiency.
Network Management System	Software and network management protocols for managing and controlling multi-point networks from a central or remote location.
Network Management Tasks	<p>Configuration management deals with installing, accessing, “boot” modifying and tracking the configuration parameters of network hardware and software in a network.</p> <p>Fault Location and Repair Management tools give information to help the network administrator find out what’s going wrong with the network equipment or lines in order to fix those resources. This is done by rerouting traffic or reporting problems to the carrier, or suggesting that certain equipment should be replaced. Fault location and management tools have strong error and alarm characteristics.</p> <p>Security Management tools allow the network manager to restrict access to various resources in the network.</p> <p>Performance Management tools provide real-time and historical statistical information about the network’s operation. Such tools show, for example, how many packets are being transmitted at any given moment, the number of users logged into a specific server, and use of network lines.</p> <p>Accounting Management applications help users allocate the costs of the various network resources.</p>
Network Operating System (NOS)	The software program that provides the LAN user an interface and control of the user network interface. Network operating system communicates with the LAN hardware and the computer operating system.
Network Topology	The physical layout of a computer network; the way various systems are interconnected. The most common network topologies are bus, ring, and star.
Node	An intelligent connection on a network which has its own unique network address, capable of communicating to another station. Also known as a point in a network where service is provided.

Nonrestricted Token	A Token denoting the normal mode of asynchronous bandwidth allocation, wherein the available bandwidth is time-sliced among all requesters.
Nonreturn to Zero (NRZ)	An encoding technique used in which a polarity level high, or low, represents a logical "1" (one), or "0" (zero).
Nonreturn to Zero Invert on Ones (NRZI)	An encoding technique used in which a polarity transition represents a logical "1" (one). The absence of a polarity transition denotes a logical "0" (zero).
Octet	A data unit composed of eight ordered bits. In FDDI, a pair of data symbols.
Open Systems Interconnection Model (OSI)	Internationally accepted framework of standards for intersystem communication. A seven layer model, developed by ISO, that covers all aspects of information exchange between two systems and designed to allow different devices to communicate without regard to the manufacturer. The layers perform specific communications functions relating to data transmission, routing and user application. The seven layers are Physical, Data Link, Network, Transport, Session, Presentation and Application.
Optical Fall Time	The time interval for the falling edge of an optical pulse to transition from 90 % to 10% of the pulse amplitude.
Optical Receiver	An optoelectronic circuit that converts an incoming optical signal to an electrical signal; typically a photodetector.
Optical Rise Time	The time interval for the rising edge of an optical pulse to transition from 10% to 90% of the pulse amplitude.
Optical Transmitter	An optoelectronic circuit that converts an electrical signal to an optical signal; typically a light emitting diode or laser diode.
Network Topology	The physical layout of a computer network; the way various systems are interconnected. The most common network topologies are bus, ring, and star.
Node	An intelligent connection on a network which has its own unique network address, capable of communicating to another station. Also known as a point in a network where service is provided.
Nonrestricted Token	A Token denoting the normal mode of asynchronous bandwidth allocation, wherein the available bandwidth is time-sliced among all requesters.

Nonreturn to Zero (NRZ)	An encoding technique used in which a polarity level high, or low, represents a logical "1" (one), or "0" (zero).
Nonreturn to Zero Invert on Ones (NRZI)	An encoding technique used in which a polarity transition represents a logical "1" (one). The absence of a polarity transition denotes a logical "0" (zero).
Octet	A data unit composed of eight ordered bits. In FDDI, a pair of data symbols.
Open Systems Interconnection Model (OSI)	Internationally accepted framework of standards for intersystem communication. A seven layer model, developed by ISO, that covers all aspects of information exchange between two systems and designed to allow different devices to communicate without regard to the manufacturer. The layers perform specific communications functions relating to data transmission, routing and user application. The seven layers are Physical, Data Link, Network, Transport, Session, Presentation and Application.
Optical Fall Time	The time interval for the falling edge of an optical pulse to transition from 90 % to 10% of the pulse amplitude.
Optical Receiver	An optoelectronic circuit that converts an incoming optical signal to an electrical signal; typically a photodetector.
Optical Rise Time	The time interval for the rising edge of an optical pulse to transition from 10% to 90% of the pulse amplitude.
Optical Transmitter	An optoelectronic circuit that converts an electrical signal to an optical signal; typically a light emitting diode or laser diode.
Physical Layer	Layer 1 of the OSI model that defines and handles the electrical/optical and physical media connections.
Physical Layer Protocol (PHY)	A portion of the FDDI standard that defines symbols, line states, clocking requirements, and the encoding of data for transmission.
Physical Link	The simplex path (via PMD and attached medium) from the transmit function of one PHY entity to the receive function on an adjacent PHY entity (in concentrators, repeaters, or stations) in an FDDI ring.
Physical Medium Dependent (PMD)	A portion of the FDDI standard that defines the medium and protocols to transfer symbols between PHYs.
Physical Topology	The actual arrangement of cables and hardware that make up the network. E.g. bus, ring, star, etc.

Point-to-Point	A direct connection established between and dedicated to only two stations used for data transmission.
Port	The entrance or physical access point to a computer, multiplexer, device or network where signals may be supplied, extracted or observed.
Power Budget	The difference between transmit power and receiver sensitivity, including any safety margins.
Power Penalty	The total loss introduced by planned-for splices in the fiber link. Typically, extra splices are planned but not immediately implemented .
Presentation Layer	The sixth layer of the OSI model of data communications. It controls the formats of screens and files. Control codes, special graphics, and character sets work in this layer.
Primitive	An element of the services provided by one entity to another.
Print Server	A computer and/or program providing LAN users with access to a centralized printer, in which print jobs are usually handled in the order they are received
Propagation Delay	The time it takes for a signal to travel between two points on the network.
Protocol	A set of rules for communicating peer-to-peer over a computer network. The use of standard protocols allows products from different vendors to communicate on a common network.
Protocol Data Unit (PDU)	Information delivered as a unit between peer entities that may contain control information, address information, and data (e.g., a Service Data Unit (SDU) from a higher layer) or any combination of the three. For example, the FDDI MAC PDUs are Tokens and Frames.
Protocol Filtering	A feature in which some bridges can be programmed to always forward or always reject transmissions that are originated under specific protocols.
Protocol Independent Router	A routing device that provides the functionality of protocol specific routers such as TCP/IP or DECnet routers but is independent of protocols
Public Data Network	A network available to the public for the transmission of data usually using packet switching. See Packet Switching Network.

Receive	The action of a station of accepting a frame, token, or control sequence from the medium.
Receiver	An electrical/optical circuit that converts an electrical/optical signal to an electrical logic signal.
Remote Bridge	A high-throughput device for connecting remote LANs via a wide area network.
Remote File Service (RFS)	A distributed file system protocol development by AT&T and used by other vendors.
Repeat	In token passing networks, a station receives a frame or token from an upstream station, returns it, and places it onto the ring for its downstream neighbor. A repeating station can examine, copy to a buffer, or modify control bits in the frame as appropriate.
Repeater	A physical layer hardware device used on a network to extend the length, topology, or interconnectivity of the physical medium beyond that imposed by a single segment, up to the maximum allowable transmission line length. It performs the basic actions of restoring signal amplitude, waveform, and timing of signals, before transmission onto another network segment.
Restricted Token	A Token denoting a special mode of asynchronous bandwidth allocation, wherein the bandwidth available for the asynchronous class of service is dedicated to a single extended dialogue between specific requesters.
Ring	The topology of a local area network in which the wiring is sequentially connected from one workstation to another. Data is passed from each workstation around the ring in the same direction. Each workstation examines/copies and repeats the data which finally returns to the originating station. Network control is distributed in a ring network.
Ring Management (RMT)	The pan of SMT which ensures the integrity of unique addresses on the FDDI ring.
Router	A device that forwards packets of a specific protocol type (such as IP) from one logical network to another. A router receives physical layer signals from a network, performs data link and network layer protocol processing, then sends the signals via appropriate data link and physical layer protocols to another network.

Sensitivity	The minimum power of an incoming optical signal that is necessary for a receiver to be able to read the signal.
Server	A combination of hardware and software providing a service, such as shared access to a file system, a printer, or an electronic mail system to LAN users or clients.
Service Data Unit (SDU)	The unit of data transfer between a service user and a service provider.
Services	A set of functions, or services, provided by one OSI layer or sublayer entity, for use by a higher layer or sublayer entity or by management entities.
Session Layer	The fifth layer in the OSI Reference Model, responsible for binding and unbinding logical links between users. It manages, maintains, and controls the dialogue between the users of the service.
Shielded Twisted-Pair (STP)	See Twisted-Pair
Simple Network Management Protocol (SNMP)	SNMP is a network management architecture for the needs of the typical internetwork. It can manage virtually any network type and includes non TCP devices such as 802.1 Ethernet bridges. SNMP is widely deployed in TCP/IP (Transmission Control Protocol/Internet Protocol) networks, but actual transport independence means it is not limited to TCP/IP. SNMP has been implemented over Ethernet and OSI transports.
Single Attachment Concentrator (SAC)	A concentrator that offers one Slave port for attachment to the FDDI network and Multiple Master ports for the attachment of stations or other concentrators.
Single Attachment Station (SAS)	An FDDI station that offers one Slave port for attachment to the FDDI network. They are connected to the FDDI ring through a concentrator.
Singlemode	An optical fiber which allows the signal carrying light to travel along only one path. Also called monomode.
Source Address Filtering	A feature of some bridges where messages from designated source addresses are either always forwarded or always rejected.

Source Routing	A method used by a bridge for moving data between two networks. Originally developed by IBM for Token-Ring networks, it relies on information contained within the token to route the packet between the two networks. For source routing to work, every computer and every bridge on all networks must support this protocol. See Bridge. Compare to Transparent Routing.
Source Routing Transparent (SRT)	SRT is a Token-Ring bridging standard jointly sponsored by the IEEE and IBM. Combines IBM Source Routing and Transparent Bridging (IEEE 802.1) in the same unit. This provides a way for universal bridging of Token-Ring LANs supporting IBM and all non-EM LAN protocols. An SRT bridge examines each data packet on the ring to discover whether the packet is using a source routing or non-source routing protocol. It then applies the appropriate bridging method. See Bridge, Source Routing, and Transparent Routing.
Spanning Tree	A method of creating a loop-free logical topology on an extended LAN. Formation of a spanning tree topology for transmission of messages across bridges is based on the industry-standard spanning tree algorithm defined in IEEE 802.1d.
ST Connector	One type of connector used for terminating optical fibers.
Star	A network topology in which each station is connected only to a central station by a point-to-point link, and communicates with all other stations through the central station.
Station	An addressable logical and physical node on an FDDI ring capable of transmitting, repeating and receiving information. A station has one instance of SMT, at least one instance of PHY and PMD, and an optional MAC entity.
Station Management (SMT)	Software and hardware in the FDDI specification which provides control at the station level to manage processes such that the station may work cooperatively on a network
Step Index	A characteristic of fiber optic cable in which the refractive index of the core material is uniform. A sudden change (or step) of the refractive index exists at the core-cladding boundary.
Structured Query Language (SQL)	A standard language for database access. It is evolving as a database standard for client/server computing.
Stuck Beacon	The condition where a station is locked into sending continuous Beacon frames.

Symbol	The smallest signaling element used by the MAC sublayer. The symbol set consists of sixteen data symbols and sixteen nondata symbols. Each symbol corresponds to a specific sequence of code bits group to be transmitted by the Physical layer.
Synchronous	A class of data transmission service whereby each requester is preallocated a maximum bandwidth and guaranteed a response time not to exceed a specific delay.
Synchronous Optical Networking Standard (SONET)	A high-speed (45 Mbps to 1.5 Mbps) transport network standard for optical media. The protocol is hierarchical in structure.
System Network Architecture (SNA)	The proprietary architecture developed by IBM for mini and mainframe computers. SNA may be viewed as three distinct byte related entities: a specification, a plan for constructing a network, and a set of products. SNA is a specification governing the design of products for an SNA network. It is called an architecture because it specifies the operating relationships of those products. SNA provides a structure that enables users to establish and manage their networks and, in response to new requirements and technologies, to change or expand them. SNA may be viewed as a set of products: hardware and programs designed to the SNA specifications. A digital transmission link with a capability of 1.544 Mbps. T1 uses two pairs of normal twisted wires to handle 24 voice channels, each one digitized at 64 Kbps. T1 is usually provided by phone companies and used for connecting networks across remote distances.
T1	A digital transmission link with a capability of 1.544 Mbps. T1 uses two pairs of normal twisted wires to handle 24 voice channels, each one digitized at 64 Kbps. T1 is usually provided by phone companies and used for connecting networks across remote distances.
Target Token Rotation Time (TTRT)	The target time for the token to pass every FDDI node in the token path. The value used by the MAC receiver to time the operations of the MAC layer. The TTRT value varies, depending on whether or not the ring is operational.
Terminal	A personal computer or diskless workstation connected to a mainframe that acts as a keyboard and display, using the mainframe processor to execute mainframe applications.

Thin Ethernet	A coaxial cable (0.2-inch, RG58A/U 50-ohm) that uses a smaller diameter coaxial cable than standard thick Ethernet. Thin Ethernet is also called "CheaperNet" due to the lower cabling cost. Thin Ethernet systems usually have transceivers on the network interface card, rather than in external boxes. PCs connect to Thin Ethernet bus via a coaxial "T" connector.
Throughput	The amount of useful and non-redundant information which is transmitted or processed.
Timed-Token Protocol	The rules defining how the target-token-rotation-time (TTRT) is set, the length of time a station can hold the token, and how the ring is initialized.
Token	In networking, an explicit indication of the right to transmit on a shared medium. On a Token Ring, the Token circulates sequentially through the stations in the ring. At any time, it may be held by zero or one station. FDDI uses two classes of Tokens; restricted and non-restricted.
Token Holding Timer	A timer that controls the amount of time a station may hold the token in order to transmit asynchronous frames.
Token Passing	A protocol used to assure the orderly transmission and reception of data on a local area network. A data packet, called a token, is passed around the network from computer to computer in a specific sequence. The token is usually a few bytes (3 bytes) long, and conveys the exclusive right to transmit on the network. If a computer has something to send and the token is available, the computer "attaches" its message to the token, along with source and destination addresses. When the package of token and message reaches its destination, the computer copies the message. The package is then put back on the network where it continues to circulate until it returns to the source computer. The source computer then removes the returned packet and then releases the token for the next computer in the sequence. One device on the network designated the token monitor, generates the token. If that device is turned off or fails, another device will assume monitoring of token generation. See Token, Token-Ring, and FDDI.

Token-Ring	The IEEE 802.5 and IBM's LAN technology that uses the token passing access method, is logically configured as a ring, but often physically wired in a star configuration. In a star configuration, each station is wired directly to a device called a multi-station access unit (MAU). The MAU automatically recreates the ring in case of a failure on one of the ports. Token-Ring LANs can operate at transmission rates of either 4Mbps or 16Mbps
Token-Ring Card	Name given to the circuit board inserted into a computer device for connection to a Token-Ring LAN. This board provides the physical connection to the LAN. It also participates in the collective management of the token by sending various messages to other Token-Ring cards. Usually, one Token-Ring card on the network is the token monitor. The sending of messages between Token-Ring cards can be used to gather information about network activities.
Token Rotation Timer (TRT)	A clock that times the period between the receipt of tokens.
Topology	A map of the network, describing how it is configured and how the transmissions flow. The principle network topologies are star, bus, and ring.
Trace	In FDDI, diagnostic process to recover from a stuck-Beacon condition. The fault is localized to the Beaconsing MAC and its upstream neighbor MAC.
Transceiver	A combined transmitter and receiver, required at each node of a LAN .
Translating Bridge	A nonproprietary MAC layer device used to connect similar and dissimilar LANs according to 802.1d rules.
Transmission Control Protocol	As specified in RFC-793, TCP is a transport layer, connection-oriented end-to-end protocol. It provides reliable, sequenced, and unduplicated delivery of bytes to a remote or local user. TCP provides reliable byte stream communication between pairs of processes in hosts attached to interconnected networks.
Transmission Control Protocol/Internet Protocol (TCP/IP)	Protocols developed by the Department of Defense to link computers from multiple vendors across networks. It works at the third through fifth layers of the OSI model.

Transmit	The action of a station that consist of generating a frame, token, or control sequence, and placing it on the medium to the next station.
Transmitter	An electrical/optical circuit that converts an electrical logic signal to an electrical/optical signal.
Transparency	In data communications, a condition that allows equipment to send and receive bit patterns of virtually any form. The user is unaware that he/she is transmitting to a machine that receives faster or slower, or transmits to him faster or slower, or in a different bit pattern.
Transparent Routing	A method used by a bridge for moving data between two networks. With this type of routing, the bridge determines which computers are operating on which network. Then it routes packets between networks appropriately. See also Bridge, SRT and Source Routing.
Transport Layer	Layer 4 in the OSI data communications model that, along with the underlying network, data link and physical layers, is responsible for the end-to-end control of transmitted information and the optimized use of network resources . Also serves the session layer.
Transport Medium	The actual medium over which transmission takes place including copper wire, fiber optics, microwave and satellites.
Twisted-Pair Cable	Two insulated copper wires twisted around each other to reduce induction (and thus interference) from one wire to the other. Several sets of twisted pair wires may be bundled in a single cable. Shielded Twisted-Pair (STP) has a shielding wrapped around the insulated wires for greater interference immunity. Unshielded Twisted-Pair (UTP) which does not have shielding, is commonly used in modem telephone wiring systems.
Unshielded Twisted-Pair	See Twisted-Pair Cable.
Upstream	A term that refers to the relative position of two stations in a ring. A station is upstream of its neighbor if it receives the token before its neighbor received the token.
Valid Transmission Timer	A timer that times the period between valid transmissions on the ring; used to detect excessive ring noise, token loss, and other faults.

Wavelength	A measurement of the length of any electromagnetic wave The shorter the wavelength, the higher the frequency.
Wide Area Network (WAN)	A voice data network that extends a LAN (local area network) outside the building or facility, using telephone common carrier lines to other LANs on a regional, national, or international basis. The connection between a LAN and WAN is typically made using a bridge or a router. Usually not owned by the user.
Window	As relates to a fiber optic cable, a window refers to a wavelength region of relatively high transmittance, surrounded by regions of low transmittance.
Wiring Technology	The communication protocol-cabling combinations required for laying out a network.
Workgroup	A network configuration characterized by the small number of attached devices spread over a limited geographical area.
Workstation	A high-performance desktop computer which is most often used by technical applications such as CAD, mathematical modeling, and programming, etc. Typically comprised of high resolution screens, local graphics processing, keyboard, pointing device, and network connection.
X3T9.5	The ANSI committee responsible for specifying the FDDI standard.