Contents

Click Contents button to display the Content List.

Introducing NetXRay

Welcome

Registering NetXRay

Please complete the registration form included in the shipping package. You can either fax it or mail it to Cinco Networks, Inc. using the Fax Number or Mailing address printed on the registration form.   Registration ensures that you receive product support, product update information, and other benefits.

Licensing Agreement

NetXRay SOFTWARE LICENSE AGREEMENT
Please read this License carefully.

You are purchasing a license to use the NetXRay Software. The Software is owned by and remains the property of Cinco Networks, Inc. is protected by international copyrights, and is transferred to the original purchaser and any subsequent owner of the Software media for his/her use only according to the license terms set forth below. Opening the packaging and / or using the Software indicates your acceptance of these terms. If you do not agree to all of the terms and conditions herein return the Software, manuals and any partial or whole copies you have made within thirty days of purchase to the party from whom you purchased it for a refund, subject to our restocking fee.

1. Grant of License: Cinco Networks, Inc. (Cinco Networks), grants the original purchaser (Licensee) the limited rights to possess and use the Cinco Networks NetXRay (Trademark pending) Software (Software) and User Manual, on the terms and conditions specifically set out in this License.

2. Term: This License is effective as of the time Licensee receives the Software, and shall continue in effect until Licensee ceases all use of the Software and returns or destroys all copies thereof, or until automatically terminated upon the failure of Licensee to comply with any of the terms of this License.

3. Your Agreement:

Single User License

- The Software is provided under a Single User License. This means that one specific individual is licensed to install and use the Software on his/her PC. That specific individual may also use the Software on his/her portable or home computer.
- If the Software is installed on a networked system, or on a computer connected to a file server or other system that physically allows shared access to the Software, Licensee agrees to provide technical or procedural methods to prevent use of the Software by more than one user.

Multiple Users License

- If you want to install the Software on a network and provide access for more than one user, you can purchase additional single-user licenses. Each additional single-user license allows one other specific individual to install and use the Software. There is no limit to the number of additional single-user licenses that may be purchased.
- Additional single-user licenses are not concurrent-user licenses (that is, each additional single-user license is associated with a specific individual). There is no restriction on the number of additional single-user licensees who may access the Software at any given time. For example, a group of 25 users who want access to a single copy of the Software must purchase 24 additional single- user licenses so the entire workgroup has access (e.g., 25 licenses total). If only 5 specific individual users want access the Software, 4 additional user licenses would be sufficient (e.g., 5 licenses total).

- One machine-readable copy of the Software may be made for BACK-UP PURPOSES ONLY, and the copy shall display all proprietary notices, and be labeled externally to show that the back-up copy is the property of Cinco Networks, and that its use is subject to this License. Documentation in whole or part may not be copied.

- Licensee may transfer its rights under this License, PROVIDED that the party to whom such rights are transferred agrees to the terms and conditions of this License, and written notice is provided to Cinco Networks. Upon such transfer, Licensee must transfer or destroy all copies of the Software.

- Licensee agrees and certifies that neither the Software nor any software product containing code generated by the Software: (a) is being or will be shipped, transferred or re-exported, directly or indirectly, into any country prohibited by the United States Export Administration Act and the regulations thereunder, or (b) will be used for any purpose prohibited by same.

- Except as expressly provided in this License, Licensee may not use, copy, disseminate, modify, distribute, sub-license, sell, rent, lease, lend, give or in any other way transfer, by any means or in any medium, including telecommunications, the Software. This license is for machine readable object code only, and Licensee will not attempt to disassemble, de-compile, or otherwise reconstruct the source code of the Software. Licensee will use its best efforts and take all reasonable steps to protect the Software from unauthorized use, copying or dissemination, and will maintain all proprietary notices intact.

4. LIMITED WARRANTY

Cinco Networks warrants the Software media to be free of defects in workmanship for a period of ninety days from purchase. During this period Cinco Networks will replace at no cost any such media returned to Cinco Networks, postage prepaid. This service is Cinco Network's sole liability under this warranty. LICENSE FEES FOR THE SOFTWARE DO NOT INCLUDE ANY CONSIDERATION FOR ASSUMPTION OF RISK BY CINCO NETWORKS OR ITS LICENSOR, AND CINCO NETWORKS AND ITS LICENSOR DISCLAIM ANY AND ALL LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR OPERATION OR INABILITY TO USE THE SOFTWARE, OR ARISING FROM THE NEGLIGENCE OF CINCO NETWORKS AND ITS LICENSOR, OR THEIR EMPLOYEES, OFFICERS, DIRECTORS, CONSULTANTS OR DEALERS, EVEN IF ANY OF THESE PARTIES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHERMORE, LICENSEE INDEMNIFIES AND AGREES TO HOLD CINCO NETWORKS AND ITS LICENSOR HARMLESS FROM SUCH CLAIMS. THE ENTIRE RISK AS TO THE RESULTS AND PERFORMANCE OF THE SOFTWARE IS ASSUMED BY THE LICENSEE. THE WARRANTIES EXPRESSED IN THIS LICENSE ARE THE ONLY WARRANTIES MADE BY CINCO NETWORKS AND ITS LICENSOR, AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND OF FITNESS FOR A PARTICULAR PURPOSE. THIS WARRANTY GIVES YOU SPECIFIED LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF WARRANTIES, SO THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU.

5. General

This License is the complete and exclusive statement the agreement of the parties. Should any provision of this License be held to be invalid by any court of competent jurisdiction, that provision will be enforced to the maximum extent permissible, and the remainder of the License shall nonetheless remain in full force and effect. This License shall be controlled by the laws of the State of California, and the United States of America.

6. United States Government Restricted Rights

Use of the Software by any department, agency or other entity of the United States Federal Government is limited as follows:

(1) The Software and User Manual are provided with RESTRICTED RIGHTS, and are trade secrets of Cinco Networks for all purposes of the Freedom Of Information Act.

(2) Use, duplication or disclosure is subject to restrictions set forth in subparagraph (c)(l)(ii) of the Rights in Technical

Data and Computer Software clause at 252.227-7013 or in subparagraphs (c)(1) and (2) of the Commercial Computer Software - Restricted Rights at 48 CFR 52.227-19, as applicable. Manufacturer: Cinco Networks, Inc., 1102 Lund Ranch Road, Pleasanton, CA 94566.

(3) If the Software was acquired under a GSA Schedule, the Government has agreed to refrain from changing or removing any insignia or lettering from the Software or Documentation or from producing copies of the manuals or disks (except for backup purposes) and: (a) Title to and ownership of the Software and Documentation and any reproductions thereof shall remain with Cinco Networks and its licensor; (b) use of the Software shall be limited to the facility for which it is acquired; and (c) if the use of the Software is discontinued at the original installation and the Government wishes to use it at another location, it may do so by giving prior written notice to Cinco Networks, specifying the new location site and class of computer.

(4) Government personnel using the Software, other than under a Department of Defense contract or GSA Schedule, are hereby on notice that use of the Software is subject to restrictions that are the same or similar to those specified above.

Technical Support

Before you contact Cinco Networks for technical support, please fill in all appropriate information for your NetXRay technical support request, bug report, or product suggestion completely and provide us with exact and specific details. A technical support request form in .WRI format is provided for you under NetXRay directory. The more specific and detailed your information is, the better we will be able to help you.

Display the NETXRAY.EXE About box to report the version number of your software. **Every Technical Support request must include a NetXRay version number.**

Before, sending your questions, please view the README file

After you complete the form, save the file to disk or print it on your printer. There are three ways that you can forward this information to us:

1. FAX the printed file and any attachments to (770) 390-9947, to the attention of "NetXRay Technical Support."

2. Send the file and any floppy disks (if necessary) by mail/Fed Ex to:

   NetXRay Technical Support
   Cinco Networks, Inc.
   1340 Center Drive, Suite 103
   Atlanta, GA 30338

3. E-mail to us via

Compuserve:	70530,3661
Internet:	sales@cinco.com

Overview

Packet Capturing and Decoding

NetXRay is capable of capturing all packets at near wire speed. When used with various address, protocol, and data pattern filters, it allows you to capture and pinpoint network trouble areas accurately and effectively. The **IP address filter** provides a powerful means to capture conversations between nodes that span across routers.

NetXRay decodes all major protocols. It provides SNMP decode to help you see standard and proprietary MIB OID names and enumerate symbolic names. NetXRay also supports SNMP over IP, IPX, and MAC.

Viewing packets is a pleasure with NetXRay. With multi-thread design to support decode and display simultaneously, the packets display immediately after you open the captured buffer or file, no matter how large it may be. Protocols are displayed in color coded summary, detail, and hex panes, and each may be individually sized and positioned. NetXRay’s address book provides a method to associate a hexadecimal hardware address with its more human-readable symbolic name. It is used in designing filters and displaying decodes and host table.

Monitoring Network Statistics

NetXRay provides real time view and long term traffic analysis in graphical format. It is capable of monitoring multiple network statistics variables concurrently, allowing you to predict future network needs and plan for them accordingly. Alarms are generated anytime preset threshold parameters are exceeded, informing you about network exception conditions requiring immediate attention.

NetXRay monitors and displays network segment's packet rate, utilization and error rate in real time. Statistical counters for all network detail parameters are maintained in memory and may be exported to Excel format for tabulation or charting. Each network node's traffic pattern in total input/output packets and octets are kept in the host table, and may be viewed in real time. The host table may be sorted by any statistical variable of your choice, in either ascending or descending order. It's easy to view traffic load patterns among all network nodes.

NetXRay Matrix tracks conversation traffic statistics between pairs of network nodes. The total packets and octet counts are maintained.

NetXRay Protocol Distribution function allows the reporting of network usage based on the network protocols, i.e. IPX/SPX, TCP/IP, NetBIOS, AppleTalk, DECnet, SNA, Banyan and others in real time; it also supports for 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, POP2, POP3, HTTP (WWW), Gopher, NNTP, SNMP, X-Window, and others.

Generating Traffic Load

NetXRay's traffic generator is a great tool for application developers and anyone else who needs to test network hardware and software components. NetXRay will play back captured packets one at a time or in a batch. Individual packet may be edited before transmission. You may modify the time delay between packets to generate various traffic loads, and packets may be played back continuously. NetXRay also allows **transmitting and capturing packets simultaneously**, giving you greater savings in equipment and desk space.

Taking Advantages of Windows 95 Features

NetXRay is written as a true Windows 95 application, including a Windows 95 compliant graphical user interface. It supports many advanced features including property page, drag & drop, split windows, tab view, context menus, long file names, tool tips, and dockable windows. Standard Win95 installation and de-installation support is also included.

Since Win 95 supports true 32 bit multi-tasking, data capture and network monitoring may occur concurrently with other applications running. In fact, NetXRay is capable of capturing network traffic transmitted by or received by other applications running in the same computer at the same time

NetXRay's interactive Help function is tightly integrated into Windows 95 environment and supports many advanced Help functions previously unavailable under Windows 3.1**.**

Setup

Installing and Setting Up Network Adapter

If your have already installed your own network adapter that supports NDIS 3.0/3.1, skip this topic.

If you have purchased a network adapter from other sources, follow the manufacturer's guide to install and setup the adapter for Win95 system.

Installing NetXRay

1. Insert NetXRay Disk 1 in the floppy drive.
2. Click the Start button, then click Run....
3. Enter ‘a:setup’ if Disk 1 is in drive a. Otherwise enter the appropriate drive letter.
4. Click OK.

Follow the instructions on your screen until NetXRay is installed successfully.

- OR -

1. Double click the My Computer icon.
2. Double click the Control Panel Folder.
3. Double click the Add/Remove Programs icon.
4. Click Install... button, follow the instructions on your screen until NetXRay is installed successfully.

Notes

- NetXRay installation program is Win95 and Windows NT compliant. It places standard entries into the Registry and creates program icons under the recommended Programs menu. To un-install NetXRay, see Related below.

Installing Copy Protection Key

Running NetXRay requires the installation of a small hardware device (protection key) on your PC’s parallel printer port. The installation procedure is very simple and requires little efforts on your part. The protection key functions as a pass-through device for your printer operation. It will not interfere with normal print function. NetXRay protection key can be attached to LPT1, LPT2, or LPT3 port.

1. Locate an empty DB-25 parallel printer port on your PC. If your PC has only one Printer port and is currently connected to a printer cable, disconnect it.
2. Connect the pin side (male) of the protection key to the printer port.
3. Turn the thumb screws, and secure the protection key on the printer port.
4. If you have disconnected the printer cable in Step 1, re-connect the cable to the female side of the protection key.
5. Now you are ready to start NetXRay.

Notes

- If you have other hardware type protection key already in place, disconnect it and place NetXRay protection key between the parallel port and disconnected key.

Un-installing NetXRay

1. Double click the My Computer icon on the Windows desktop.
2. Double click the Control Panel Folder.
3. Double click the Add/Remove Programs icon.
4. Click NetXRay to select.
5. Click Add/Remove.... button to start removing NetXRay.
6. Click OK, when un-install completes.

Notes

- NetXRay will create additional data files in its local directory. Uninstall program is not aware of their presence, and will not be able to remove them. You need to manually review and remove them yourself.

How To....

Start NetXRay

Invoking NetXRay

1. Click the Start button, and then point to Programs.
2. Click the NetXRay program to start it.
3. If you have more than one NDIS 3.1 compliant adapters installed in the system, an Adapter dialog box will be displayed to ask you to select a network adapter as the target network for NetXRay to monitor.

Tip

- If you selected 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 wish to monitor traffic between your PC’s and the remote host or server.

Arranging the Dockable Windows

Packet Viewer, Dashboard, and Packet Generator all have two types of display characteristics; dockable, and normal MDI.

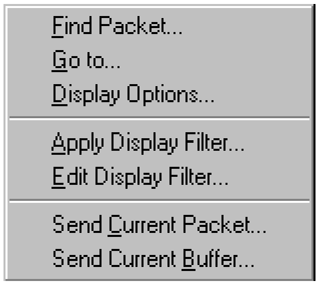
Dockable window is a new feature in Windows 95. It has characteristics very similar to the Tool Bar. It always stays on top of other MDI windows, and will be visible all the time. When it is dragged and attached to the border of the main window, it will dock (merge) with the border. To undock the window from the border, click on the small stripe between the border of the inside box and the border of the dockable window, a black rectangular box will be visible. (Picture showing is necessary)   Hold the mouse button, and press the Control key down, you can drag the window out of its docking position.

Unless you have a large windows space, and wish to view these windows at all time, you can configure them into normal MDI windows. To change dockable windows back to normal MDI window, click the right hand button of your mouse to bring up a context menu. A context menu is shown, select MDI window.

Alternatively, go to Tools/Options.... and click Workspace tab. Uncheck the ones you wish to turn into MDI windows.

Using Context Menu

Context menu is invoked when you press on the right hand button of your mouse. It is short cut to get to some of the menu commands.



The menu displays a list of commands that you can use to perform operation on this object (window). It general lists all the commands in the main menu that are relevant to the object, and a few extra short cuts.
Select you choice by click on the context menu line.

Capture Packets

Capturing All Network Packets

1. From the View menu bar, Click Capture. A Capture window is displayed.
2. Select Default from the profile list box.
3. Click ▶ to start capture. The capture gauge shows the capture status in progress.
4. Capture will stop when the buffer is full (default 256 K bytes). Or Click ■ to stop the Capture.
5. If you want to pause the capture, click ⏸ to pause temporarily. Then Click ▶ to resume capture again.

Tip

- The default profile shipped with NetXRay has no capture filter set, and the capture buffer is set at 256 K bytes. The buffer full action is set to stop capture.
- The Capture window displays current capture progress status in # of packets captured and % of the buffer space full. You can view the data in either graphic or tabular form by clicking the Gauge or the Detail tab.

Capturing Conversation Over IP Routers

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 new profile name, e.g., my IP filter. Click OK.
4. Click the Done button to close the Profile dialog box.
5. Select IP from the Address Type list box.
   Click the Include radio button.
6. Enter the first IP address (e.g. 192.44.81.128) under Station 1.
   Enter the second first IP address (e.g. 192.55.90.133) under Station 2.
   Select 🖳↔🖳 (both directions).
7. Click OK. You have just setup a capture filter profile: my IP filter to capture conversation between a pair of IP stations.
8. Click ▶ to start capture.

Tip

- Using the Address Book facility, you can pre-assign logical name and IP address for each host or server in your network. Then you can simply find the host name you wish to use from the address book list box , and drag it to the station cell in the address filter.
- If you wish to capture traffic to and from only one station, enter ‘any’ into Station 1 or Station 2.

Capturing Unique Protocol Packets

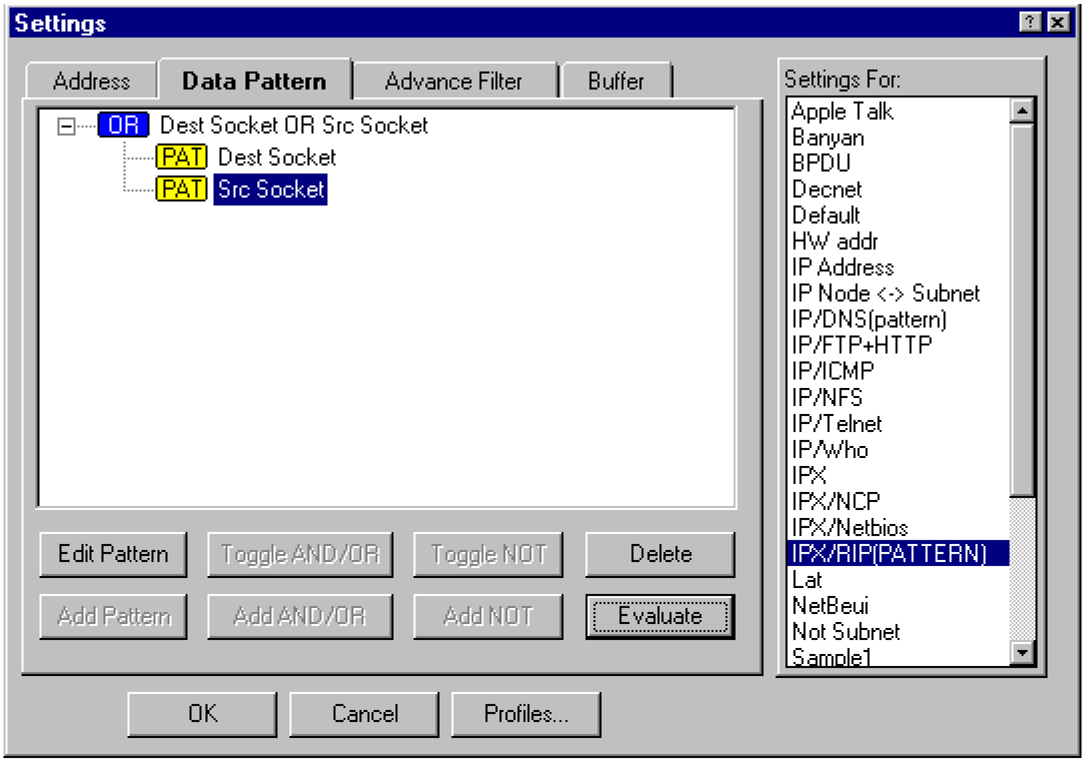
NetXRay has an unique ability to setup Advance Filter to capture packets that match one of the protocol or sub-protocol types. The procedure listed below shows the steps to capture IPX packets.

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 new profile name, e.g., my IPX filter. Click OK.
4. Click the Done button to close the Profile dialog box.
5. Click the Advance Filter property page tab.
6. Select IPX from the Available Protocols list box.
7. Click OK.
8. Click ▶ to start capture.

Capturing Packets Matching Certain Data Pattern

NetXRay has an unique ability to setup Data Pattern Filter to capture packets that match only a certain data pattern. The procedure listed below shows the steps to capture IPX RIP packets.

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 new profile name, e.g., IPX/RIP(PATTERN). Click OK.
4. Click the Done button to close the Profile dialog box.
5. Click the Advance Filter property page tab.
6. Select IPX from the Available Protocols 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 Offset field. (Hint: 16 bytes offset from beginning of IPX packet is the Destination Socket field).
11. Enter 2 in Len field. Select Hex from Format field. Enter hex number 04 at column 0 row 1, then 53 at column 1 row 1. (Hint: 0453 hex is the socket number for IPX/RIP).
12. Enter a symbolic name in the Name field, e.g. 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 Offset field. (Hint: 28 bytes offset from beginning of IPX packet is the Source Socket field).
17. Enter 2 in Len field. Select Hex from Format field. Enter hex number 04 at column 0 row 1, then 53 at column 1 row 1. (Hint: 0453 hex is the socket number for IPX/RIP).
18. Enter a symbolic name in the Name field, e.g. 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.



Dest Socket OR Src Socket

Dest Socket

Src Socket

Notes

- Using capture filter requires additional CPU processing time to examine each packet for matching criteria. In a network with heavy traffic load, you may miss packets. To avoid losing packets, you can use capture all traffic, then apply display filter to select the packets you want to see. Or you can use high performance PCI network adapter cards

Create New Filter Profile from Existing Profile

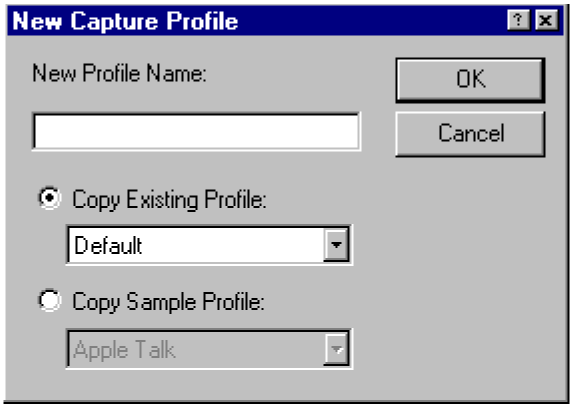
Copying Existing Profile

NetXRay uses the same set of filter profile for packet capture and for post filtering of captured packets during packet viewing. NetXRay comes with a pre-defined set of sample filter profiles that you can copy into your own profile name during filter creation. Alternatively, you can copy from the existing filter defined by yourself.

NetXRay maintains a sample filter set in file NXSAMPLE.CSF, and current filter set in a separate file NETXRAY.CSF. If you wish to use sample filters created by others, you need to save NXSAMPLE.CSF first, then copy the filter profile NETXRAY.CSF created by others into NXSAMPLE.CSF.

To copy filter from existing filter profile:

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 to bring up the New Capture Profile dialog,



New Capture Profile

New Profile Name:

● Copy Existing Profile: Default

○ Copy Sample Profile: Apple Talk

4. Enter a new profile name, e.g., my IPX filter.
5. Click the appropriate radio button depending on whether you wish to copy from Existing Profile or from Sample Profile.
6. Open the combo box. Scroll the list to pick a filter to copy. Click OK.
7. Click Done to return to the Capture Setting dialog box.
8. Now you can proceed to make other changes.

Display and Save Captured Packets

Displaying Captured Packets

1. From the Capture window, click the Stop and View button or View button to bring up the Packet Viewer window.

Tip

- While packet capturing is in progress, only the button will be active.

Saving Captured Packets to File

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

1. Select File from the Menu bar, click on Save As.... A Save As dialog box is 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. Click OK.

Marking Packets for Separate Viewing

To mark packets of your choice,

1. Simply click the check box in front of the index number
2. Click the rihgt hand mouse to bring up the context menu. Select Saved Marked....
3. A new packet viewer window is shown with only the marked packets.

Optionally, you can save these packets for later review, or use it as source file for packet playback.

Displaying Packets from Capture File

1. Select File from the Menu bar, click on Open... A File Open dialog box is 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. Click OK.
3. A Packet Viewer window is displayed.

Use Display Filter in Packet Viewer

Specifying Protocol Display Filter

Display filter allows you to filter out unwanted packets from the captured buffer. The profile defined for capture filter can also be used for filtering out packets from the packet viewer. Defining a display filter is identical to the procedure of that a capture filter. To create or change a filter,

1. Choose Edit Display Filters.... from the Packet menu.
2. A Setting property dialog box is displayed. Follow the same procedures as in defining the capture filter to specify your display filter

Applying Display Filter

To apply display filter,

1. Choose Apply Display Filters.... from the Packet menu.
2. A Post Filter property dialog box is displayed.
3. Select a previously defined filter from the list. And click OK.
4. A new packet viewer window is displayed with the packets that match the filter criteria you specified. If no packet that matches the criteria, a “No packets!” dialog box is displayed .
5. You can now view or save the contents in the packet viewer.

Customize and Use Packet Viewer

Setting Up Protocol Color Highlight

The packets in summary pane can be colored coded based on their protocol type. This feature allows you to group packets with the same protocol or sub-protocol reference, and to assist you visually in identifying the packets of you choice. To set up protocol color highlight,

1. Choose Display Options... from the Packet menu. An Options property dialog box is displayed.
2. Click and select the Summary Color tab.
3. Select and click on the protocol type you wish to change color display.
4. Select the Text and the Background color of you choice. The protocol type color will change to reflect your selection.
5. When you are satisfied with the color selection, click OK.

Using One Line Protocol Summary in Detail Window

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 sub-layer 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.

The expand or contract state of each sub-protocol field is ‘memorized’ by the packet viewer. The same state for that sub-protocol will be maintained, when you view the next or the previous packet. For example, 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 sub-protocol, follow these steps:

1. Choose Display Options... from the Packet menu. An Options property dialog box is displayed.
2. Click and select the Protocol Display tab.
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 on the Close All button will do the opposite to set all protocol layers in contracted view.
5. When you are satisfied with the selection, click OK.

Anchoring a Selected Field in Detail Window

By simply click on a selected field or protocol summary line to highlight it, you have anchored that 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 user to go back and forth between several packets without having to re-position the detail pane by using scroll bar.

Viewing Packets

Packet Viewer is a MDI child window that contains three separate panes for Summary, Detail, and Hex. Each pane can be re-sized by click and drag the separator bar between the panes. Each pane contains scroll bars that you can use the mouse to manipulate the viewing position in the pane. Cursor, page up and down keys can also provide the similar function for the pane window that has the focus.

To maximize the efficiency in scanning packets for details, we recommend you follow the tips 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/down keys will now apply to the detail pane.
- Use F7 key to move to the previous packet. Use F8 to the next packet.
- If you wish to move the viewing area in the detail pane, use cursor, and page up/down keys.

Generate Network Traffic

Sending a Single Packet

Packet generator gives you the ability to send data packets back to the network. It can be used to produce packets to feed your application for testing, or to generate traffic load onto the network. To start the packet generator,

1. Choose Packet Generator from the Tools menu. A packet generator window is displayed.
2. Click the 0101 Send New Packet button. A Send new packet dialog page is displayed.
3. Click the Size button to adjust the size of your packet.
4. Edit the packet contents in the hex window.
5. Choose between send continuously, or send a number of times.
6. Select the delay time in # of milliseconds.
7. Click OK to start packet generation.
8. Click the Anim tab to view the packet generator progress in animated graphic mode. Please note that the rate of the small ball going through the network link does not reflect the speed of transmission. You can also click the Detail tab to see actual transmission rate.
9. click the 🟥 button, if you wish to stop the transmission of packets.

Notes

- If you have a PCI NIC card, pick zero delay time will give you maximum traffic load. Zero delay is NOT allowed for ISA NIC card, because ISA NIC card lacks the performance feature to sustain high rate of packet generation.
- Click the Decode tab gives you instant analysis of the data pattern you just entered in decoded form.

Playing Back a Captured File

1. Choose Packet Generator from the Tools menu. A packet generator window 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. Click OK.
4. 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. Please note that the rate of the small ball going through the network link does not reflect the speed of transmission. You can also click the Detail tab to see actual transmission rate.
9. click the 🟥 button, if you wish to stop the transmission of packets.

Tips

- You can also click the to edit and send a single packet from the capture file.

Manage Address Book

Creating an Entry

The Address Book allows you to pre-define your network nodes in human readable symbolic names. NetXRay uses the address book in Filter definition, Packet Viewer, and Host Table. NetXRay replaces the 6 byte hardware address of the network node with its respective symbolic name.

1. Select Address Book from the Tools menu. An Address Book window is displayed.
2. Click the right hand button of the mouse, a small context menu is shown.
3. Click New... to invoke a New/Edit Address dialog box.
4. Enter the Name, and Hardware address. Other entries are informational only. NetXRay does not interpret them.
5. Click Save to add the new entry in the Address Book, Or click Save and Next to save and continue adding another entry.
6. When you complete entering all new entries, you can close the address book, or leave it on the window.

Modifying an Entry

1. Select Address Book from the Tools menu. An Address Book window is displayed.
2. Select the entry of your choice by pointing and clicking the row to highlight the selection
3. Click the right hand button of the mouse, a small context menu is shown.
4. Click Edit... to invoke a New/Edit Address dialog box.
5. Enter the Name, and Hardware address. Other entries are for user reference only. NetXRay does not interpret them.
6. Click Save to add the new entry in the Address Book, Or click Save and Next to save and continue adding another entry.

Importing an IP Host Table

NetXRay provides a sample Basic script to let you import an IP host table containing entries of IP address, hardware address and its corresponding host name into NetXRay Address Book without having to enter them one-by-one. The sample Basic script ‘Ripcsv.bas’ and the sample IP host table ‘Ipdbsamp.csv’ are located in NetXRay program directory. The sample IP host table is a comma-separated-value 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. The NetXRay has a capacity of 5,000 entries in Address Book.

To import the sample IP host table,

1. Select Run Macro... from the Tools menu.
2. Select ‘Ripcsv.bas’ from the dialog box, then click Open.
3. From the Open dialog box, Select ‘Ipdbsamp.csv’, click Open.
4. The IP address and the associated fields will be added to the Address Book.

If you are an experience Basic programmer, you can modify the sample Basic script to suit your need. **However, the built-in Basic interpreter does not contain debugging facility. Trouble-shooting any mistakes you made will be difficult.** We recommend you to visit Cinco Web site at WWW.CINCO.COM to retrieve additional Basic scripts that might handle your particular address table format. If you have special requirements, please contact Cinco Sales at (770)-671-9272, or e-mail to sales@cinco.com.

Tip

- If you wish to save the current address book and create a new one, simply close NetXRay first. Then rename the file ‘NetXRay.nab’ under ‘netxray\program’ directory. The next time you invoke NetXRay, an empty address book will be created.

Arrange Host Table Viewing Format

Sorting the Contents of a Field Counter

You can sort the host table entries by the contents of a particular counter. By sorting the table in descending order, the host table gives you a better view of which are the most active nodes in transmitting or receiving certain types of packets

- Click the table's column heading will sort the table in descending order based on the contents of the selected field.
- Hold the Control key, and then click the table's column heading will sort the table in ascending order.

Notes

- The default sorting order of the address field is the reverse of the counter fields, i.e., clicking address field header will sort in ascending order.

Learn IP Addresses and Domain Names in Your Network

Auto-discovering IP Addresses and Domain Names

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 table. 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 in your network. Since 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. This router characteristics makes the IP address auto discovery process difficult if the user does not manually identify the router in the address book first. The key is to enter your IP network routers' IP address, hardware address, and domain name in the address book first, and select the node type as Router.

The proper steps to perform IP address and DNS name discovery are listed below:

1. Click Auto Discovery button on the Address Book window.
2. Click the Range (IP Address) radio button, enter the local subnet address where NetXRay is monitoring. Click OK.
3. A small modeless dialog will show you the discovery in process. When the search is finished, The dialog box will be removed.
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 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 DNS name will be entered to replace the name field.

Once you have identified the local nodes and the routers, you can optionally use NetXRay to monitor and attempt to resolve any IP node's domain name. To do this, follow these steps:

1. Click Auto Discovery button on the Address Book window.
2. Click the Any IP address on the network radio button. Click OK.
3. A small modeless dialog 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 name is not found the IP address is dropped, and not entered in the address book.
4. To stop the discovery, click the Cancel button on the modeless dialog box.

Note

- Auto discovery function makes use of Microsoft TCP/IP ICMP.DLL. If you have not installed Microsoft TCP/IP, Auto Discovery will fail with an error message displayed.
- Some network systems use Dynamic IP address assignment. Using the Auto Discovery will not be very useful, since the IP address for a network node can change from time to time.

Detecting Duplicate IP Address

By using the Auto-discovery of IP address in your network, you can detect duplicate IP addresses. This feature is a very useful tool for network administrators. NetXRay can fore warn you about the presence of a duplicate IP address and its associated hardware address. A duplicate IP address can potentially causing other network nodes to malfunction, and it is important this problem to be discovered and fixed immediately.

To start duplicate IP address detecting, you must auto learn your network's IP addresses and save them in the address book as described in **Auto-discovering IP Addresses and Domain Names** first. Then,

1. Click Auto Discovery button on the Address Book window.
2. Click the Any IP address on the network radio button. Click OK.
3. A small modeless dialog 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 name is not found the IP address is dropped, and not entered in 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.
4. To stop the discovery, click the Cancel button on the modeless dialog box.

Use Advanced NetXRay Features

Monitoring More Than One Network Adapters Concurrently

NetXRay allows user to launch multiple copies of NetXRay with each one monitoring a separate adapter. To launch a new NetXRay,

1. Go to Programs, then Click NetXRay icon. An Adapter dialog box is shown.
2. Click New Probe button to bring up a New Probe dialog box.
3. Enter description, select Local Probe radio button, then click OK. Optionally, you can copy a work space setting for the new probe from the existing probes. Click open the combo list box and select an existing probe as the source to copy from. A probe's work space setting includes the address book, capture filter setting, packet display options, update frequency, alarm thresholds.
4. Now select an adapter which is not being monitored by another NetXRay session., Click OK.
5. Wait a few seconds, a new NetXRay session is created to monitor the selected adapter.

Once you have created multiple local probes, you can simply launch new NetXRay session without creating new probes again.

Maintaining Multiple NetXRay Setting Files

If you are a network support personnel maintaining multiple sites, the NetXRay multiple work space feature lets you maintain separate address book, and other setting for each site conveniently. Since 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. You can create a new local probe named after each site that you manage.

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 description, select Local Probe radio button, then click OK. Optionally, you can copy a work space setting for the new probe from the existing probes. Click open the combo list box and select an existing probe as the source to copy from. A probe's work space setting includes the address book, capture filter setting, packet display options, update frequency, alarm thresholds.
4. Now select an adapter, Click OK.

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 name.
3. Now select an adapter, Click OK.

Now NetXRay will switch to all news settings that were previously defined for this site.

View Network Statistics

Opening the Dashboard

1. Select Dashboard from the Tools menu. A graphical Dashboard window is displayed..
2. It displays the network traffic; packets per second, utilization, and errors per second in real time.
3. Click Detail tab to view the total network traffic load cumulated since NetXRay is started.

Notes

- If the numbers displayed are truncated, you can place the mouse pointer 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.

Monitor Network Activity

Using Network Monitor: History

The network monitor allows you to collect history statistics for a particular variable over a period of time. To start monitoring,

1. Select History from the Tools menu, or click the 📊 icon. A History folder is displayed.
2. Click and select a network variable icon of your choice to be monitored from the History folder.
3. Click the right hand button to invoke the context menu.
4. Select Property... A History dialog box is displayed.
5. Enter the sampling period of your choice. NetXRay maintains a maximum of 1,000 samples in the system. For example, if you enter 60 seconds, History graph will plot 1,000 minutes (16 hours and 40 minutes) worth of statistical samples.
6. Enter the high threshold value for the network statistics you wish to monitor. If the sampled value exceeds the high threshold value, the above normal color will be shown in the bar graph.
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 line chart, or line with solid area chart.
12. The history graph will stop when the maximum number of samples are collected, or the history window is closed.

Notes

- You can launch as many as ten (10) network activities concurrently. You can also start the same network variable multiple times.

Exporting History Trend Data to Excel

You can export the data collected in History Sampling directly to a text file in CSV format, or into Excel spreadsheet.

To export sample data to a text file,

1. Simply click the icon on the side of the History window, a Export dialog box is displayed.
2. Enter the file name, and click Save.

To export sample data to Excel,

1. Select the History window you wish to export its trend data by clicking anywhere inside the window.
2. Select Run Macro... from the Tools menu.
3. Select ‘hi2excel.bas’ from the dialog box, then click Open.
4. Click OK on the dialog box, if you wish to proceed with the export operation. Click Cancel, if you have NO History graph running.
5. Excel program will be spawned with the a new spreadsheet showing the current History sample data.

Warning!!

- hi2excel.bas contains Basic script used by NetXRay to perform the exporting function. Do Not attempt to make any modification to it. It may cause un-predictable results.
- You must have at least one History graph running to perform data exporting to Excel, otherwise, NetXRay will terminate abnomally.

Monitoring Network Protocol Distribution

NetXRay Protocol Distribution function allows the reporting of network usage based on the network layer protocols, i.e. IPX/SPX, TCP/IP, NetBIOS, AppleTalk, DECnet, SNA, Banyan and others in real time; it also support for 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 will monitor popular applications, such as NFS, FTP, Telnet, SMTP, POP, HTTP (WWW), Gopher, NNTP, SNMP, X-Window, and others

To start Protocol Distribution monitoring,

1. Select Protocol Distribution from the Tools menu, or click the icon. A Protocol Distribution window is displayed.
2. Click the icon to view the network layer usage. Or, click the icon to view the TCP/IP layer application usage.
3. To exit, simply close the window.

Notes

- The Protocol Distribution window refreshes itself every ten (10) seconds. It does not draw the graph until at least one valid packet is seen.

Tip

- If you make the Protocol Distribution window size too small, the color legends may not be legible. To view the legens, enlarge the window size.

Monitoring Traffic Volume Between Nodes: Matrix

Matrix provides a table view of the traffic volume generated between pairs of nodes. Matrix Table lets you see who is communicating to whom and at what frequency.

To start Matrix,

1. Select Matrix from the Tools menu, or click the icon. A Matrix window is displayed.
2. 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 Source Station to the Destination Station, while the columns on the right show the traffic volume flow from the Destination to the Source.
3. To exit, close the window.

Applying Pre-filter to Network Statistics Gathering

NetXRay lets you apply pre-filter to network statistics gathering in real time. To setup a filter for statistics gathering, please refer to On-Line Help: NetXRay References, Packet Capture Section. The filter you set for statistics is applied to Dashboard, Host Table, Matrix Table, History, and Protocol Distribution equally.

Use 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. History graph will plot traffic load at the router over time.

If you want to look at matrix and host table statistics only for IP traffic, you can create and apply IP protocol filter to statistics. Same can be done to other protocol types, e.g., IPX, Appletalk, etc.

To apply a pre-filter to statistics gathering,

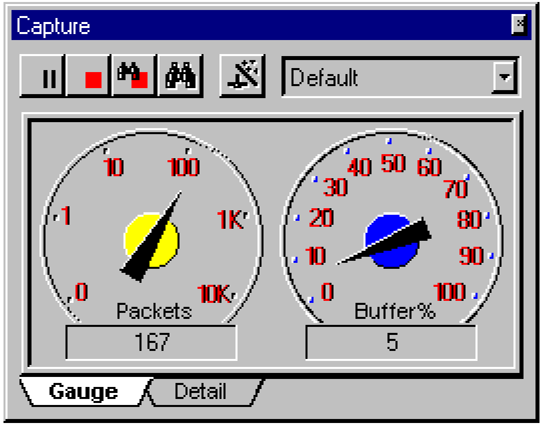
1. Select Tools/Options..
2. Check Apply Filter for Statistics.
3. Select a filter of your choice from the combo list box, and click OK.

NetXRay References

Packet Capture

Capture Window

Packet Capture allows you to capture packets and store them in memory, stop packet capturing in your discretion. Later, you can display these packets and examine their contents. By clicking the Setting button, You can also define or change capture criteria.



Start or Pause Button

⏸ (Pause) button allows you to pause the collection of packets temporarily. Click the ⏸ (Pause) button will turn it into a ▶ (Start) button.

▶ (Start) button allows you to resume or start packet capture.

Stop Button

⏸ (Stop) button stops the capturing of packets.

Stop and View Button

II button stops the capture, and invokes the decode window immediately to let you examine the captured packets.

View Button

⏸ button allows you to invoke the decode window to examine packets captured and saved in the memory buffer.

Setting Button

⏸ button brings up the Capture Setting property page. You can change the filter rules, and other capture criteria.

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

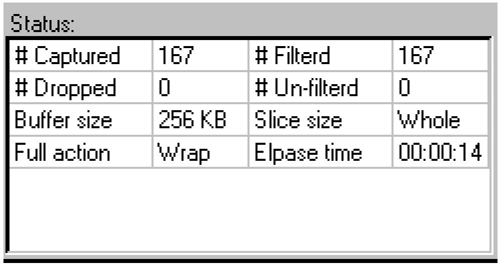
Displays % of capture buffer used.

Gauge Tab

Click here to show the capture gauge.

Detail Tab

Click here to show capture status in table form.



Status:

# Captured	167	# Filterd	167
# Dropped	0	# Un-filterd	0
Buffer size	256 KB	Slice size	Whole
Full action	Wrap	Elpase time	00:00:14

Capture Setting Address Filter Page

The Capture Setting Address Filter page can be invoked by clicking the Setting button. From the Address page, you can define a capture filter to single out specific network information.

A filter can be specified to capture

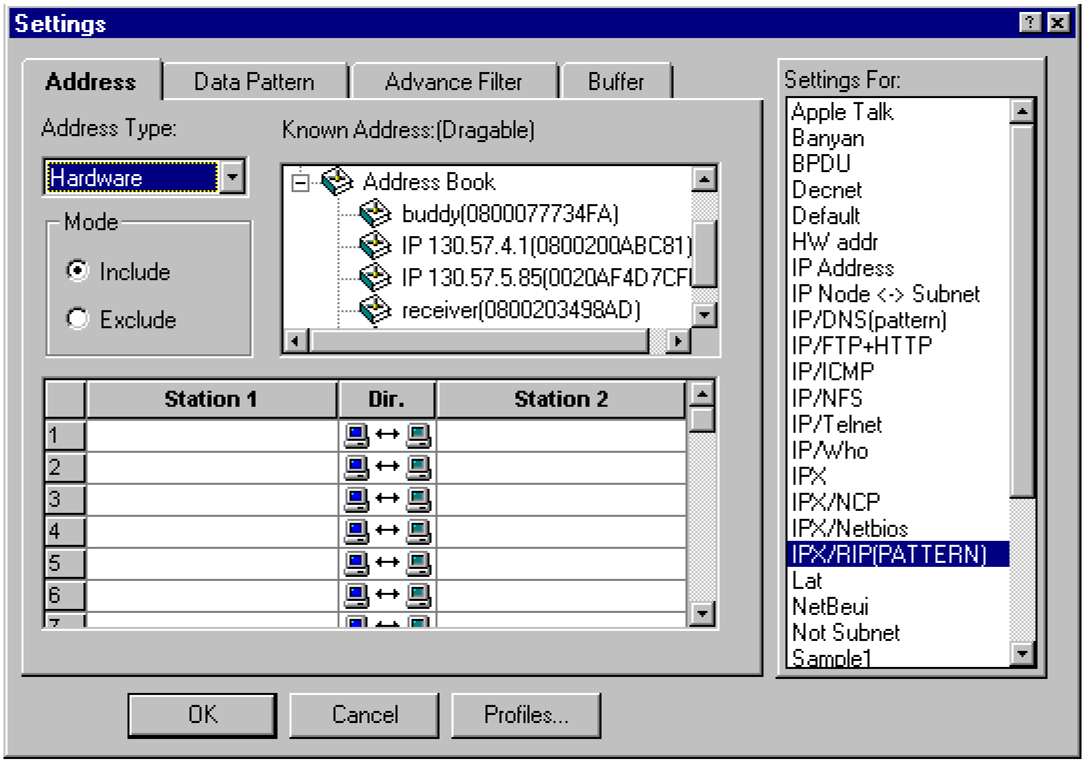
- Data transmitted between network nodes (or address pairs),
- Packets that belong to one or more than one protocol group(s),
- Packets with specified size range,
- Packets that match data patterns rules joined by AND/OR/NOT logical operators , or
- Various combination of the above specifications

Address and Protocol filters are very easy to use. They can be setup quickly to allow user to capture packets of their choice.

Data Pattern filter provides a generic method for user to define and argument other filter conditions that can not be covered by Address and Protocol filters.

When you define a filter that requires more than one filter types, e.g., Address and Protocol filters, there is an imply AND operation built-in in the filter definition. That is a packet must meet both Address and Protocol filter specifications before it can be captured.

Each capture setting can be saved in a profile. NetXRay supports and saves multiple profiles. You can easily retrieve and apply the previously defined capture profile before you activate capture.



Address Type: Hardware

Mode
● Include
○ Exclude

Address Filter Page

Displays the address filter definition.

Data Pattern Filter Page

Allows the construction of filters with logical operation of data patterns.

Advance Filter Page

Displays the protocol filter selection, and packet size filter definition.

Buffer Option Page

Allows you to select capture buffer size, define the size of packet to save, and define the capture action when buffer is full.

Address Type

Lets you define the address monitored be either network hardware address (6 bytes in hexadecimal value) or network IP address (4 octets).

Filter Mode

INCLUDE lets you capture packets that match the address specification. EXCLUDE captures packets that do not match the address specification.

Known Addresses

Displays the pre-defined broadcast and multicast addresses, and the user defined network address book. You can open and examine the detail list by clicking on the address icon ⊞ . Known Address list is used to simplified the definition of address filter pairs. You can drag and drop the symbolic address of your choice into either the Station 1 or Station 2 field.

Profile Button

Invokes the profiles dialog box to Create (New....), Delete, or Rename.... profile.

Station 1

Enters the address of the 1st station. 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, e.g. 100889ACD908
- IP Address 4 decimal octets separated by . (dot), e.g. 198.90.123.98

Station 2

Enters the address of the 2nd station. 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, e.g. 100889ACD908
- IP Address 4 decimal octets separated by . (dot), e.g. 198.90.123.98

Dir.

Selects the direction of the data traffic to be filtered:

- II for both directions.
- 🖳 → 🖳 from Station 1 to Station 2
- 🖳 ← 🖳 from Station 2 to Station 1

Settings For

Displays a list of capture setting profiles.

OK

Accepts the changes.

Cancel

Ignores the changes.

Help

Invokes NetXRay Help.

Capture Setting Data Pattern Filter Page

The Capture Setting Data Pattern Filter page can be invoked by clicking the Setting button, then the Data Pattern tab. You can define a data pattern filter to capture only those packets that match the data pattern criteria you specified.

A data pattern filter can be a simple data pattern filter, or a very sophisticated filter which involves multiple data pattern definitions that are 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. IPX protocol is a good example. It starts from offset byte 14 in Ethernet II type packet, but from byte 17 in 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 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 profiler. 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 tree-like 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.)

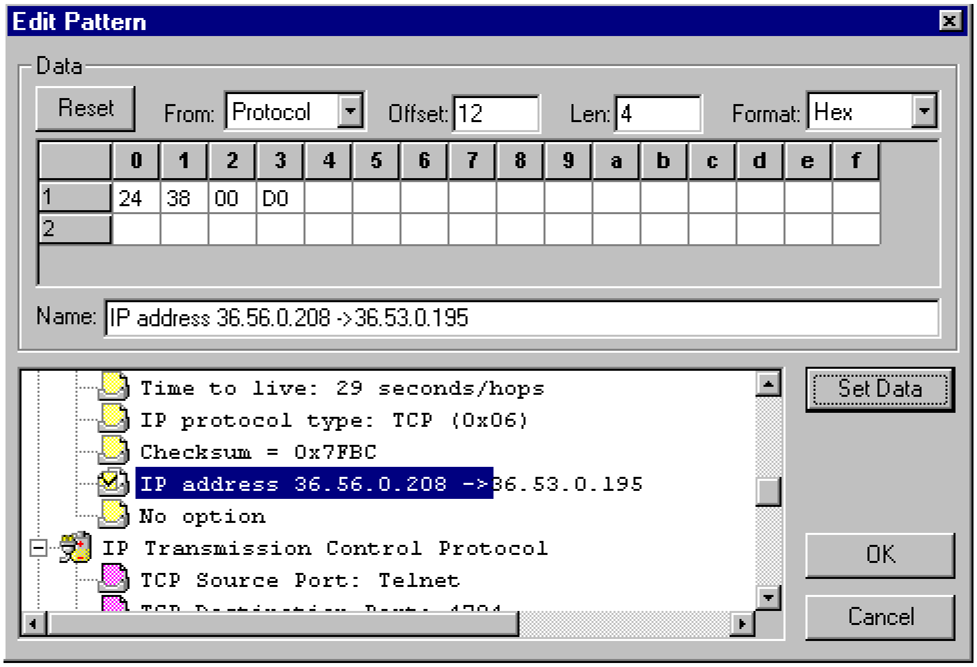
Suppose that you want to capture all IP traffics except ones to and from subnet 36.56.0. The first step is writing down a data pattern Boolean equation that represents this operation:

Not (Src Subnet 36.56.0 OR Dest Subnet 36.56.0)

If you already have a capture packet file that contain this subnet address, you should open this file and select the packet containing the source subnet address 36.56.0 now. This will substantially ease the data entry operation later, when you define the data pattern for the subnet 35.56.0.

Now, you should start defining the data pattern filter by following these steps:

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 new profile name, e.g., 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 the 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 contain 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. And the Edit Pattern dialog box will look like this:



Edit Pattern

Data

From: Protocol Offset: 12 Len: 4 Format: Hex

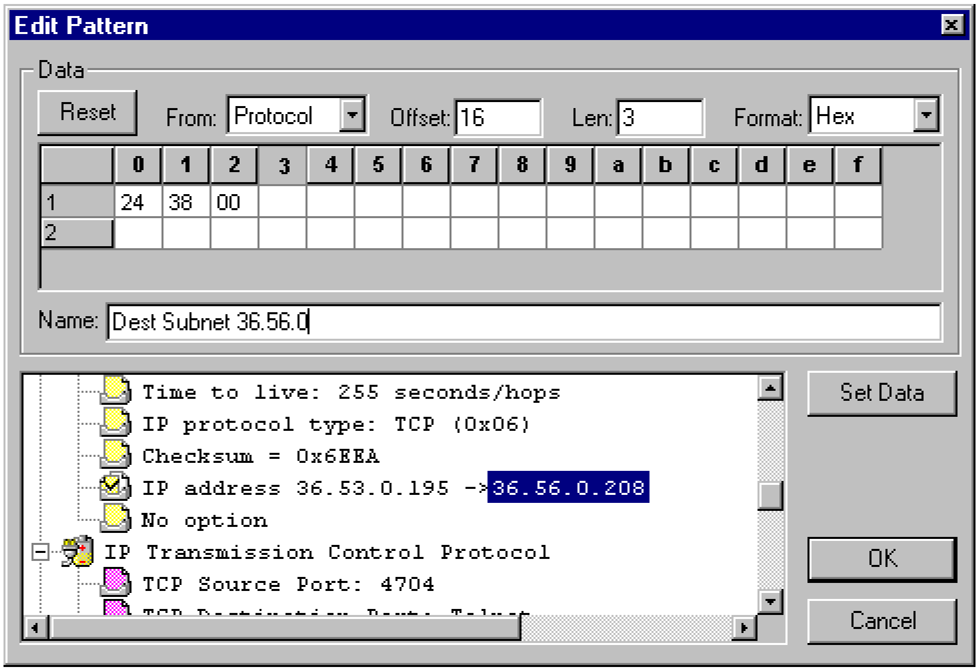
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
1	24	38	00	D0												
2																

Name: IP address 36.56.0.208 ->36.53.0.195

```
Time to live: 29 seconds/hops
IP protocol type: TCP (0x06)
Checksum = 0x7FBC
IP address 36.56.0.208 ->36.53.0.195
No option
IP Transmission Control Protocol
TCP Source Port: Telnet
```

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 Set Data button to tell NetXRay to fill in a dummy data pattern (place holder) for the Dest Subnet. And click OK.

21. Click OK again on the Setting dialog box to save the filter.
22. Select the next packet containing the destination IP subnet address from the Packet Viewer.
23. From the Capture window, click ⏸ to bring up the Capture Setting property dialog box for My Subnet.
24. Click the Data Pattern property page tab to review the Data Pattern filter defined so far.
25. Select and highlight the second PAT (was the place holder created previously). And click the Edit Pattern button to invoke the Edit Pattern dialog box.
26. Scroll the detail decode window to locate the IP destination address contain subnet 35.56.0. Highlight the field.
27. Select Protocol in the From combo box. This will tell NetXRay to calculate the destination IP address offset from the beginning of the IP protocol data packet.
28. Click the Set Data button to tell NetXRay to fill in the field for source IP address.
29. Change Len from 4 to 3 for the length of subnet of 3 bytes. Delete the 4th octet from the data pattern field.
30. Edit the Name field, so it shows Dest Subnet 36.56.0. And the Edit Pattern dialog box will look like this:



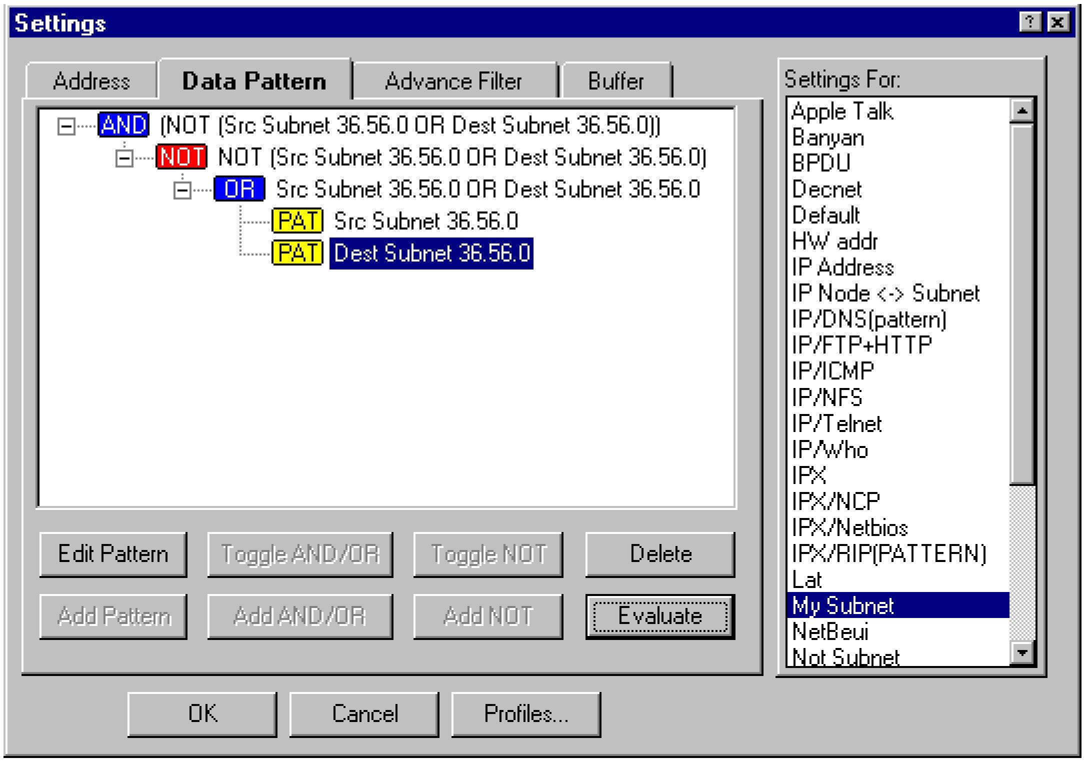
From: Protocol Offset: 16 Len: 3 Format: Hex

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
1	24	38	00													
2																

Name: Dest Subnet 36.56.0

```
    Time to live: 255 seconds/hops
    IP protocol type: TCP (0x06)
    Checksum = 0x6EEA
    IP address 36.53.0.195 ->36.56.0.208
    No option
 IP Transmission Control Protocol
    TCP Source Port: 4704
    TCP Destination Port: Telnet
```

31. Click OK. A second data pattern Dest Subnet 36.56.0 is created and connected to the OR operator.
32. Click the Evaluate button. The resulting operation **Not (Src Subnet 36.56.0 OR Dest Subnet 36.56.0)** is shown on the top line. And the Data Pattern Filter page will look like this:



```
⊟ AND (NOT (Src Subnet 36.56.0 OR Dest Subnet 36.56.0))
    ⊟ NOT NOT (Src Subnet 36.56.0 OR Dest Subnet 36.56.0)
        ⊟ OR Src Subnet 36.56.0 OR Dest Subnet 36.56.0
            PAT Src Subnet 36.56.0
            PAT Dest Subnet 36.56.0
```

Settings For:

```
Apple Talk
Banyan
BPDU
Decnet
Default
HW addr
IP Address
IP Node <-> Subnet
IP/DNS(pattern)
IP/FTP+HTTP
IP/ICMP
IP/NFS
IP/Telnet
IP/Who
IPX
IPX/NCP
IPX/Netbios
IPX/RIP(PATTERN)
Lat
My Subnet
NetBeui
Not Subnet
```

33. Click OK to save the filter.

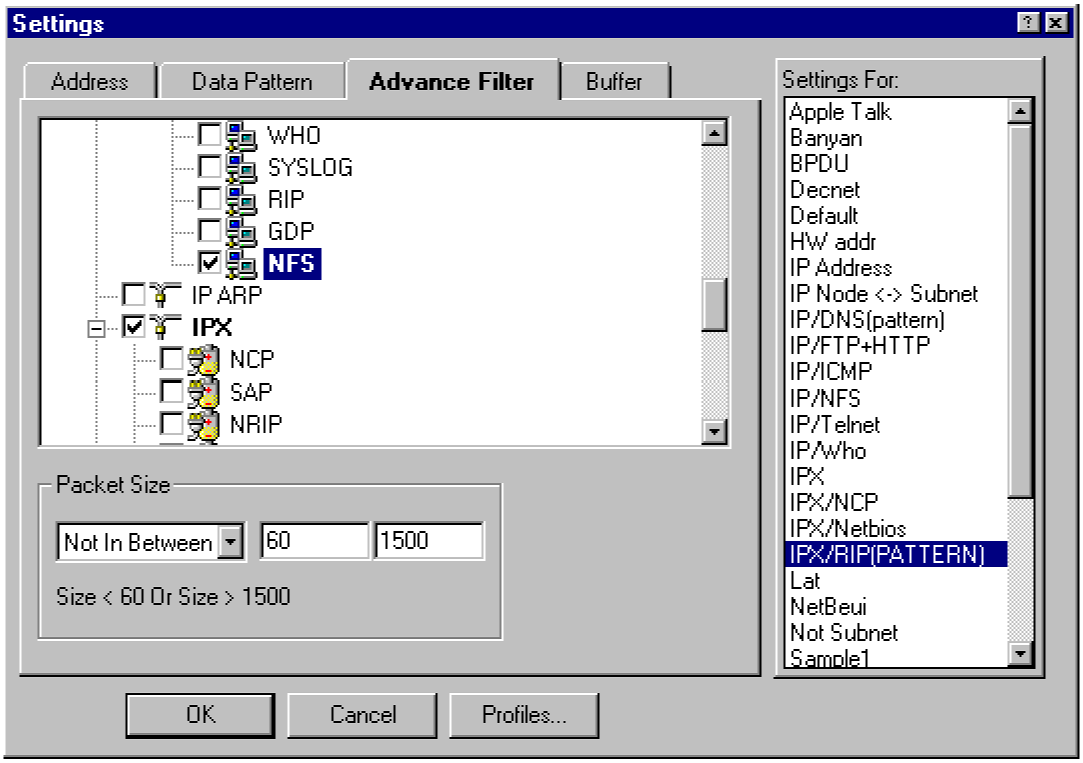
Capture Setting Advance Filter Page

The Capture Setting Advance Filter page can be invoked by clicking the Setting button, then the Advance Filter tab. From the page, you can select one or more first or second level protocols to filter. If the packet matches one of the selected protocol types, it will be captured in the memory buffer.

You can also specify a packet size filter. You can capture packets based on packet size that is, Equal to, Greater than, Less than, in Between, Not in Between certain ranges.

Protocol filter for IP has been expanded to include transport layer, i.e. TCP, UDP, ICMP, IGMP, ISO-TP4, Hello, IP-VINES, OSPF, GGP, EGP, IGRP, as well as, TCP and UDP application layer sub-protocols, i.e., 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.

Protocol filter for IPX is also expanded to filter on various sub-protocols, such as, RIP, SAP, NCP, SPX, NBIOS, Diagnostic, Serialization, NMPI, NLSP, SNMP.



☐ WHO
☐ SYSLOG
☐ RIP
☐ GDP
☑ NFS
☐ IP ARP
☑ IPX
☐ NCP
☐ SAP
☐ NRIP

Packet Size

Not In Between | 60 | 1500

Size < 60 Or Size > 1500

Settings For:

Apple Talk
Banyan
BPDU
Decnet
Default
HW addr
IP Address
IP Node <-> Subnet
IP/DNS(pattern)
IP/FTP+HTTP
IP/ICMP
IP/NFS
IP/Telnet
IP/Who
IPX
IPX/NCP
IPX/Netbios
IPX/RIP(PATTERN)
Lat
NetBeui
Not Subnet
Sample1

Protocol Filter

Select one or more protocol or sub-protocol types to filter.

Packet Size Type

Select from one of the size type; All, Equal, Greater than, Less than, in Between, Not in Between.

Packet Size Range

Define the actual size range. Only one field is needed for Equal, Greater than, Less than.

Data Pattern Offset Beginning Boundary

Select data pattern’s offset from either the beginning of the packet, or the beginning of protocol layer.

Data Pattern Offset

Specify the data pattern offset in decimal value.

Data Pattern

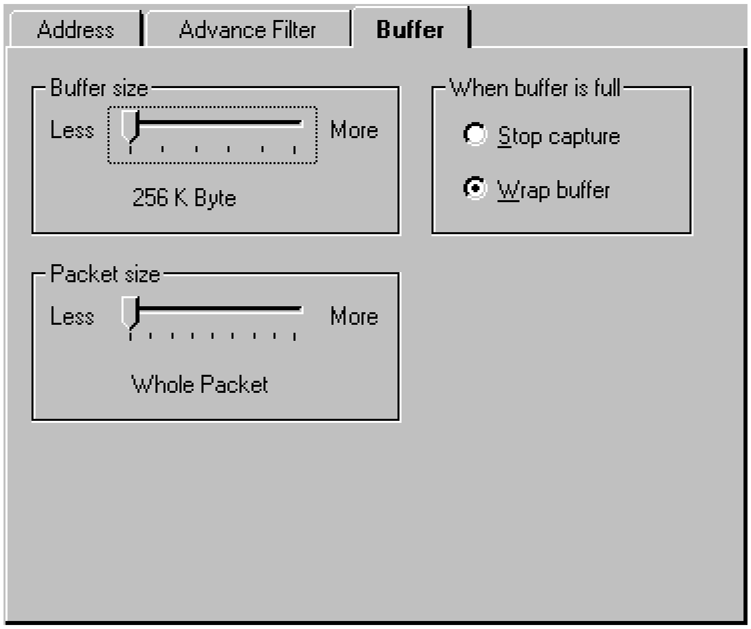
Enter the data pattern value of up to 32 octets.

Data Pattern Type

Select the data pattern type in Hex, ASCII, or EBCDIC.

Capture Setting Buffer Option Page

The Capture Setting Buffer Option page can be invoked by clicking the Setting button, then the Buffer tab. From the page, you can select a capture data buffer in memory to accommodate the mount of network traffic you wish to capture. Selecting a smaller packet size let you save buffer space, and ignore unnecessary data. You can also define the action when buffer is full.



Buffer size

256 K Byte

When buffer is full

○ Stop capture

● Wrap buffer

Packet size

Whole Packet

Buffer Size

Move the slider to select the memory size for the capture buffer. You can select 256K, 512K, 1M, 2M, 4M, or 8M Bytes.

Packet Size

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

Buffer Full Action

Choose the capture action when the memory buffer is full. You can select to stop capture, or let capture wrap the memory buffer. Buffer wrap mode will overwrite the oldest packets in the memory buffer.

Packet Viewer

Packet Viewer Overview

Packet Viewer is invoked when you stop and view a captured buffer, or when you open a previously captured file. You can invoke as many as Packet Viewer as you wish, as long as your Windows 95 virtual memory set up can handle them.

Packet Viewer is a MDI child window that contains three separate panes for Summary, Detail, and Hex.

The Summary pane shows all packets in line by line summarized format with the following information:

- Packet Sequence No.
- Source Address
- Destination Address
- Highest Protocol Layer Interpreted
- Summary Information for the Protocol Layer
- Length of the Packet
- Relative Time
- Delta Time
- Absolute Time

The Detail pane displays the interpreted protocol layer detail fields in each layer for the current highlighted packet.

The Hex shows the whole packet in Hex, and the respective ASCII, and EBCDIC view.

Each pane can be re-sized by click and drag the separator bar between the panes. Each pane contains scroll bars that you can use the mouse to manipulate the viewing position in the pane. Cursor, page up and down keys can also provide the similar function for the pane window that has the focus.

Keyboard Usage

Aside from supporting full mouse action to allow easy viewing of the packets. The Packet Viewer supports the following keys to enhance user's ability to advance packets quickly:

- 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

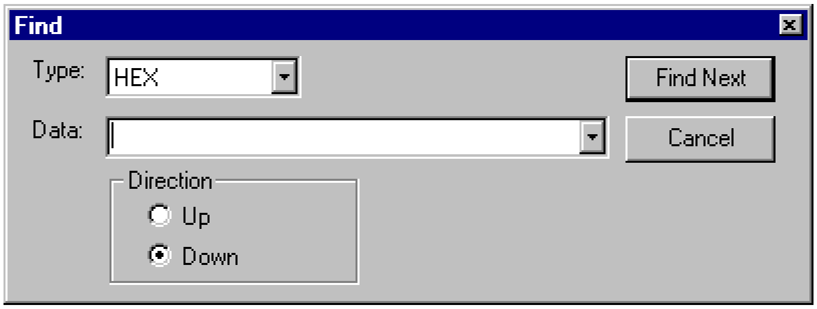
To maximize the efficiency in scanning packets for details, we recommend you follow the steps below:

- 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/down keys will now apply to the detail pane.
- Use F7 key to move to the previous packet. Use F8 to the next packet.
- If you wish to move the viewing area in the detail pane, use cursor, and page up/down keys.

Search Packets

NetXRay gives you ability to search packets that match a certain pattern, or advance to a particular packet number.

To search a packet, highlight a protocol field or a data pattern in the detail pane window of the packet viewer, then select FindPacket..... from Packet menu, or from the context menu in Packet Viewer. Click the Find Next button.



Type: HEX

Data:

Direction
○ Up
● Down

To advance to a packet, select Go To... from the Packet menu, or from the context menu in Packet Viewer. Enter packet number, then hit OK.

Special Viewing Tips

Color Coded Summary Pane

The packets in summary pane can be colored coded based on their protocol type. This feature allows you to group packets with the same protocol or sub-protocol reference, and to assist you visually in identifying the packets of you choice. To set up protocol color highlight,

1. Choose Display Options... from the Packet menu. An Options property dialog box is displayed.
2. Click and select the Summary Color tab.
3. Select and click on the protocol type you wish to change color display.
4. Select the Text and the Background color of you choice. The protocol type color will change to reflect your selection.
5. When you are satisfied with the color selection, click OK.

One Line Protocol Summary in Detail Pane

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 sub-layer 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.

The expand or contract state of each sub-protocol field is ‘memorized’ by the packet viewer. The same state for that sub-protocol will be maintained, when you view the next or the previous packet. For example, 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 sub-protocol, follow these steps:

1. Choose Display Options... from the Packet menu. An Options property dialog box is displayed.
2. Click and select the Protocol Display tab.
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 on the Close All button will do the opposite to set all protocol layers in contracted view.
5. When you are satisfied with the selection, click OK.

Anchor a Field in Detail Pane

By simply click on a selected field or protocol summary line to highlight it, you have anchored that 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 user to go back and forth between several packets without having to re-position the detail pane by using scroll bar.

Mark Packets for Separate Viewing or as Book Marks

NetXRay lets you mark individual packets, or a group of packets in the summary pane of the packet viewer, and then save them into a separate decode window.

To mark individual packets:

Simply click the check box in front of the packet's index number.

To mark a group of packets:

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

To clear all marked packets:

1. Click the right hand mouse button, and select the Mark Range....
2. Click All nnn Packets radio button.
3. Click Unmark button

To mark all packets except a few un-desired packets

1. Click the right hand mouse button, and select the Mark Range....
2. Click All nnn Packets radio button.
3. Click Mark button
4. Scroll the summary pane to locate the un-desired packets. Click the check box in front of the un-desired packets to de-select it.

Once you have marked the packets, you can

1. Save the marked packets into a new decode window by selecting 'Saved Marked..' from the context menu (by clicking the right hand mouse button). Or,
2. Use the marked packets as 'Book Marks'. Use F2 key to advance from one marked frame to another.

Notes

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

Use Display Filter

Display filter allows you to filter out unwanted packets from the captured buffer. You can use display filter to view only:

- Packets transmitted between network nodes (or address pairs),
- Packets that belong to one or more than one protocol group(s),
- Packets that matches a defined data pattern, or
- Packets that match various combination of the above specifications

The profile defined for capture filter can also be used for filtering out packets from the packet viewer.

To create a new filter, select Edit Display Filters.... from the Packet menu. See instructions in Capture Filter Setting for details.

To apply a filter, simply select Apply Display Filters.... from the Packet menu. Pick a pre-defined filter of your choice, then click OK.

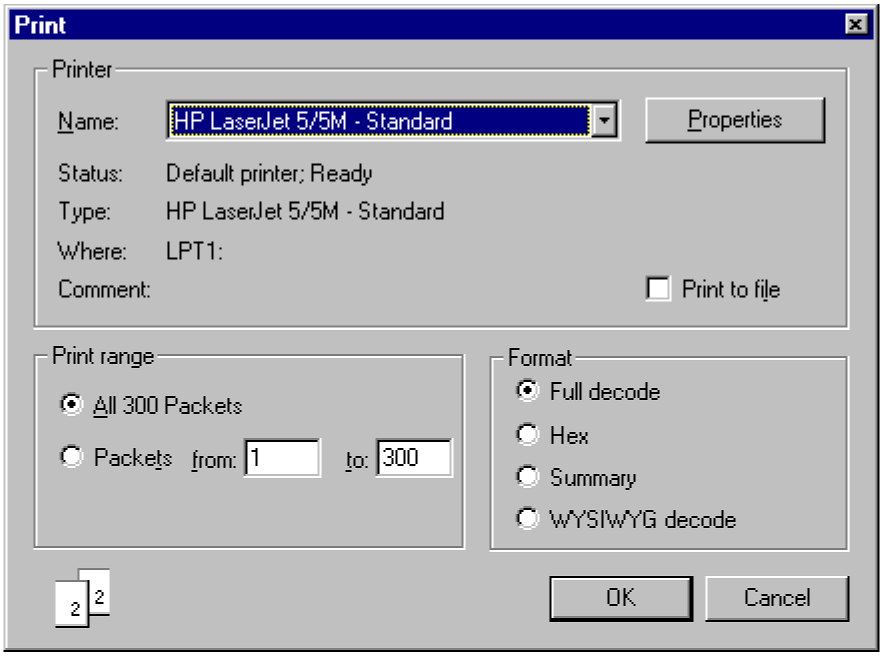
Print Decoded Packets

The decoded data packets in the Packet Viewer can be printed on paper or to a printer output file. You can select from four different decode views to print out:

- Full Decode: a complete fully expanded list of protocol fields in Detail pane
- Hex: the hex data in Hex pane
- Summary: a line by line list of the packets in Summary pane
- WYSIWYG Decode: prints exactly what is shown in the detail pane window.

To print, select Print... from File menu, or click the Printer icon on the Tool Bar. From the printer dialog box, select range of packets and type of decode format. Then click OK.

If you wish to output the print out to a printer file, check Print to file.



Print

Printer

Name: HP LaserJet 5/5M - Standard

Status: Default printer; Ready

Type: HP LaserJet 5/5M - Standard

Where: LPT1:

Comment:

□ Print to file

Print range

● All 300 Packets

○ Packets from: 1 to: 300

Format

● Full decode

○ Hex

○ Summary

○ WYSIWYG decode

Import Third Party Captured File

NetXRay recognizes many Ethernet (.ENC) and Token Ring (.TRC) capture files created by Network General’s Expert Sniffer Network Analyzer. Files created using versions 4.1 and earlier are supported. For files created by later versions, you must save them in un-compressed format. Consult Sniffer User’s Guide about how to save file in un-compressed format.
Novell LANalyzer for Windows capture files (.TR1) can also be displayed by NetXRay.

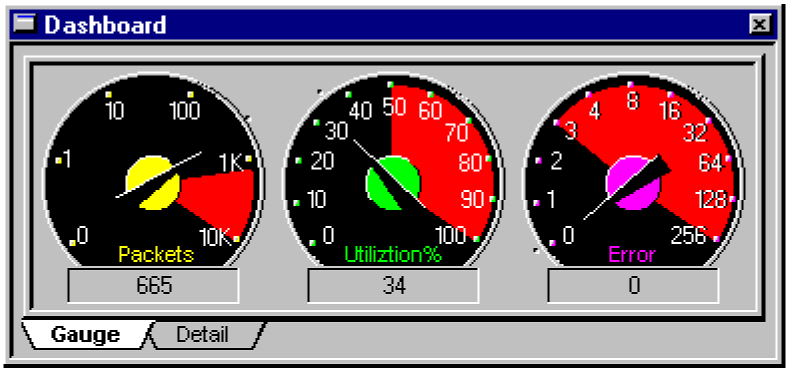
Global Statistics

Graphical View

NetXRay collects the network segment's statistics immediately upon starting up. To view the network statistics in real time, go to Tools menu, and select Dashboard. A Dashboard window is displayed.

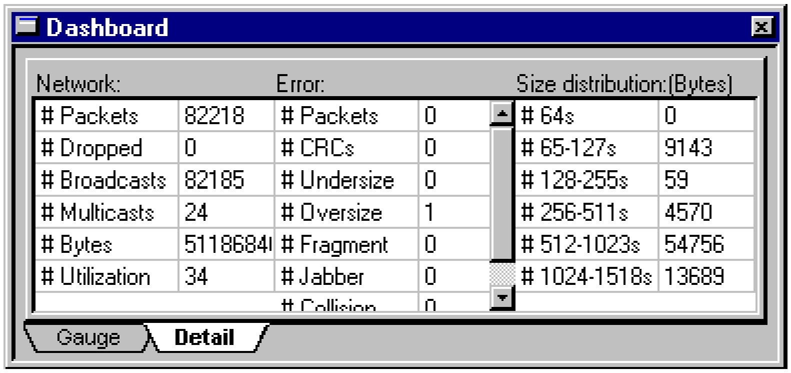
It displays the network load in number of Packets per Second, % Utilization rate, and number of Errors per Second in real time.

The red zone defines the area of the network activity which exceeds the high threshold set by you. To set high threshold for these three variables, go to Tools, and select Options....Set you desired high threshold from the Threshold page.



Ethernet Detail Summary

To view the detail total summary, click the Detail tab.



Network:		Error:		Size distribution:(Bytes)	
# Packets	82218	# Packets	0	# 64s	0
# Dropped	0	# CRCs	0	# 65-127s	9143
# Broadcasts	82185	# Undersize	0	# 128-255s	59
# Multicasts	24	# Oversize	1	# 256-511s	4570
# Bytes	5118684	# Fragment	0	# 512-1023s	54756
# Utilization	34	# Jabber	0	# 1024-1518s	13689
		# Collision	0		

The ethernet network statistics details are displayed in three groups.

1. Network

- Total # of all packets
- Total # of packets dropped
- Total # of broadcast packets
- Total # of multicast packets
- Total # of octets
- Current % network utilization

2. Errors

- Total # of error packets
- Total # of CRC error packets
- Total # of undersize packets (packets < 64 bytes in length)
- Total # of oversize packets (packets >1518 bytes in length)
- Total # of fragment packets
- Total # of jabber packets
- Total # of collision packets

3. Packets count grouped in different size distributions

- Total # of packets in 64 byte size
- Total # of packets in size from 65 to 127 bytes
- Total # of packets in size from 128 to 255 bytes
- Total # of packets in size from 256 to 511 bytes
- Total # of packets in size from 512 to 1023 bytes
- Total # of packets in size from 1024 to 1518 bytes

Notes

- The packet size defined here includes 4 bytes of CRC.
- If the numbers displayed are truncated, you can place the mouse pointer 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.

- The current version of NDIS 3.1 specification does not support counting of fragment, jabber packets. They will be displayed as zeroes. Detection of CRC, and collision errors may not be supported by certain NIC card drivers. Contact your NIC card manufacturer for detail.

Token Ring Detail Summary

The token ring network statistics details are displayed in two groups.

1. LLC
   - Total # of all packets
   - Total # of packets dropped
   - Total # of broadcast packets
   - Total # of multicast packets
   - Total # of bytes
   - Current % network utilization
   - Total # of error packets
   - Total # of packets in size from 18 to 64 bytes
   - Total # of packets in size from 65 to 127 bytes
   - Total # of packets in size from 128 to 255 bytes
   - Total # of packets in size from 256 to 511 bytes
   - Total # of packets in size from 512 to 1023 bytes
   - Total # of packets in size from 1024 to 2047 bytes
   - Total # of packets in size from 2048 to 4095 bytes
   - Total # of packets in size from 4096 to 8191 bytes
   - Total # of packets in size from 8192 to 18000 bytes
   - Total # of packets in size greater than 18000 bytes

2. MAC
   - Total # of MAC layer bytes
   - Total # of MAC packets
   - Total # of ring purge packets
   - Total # of beacon packets
   - Total # of claim token packets
   - Total # of NAUN changes
   - Total # of line errors
   - Total # of internal errors
   - Total # of burst errors
   - Total # of AC errors
   - Total # of abort errors
   - Total # of lost frame errors
   - Total # of congestion errors
   - Total # of FC errors
   - Total # of frequency errors
   - Total # of token errors
   - Total # of soft errors

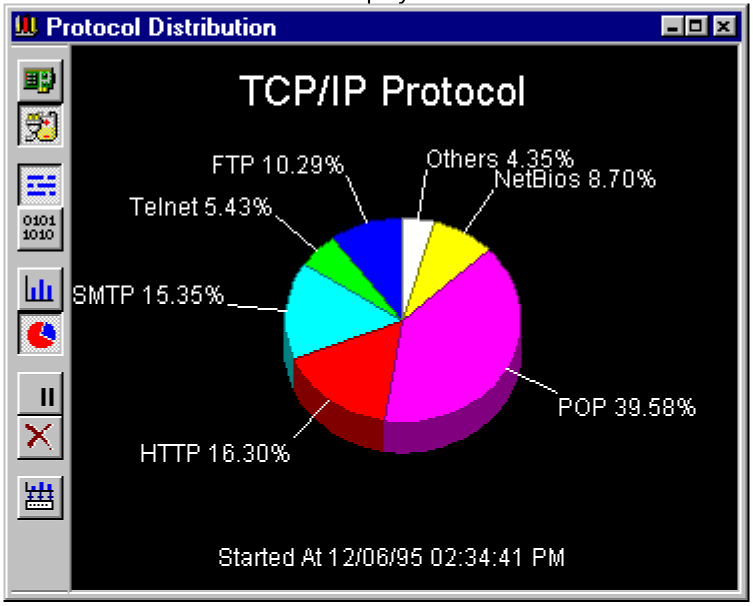
Protocol Distribution

NetXRay Protocol Distribution allows the reporting of percentage network usage based on the network layer protocols in real time.

Network layer protocol 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.

To start Protocol Distribution monitoring, Select Protocol Distribution from the Tools menu, or click the ▶ icon. A Protocol Distribution window is displayed.



To change the viewing options, click the buttons on the left side of the window. These button functions are described in the following:

- ▶ View network layer protocol distribution
- ▶ View TCP/IP application distribution
- Select % calculation based on total packet seen
- 1010 Select % calculation based on total octet seen
- Display bar graph
- Display pie graph
- ▶ Freeze protocol distribution update
- Reset all counters to zero
- ▶ Export protocol distribution data to CSV file

Notes

- The Protocol Distribution window refreshes itself every ten (10) seconds. It does not draw the graph until at least one valid packet is seen.

History Statistics

History Overview

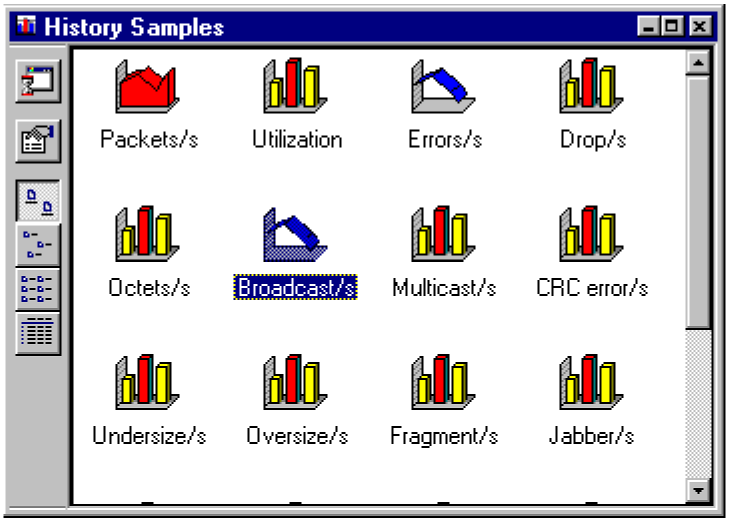
History Statistics records network activities over a period of time. You can use the recorded data to establish the network performance base line so that threshold can be set to trigger alarms when above normal network activities occur. The history statistics is also useful for determining the network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

NetXRay supports the monitoring of ten (10) 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.

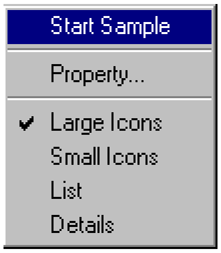
Monitor History Statistics

To start monitoring history statistics, go to Tools menu and select History or select History ▶ icon from the Tool bar..

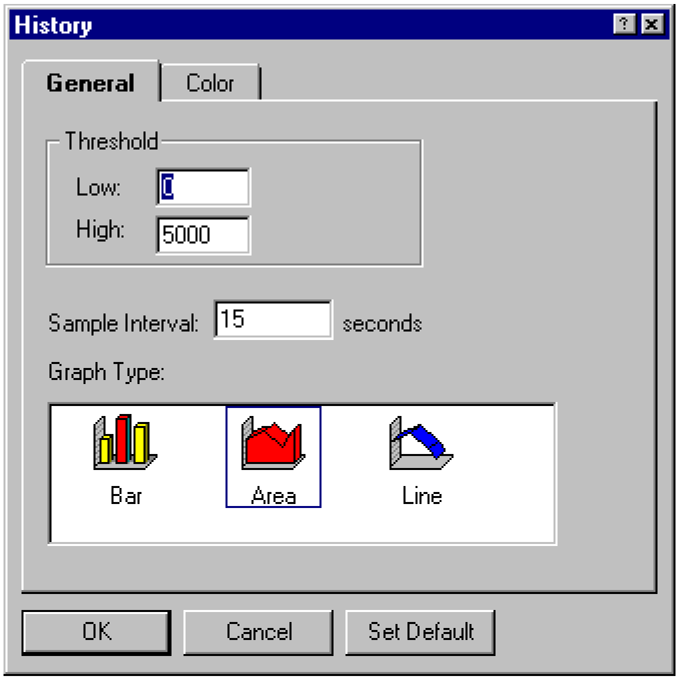
A History folder is displayed.



Click and select a network variable icon of your choice to be monitored from the History folder. Click the right hand button to invoke the context menu.



Select Property... A History dialog box is displayed.



Threshold

Low: 0

High: 5000

Sample Interval: 15 seconds

Graph Type: Bar [✓ Area] Line

Enter the threshold level, the sampling interval. Optionally, Click the Color tab to view the color selection for the History graph. Choose color for Above Normal (threshold), Normal, Foreground, and Background colors. Click Start button to activate the statistics monitoring.

Double click the statistical variable icon. A history window is displayed showing the on-going sampling of the network data. When a total of 2,000 samples are recorded, the statistics monitoring stops automatically. You can also stop the monitor by closing the History window.

When you close the History monitoring window, you will be given an option to save the recorded sampling data to a file. To review a saved history statistics, go to File menu and select Open..... From the Open dialog box, select a saved history statistics file and click OK.

Notes

- 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.

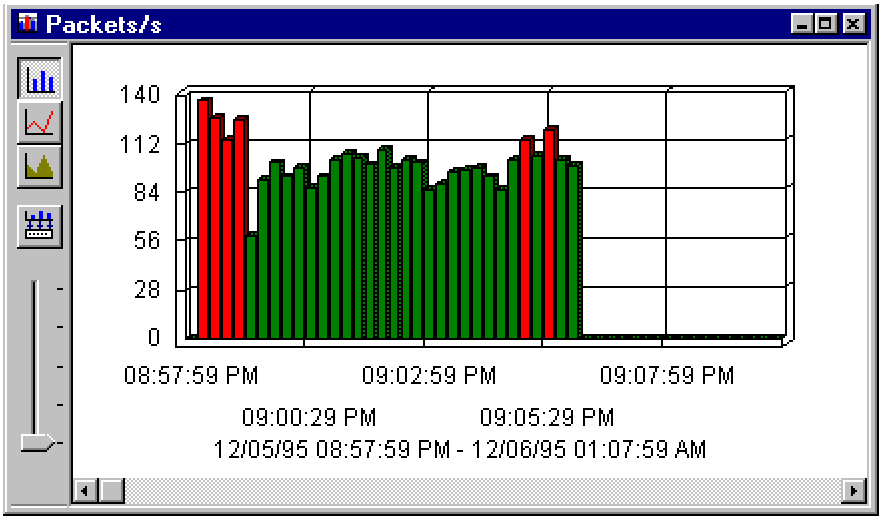
{button ,KL(`Exporting History Trend Data to Excel',2)} See Also: Exporting History Trend Data to Excel

Customize 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; one button to export the history trend data to a CSV file:

- Bar chart
- Line chart
- Area chart
- ▶ Export History data

The slider allows you to adjust the vertical scale of the graph chart. While the horizontal scroll bar lets you move the history graph back and forth in time.



History Threshold

Enter a threshold level for the sampled data. Any sampled data value exceeds the threshold level will be displayed in the above normal color in the history statistics bar graph.

History Sample Interval

Enter the sampling interval in # of seconds. The maximum sample interval is 3,600 seconds (1 hour).

History Sample Data

Select a network statistics variable for monitoring.

Set History Default

Set the threshold, and the sampling interval back to default values defined by NetXRay.

Start History

Start monitoring the selected network variable.

Packet Generator

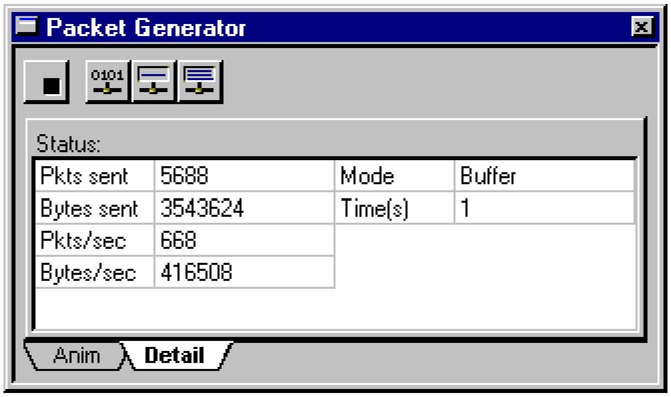
Packet Generator Overview

Transmitting packets onto the network gives you the ability to

- Reproduce network problems so you can trouble shoot and verify fixes for your network equipment or applications.
- Generate a level of network traffic load so you can simulate the type of network condition for your equipment to handle.

To invoke the packet generator, choose Packet Generator from the Tools menu. A packet generator window is displayed.

To see packet transmitting status in progress, click the Detail tab.



Status:

Pkts sent	5688	Mode	Buffer
Bytes sent	3543624	Time(s)	1
Pkts/sec	668		
Bytes/sec	416508		

Caution

- 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.
You can change the following packet send parameters:

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

Decode page in the Send Packet dialog box gives you instant analysis of the hex data pattern you just entered in decoded form.

Delay time set to zero millisecond produce the maximum # of packet transmitted per second. The rate of transmission is depended on the size of the packet and the PC's CPU speed. To achieve maximum transmission rate, use PCI NIC cards.

Since NetXRay is designed to run in Windows 95's multi-tasking environment, the delay time used in packet transmission can not be accurately controlled. It may vary depends on the kind of applications you are running in the PC.

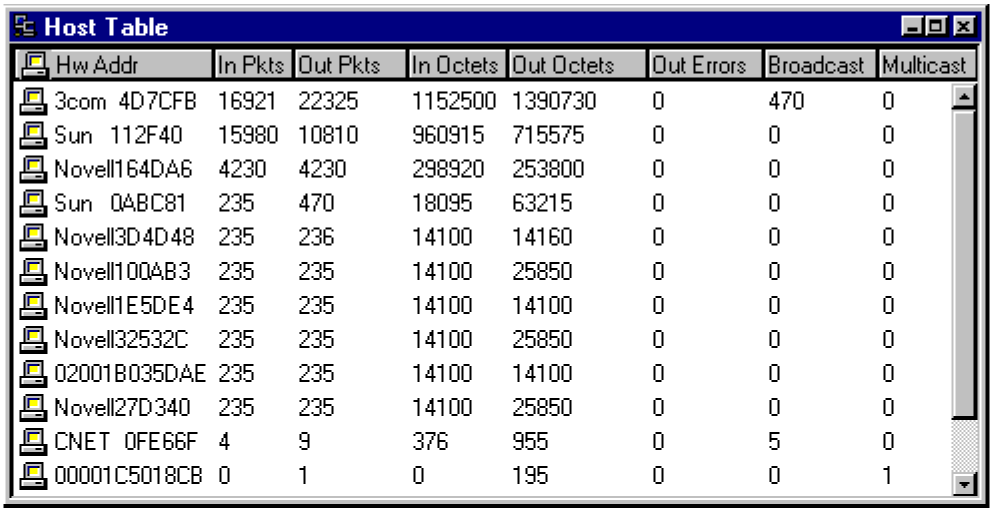
Transmitting an Entire Captured File

Click the ▶ to invoke the Send Current Buffer button, when a captured file or buffer is displayed in Packet Viewer. You can send the entire buffer # 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 exactly reproducible because Windows 95 system timer's smallest resolution is 1 millisecond, and the delay time may vary greatly depending on the type of application you run concurrently with NetXRay.

Station Statistics

Host Table View

NetXRay Host Table collects network statistics details for all active nodes (stations) on the network segment it monitors. To bring up Host Table and start collecting statistics, go to Tools menu, and select Host Table, a host table view is displayed:



Host Table

Hw Addr	In Pkts	Out Pkts	In Octets	Out Octets	Out Errors	Broadcast	Multicast
3com 4D7CFB	16921	22325	1152500	1390730	0	470	0
Sun 112F40	15980	10810	960915	715575	0	0	0
Novell164DA6	4230	4230	298920	253800	0	0	0
Sun 0ABC81	235	470	18095	63215	0	0	0
Novell3D4D48	235	236	14100	14160	0	0	0
Novell100AB3	235	235	14100	25850	0	0	0
Novell1E5DE4	235	235	14100	14100	0	0	0
Novell32532C	235	235	14100	25850	0	0	0
02001B035DAE	235	235	14100	14100	0	0	0
Novell27D340	235	235	14100	25850	0	0	0
CNET 0FE66F	4	9	376	955	0	5	0
00001C5018CB	0	1	0	195	0	0	1

In the Host Table view for Ethernet LAN, the following statistics are displayed:

- HW Address: 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

In the Host Table view for Token Ring LAN, the following statistics are displayed:

- HW Address: Station's symbolic name or Hex address
- Order: Shows the stations' polling order in this ring with respective 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.
- 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
- Broadcast: Total # of broadcast packets transmitted by the station
- Multicast: Total # of multicast packets 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
- 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

The column width of the Host Table can be adjusted to fit your viewing. You can simply click and drag the column divider to the left or right to narrow or widen the column width.

To access additional commands, press the right hand mouse button on the Host Table view to bring up the context menu:

- Pause Update Suspend the host table counter update temporarily
- Reset Clear all counters in the Host table
- Capture Hot link to invoke capture directly. The capture filter is set up to capture any packets sent to and from the station selected.
- Create Capture Filter... Hot link to invoke Capture Filter Setting dialog box. The hardware address pair is set up automatically with the station hardware address to and from any.
- Properties... Invoke a dialog box to change the host table viewing options. You can show either the station’s hardware address or station’s symbolic name.
- Export... Save the Host Table data to a CSV format file.

Sorting Host Table

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

Clicking a column heading of a counter field 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.

The address column sorting order is the opposite of the counter column.

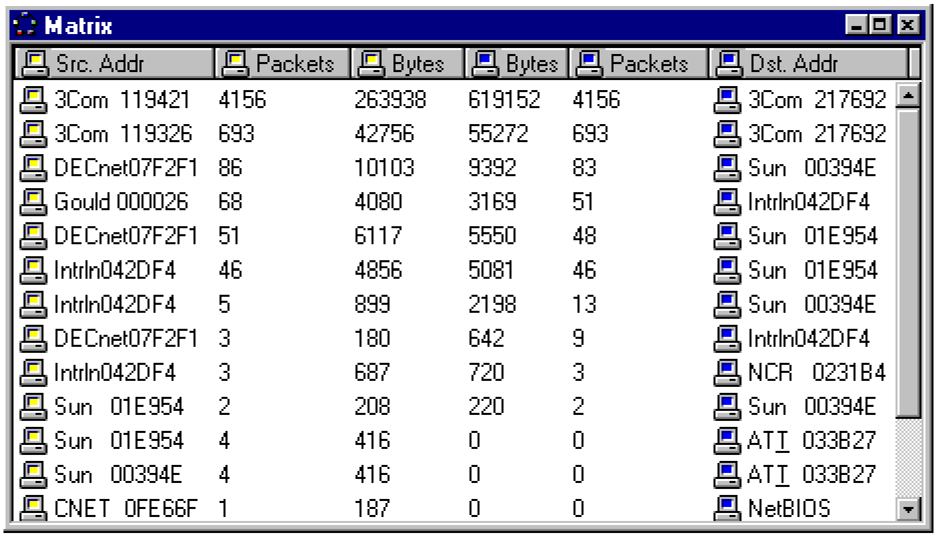
The Host Table is updated every second. It is re-resorted every ten seconds.

Matrix View

Matrix provides a table view of the traffic volume generated between pairs of nodes. Matrix Table lets you see who is communicating to whom and at what frequency.

To start Matrix, Select Matrix from the Tools menu, or click the ▶ icon.

A Matrix window is displayed.



Src. Addr	Packets	Bytes	Bytes	Packets	Dst. Addr
3Com 119421	4156	263938	619152	4156	3Com 217692
3Com 119326	693	42756	55272	693	3Com 217692
DECnet07F2F1	86	10103	9392	83	Sun 00394E
Gould 000026	68	4080	3169	51	Intrln042DF4
DECnet07F2F1	51	6117	5550	48	Sun 01E954
Intrln042DF4	46	4856	5081	46	Sun 01E954
Intrln042DF4	5	899	2198	13	Sun 00394E
DECnet07F2F1	3	180	642	9	Intrln042DF4
Intrln042DF4	3	687	720	3	NCR 0231B4
Sun 01E954	2	208	220	2	Sun 00394E
Sun 01E954	4	416	0	0	ATT 033B27
Sun 00394E	4	416	0	0	ATT 033B27
CNET 0FE66F	1	187	0	0	NetBIOS

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 Source Station to the Destination Station, while the columns on the right show the traffic volume flow from the Destination to the Source.

To access additional commands, press the right hand mouse button on the Host Table view to bring up the context menu:

- Pause Update Suspend the Matrix table counter update temporarily
- Reset Clear all counters in the Matrix table
- Capture Hot link to invoke capture directly. The capture filter is set up to capture any packets sent to and from the station address pair selected.
- Create Capture Filter... Hot link to invoke Capture Filter Setting dialog box. The hardware address pair is set up automatically with the station hardware address pair selected in the Matrix table.
- Properties... Invoke a dialog box to change the Matrix table viewing options. You can show either the station’s hardware address or station’s symbolic name.
- Export... Save the Matrix table data to a CSV format file.

NetXRay Data Base

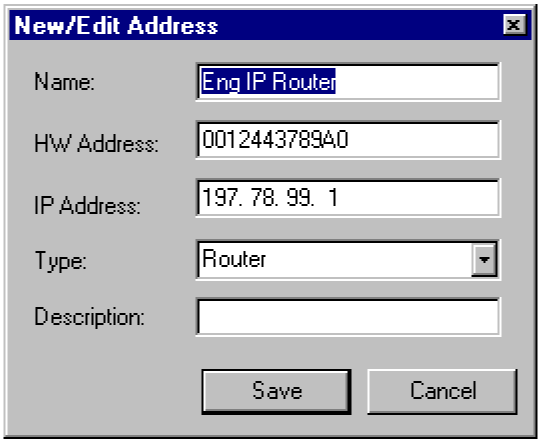
Address Book

The Address Book allows you to pre-define your network nodes in human readable symbolic names. NetXRay uses the address book in Filter definition, Packet Viewer, and Host Table to replace the 6 byte hardware address of the network node with its respective symbolic name.

The Address Book is invoked from the Tools menu. When the Address Book is displayed, click the right hand button to bring up a context menu. You can create, edit , or delete an entry. You can also undo or redo a change to the entry. The same functions can also be accessed through the tool bar buttons on the left of the address book.

An address book entry contains:

- Name
- HW Address
- IP Address
- Type
- Description



Name: Eng IP Router

HW Address: 0012443789A0

IP Address: 197. 78. 99. 1

Type: Router

Description:

NetXRay only uses the HW address in this release. Other items are for informational only, and may be used in the future.

The Node Type selections are Workstation, Host Computer, Server, File Server, Printer Server, Router, Bridge, and Hub.

NetXRay allows you to import IP host table into the Address Book. See the section *in How to..../Manage Address Book/Importing an IP Host Table*.

{button ,KL(`Importing an IP Host Table',2)} See Also: Importing an IP Host Table
{button ,KL(`Importing an IP Host Table',2)} See Also: Importing an IP Host Table

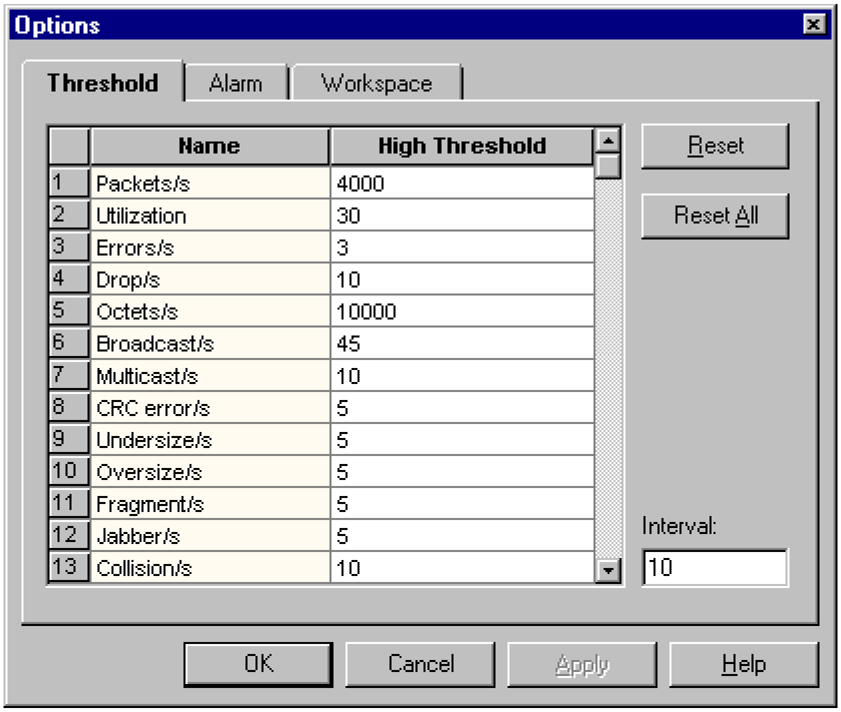
Alarm

Alarm Overview

Alarm allows you to set threshold limit for Network Statistics monitoring. When the statistics exceeds the threshold level, the NetXRay monitor logs the event and time stamp in the alarm log. You can optionally set audible alarm sound to alert the user.

Alarm Log

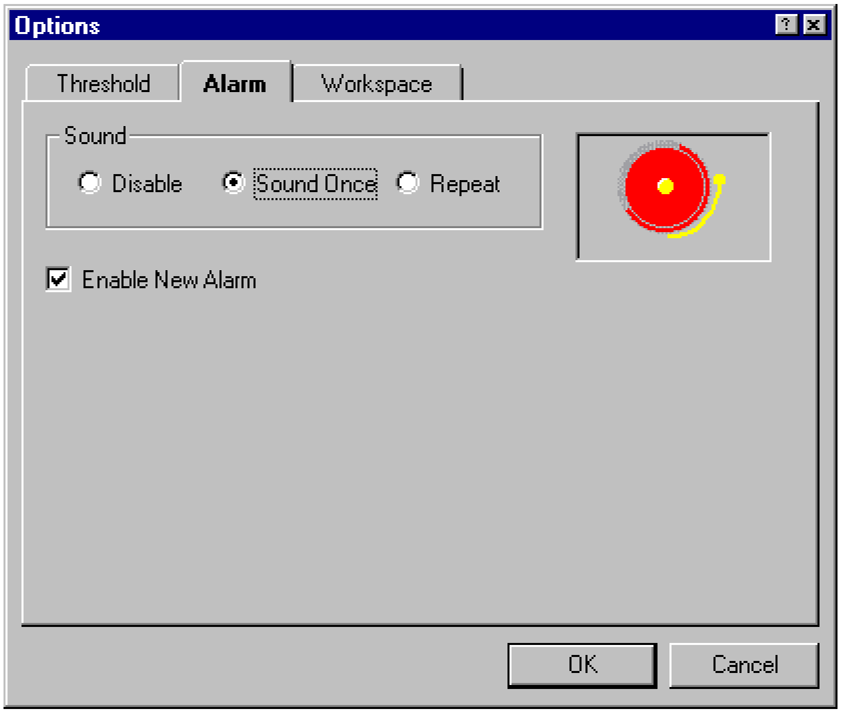
To use the NetXRay Alarm facility, you must first set up the threshold level for the network variables that you wish to monitor for abnormal activities. Select Options... from Tools menu,   a Threshold dialog page is displayed. Adjust the threshold level, and the alarm monitoring Interval.



	Name	High Threshold
1	Packets/s	4000
2	Utilization	30
3	Errors/s	3
4	Drop/s	10
5	Octets/s	10000
6	Broadcast/s	45
7	Multicast/s	10
8	CRC error/s	5
9	Undersize/s	5
10	Oversize/s	5
11	Fragment/s	5
12	Jabber/s	5
13	Collision/s	10

Interval: 10

Next, click the Alarm tab to show the Alarm options.



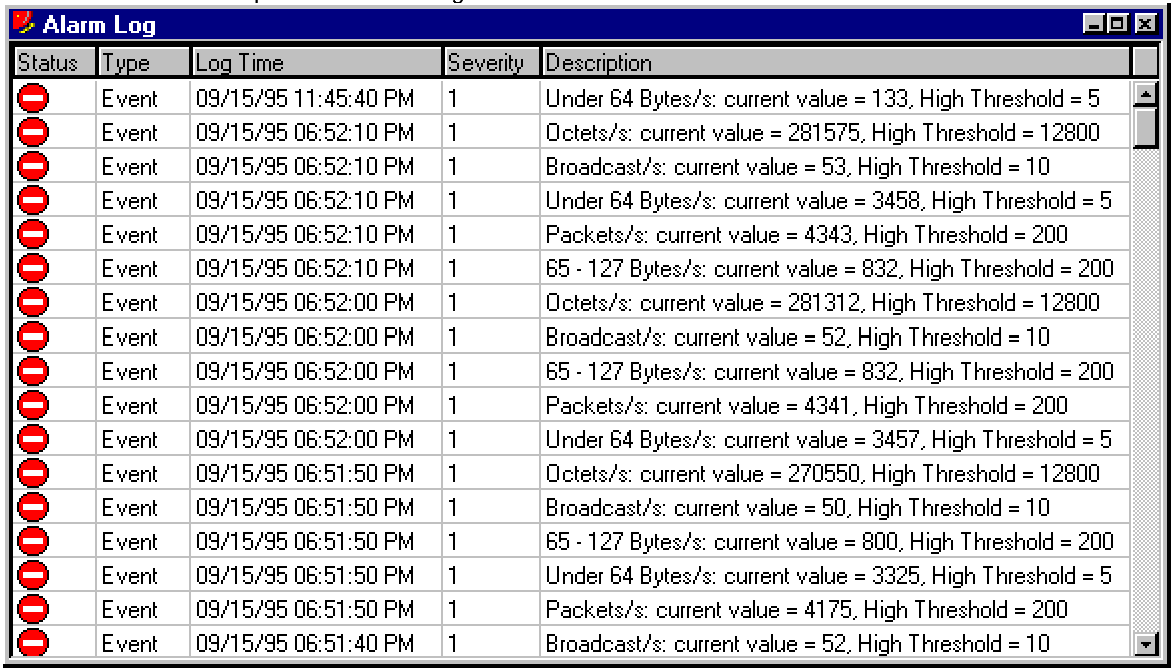
Sound

○ Disable ● Sound Once ○ Repeat

☑ Enable New Alarm

Enter the maximum log entries, alarm log sorting order, and sound option. Click OK.

NetXRay samples all network statistics based on the alarm monitor interval. Any statistics value exceeds the threshold are time stamped in the alarm log.



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

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

Multiple Network Adapters

Select Network Adapter

If you have more than one NDIS 3.1 compliant adapters installed in the system, NetXRay lets you attach to the adapter of your choice. To select an adapter, go to Tools menu and click Select Network Adapter, an Adapter dialog box will be displayed to ask you to select a network adapter as the target network for NetXRay to monitor.

Tip

- If you selected 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 wish to monitor traffic between your PC's and the remote host or server.

SNMP Mib Decode

Compiling MIB File

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 to 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 the Bay Networks' SMIC SNMP MIB compiler from Cinco's FTP server.
To download the MIB compiler,

1. Log on to ftp.cinco.com anonymously.
2. Change directory to 'users/cinco/snmp'
3. Get 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 upzip the files.

SMIC.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 file name with the prefix of 'snmp' and the file extension 'lst', then stores the OID entries into its working memory. 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. A MS-DOS window is displayed.
2. Change directory to where you saved and unziped the SMIC compiler.
3. Type in the Batch file name of you just constructed to start compiling your Mib file.
4. A SMIC output windows is displayed to list the results of the compilation.
5. Close the SMIC output window.
6. Repeat steps 3-5 until there is no error.
7. Copy the compiler output file SNMP*.LST to NetXRay program sub-directory.
8. Now you are ready to use NetXRay to decode your specific MIBs.

Context Help Objects

Post Filter

Select a filter to apply to the captured packets in the currect Packet Viewer so that unwanted packets can be filtered out.

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

No Function. Reserved for futire use.

Sample Interval

Enter the sampling interval in # of seconds. The maximum sample interval is 3,600 seconds (1 hour).

History Foreground Color

Select a foreground (legend) color for the History Graph.

History Background Color

Select a background color for the History Graph.

History Above Normal Color

Select a bar chart color for samples that exceed high threshold level. This color has no effect if you choose line or area chart.

History Normal Color

Select a bar chart color for samples that falls below high threshold level. This color has no effect if you choose line or area chart.

Send Continuously

Send the current packet continuously.

Send # of Times

Send the current packet # of times.

Set Delay

Set the delay time between packet send in milliseconds. If 0 delay is entered, NetXRay will send as fast as the system allows it to send. The overall through-put rate is depending upon the NDIS driver and CPU performance.

Edit Packet

Allow you to edit the packet content before sending. To view the packet data in the decoded form, click the Decode page.

New Packet Size

Click to invoke the Set Packet Size dialog box.

Current Packet Size

Display the current packet size.

Packet Detail Decode

Display the edited packet in detail decode format.

Send Buffer Continuously

Select this radio button for sending the current packet buffer continuouosly.

Send Buffer # of Times

Select this radio button to enter the # of times the current packet buffer to be sent.

Docking View

Check the item to make it into a Docking window. Dashboard, Capture window, and Packet Generator have been preset as normal window view.

Display Tool Bar

Check to display Tool bar.

Threshold Value

Enter threshold values to trigger the alarm. All statistical variables are monitored. If the average sampled value exceeds the threshold value, an alarm is sound. In addition, the actual statistical value and the time stamp of the alarm are logged in the event log.

Reset

Reset the current selected variable to its default value.

Reset All

Reset all variables to their default values.

Threshold Sample Interval

Set the time interval in seconds that all statistical variables are sampled and averaged.

Display Status Bar

Check to display Status bar.

Enable Alarm

Check this item to enable the generation of audible alarm and event log entries.

Disable Audible Alarm

Select this radio button to disable the audible alarm sound only.

Enable Single Audible Alarm

Select this radio button to generate the audible alarm sound once per alarm event.

Enable Repeated Audible Alarm

Select this radio button to generate the audible alarm sound repeatedly so long as at least one alarm event remained un-acknowledged in the alarm even log.

Address Type

Lets you define the address monitored be either network hardware address (6 bytes in hexadecimal value) or network IP address (4 octets).

Filter Mode: Include

INCLUDE lets you capture packets that match the address specification.

Filter Mode Exclude

EXCLUDE captures packets that do not match the address specification.

Known Addresses

Display the pre-defined broadcast and multicast addresses, and the user defined network address book. You can open and examine the detail list by clicking on the address icon ▶. Known Address list is used to simplified the definition of address filter pairs. You can drag and drop the symbolic address of your choice into either the Station 1 or Station 2 field. If you wish to capture packets that are transmitted from one network node to ANY other nodes and vice versa, drag the ‘ANY’ from the known address list to one of the station fields in the address grid.

Address Grid

Enter the address of the station 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, e.g. 100889ACD908
- IP Address 4 decimal octets separated by . (dot), e.g. 198.90.123.98

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

Protocol Filter

Select one or more protocol and sub-protocol types to filter. To reveal additional sub-protocol types, click the + sign in front of the protocol type.

Packet Size Filter Type

Select from one of the size type; All, Equal, Greater-than, Less-than, in Between, Not-In-Between.

Packet Size Filter Range 1

Enter the packet size range for the Equal, Greater-than, Less-than filters, or the first packet size range for the In-Between and Not-In-Between filters.

Packet Size Filter Range 2

Enter the second packet size range for the In-Between and Not-In-Between filters.

Current Packet Size Fitler

Display the packet size filter currently defined.

Buffer Size

Move the slider to select the memory size for the capture buffer. You can select 256K, 512K, 1M, 2M, 4M, 8M, 12M or 16M Bytes.

Packet Size

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

Stop Capture

Choose the capture action when the memory buffer is full. You can select to stop capture, or let capture wrap the memory buffer. Buffer wrap mode will overwrite the oldest packets in the memory buffer.

Wrap Buffer

Choose the capture action when the memory buffer is full. You can select to stop capture, or let capture wrap the memory buffer. Buffer wrap mode will overwrite the oldest packets in the memory buffer.

Protocol Display Open All

Click the Open All button to check all the protocols in the list box. This will expand each protocol layer details in the detail pane when viewing packets.

Protocol Display Close All

Click the Close All button to un-check all the protocols in the list box. This will contract each protocol layer into one-line summary form in the detail pane when viewing packets.

Protocol Display List

List all protocols supported by NetXRay. You can select individual protocol layer’s default display mode in fully expanded mode by checking the protocol. To display the protocol layer decode in one-line summary form, un-check it.

Packet Display Font

Select a font for the Packet Veiwer window.

Packet Display Font Style

Select a font style for the Packet Veiwer window.

Packet Display Font Size

Select a font size for the Packet Veiwer window.

Packet Display Font Sample

Display a sample of the current font and size selected

Packet Display Current Font

Display the font and point size selected

Set Packet Display Default Font

Click button to set the selected font, style and point size as the default ones for packet viewer window.

Summary Color List

The list box show all protocols that can be configured to have their unique colors in the packet viewer summary pane. To set the color, select the protocol of your choice. Then pick the color for text and background.

Summary Color Reset Button

Click Reset button to reset the protocol color back to black text and white background.

Summary Color Reset All Button

Click Reset All button to reset all protocol colors back to black text and white background.

Protocol Summary Text Color

Choose a color for the protocol summary text.

Protocol Summary Background Color

Choose a color for the protocol summary background.

New Profile Name

Enter a new name for the capture filter profile.

Copy Existing Profile

Click this radio button in order to copy from the existing capture profile into the new profile.

Existing Profiles

Select an existing capture profile to copy from.

Copy Sample Profile

Click this radio button in order to copy from the sample capture profile into the new profile.

Sample Profiles

Select a sample capture profile to copy from.

Rename: New Profile Name

Enter a new capture profile name.

Capture Profile List

Select an existing profile for rename or delete.

Done

Click this button when you finish editing the profile names.

New

Click this button to invoke the New capture profile dialog box to enter the new capture profile name.

Delete

Click this button to delete the selected profile.

Rename

Click this button to rename the selected profile.

Address Book: Name

Enter a symbolic name for the new address book entry.

Address Book: HW Address

Enter a Mac (or Hardware Address). It is typically in the form of 12 hexidecimal digits.

Address Book: IP Address

Enter an IP address for this entry. It should be in xxx.xxx.xxx.xxx notation.

Address Book: Node Type

Select from a list of node types.

Address Book: Description

Enter a free from text description for the node.

Address Book: Save/Next

Click this button to save the current entry and let you enter the next one.

Address Book: Save

Click this button to save the current entry and close the dialog box.

Go To Packet

Enter the packet number you wish to display in the packet viewer.

Find Next Packet

Click this button to search for the next packet that contains the data pattern.

Find Packet: Type

Select the data pattern type for the pattern search.

Find Packet: Data Pattern

Enter the data pattern for the packet search.

Search Direction: Up

Click this radio button to set the search direction toward the beginning of the capture buffer.

Search Direction: Down

Click this radio button to set the search direction toward the end of the capture buffer.

Save New Capture Buffer

Un-check this option so that the ‘Save as’ dialog box will not be prompted when you close the packet viewer.

Save New History Sample

Un-check this option so that the ‘Save as’ dialog box will not be prompted when you close the History graph.

Boolean Tree

An area that displays the current Boolean tree that has been defined so far.

Edit Pattern

Invoke the Edit Pattern dialog box. Allow you to modify the data pattern field contents.

Add Pattern

Invoke the Edit Pattern dialog box. Allow you to create a new data pattern.

Toggle And/Or

Toggle Boolean operator between AND and OR.

Add And/Or

Create a new Boolean Operator AND.

Toggle Not

Turn on or off the NOT operator.

Add Not

Create a NOT operator.

Delete

Delete the selected Operator or Pattern. If the Operator has other child operators or patterns, they will all be deleted.

Evaluate

Evaluate the Boolean equation immediately. If the equation is incomplete, an error message will be prompted.

Reset Data Pattern

Click this button to clear all entry fields.

Data Pattern Offset From

Select data pattern’s offset from either the beginning of the packet or the beginning of protocol layer.

Data Pattern Offset

Enter the data pattern offset in decimal value.

Data Pattern Length

Enter the data pattern length in decimal value.

Data Pattern Type

Select the data pattern type in Hex, Binary, ASCII, or EBCDIC.

Data Pattern

Enter the data pattern.

Data Pattern Name

Enter a symbolic name for the data pattern.

Data Pattern: Packet Decode

An area displays the current selected packet in detail decode form. You can select one of the fields as the desired data pattern, then click the Set Data button to fill the entry fields automatically.

Data pattern: Set Data

Click the Set Data button to fill the entry fields with data from the selected data field automatically.