Obtaining Customer Support

Intellimax distributors are responsible for first level technical support. Please contact your local vendor for technical support. You may also find answers on the Intellimax web page, or send other questions via email.

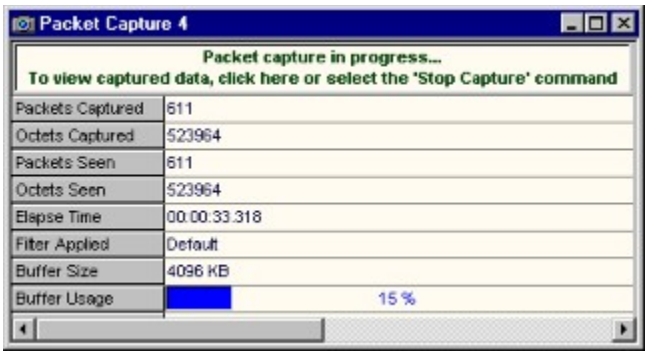
Email: support@intellimax.com
Web: http://www.intellimax.com/support.htm
Fax: (408) 588-9807

Product Overview

LanExplorer includes a protocol analyzer and our LanTrend network monitor. View network traffic from high-level statistics down to the contents of a packet. The protocol analyzer features packet capture, decode, exporting, and a traffic generator to replay captured packets. It includes:

- Protocol analyzer & network monitor with Internet traffic analysis.
- Native Win32 application program for Windows 95/98/NT4.0/2000.
- Uses existing Ethernet, Fast Ethernet, Token Ring, or WAN (e.g. 56K Modem) adapter.
- Intercepts packets in and out of the workstation or server.
- Captures all packets from the network segment (promiscuous mode).
- Decodes 802.3, 802.5, VLAN, Apple, Novell, Microsoft, TCP/IP protocols.
- Displays accumulated and historical network statistics in graphical formats.
- Shows historical statistics with threshold and alarm.
- Tells who was connecting to what Internet site.
- Discovers all local PC hosts in different network segments.
- Shows host name instead of MAC/IP address in all application windows.
- Queries DNS to translate remote IP address into Internet site name.

Network Protocol Analysis- Packet Capture and Protocol Decode

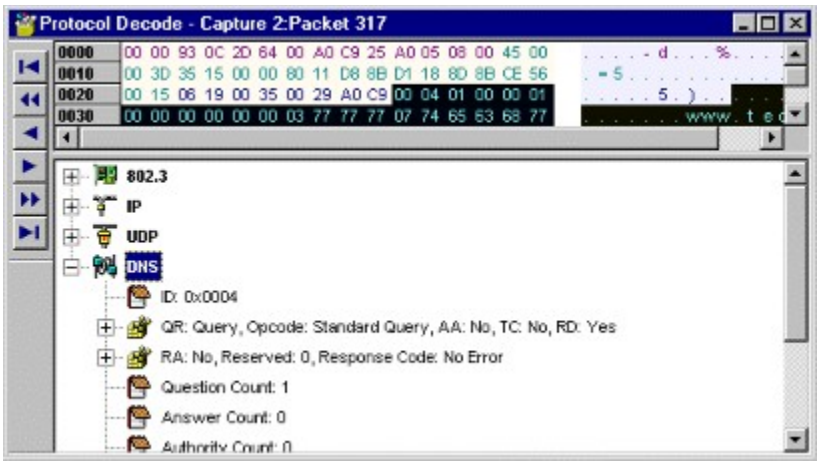


Capturing every data packets is usually an ideal way to determine and pinpoint a network problem before it becomes too complicated. LanExplorer has an internal database that recognizes the most popular network protocols and displays them in Summary, Hex, ASCII and Detail formats.

More importantly, LanExplorer can open multiple Packet Capture and Protocol Decode windows simultaneously. This is helpful where a complex problem needs packet-to-packet comparison. Double-click on any packet in the Packet Capture window; and the Protocol Decode window will be immediately displayed.

Additionally, the Packet Capture memory is flexible so users can capture several hundred Kbytes to hundreds of Mbytes - depending on the available system memory or available disk space. By using the Capture Filter feature to drop irrelevant packets, LanExplorer can capture packets for extended periods of time.

With the user-friendly GUI, clicking on destination or source stations in the Packet Capture window will allow you to select among Host Name, Network Address, and NIC Vendor Name display formats. Profile names applied to Capture Filter and Display Filter - as well as the numbers of available packets - are easily viewed at the bottom of the Packet Capture window. Time tick is in millisecond resolution and its format can be Elapse Time, Relative Time or InterPacket Time. LanExplorer also allows oversized Ethernet packets to be captured if supported by the NIC (for example, 802.1Q or Cisco's ISL VLAN packet may be larger than the maximum 1514-byte Ethernet size).


Protocol Decode - Capture 2:Packet 317
0000 00 00 93 0C 2D 64 00 A0 C9 25 A0 05 08 00 45 00
0010 00 3D 35 15 00 00 80 11 D8 8B D1 18 8D 8B CE 56
0020 00 15 06 19 00 35 00 29 A0 C9 00 04 01 00 00 01
0030 00 00 00 00 00 00 03 77 77 77 07 74 65 63 68 77
802.3
IP
UDP
DNS
ID: 0x0004
QR: Query, Opcode: Standard Query, AA: No, TC: No, RD: Yes
RA: No, Reserved: 0, Response Code: No Error
Question Count: 1
Answer Count: 0
Authority Count: 0

Network Traffic Monitoring- Network Statistics and Alarm Log

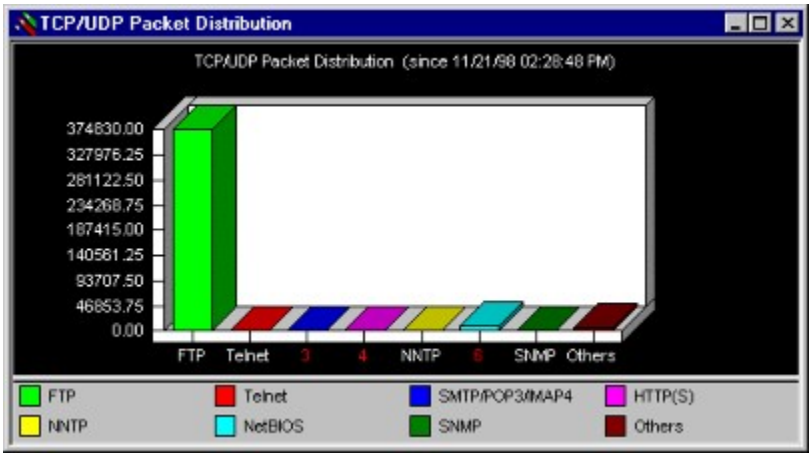
Network monitoring is a simple way to read network performance at different levels. LanExplorer provides various charts and counters for understanding the network flow and quickly responding to abnormal network activities.

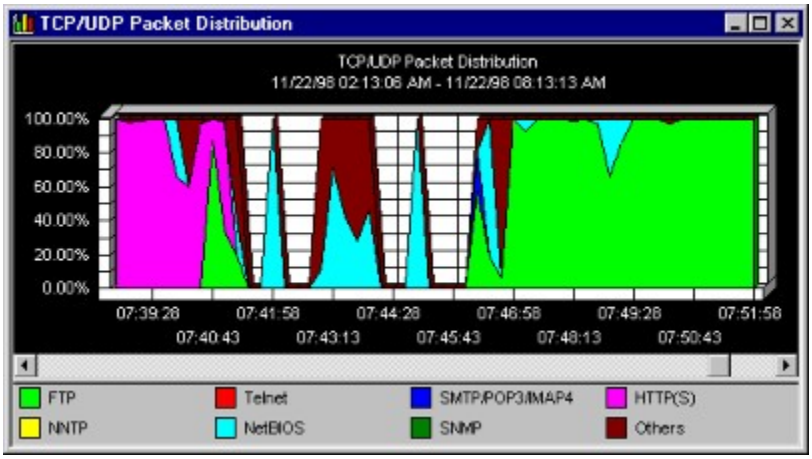
LanExplorer provides accumulated and historical statistics. The historical charts show real-time statistics that are sampled periodically - while the accumulated charts record the total activities since beginning collection.

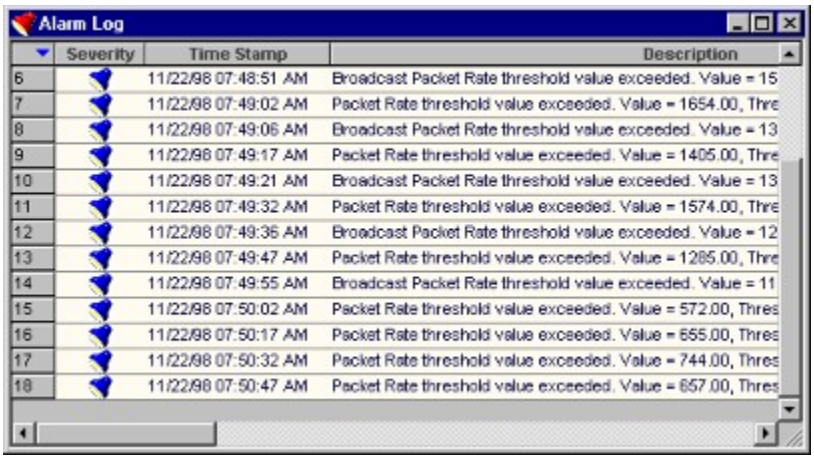
Threshold and Alarm is a very useful feature to quickly catch network problems by predefined event triggers. For example, to avoid a broadcast storm in the network, an alarm can be set if more than "1000 broadcast packets" have been seen in a "15-second" period.

To display information, LanExplorer allows user to choose from many predefined formats such as area, pie or bar charts. Following are the available network monitoring features in LanExplorer:

- TCP/UDP Distribution
- Protocol Distribution
- Packet Size Distribution
- Layer 2 Distribution
- Error Rate Counter
- Network Utilization
- Accumulated and Historical Statistics
- Threshold and Alarm





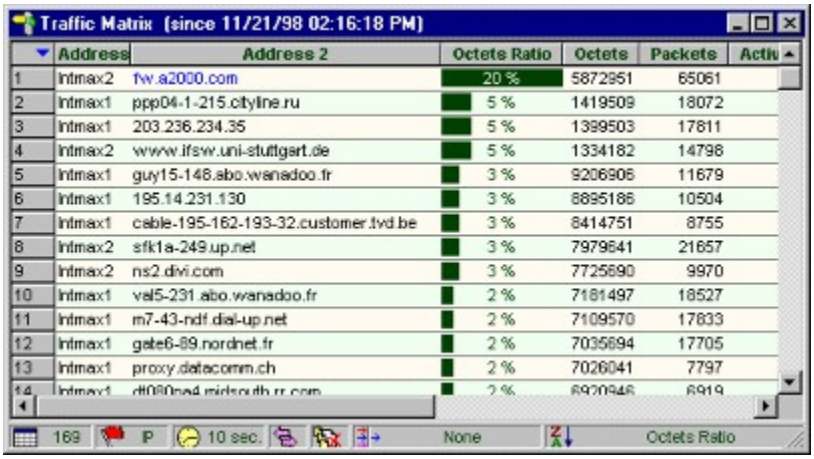

Alarm Log
Severity
Time Stamp
Description
6 11/22/98 07:48:51 AM Broadcast Packet Rate threshold value exceeded. Value = 15
7 11/22/98 07:49:02 AM Packet Rate threshold value exceeded. Value = 1654.00, Thre
8 11/22/98 07:49:06 AM Broadcast Packet Rate threshold value exceeded. Value = 13
9 11/22/98 07:49:17 AM Packet Rate threshold value exceeded. Value = 1405.00, Thre
10 11/22/98 07:49:21 AM Broadcast Packet Rate threshold value exceeded. Value = 13
11 11/22/98 07:49:32 AM Packet Rate threshold value exceeded. Value = 1574.00, Thre
12 11/22/98 07:49:36 AM Broadcast Packet Rate threshold value exceeded. Value = 12
13 11/22/98 07:49:47 AM Packet Rate threshold value exceeded. Value = 1285.00, Thre
14 11/22/98 07:49:55 AM Broadcast Packet Rate threshold value exceeded. Value = 11
15 11/22/98 07:50:02 AM Packet Rate threshold value exceeded. Value = 572.00, Thres
16 11/22/98 07:50:17 AM Packet Rate threshold value exceeded. Value = 655.00, Thres
17 11/22/98 07:50:32 AM Packet Rate threshold value exceeded. Value = 744.00, Thres
18 11/22/98 07:50:47 AM Packet Rate threshold value exceeded. Value = 657.00, Thres

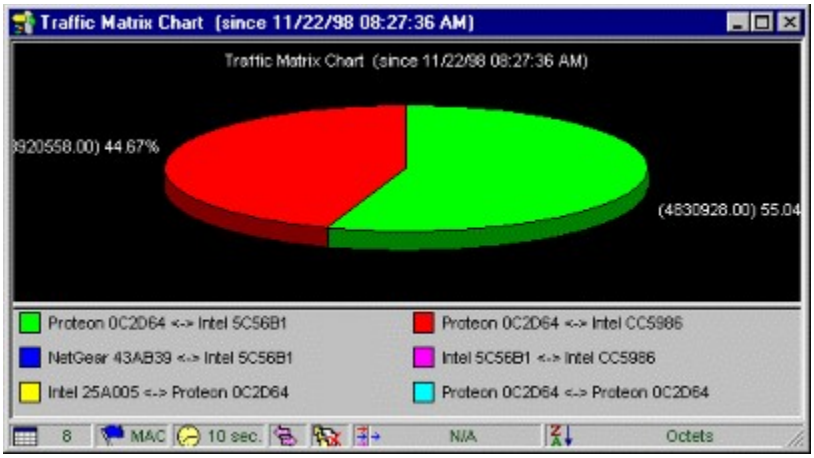
Node to Node Traffic- IP Traffic Matrix and MAC Traffic Matrix

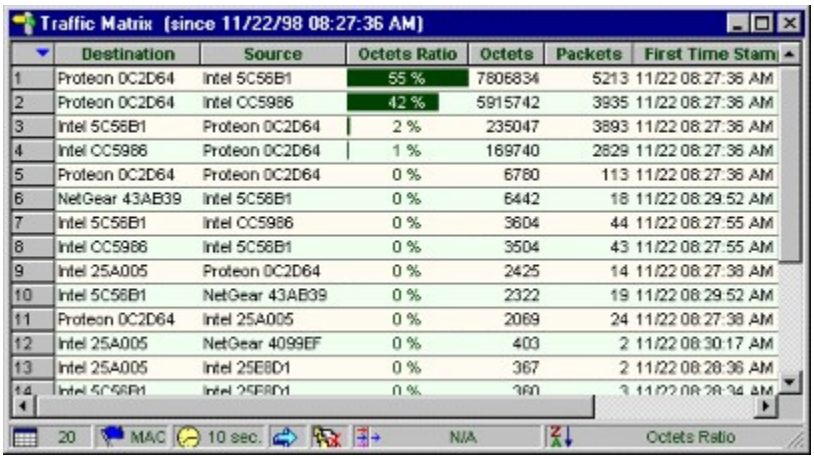
Network communication is similar to two parties talking to each other on the telephone. On networks, the parties can be two IP addresses. To receive information from the Internet, the local computer normally sends out request packets and the Internet site replies with response packets. The Traffic Matrix featured in LanExplorer is intended to collect such information between the two parties.

With a Windows 95/98 or NT computer running TCP/IP, LanExplorer can query the Domain Name Server (DNS) and identify the Internet site name while displaying the IP Traffic Matrix. At the same time, LanExplorer is polling the local network for the PC's host names. By combining the query and polling functions, the information of who (PC Host) is connecting with what Intranet or Internet site is shown in the Traffic Matrix window.

In addition to the IP Traffic Matrix, a MAC Traffic Matrix is also available to view lower level network sessions. LanExplorer provides a click-and-go method to switch between the IP Traffic Matrix and MAC Traffic Matrix. At the bottom of the Traffic Matrix window, other click-and-go flags such as one- or two-way traffic are also available.



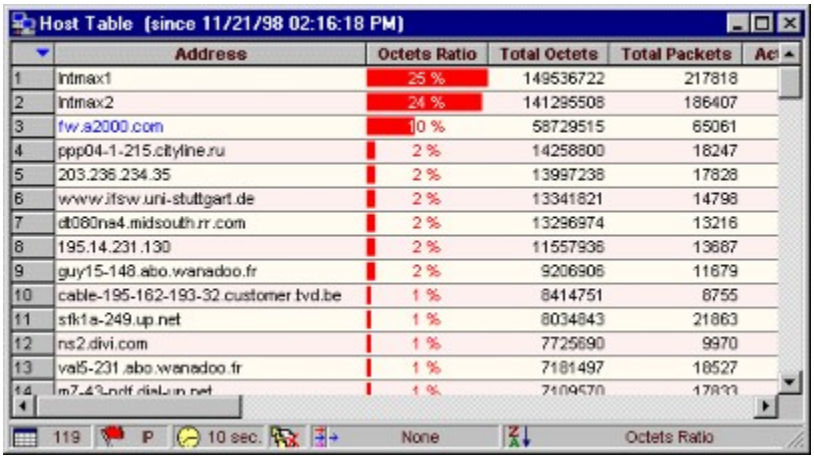


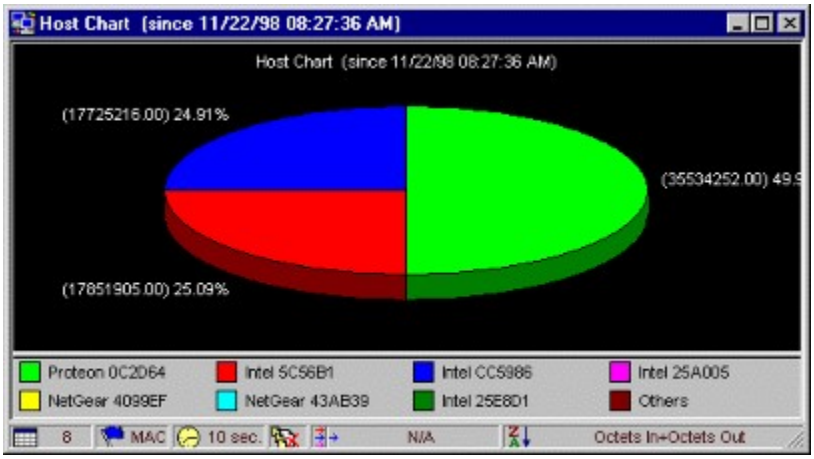

Traffic Matrix (since 11/22/98 08:27:36 AM)
Destination
Source
Octets Ratio
Octets
Packets
First Time Stam
1 Proteon 0C2D64 Intel 5C56B1 55 % 7806834 5213 11/22 08:27:36 AM
2 Proteon 0C2D64 Intel CC5986 42 % 5915742 3935 11/22 08:27:36 AM
3 Intel 5C56B1 Proteon 0C2D64 2 % 235047 3893 11/22 08:27:36 AM
4 Intel CC5986 Proteon 0C2D64 1 % 169740 2829 11/22 08:27:36 AM
5 Proteon 0C2D64 Proteon 0C2D64 0 % 6780 113 11/22 08:27:36 AM
6 NetGear 43AB39 Intel 5C56B1 0 % 6442 18 11/22 08:29:52 AM
7 Intel 5C56B1 Intel CC5986 0 % 3604 44 11/22 08:27:55 AM
8 Intel CC5986 Intel 5C56B1 0 % 3504 43 11/22 08:27:55 AM
9 Intel 25A005 Proteon 0C2D64 0 % 2425 14 11/22 08:27:38 AM
10 Intel 5C56B1 NetGear 43AB39 0 % 2322 19 11/22 08:29:52 AM
11 Proteon 0C2D64 Intel 25A005 0 % 2069 24 11/22 08:27:38 AM
12 Intel 25A005 NetGear 4099EF 0 % 403 2 11/22 08:30:17 AM
13 Intel 25A005 Intel 25E8D1 0 % 367 2 11/22 08:28:36 AM
20
MAC
10 sec.
N/A
Octets Ratio

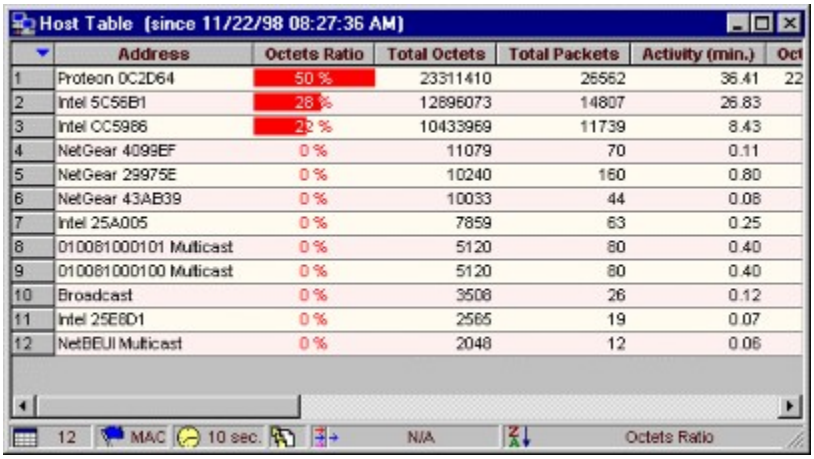
Identifying Network Nodes- Host Table and Address Book

To find active stations in the network and their traffic statistics, the Host Table displays information on every station that sends packets to and receives packets from the network. The Host Table clearly displays the most active users and the most active sites.

Address Book keeps a record of the MAC Address, IP Address and Host Name for all stations. For duplicate IP addresses in the network, Address Book highlights the stations and warns that further action might be required. Information stored in Address Book is obtained from the DNS query and auto-discovery by LanExplorer.

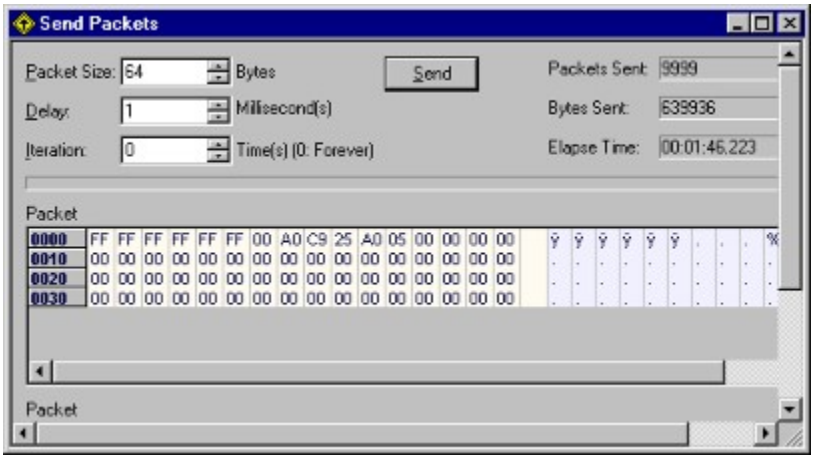


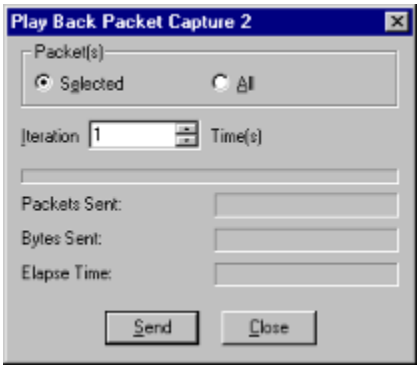




Traffic Generator- Send Packets and Playback Captured Packets

Send Packets is a traffic generator to help test new software or hardware. LanExplorer is capable of sending packets to the network while capturing packets from the network. All sent packets are looped back internally and stored in memory with the received packets. The user can copy, paste and edit existing packets to be sent. Inter-packet gaps can also be set at 1 millisecond or higher in the Send Packets window.





System Requirements

- Personal computer with a Pentium or higher processor
- Microsoft Windows 95, 98, NT 4.0, or 2000 operating system
- 32MB of memory (RAM)
- 10MB of available hard-disk space required
- VGA or higher-resolution video adapter (Super VGA, 256-color recommended)
- Mouse or compatible pointing device
- An Ethernet, Fast Ethernet, Token Ring or WAN (e.g. 56K Modem) adapter installed and configured with Microsoft TCP/IP protocol. Visit http://www.intellimax.com/network.htm for the latest list of adapters LanExplorer supports.

Hint: When running LanExplorer in the background, minimize LanExplorer instead of "toggling" to other applications. This will minimize use of system resources.

Pre-installation

Intellimax NT Service - For Windows NT/2000 only

You need to know the directory of the following Intellimax NT/2000 Service files. You will be asked at the end of LanExplorer installation for these files if you are installing under Windows NT/ 2000. These files can be found in the \DRIVERS directory on the CD, or the \DRIVERS subdirectory of the product directory (usually C:\TMAX\DRIVERS), or from the Intellimax web site.

For NT: isproto.sys and oemsetup.inf
For 2000: isproto.sys and isproto.inf

Winsock2 Component - For Windows 95 only

At the end of LanExplorer installation for Windows 95, you will be asked to install the Winsock2 component. Winsock2 is a superset of Winsock. Windows 95 includes Winsock but not Winsock2. LanExplorer requires the Winsock2 component for some features to work properly. Note: Winsock2 is a default component in Windows 98, NT 4.0 and 2000.

Installation

Install from a CD-ROM

- Get a valid Serial Number from the package you have received.
- Insert the LanExplorer CD-ROM into the CD-ROM drive.
- Double click My Computer.
- Double click the CD-ROM drive (e.g. D:\)
- Double click the SETUP.EXE file.
- Follow instructions to install the application.

Installation from a downloaded file

- Get a valid or temporary Serial Number by emailing or calling Technical Support.
- Click the self-extracting file (e.g. LANEXPLORER.EXE).
- Follow the instructions to install the application.

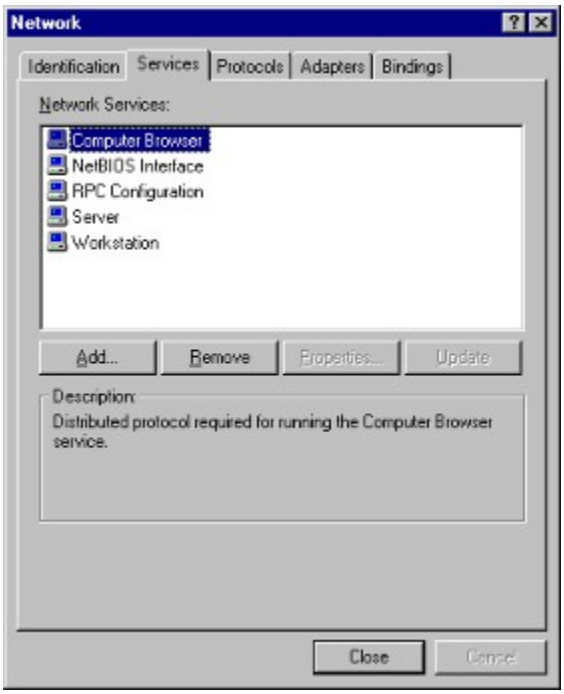
Post-installation

Intellimax NT Service - For Windows NT only

At the end of LanExplorer installation for Windows NT, you will be asked to install the Intellimax NT Service when the Network Control Panel (applet) appears. You may also click Network Control Panel at any time if you wish to reinstall or remove the network service.

- Click the Services tab.
- Click the Add button.
- Click the Have Disk button.
- Enter the path for the Intellimax NT Service (ISPROTO.SYS and OEMSETUP.INF).
- Click the OK button.
- Click the OK button again.
- Follow the instructions to reboot your system.

Before the Service Installation



After the Service Installation

Intellimax 2000 Service - For Windows 2000 only

At the end of the product installation, you will be asked to install the Intellimax Network Service when the Local Area Connection Properties (applet) appears. You may also run 1.) Control Panel 2.) Network and Dial-Up Connections 3.) Property of Local Area Connection at any time if you wish to reinstall or remove the Network Service driver.

- Click the Install button.
- Select Protocol then click the Add button.
- Click the Have Disk button.
- Enter the path for the Intellimax Network Service (ISPROTO.SYS and ISPROTO.INF).
- Click the OK button.
- Click the OK button again.
- Click the Close button and reboot your system.

Uninstalling LanExplorer

Uninstalling the LanExplorer application

- Click the Desktop Start button.
- Move mouse to Programs
- Move mouse to Intellimax
- Click LanExplorer unInstallShield.
- Follow the instructions to remove LanExplorer from your system.

Uninstalling Intellimax NT Service – Additional Procedure for Windows NT only

- Click Network Control Panel (applet).
- Click the Services tab.
- Click Intellimax NT Service.
- Click the Remove button.
- Follow the instructions to reboot your system.

Uninstalling Intellimax 2000 Service – Additional Procedure for Windows 2000 only

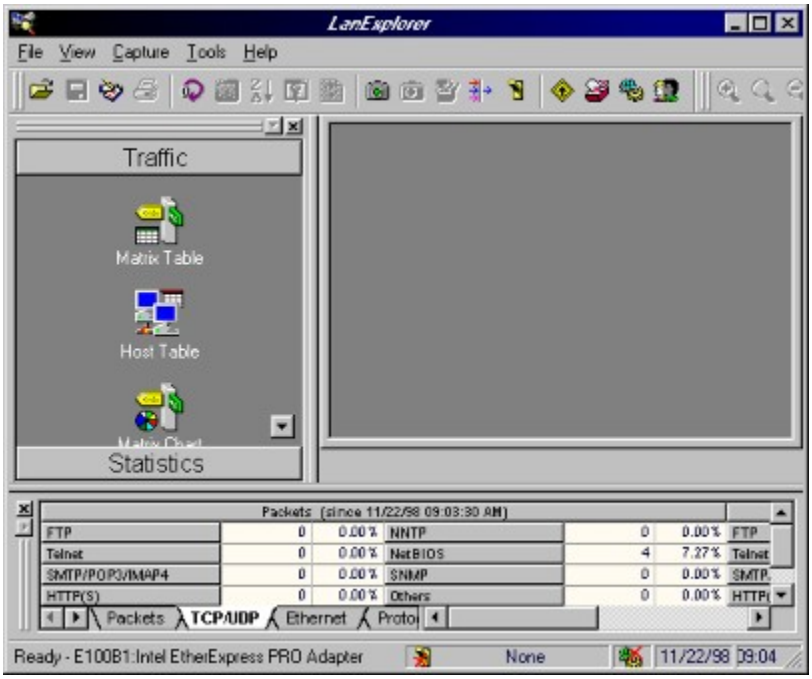
- Run 1.) Control Panel 2.) Network and Dial-Up Connections 3.) Property of Local Area Connection
- Click Intellimax Network Service.
- Click the Uninstall button.
- Follow the instructions to reboot your system.

Starting LanExplorer

To launch the LanExplorer application, do the following steps on the Desktop.

- Click the Desktop Start button.
- Move mouse to Programs.
- Move mouse to Intellimax.
- Click LanExplorer2.1.

You can also create a shortcut of the LanExplorer2.1 application (probe.exe) on the Desktop and launch the application from the shortcut. The following window, the main window of LanExplorer2.1, appears after launching the application.



Menu Bar

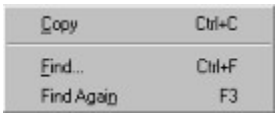
Menu bar consists of a set of menus at the top of the LanExplorer main window. Clicking any Menu in the Menu bar will bring up a list of menu items.

File Menu

File menu has commands to open file, choose preferences, set up printer, set up page and exit from LanExplorer.

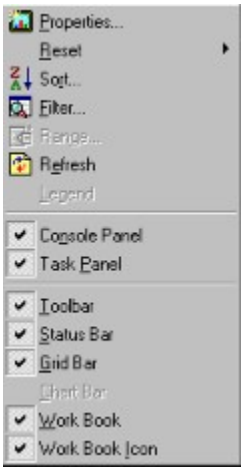
Edit Menu

Edit menu has commands to copy packets to Clickboard and find name in the active window.



View Menu

View menu has commands to bring up windows, Toolbar, Status bar, etc.

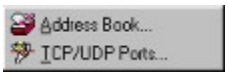


Capture Menu

Capture menu has commands to start capture, stop capture, set up filters, set up triggers and reset statistics counters.

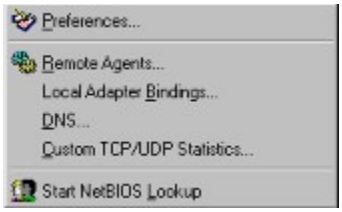
Profiles Menu

Profiles Menu has commands to call up Address Book and TCP/UDP Ports.



Settings Menu

Settings Menu includes global configuration options such as general preferences, remote agents, and DNS. These should be defined after installing the program, but may also be updated at any time.

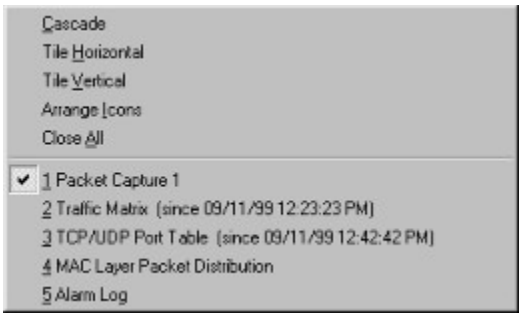


Tools Menu

Tools Menu has commands to playback packets and to send packets.

Window Menu

Window menu has commands to manipulate LanExplorer windows.



Toolbar

Toolbar is a pictorial menu of commands that you might use frequently. LanExplorer provides the icon-driven commands for easy use. You can place the mouse pointer over a Toolbar command to see the command tool tip. User can hide the Toolbar by deselecting the "Toolbar" menu item of the View Menu. Toolbar can be docked at either side of the main window.


Open


Save


Print


Reset Console Statistics


Display Properties


Sort


Display Filter


Refresh


Start/Stop Packet Capture


Show Protocol Decode


Capture Filter


Capture Trigger


Send Packets


Address Book


TCP/UDP Port Definition


Preferences


Remote Agent


NetBIOS Lookup

Status Bar

Status Bar is at the bottom of the main window to show the application status and brief command description. You can hide the Status Bar by deselecting the "Status Bar" menu item of the View Menu. There are two commands you can invoke from the Status Bar, Packet Capture Trigger and Remote Agents.

Packet Capture Trigger

Packet Capture Trigger is off.

Click the Packet Capture Trigger pane of the Status Bar will bring up the Packet Capture Trigger window and then you can configure the trigger.

Remote Agent

Remote Agents is off.

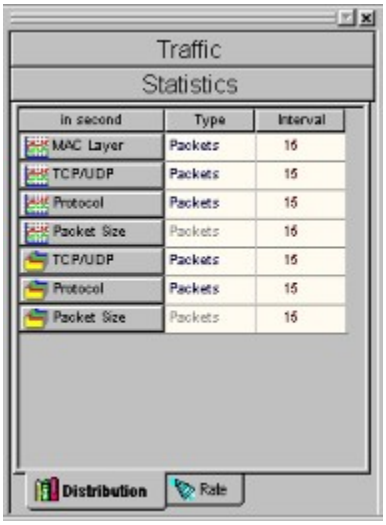
Click the Remote Agents pane of the Status Bar will bring up the Remote Agents control window and then you can switch between local and remote adapters.

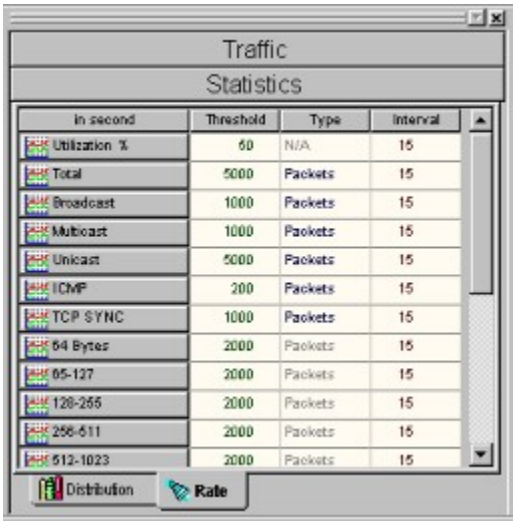
Traffic Task Panel

Traffic Task Panel shows all available windows that can be opened. It includes Traffic Matrix Table, Traffic Matrix Chart, Host Table, Host Chart and Alarm Log. Simply click the icon to bring up the application window. If the Statistics Task Panel is shown, click the Traffic bar of the Task Panel to switch to the Traffic Task Panel.

Statistics Task Panel

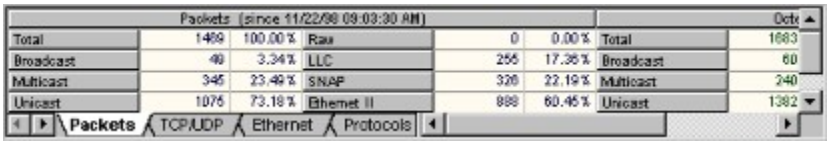
If the Traffic Task Panel is shown, click the Statistics bar of the Task Panel to switch to the Statistics Task Panel. Statistics Task Panel displays a list of Distribution, Rate and TCP/UDP selections. The Distribution category (by selecting the Distribution tab) consists of accumulated and historical charts such as Protocol distribution, TCP/UDP distribution and Packet Size distribution. In the Rate category (by selecting the Rate tab), rate can be selected to view and also trigger an alarm if the threshold is exceeded in a certain Interval. The TCP/UDP category (by selecting the TCP/UDP tab) contains charts for FTP, Telnet, etc. In any category, clicking any parameter cell can modify the parameter. To launch a window, simply click the button such as "MAC Layer" or "Utilization".





Console Window

Console Window is in tabular format at the bottom of the LanExplorer main window. The statistics in the Console Window are the same as the accumulated statistics in the History Panel but are shown in different format. You can hide the History Panel by deselecting the "Console Window" menu item of the View Menu or clicking the close button at the upper left corner of the Console Window. Console Window can be docked at the top or bottom of the main window.

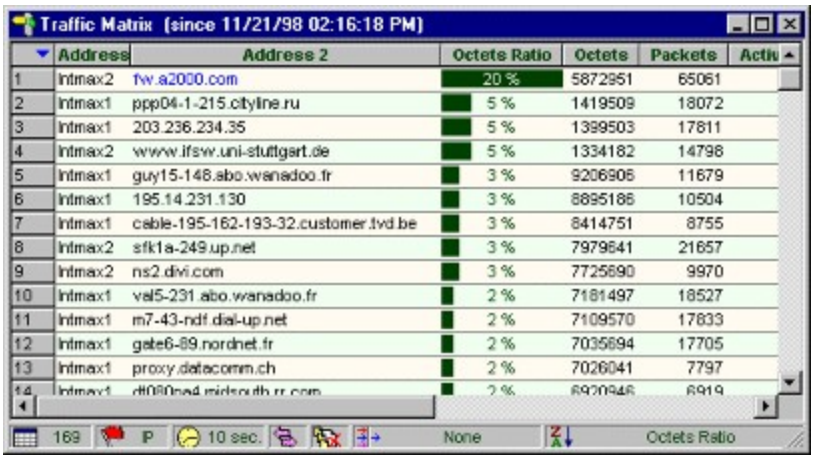


Click a tab at the bottom of the Console Window to see different kinds of accumulated statistics. Available tabs are:

- Packets
- TCP/UDP
- Ethernet or Token Ring
- Protocols
- Packet Size

Launching Traffic Matrix Table

Click the Matrix Table icon in the Traffic Task Panel to launch the Traffic Matrix Table window. Traffic Matrix Table shows the conversation between two stations. Traffic Matrix Table Status Bar at the bottom of the Traffic Matrix Table window shows the current status and also allows changes such as selecting between the IP and MAC Traffic Matrix Table.



Traffic Matrix Table displays the following information.

- Address1 (Source address if one-way traffic; Address 1, Address 2 based on packet contents)
- Address2 (Destination address if one-way traffic)
- Octets Ratio (Based on the octet count in the Traffic Matrix table)
- Number of octets (for most purposes, octets = bytes)
- Number of packets (Network traffic travels in packets)
- Activity in minutes
- Hits/Calls (Number of TCP connections)
- IP Packet Type
- First Access Time Stamp
- Last Access Time Stamp

Tip: Use ‘‘drag and drop’’ to change the order of the columns on the Traffic Matrix. Click on a column heading with the left mouse button; then while holding down the mouse button, drag the column to its new place. Release the mouse button to drop the column in place.

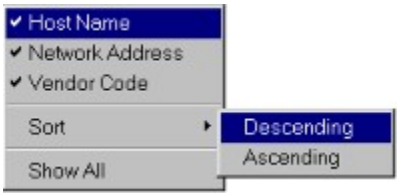
Traffic Matrix Table Options

Cell Options

There are several options to display Address1 and Address2. The table will automatically attempt to resolve and display names in the following order. For example, if the Host Name cannot be resolved, then the Network Address will be displayed.

- Host Name or Domain Name (discovered from NetBIOS or DNS queries)
- Network Address (e.g. IP Address)
- MAC address with IEEE Vendor Code or 12-byte MAC Address

Click the right mouse button on any address cell (except the blue hyperlink address) in the Traffic Matrix Table or Host Table window, and a popup menu will appear with display options. The IP tables (for the Traffic Matrix Table and Host Table) will not show "Network Address" and "Vendor Code" options. "Network Address" and "Vendor Code" options are only available on the MAC tables.



The menu gives you the following options:

- If the Host Name item is checked, program will display host name or domain name for the Address field, if available. This is only displayed if the item can be resolved.
- If the Network Address item is checked, program will display network IP address for the Address field, if available. This is only displayed if the item can be resolved.
- If the Vendor Code item is checked, program will display MAC address with IEEE Vendor Code for the Address field. This is only displayed if the item can be resolved.
- If none of the menu items are checked, program will display the 12-byte MAC address for the Address.
- Sort the entries in the Traffic Matrix Table window by the column you selected.
- Show all columns and rows in the window. This option is useful to get all columns and rows back to the table if any of them were removed from the table. Feature: column or row can be removed from the current table display by dragging the line between any two column title cells or row title cells to the left or right to close the column or row.

Traffic Matrix Sorting

Any column in the Traffic Matrix Table window can be sorted in descending or ascending order. First, select a column to sort by clicking any cell in that column. Below is an example that the "8576" cell in the first row was selected before sorting the Octets column. Then click the right mouse button and select "Sort Descending" from the popup menu. After sorting the Octets column in descending order, the Traffic Matrix Table entry with the most octets "13470" will be listed first on the Traffic Matrix Table window.

	Address 1	Address 2	Packets	Octets
1	Lockhaven	02FFFFFFFFF	134	8576
2	Lockhaven	Broadcast	113	13470
3	02A0C95C56B1	02FFFFFFFFF	76	4864
4	Lockhaven	01FFFFFFFFF	72	4608
5	04A0C95C56B1	02FFFFFFFFF	63	4032
6	Lockhaven	NetBEUI Multicast	51	10287

Before sorting Octets descending

	Address 1	Address 2	Packets	Octets
1	Lockhaven	Broadcast	113	13470
2	Lockhaven	NetBEUI Multicast	51	10287
3	Lockhaven	02FFFFFFFFFF	134	8576
4	02A0C95C56B1	02FFFFFFFFFF	76	4864
5	Lockhaven	01FFFFFFFFFF	72	4608
6	04A0C95C56B1	02FFFFFFFFFF	63	4032

After sorting Octets descending

Tip: Use a ''quick'' sort by double clicking anywhere in the column on the table.

Tip: Sorting options are also accessible from the Status Bar - see below.

Another example of sorting the Address 2 column in "Ascending" order is shown below. The "Broadcast" cell was selected before the sorting action was taken. Notice numbers come before alphabets after sorting is completed.

	Address 1	Address 2	Packets	Octets
1	Lockhaven	Broadcast	150	18088
2	Lockhaven	NetBEUI Multicast	68	13874
3	Lockhaven	02FFFFFFFFFF	134	8576
4	02A0C95C56B1	02FFFFFFFFFF	76	4864
5	Lockhaven	01FFFFFFFFFF	72	4608
6	04A0C95C56B1	02FFFFFFFFFF	63	4032

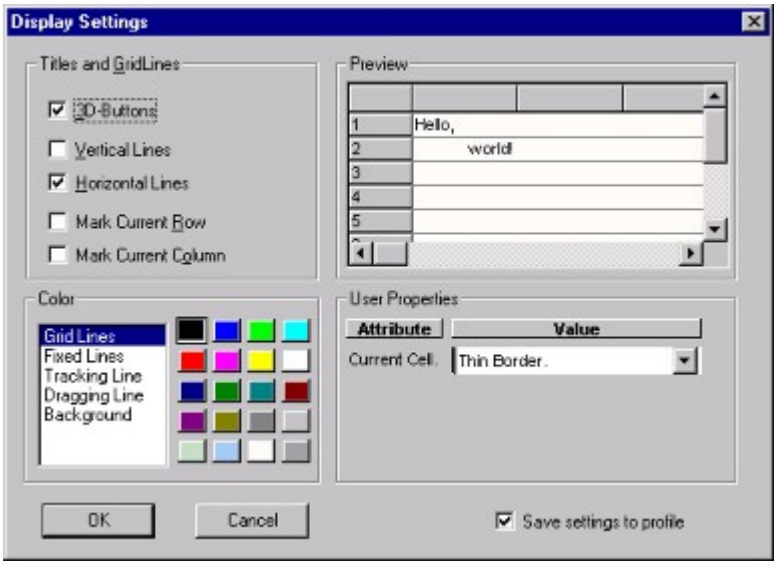
Before sorting Address2 ascending

	Address 1	Address 2	Packets	Octets
1	Lockhaven	01FFFFFFFFFF	72	4608
2	Lockhaven	02FFFFFFFFFF	134	8576
3	02A0C95C56B1	02FFFFFFFFFF	76	4864
4	04A0C95C56B1	02FFFFFFFFFF	63	4032
5	Lockhaven	Broadcast	151	18340
6	Lockhaven	NetBEUI Multicast	68	13874

After sorting Address2 ascending

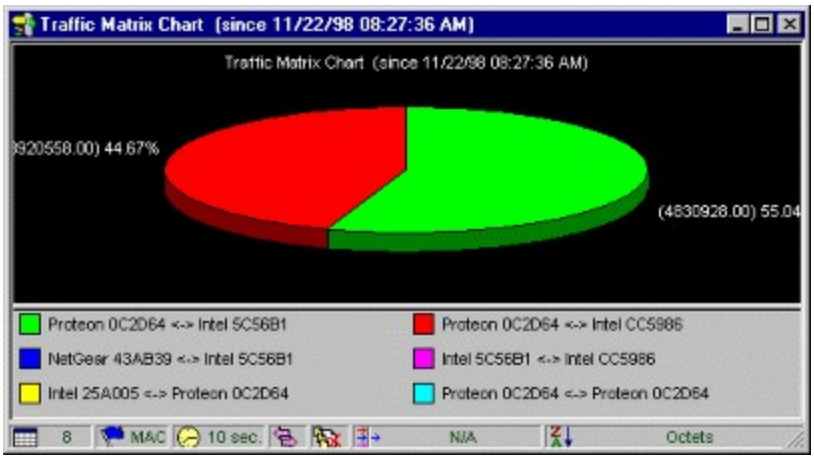
Display Settings

Click the left mouse button once on the Traffic Matrix Table window to select the active window. Click the Display Properties command in Toolbar or the Properties item of the View menu to launch the Display Settings window. Please refer to the general information section of Grid (Table) window for more information on changing the display settings.



Launching Traffic Matrix Chart

Click the Matrix Chart icon in the Traffic Task Panel to launch the Traffic Matrix Chart window. Traffic Matrix Chart shows the distribution of Traffic Matrix. Traffic Matrix Chart Status Bar at the bottom of the Traffic Matrix Chart window shows the current status and also allows for changes such as selecting between the IP and MAC Traffic Matrix Chart.

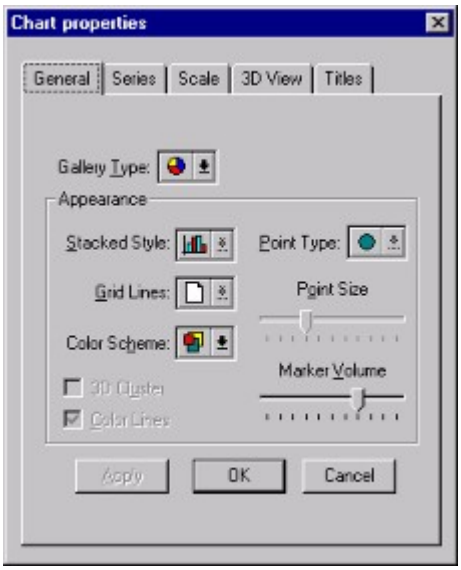


Tip: Double click on any piece of the chart to see a quick statistic.
Tip: Double click on the legend to minimize the legend.
Tip: Adjust the legend size by clicking anywhere in the legend.
Tip: Statistics can be saved to file by selecting File, Save, and TSV (tab separated value) for the "Save as type."

Traffic Matrix Chart Options

Chart Properties

Click the left mouse button once on the Traffic Matrix Chart window to select the active window. Click the Display Properties command on the Toolbar or the Properties item of the View menu to launch the Chart Properties window. Please refer to the general information section of the Chart window for more information on changing chart properties.



Tip: Many items on the charts are clickable or adjustable. Just give it a try.

Traffic Matrix Status Bar

This section described the status bar at the bottom of the Traffic Matrix Table and Traffic Matrix Chart windows. Each window has independent parameters when changing the configurations except the polling interval that can also be changed in Settings/Preferences and the change applies to both table and chart windows.

Toggle MAC Window and IP Window

Click the MAC or IP pane in the Traffic Matrix Status bar to toggle the current Traffic Matrix selection. If IP Traffic Matrix is selected, all non-IP traffic such as IPX and NetBEUI protocol packets will not be counted and displayed.

MAC Traffic Matrix (next to a blue flag) is the current selection.

IP Traffic Matrix (next to a red flag) is the current selection.

Tip: Use the IP table to shows IP addresses (across routers), and the MAC table to identify traffic by physical addresses (bound by router). This difference will be helpful in understanding the traffic patterns.

Changing Polling Interval

Polling Interval Pane

Polling interval can be changed by clicking the pane or by selecting Settings, Preferences from the menu. For more information, please refer to the chapter that describes the LanExplorer preferences.

Tip: Increase the polling interval to minimize processing for screen refreshes.

Toggle One-way and Two-way

Click the one-way or two-way pane in the status bar to toggle the traffic direction display option. Two-way traffic display shows only one entry for conversation between two stations. One-way traffic display shows two entries for conversations between two stations, assuming both stations are sending packets.

Two-way traffic display is the current selection.

One-way traffic display is the current selection.

Toggle Show-broadcast and No-broadcast

Click the broadcast/multicast pane in the status bar to toggle the broadcast/multicast display option. No-broadcast traffic only shows traffic between the client and server (unicast). Any broadcast or multicast packet is eliminated.

No-broadcast traffic is the current selection.

Show-broadcast traffic is the current selection.

Changing Traffic Matrix Filter

Filter Pane
↓

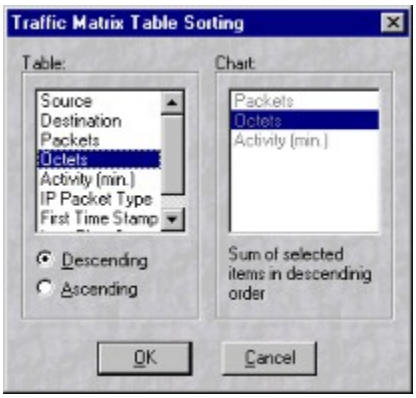
A display filter can be applied to the Traffic Matrix Table or Traffic Matrix Chart window. Please refer to the chapter that describes filters.

Tip: Change the filter by clicking on the filter pane or by selecting View, Filter from the menu.

More Sorting Options

Sorting Pane

Click the sorting pane in the Traffic Matrix Status bar or the Sort item of the View menu while the Traffic Matrix is the active window will bring up a sorting dialog box as below.



A list of sorting items for the table window is on the left of the dialog box. Only one item can be selected from the distribution list and the Descending or Ascending option must be selected as well. Available sorting items for the window are listed below.

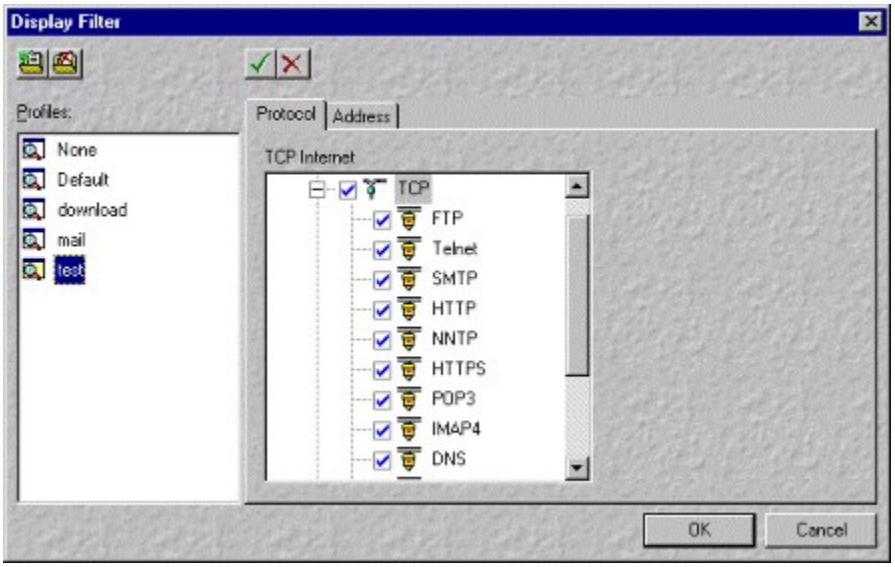
- Source address
- Destination address
- Octets Ratio
- Number of packets
- Number of octets
- Activity in minutes
- Hits/Calls
- IP Packet Type
- First Access Time Stamp
- Last Access Time Stamp

A list of sorting items for the chart window is on the right of the dialog box. More than one item can be selected at a time. To perform multiple selections, hold the control key while clicking the left mouse button. Available sorting items for the chart window are listed below.

- Number of packets
- Number of octets
- Activity in minutes
- Hits/Calls

Table & Chart Display Filters

Display filters can be applied to the Traffic Matrix Table and Traffic Matrix Chart. Select "Filter" from the View menu or click the Filter Pane of any window to launch the Display Filter window. Display Filter consists of two groups of filters, Protocol Filter and Address Filter. To change a filter, select and edit the "Default" filter profile or create a new filter profile. The "None" filter profile cannot be changed and is pre-defined in the application.



Setting up Profiles

New Profile
Delete Profile

With LanExplorer, users can define his/her own filter profile. The New Profile button is next to the Profile name box and you can see the New Profile name in the adjacent editable combo box. Simply click the New Profile button and enter a name for the new profile. Then check or uncheck the boxes below to compose the new profile. Filter profile covers both protocol and address filters. Click another tab to add or delete more filters for the new profile. Click the OK button to save the new profile. All profiles in LanExplorer are saved for later use. Clicking the combo box in the Profile will give you a list of profiles to choose from. You can delete any profile except the default profile.

Select All and Clear All

Select All
Clear All

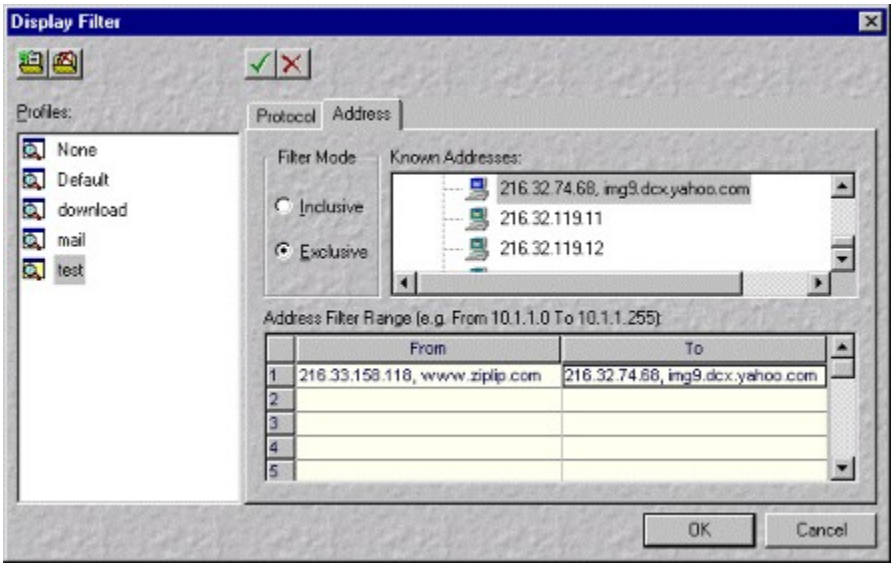
There are two buttons on the upper-center of the window available to select all filter check boxes or clear all filter check boxes. If there are 20 check boxes selected and you want to delete 19 of them, the fastest way is to clear all, then check the one you want.

Protocol Filter

Protocol Filter has a pre-defined list of Internet protocols that can be included or excluded. To change the filter, select or deselect the check box before each protocol name.

Tip: The protocol filter uses an "or" condition between each protocol. So if only "FTP" traffic is desired, then the other protocols, including the lower layer "TCP" protocol, must be deselected.

Address Filter



Address Filter takes the IP address only. Use Drag and Drop to move addresses from the Known Address table to the Address Filter list. Simply press and hold the left mouse button on the known address and move the pointer to either "From" or "To" of the Address Filter list and then release the mouse button.

- **Inclusive option**

If either address of an entry is in the Address Filter, the entry will be seen in Traffic Matrix.

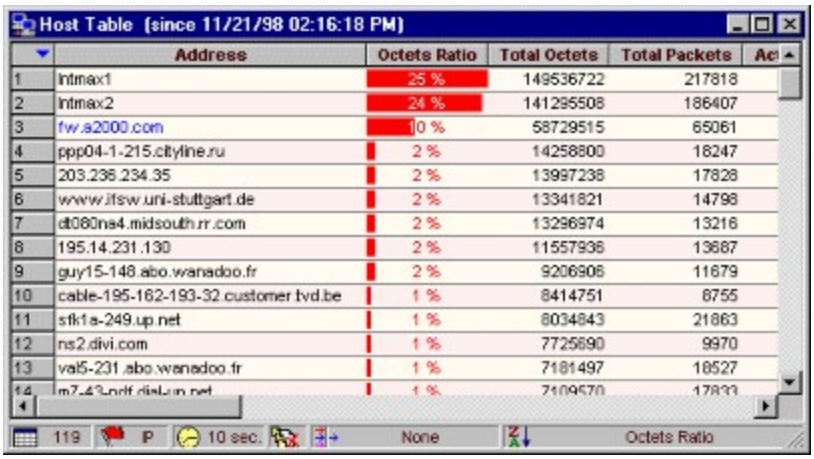
- **Exclusive option**

If both addresses of an entry are in the Address Filter, the entry will not be seen in Traffic Matrix. Given a list of all internal IP addresses in the Address Filter, Traffic Matrix will show only Internet access traffic.

Tip: IP address, host name, or domain name may be directly entered in the address field. The Filter will automatically resolve the host name or domain name to the appropriate IP address.

Launching Host Table

Click the Host Table icon in the Traffic Task Panel to launch the Host Table window. Host Table displays all individual IP or MAC stations. Host Table Status bar at the bottom of the Host Table window shows the current status and also allows changes such as selecting between the IP Host Table or MAC Host Table.



In Host Table, the following information is displayed.

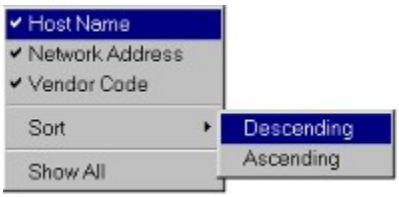
- Address
- Octets Ratio
- Total octets
- Total packets
- Activity in minutes
- Hits/Calls
- Number of packets in
- Number of octets in
- Number of packets out
- Number of octets out
- Number of broadcast packets
- Number of multicast packets
- IP Packet Type
- First Access Time Stamp
- Last Access Time Stamp

There are several ways to display Address. Please refer to the Traffic Matrix Table Options section of this chapter for details.

Host Table Options

Cell Options

Clicking the right mouse button on any address cell in the Host Table will show a popup menu as below. IP Host Table will not show “Network Address” and “Vendor Code” options. Please refer to the Traffic Matrix Table Options section of this chapter for the description of this menu.



Host Table Sorting

Any column in the Host Table window can be sorted in descending or ascending order. First, select a column that you want to sort by clicking any cell in that column. Below is an example where the "Broadcast" cell of the first row was selected before sorting. Then "Sort Descending" from the popup menu was selected. After sorting the Address column, the Host Table entry with "NetBEUI Multicast" was listed first on the Host Table window because its first letter, capital "N", is the largest ASCII number.

↓ Before sorting the Address column descending

	Address	Packets In	Octets In	Packets Out	Octets Out	Broadcast	Multicast
1	Broadcast	186	22463	0	0	0	0
2	02FFFFFFFFF	273	17472	0	0	0	0
3	NetBEUI Multicast	84	17281	0	0	0	0
4	01FFFFFFFFF	72	4608	0	0	0	0
5	04A0C95C56B1	0	0	63	4032	0	0
6	02A0C95C56B1	0	0	76	4864	0	0
7	Lockhaven	0	0	476	52928	186	156

↓ After sorting the Address column descending

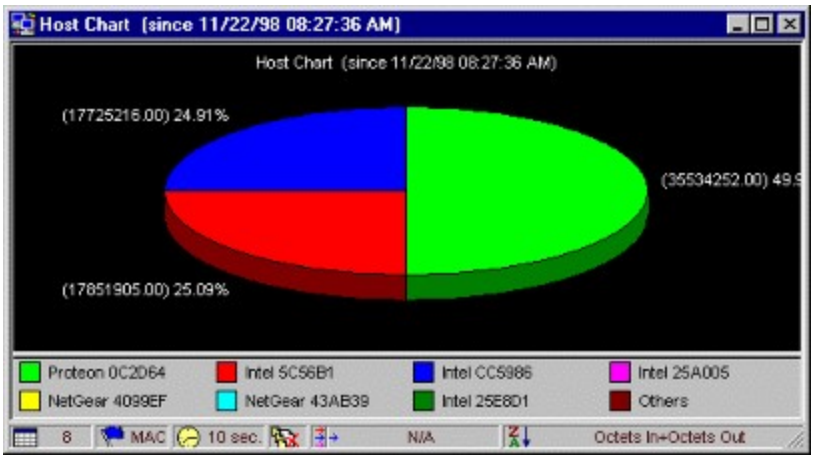
	Address	Packets In	Octets In	Packets Out	Octets Out	Broadcast	Multicast
1	NetBEUI Multicast	84	17281	0	0	0	0
2	Lockhaven	0	0	476	52928	186	156
3	Broadcast	186	22463	0	0	0	0
4	04A0C95C56B1	0	0	63	4032	0	0
5	02FFFFFFFFF	273	17472	0	0	0	0
6	02A0C95C56B1	0	0	76	4864	0	0
7	01FFFFFFFFF	72	4608	0	0	0	0

Display Settings

Click the left mouse button once on the Host Table window to select the active window. Click the Display Properties command in Toolbar or the Properties item of the View menu to launch the Display Settings window. Please refer to the general information section of Grid (Table) window for more information on changing the display settings.

Launching Host Chart

Click the Host Chart icon in the Traffic Task Panel to launch the Host Chart window. Host Chart shows the distribution of all individual IP or MAC stations. Host Chart Status bar at the bottom of the Host Chart window shows the current status and also allows changes such as selecting between the IP Host Chart and MAC Host Chart.



Host Chart Options

Chart Properties

Click the left mouse button once on the Host Chart window to select the active window. Click the Display Properties command in Toolbar or the Properties item of the View menu to launch the Chart Properties window. Please refer to the general information section of Chart window for more information on changing the chart properties.

Host Window Status Bar

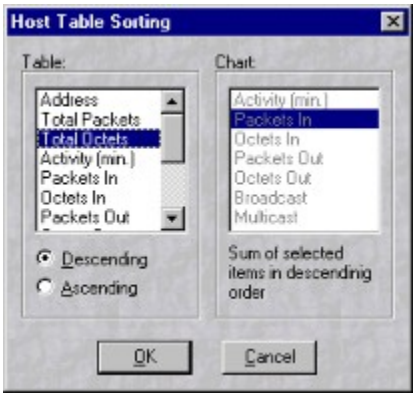
Please refer to Traffic Matrix Status Bar in this Chapter for status bar options on:

- Toggle MAC Window and IP Window
- Changing Polling Intervals
- Toggle Show-broadcast and No-broadcast
- Changing Display Filters

More Sorting Options

Sorting Pane
↓

Clicking the sorting pane in the Host window status bar or the Sort item of the View menu while the Host window is active will bring up a sorting dialog box as below.



A list of sorting items for the table window is on the left of the dialog box. Only one item can be selected from the distribution list and the Descending or Ascending option must be selected as well. Available sorting items for the table window are listed below.

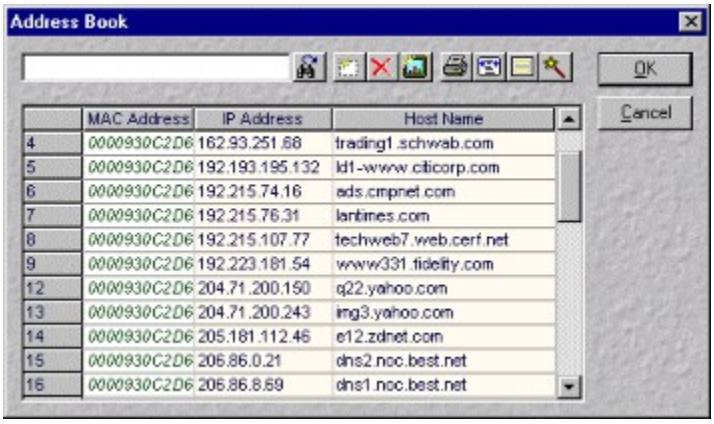
- Address
- Octets Ratio
- Total packets
- Total octets
- Activity in minutes
- Hits/Calls
- Number of packets in
- Number of octets in
- Number of packets out
- Number of octets out
- Number of broadcast packets
- Number of multicast packets
- IP Packet Type
- First Access Time Stamp
- Last Access Time Stamp

A list of sorting items for the chart window is on the right of the dialog box. More than one item can be selected at a time. To perform multiple selections, hold the control key while clicking the left mouse button. Available sorting items for the chart window are listed below.

- Activity in minutes
- Hits/Calls
- Number of packets in
- Number of octets in
- Number of packets out
- Number of octets out
- Number of broadcast packets
- Number of multicast packets

Address Book

To open the Address Book window, click the Address Book icon on the Toolbar or select "Address Book" from the Profiles Menu. Each row represents a station that can be a PC in the Local Area Network or an Internet host name.



Three columns in the Address Book identify each station in the network.

- MAC Address
- IP Address (if available)
- Host Name (if available)

MAC address is a 12-byte unique address to identify a station. For an Internet host, the MAC address is usually the local router's MAC address. If a station is not using IP as the transport protocol (e.g. IPX), the IP address column will be blank. LanExplorer discovers the local NetBIOS host name from captured NetBIOS packets and also queries the Domain Name Server (DNS) to identify the Internet host name.

When duplicate MAC or duplicate IP addresses are discovered, the Address Book displays the addresses in *Italics* and in a different color. Only the second and subsequent duplicate addresses are displayed in *Italics* and a different color.

The Host Names (or domain names) displayed in the address book are used to update the Traffic Matrix and Host tables. Changing names in the Address Book will automatically update the respective tables on the next screen refresh. Host Names may be added or overwritten in the Address Book - just click on the appropriate cell and enter a new name.

Address Book Commands

Button	***Type***	***Description***
	Find Next	Type name or address, then click this command to find.
	New	To create a new entry.
	Delete	To delete one or more entries.
	Properties	To change display settings.
	Print Table	To print the Address Book.
	Page Setup	To set up the page format.
	Header/Footer	To set up the header and the footer.
	DNS Lookup	To start DNS lookup manually.

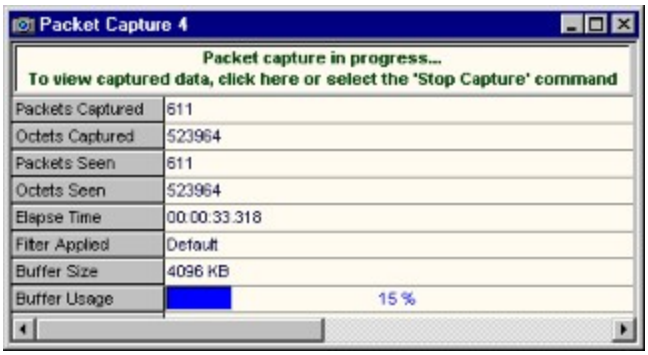
Tip: To use the Find button, first select the appropriate column by clicking on the column.

Tip: If domain names are not displaying (e.g. due to a DNS failure on the first pass), use the DNS Lookup button to start a new lookup.

Tip: The Address Book may be exported to another application - e.g. Excel - by selecting and copying the contents. To select, hold down the left mouse button and highlight the cells to copy. To copy, use Ctrl-C to copy, go to the other application, and use Ctrl-V to paste.

Starting and Stopping Packet Capture

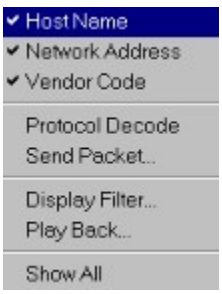
Click the Start Capture command in Toolbar or the "Start" menu item of the Capture Menu to launch the Packet Capture in-progress window. Information such as number of captured packets is updated in real time. Other information such as "Filter Applied" and "Buffer Usage" are also helpful to determine the current status of Packet Capture.



Click the Stop Capture command in Toolbar or the "Stop" menu item of the Capture Menu to stop Packet Capture. The Packet Capture window gives a snapshot of captured packets stored in memory.

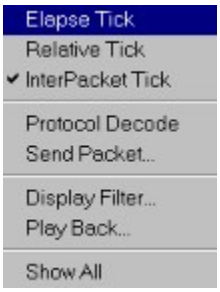
You can highlight a packet by clicking the packet. Double clicking a packet or selecting Protocol Decode command in the Toolbar menu will bring up the Protocol Decode window for the packet. To perform multiple selections, hold the control key while clicking the left mouse button.

Clicking the right mouse button on any title bar or any cell in the Packet Capture window will give you one of the popup menus as below that you can change the display format or do other functions with the packet(s).



- Destination column
- Source column

- Protocol column
- Summary column
- Size column



- Time Tick column

The menus give you the following options:

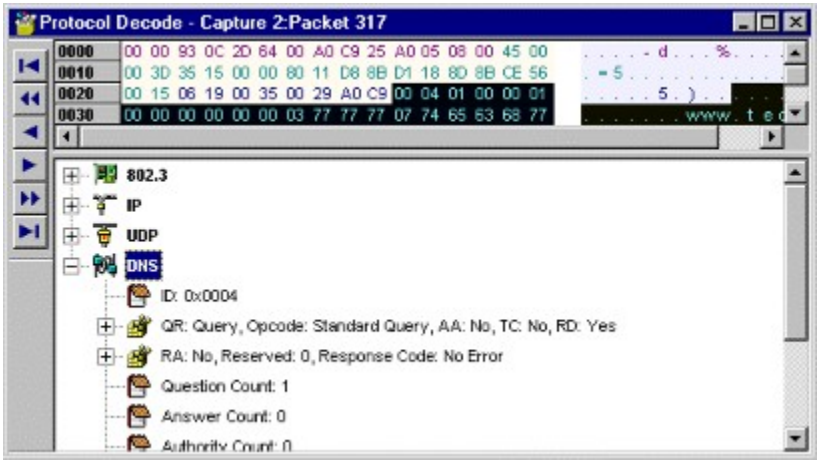
- Display host name in the Address field if available. Host Name menu item must be checked.
- Display network address in the Address field if available. Network Address menu item must be checked.
- Display MAC address with IEEE Vendor Code in the Address field. Vendor Code menu item must be checked.
- Display 12-byte MAC address in the Address field if none of the above menu items is checked.
- Bring up the Protocol Decode window.
- Bring up the Send Packets window for selected packet.
- Set up Display Filter.
- Play back the selected packets or all packets in the capture buffer.
- Show all columns and rows in the window.
- Select Elapsed, Relative or InterPacket time tick display.
  - Elapsed – measures the time of capture of each specific packet, relative to the most recent enactment of the packet capture function.
  - Relative – measures the time from each packet's capture, relative to the first packet.
  - InterPacket – measures the time between the capture of each packet, relative to the previous packet.

Viewing Packet Contents

Double click any packet in the Packet Capture window or select the Protocol Decode command, and the Protocol Decode window will be displayed with detailed protocol analysis. The upper pane of the Protocol Decode window displays the Hex and ASCII formats of the packet. The lower pane of the Protocol Decode window displays the interpreted protocols.

Click and highlight any item in either pane of the Protocol Decode window, and the corresponding item in another pane of the Protocol Decode window will be highlighted as well. This is useful for understanding the contents of a packet – byte by byte.

Six tool bar buttons on the left of the window allow for cruising of the specific packet capture buffer. They are the first, the previous-10th, the previous, the next, the 10th and the last packet from the specific Packet Capture window.



Applying Pre-capture or Post-capture Filter

Click "Capture Filter" command in Toolbar for pre-capture filter or "Display Filter" command in Toolbar for post-capture filter of a specific Packet Capture window. These filters can also be launched from the Capture Menu and the View Menu. There are five tabs for five different groups of filters. For example, click "Layer 3+" tab to set IP/TCP/UDP filters.

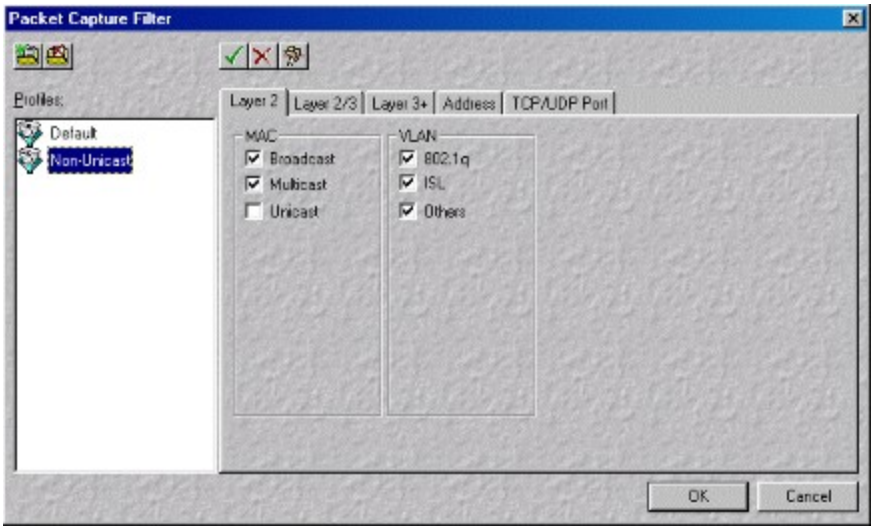
Layer 2 MAC Filter

- Broadcast
- Multicast
- Unicast

Layer 2 VLAN Filter

- 802.1q
- CISCO ISL
- Others (non-VLAN)

Layer 2 Filter Example



Layer 2/3 Ethernet II Filter

- IP/ARP
- Vines IP/Echo
- AppleTalk/ARP
- IPX
- XNS
- DEC
- Others

Layer 2/3 LLC Filter

- IP
- NetBIOS
- IPX
- SNA
- ISO
- BPDU
- XNS
- IBMNM
- RPL
- Others

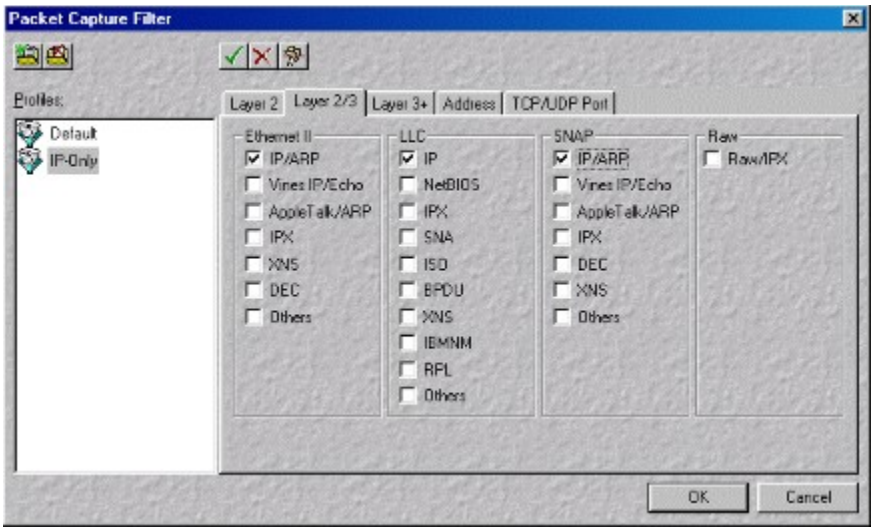
Layer 2/3 LLC SNAP Filter

- IP/ARP
- Vines IP/Echo
- AppleTalk/ARP
- IPX
- DEC
- XNS
- Others

Layer 2/3 Raw Filter

- Raw XNS/IPX

Layer 2/3 Filter Example



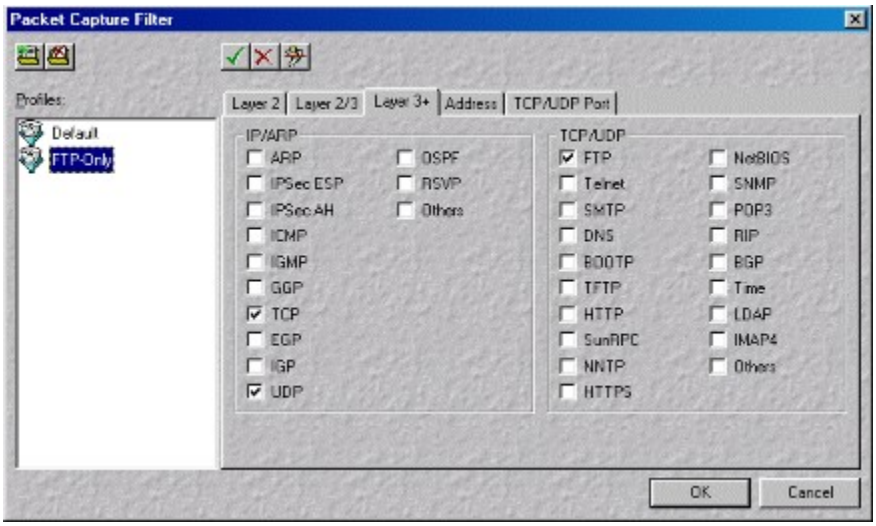
Layer 3+ IP/ARP Filter

- ARP
- IPSec ESP
- IPSec AH
- ICMP
- IGMP
- GGP
- TCP
- EGP
- IGP
- UDP
- OSPF
- RSVP
- Others

Layer 3+ TCP/UDP Filter

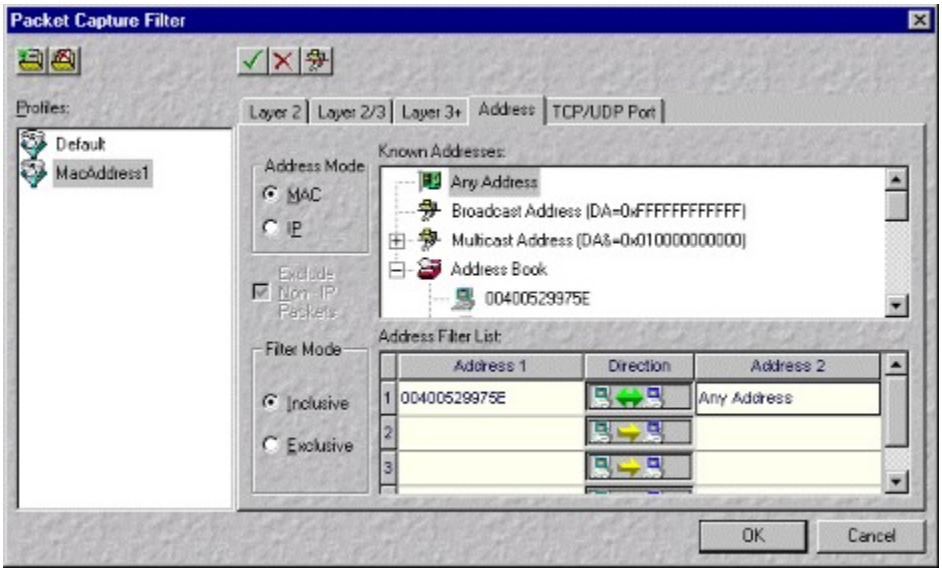
- FTP
- Telnet
- SMTP
- DNS
- BOOTP
- TFTP
- HTTP
- SunRPC
- NNTP
- HTTPS
- NetBIOS
- SNMP
- POP3
- RIP
- BGP
- Time
- LDAP
- IMAP4
- Others

Layer 3+ Filter Example



Address Filter

A maximum of four address pairs can be specified for each address filter. Configuring the address filter is described below.



- **Address Mode**

Choose between IP address and MAC address.

- **Exclude Non-IP Packets**

Do not capture non-IP packets. Option available only when Address Mode is IP.

- **Filter Mode**

Choose between Inclusive and Exclusive.

- **Known Address**

List of all predefined and learned addresses in tree view.

- **Address Filter List**

Drag and Drop is a feature to move a known address from the Known Address table to the Address Filter list in Address Filter. Press and hold the left mouse button on the known address and move the pointer to either Address1 or Address2 of the Address Filter list and then release the mouse button.

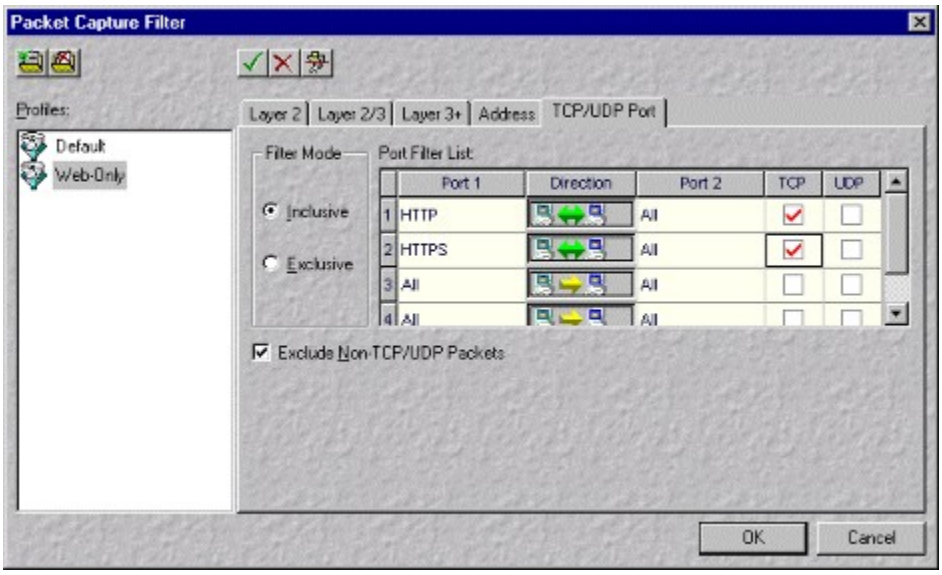
- **Direction**

Clicking a direction box between Address1 and Address2 will let you select three different ways of traffic between the two addresses.

1. Address1 to Address2 (->)
2. Address2 to Address1 (<-)
3. Address1 to Address2 and Address2 to Address1 (<->)

TCP/UDP Port Filter

A maximum of four port pairs can be specified for each TCP/UDP Port Filter. Configuring the TCP/UDP Port Filter is described below.



- **Exclude Non-TCP/UDP Packets**

Do not capture non-TCP/UDP packets. Option available only when mode is in TCP/UDP.

- **Filter Mode**

Choose between Inclusive and Exclusive.

- **Direction**

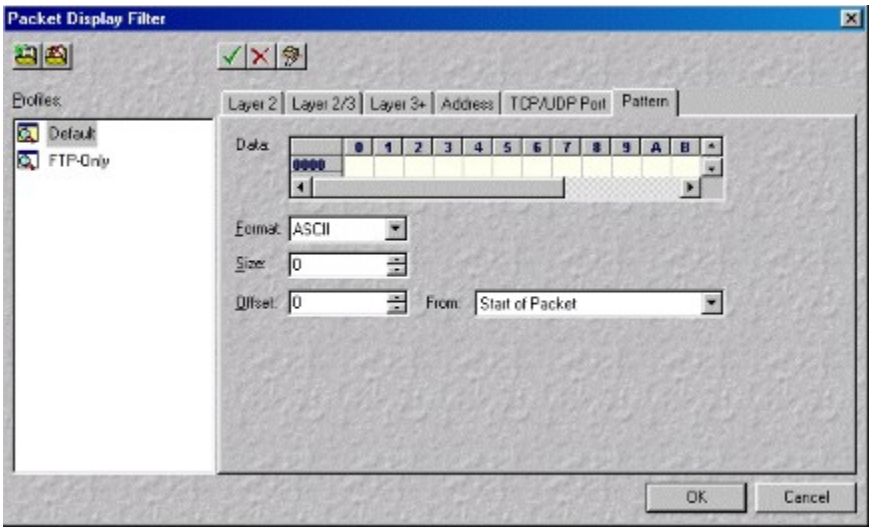
Clicking a direction box between Port1 and Port2 will let you select three different ways of traffic between the two ports.

1. Port1 to Port2 (->)
2. Port2 to Port1 (<-)
3. Port1 to Port2 and Port2 to Port1 (<->)

Pattern Filter of Post-capture Filter

Pattern Filter is a feature only available for Display Filter (post-capture filter). You can specify the data pattern to match. The packets will not be displayed in the Packet Capture window if they don't match the data pattern at the specific packet offsets. Data pattern formats can be either ASCII or HEX. Data pattern size in byte and packet offset are also available criteria for the Pattern Filter.

Below is an example where only NetBIOS Response packets will be displayed after the Pattern Filter is activated. Only packet with data pattern "0xF0" "0xF1" at the 15th and 16th byte offsets will be passed through the Pattern Filter.

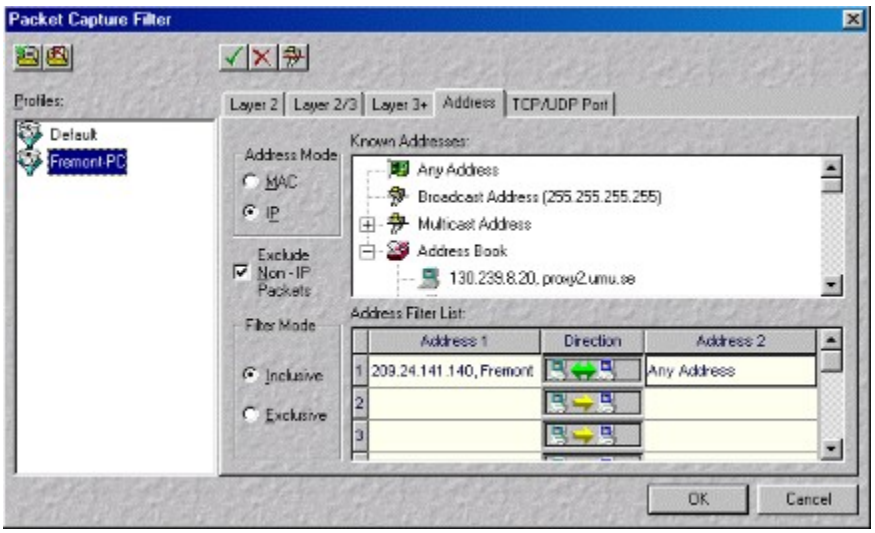

Packet Display Filter
Profiles:
Default
FTP-Only
Layer 2
Layer 2/3
Layer 3+
Address
TCP/UDP Port
Pattern
Data:
0 1 2 3 4 5 6 7 8 9 A B
0000
Format:
ASCII
Size:
0
Offset:
0
From:
Start of Packet
OK
Cancel

Setting up Profile

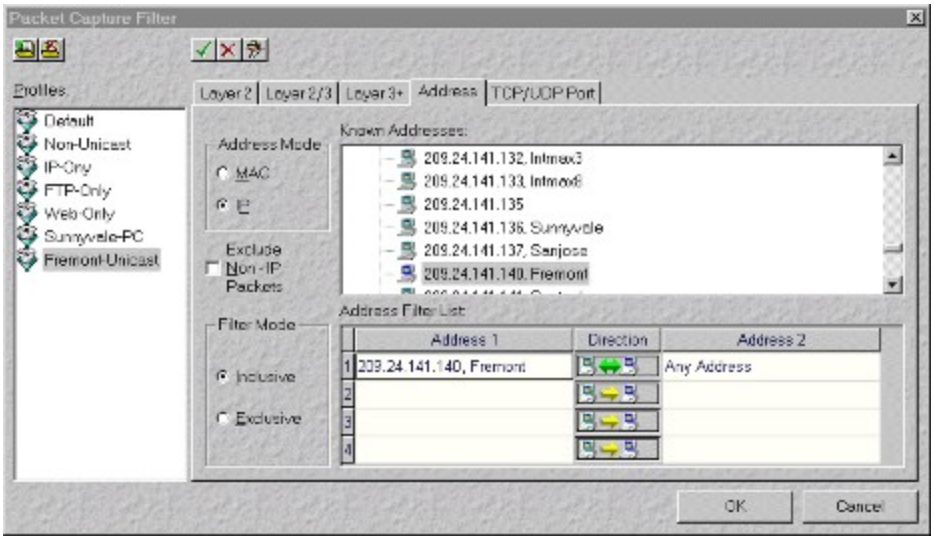
New profile
Delete Profile

With LanExplorer, users can define his/her own filter profile. The New Profile button is next to the Profile name box and you can see the New Profile name in the adjacent editable combo box. Simply click the New Profile button and enter a name for the new profile. Then check or uncheck the boxes below to compose the new profile. A filter profile covers all four groups of filters and you may click another tab to add or delete more filters for the new profile. Click the OK button to save the new profile. All profiles in LanExplorer are saved for later use. Clicking the combo box in the Profile will give you a list of profiles to choose from. You can delete any profile except the default profile.

Profiles apply to all five groups of filters. Combination profiles can be created for filters from different groups. For example, click on the New Profiles button and then type in a name for the filter (i.e. Fremont-Unicast). Click on Layer 2 and unselect all filters but Unicast.



Then click on Address. Drag the IP address "Fremont" from Known Addresses to the Address 1 column. Then drag "Any Address" from Known Addresses to the Address 2 column. Click on the Direction column in row one to change the direction to "to-and-from".



Select All and Clear All

Select All
Clear All

There are two buttons on the upper-right corner of the window available to select all filter check boxes or clear all filter check boxes. If there are total 20 filter check boxes and all selected and you want to delete 19 of them, the fastest way is to clear all of them and check the one you want.

TCP/UDP Port Definition

TCP/UDP Port Definition

The TCP/UDP Port definition table includes many applications preassigned to standard port numbers based in RFC 1700. See Part I, *LanExplorer* Chapter 5: Policy Based Blocking, *TCP/UDP Port Definitions*.

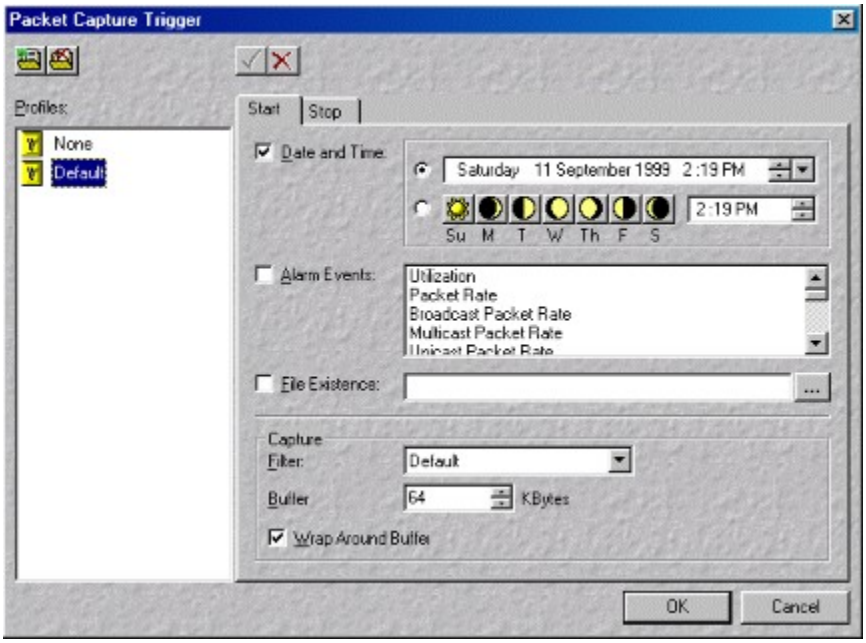
Packet Capture Trigger

Packet Capture Trigger provides a way to capture packets by user-defined events. There are two windows (tabs) to enter events and options, one is for starting Packet Capture and another is for stopping Packet Capture.

Trigger to Start Packet Capture

Any of the following trigger events can be used to start Packet Capture.

- Exact date and time to start capture packets.
- Any day or many days in a week at a pre-defined time to start capture packets.
- Any alarm event occurring to start capture packet.



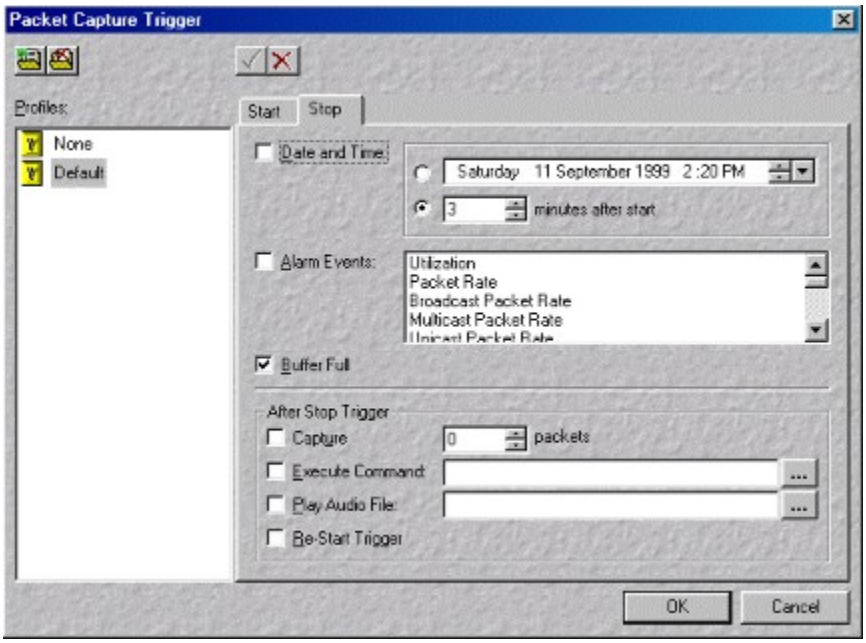
Packet Capture Options

- Filter applied to Packet Capture
- Buffer size
- Wrap around buffer if buffer is full

Trigger to Stop Packet Capture

Any of the following trigger events can be used to stop Packet Capture.

- Exact date and time to stop capturing packets.
- Minutes after starting Packet Capture to stop capturing packets.
- Any alarm event occurring to stop capturing packet.
- If the capture buffer is full, stop capturing packets.



Stop Trigger Options

There are options after stopping Packet Capture.

- Capture pre-defined number of packets after event trigger.
- Execute an application.
- Re-start the trigger and waiting for event to start Packet Capture again.

General

Use the Network Statistics to understand the overall network traffic patterns. The statistics are divided into 2 major groups: Rate and Distribution Charts. Distribution charts are further divided between Historical and Accumulated charts.

Tab/Group	Icon	Name	Description
		Rate charts	Shows traffic as a "rate" over time - integrated with (threshold) alarms and useful for monitoring
		Historical distribution	Shows traffic as a percentage of total traffic - for understanding overall traffic patterns
		Accumulated distribution	Shows traffic as a percentage of total traffic over time - useful for troubleshooting and understanding traffic patterns in specific time periods

Launching Accumulated or Historical Distribution

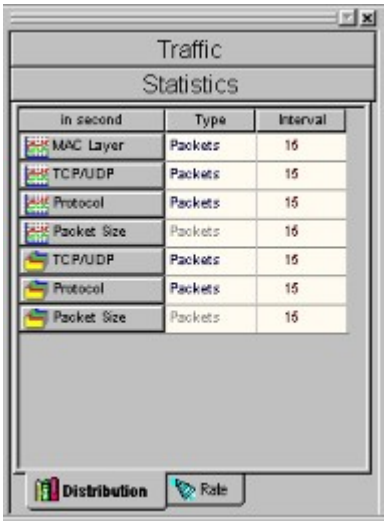
Each accumulated or historical distribution has an icon associated with the name. Click the button of accumulated or historical distribution such as "MAC Layer" in the Distribution category of the Statistics Task Panel to launch the distribution window.

Available historical distributions are:

- MAC Layer
- TCP/UDP
- Protocol
- Packet Size

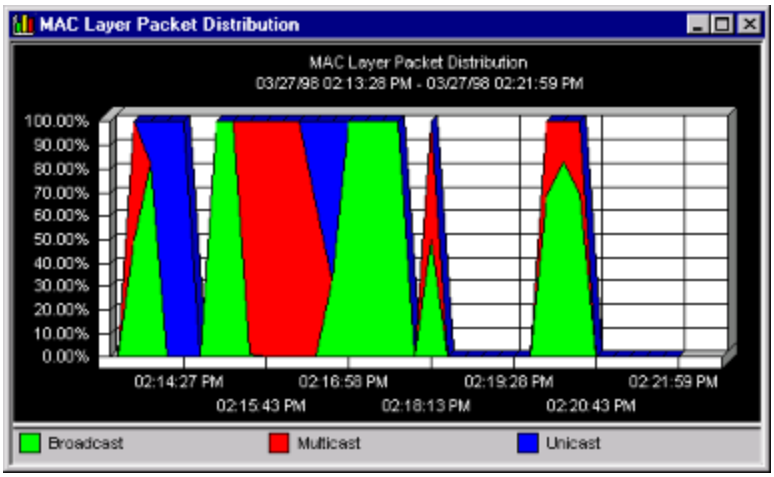
Available accumulated distributions are:

- TCP/UDP
- Protocol
- Packet Size



MAC Layer Statistics

Launch "MAC Layer" distribution from the Statistics Task Panel. A historical distribution example is shown as below.



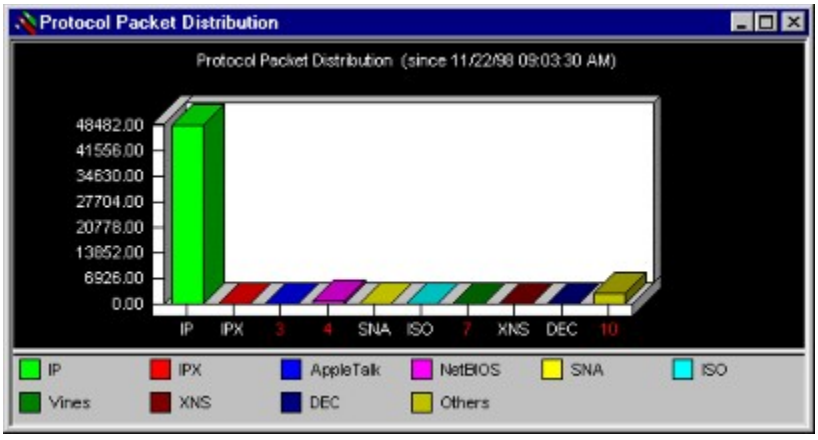
The MAC Layer distribution consists of the following members.

- Broadcast packets
- Multicast packets
- Unicast packets

You can select either packets or octets in the Type field of the Statistics Task Panel for this distribution. The total packets or octets are 100% of the MAC Layer packets or octets.

Protocol Statistics

Launch "Protocol" distribution from the Statistics Task Panel. An accumulated distribution example is shown below.



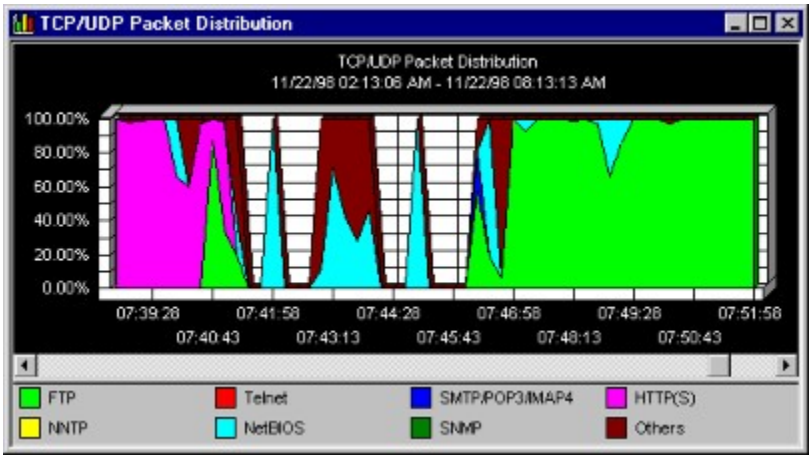
The Protocol distribution consists of the following members.

- IP packets
- IPX packets
- AppleTalk packets
- NetBIOS packets
- SNA packets
- ISO packets
- Vines packets
- XNS packets
- DEC packets
- Other packets

You can select either packets or octets in the Type field of the Statistics Task Panel for this distribution. The total packets or octets are 100% of the Protocol packets or octets.

TCP/UDP Statistics

Launch "TCP/UDP" distribution from the Statistics Task Panel. An accumulated distribution example is shown below.



The TCP/UDP distribution consists of the following members.

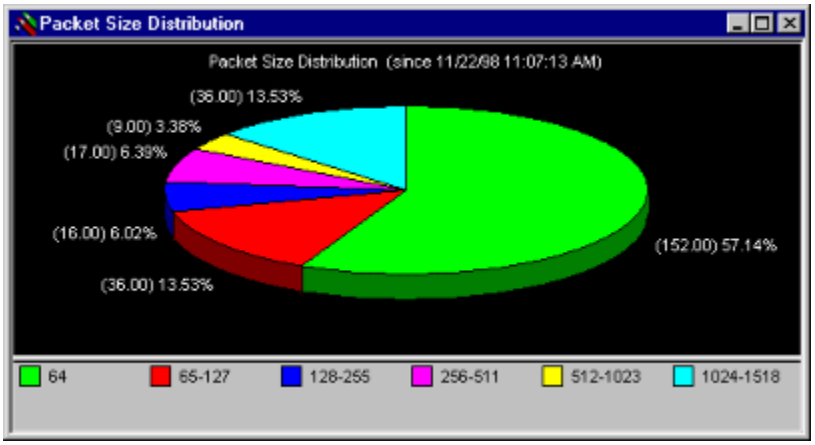
- FTP packets

- Telnet packets
- SMTP/POP3/IMAP4 packets (Mail protocols)
- HTTP/HTTPS packets (Web protocols)
- NNTP packets (News protocol)
- NetBIOS packets
- SNMP packets (Management protocol)
- Other packets

You can select either packets or octets in the Type field of the Statistics Task Panel for this distribution. The total packets or octets are 100% of the TCP/UDP packets or octets.

Packet Size Statistics

Launch "Packet Size" distribution from the Statistics Task Panel. An accumulated distribution example is shown below.



The Packet Size distribution consists of the following members.

- Packet size 64-byte packets
- Packet size 65-byte to 127-byte packets
- Packet size 128-byte to 255-byte packets
- Packet size 256-byte to 511-byte packets
- Packet size 512-byte to 1023-byte packets
- Packet size 1024-byte to 1518-byte packets

Chart Properties

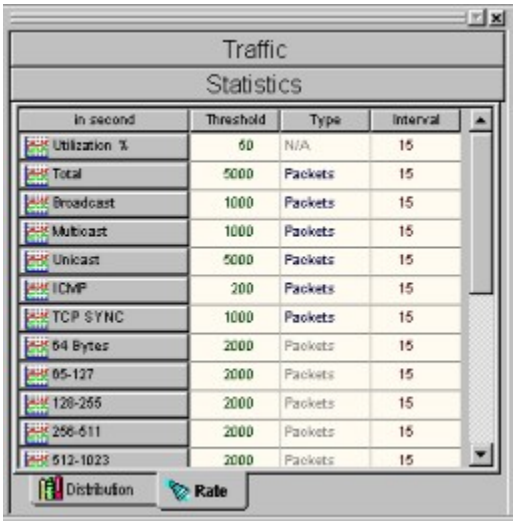
Click the Display Properties command in Toolbar or the Properties item of the View menu to launch the Chart Properties window for the active statistics window. Please refer to the section on Display Properties for additional information.

Using Threshold and Alarm

Setting up Threshold

Click any parameter cell (Threshold, Type or Interval) in the Rate tab of the Statistics Task Panel to change the parameter. For example, setting the Broadcast threshold to 1000 packets and Interval to 15-seconds means an alarm will be triggered if more than 1000 broadcast packets have been seen during a 15-second sampling period. Several ways to change parameters are described below.

- Press Backspace(s) to clear the value and type into a new value.
- Use the Up arrow to increase the value.
- Use the Down arrow to decrease the value.

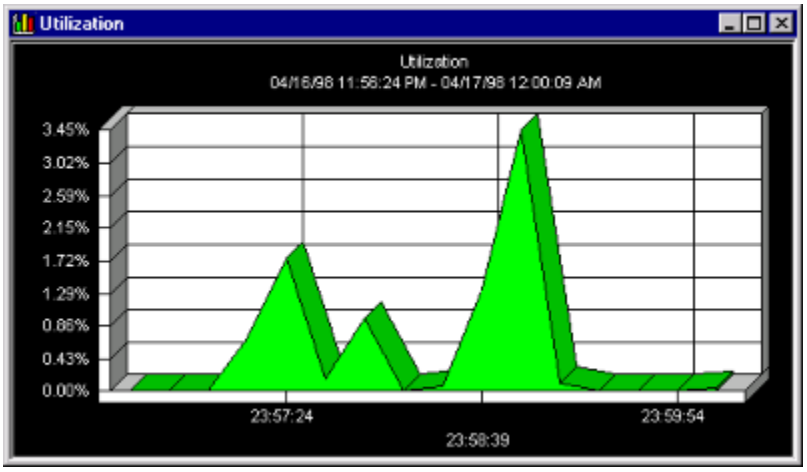


Available rate items are listed below:

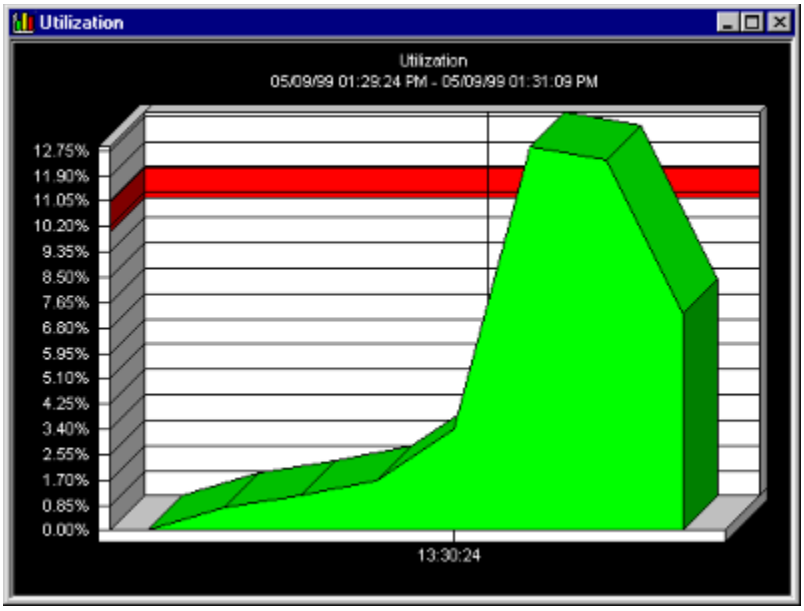
- Utilization
- Errors
- Total packets
- Broadcast packets
- Multicast packets
- Unicast packets
- ICMP (Ping) packets
- TCP SYNC (Session Start) packets
- Packet size 64-byte packets
- Packet size 65-byte to 127-byte packets
- Packet size 128-byte to 255-byte packets
- Packet size 256-byte to 511-byte packets
- Packet size 512-byte to 1023-byte packets
- Packet size 1024-byte to 1518-byte packets
- Transmit errors
- Receive errors
- Number of collisions
- Underrun errors
- CRC errors
- Alignment errors
- Overrun errors

Launching Rate Monitoring Windows

Click a Rate such as "Utilization" to launch the monitoring window. A background task for this window periodically checks the threshold value of specific items. If the task detects a higher rate than the threshold in a predefined sampling period, alarm will be set in the Alarm Log window. The next section describes how to read the alarm event from the Alarm Log window.



In this second example for the utilization table, a red bar appears across the 10% marker. The red bar indicates the threshold level that was specified for an alarm event.

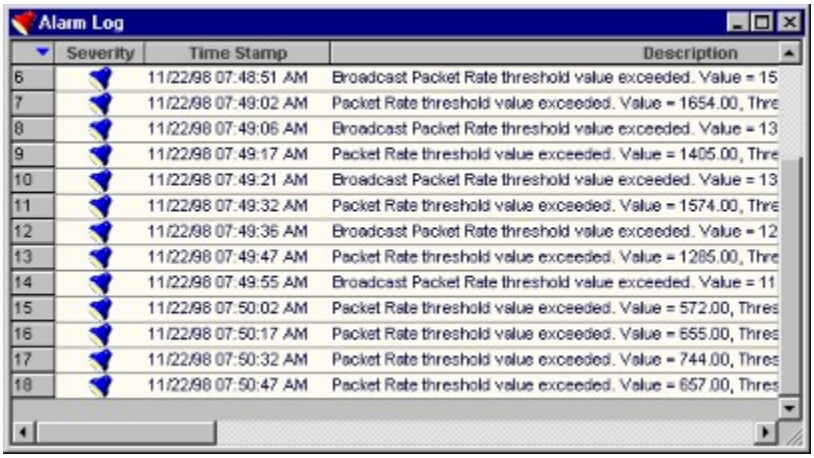


Viewing Alarm Log

If a "Rate" being monitoring from the Statistics Task Panel exceeded the threshold, an alarm event will be logged in the Alarm Log window. Click the Alarm Log icon in the Traffic Task Panel to view the logged events or the Alarm Log window will be automatically launched once there is an event to report during runtime.

Color scheme of alarm is described as below.

- Red - Critical
- Magenta - Major
- Yellow - Minor
- Green - Information
- Blue - Threshold



A popup menu will be shown as below if you click the right mouse button in the Alarm Log window. You can delete the alarm log entries by clicking any of the selections.

- Current - current entry
- Selected - highlighted entries (To select multiple entries, hold the control key while clicking the left mouse button.)
- All - all entries

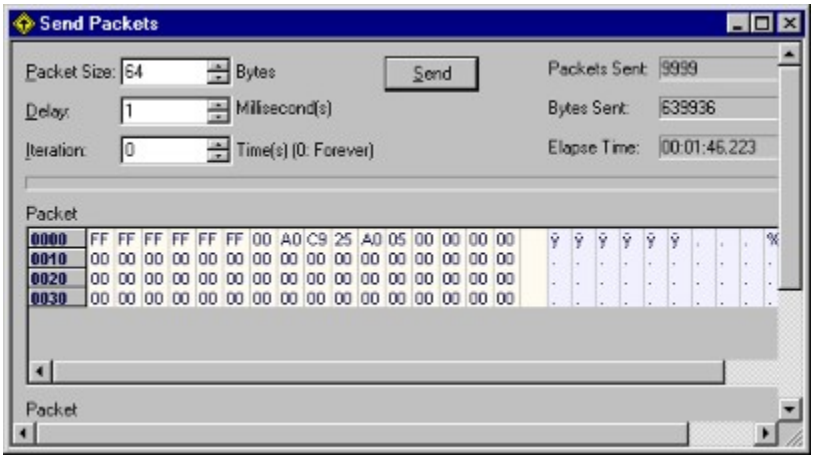
Unencrypted Password Alarm

Alarm Log captures and records successful and failed FTP logins - except logins with the user name "anonymous". POP3 logins are recorded in the Alarm Log window as well. Destination (IP address or site name), source (IP address or site name) and user name of each FTP/POP3 transaction are displayed in the Alarm Log window.

Tip: Unencrypted passwords in FTP and POP3 packets should be minimized and/or eliminated.

Sending Packet from the Packet Sends window

Clicking the "Send Packets" command on the Toolbar or the "Send Packets" menu item of the Tools Menu to launch the Send Packets window. You can change the "Send Packets" parameters. A small protocol decode window is below the packet content which displays the interpreted protocols from the packet content. Click the Send button to start sending packets to the network. Users can interrupt the sending before it finishes by clicking the Stop button.

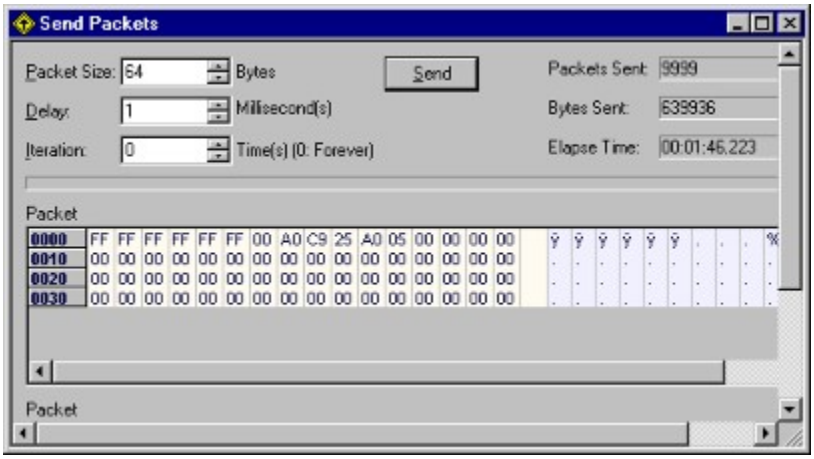


Sending Packets from the Packet Capture window

Clicking the right mouse button on any cell in the Packet Capture window shows a popup menu as below. You will have options to send an edited packet or play back a packet.

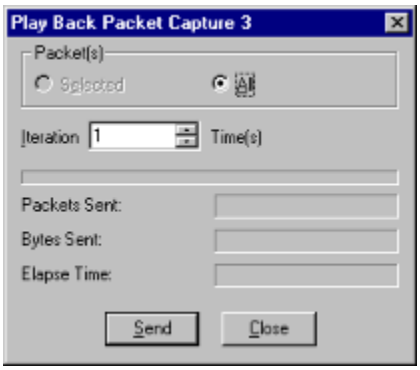
Send Packet Option

By clicking Send Packet in the menu box, the Packet Sends window will be displayed using the packet content from the Packet Capture window. Now you can edit the packet content before sending it to the network. The rest of the procedures to send packets to the network are the same as whatever mentioned above.



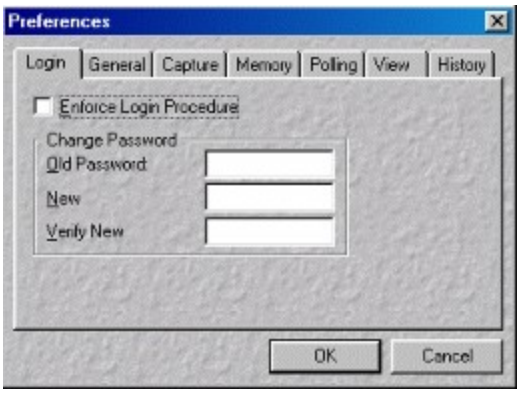
Play Back Option

The Play Back option sends packets back to the network without editing the packet content. User can send multiple selected or all packets in the capture buffer from the Packet Capture window back to the network and with as many as iterations you wish.



Enforcing Login Procedure

Click the "Preferences" menu item of the File Menu to view the Preferences window. Once the password is set, "login" will be required when launching the LanExplorer application and you won't be able to change it again until you have successfully logged into LanExplorer.



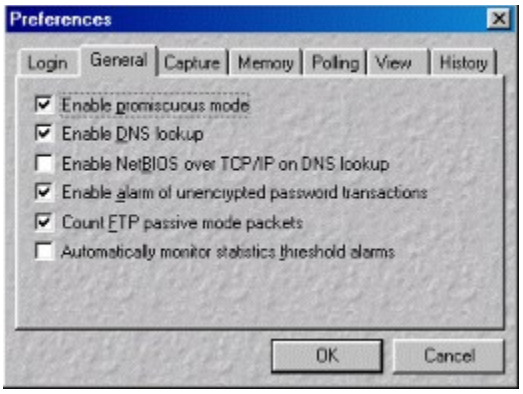
Follow the steps to change the password:

- Check the Enforce Login Procedure check box.
- Enter the Old Password or leave it blank if it was not set before.
- Enter the New password.
- Enter the New password again in the Verify New box.

To remove the Enforce Login Procedure, uncheck the Enforce Login Procedure check box.

General Preferences

Click the "Preferences" item of the Settings Menu, then click the "General" tab to change the General Preferences.



Enable promiscuous mode

When the check box is selected, all packets in the network segment will be captured even though a packet is not sent to this station. Otherwise, only broadcast/multicast packet and unicast packet sent to this station will be captured. Using LanExplorer for server statistics, promiscuous mode may be disabled.

Enable DNS lookup

When the check box is selected, a DNS reverse lookup packet will be sent to the DNS Server to resolve the Internet name of an IP address.

Enable NetBIOS over TCP/IP on DNS lookup

When the check box is selected, a NetBIOS query packet will be sent directly to the IP Address to resolve the host name.

Enable alarm of unencrypted password transactions

If the check box is selected, the Alarm Log will record any successful (Green – Information) or failed (Magenta – Major) FTP/POP3 login except user name “anonymous”.

Count FTP passive mode packets

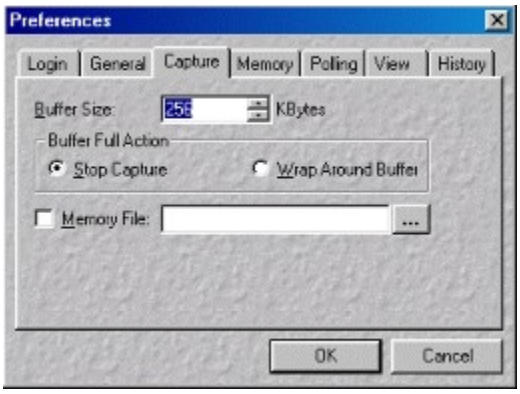
FTP Passive Mode packets are not count as FTP packets if this option is not checked.

Automatically monitor statistics threshold alarm

Alarm can be generated without launching the statistics chart. If the check box is selected, all available statistics in the Rate Pane of the Statistics Task Panel will be able to generate alarm.

Capturing Options

Click the "Preferences" menu item of the File Menu, then click the "Capture" tab to change the capture options.



Buffer Size

User can adjust the buffer size of Packet Capture. This depends on the total system memory. For example, giving 512K or 1MB is pretty reasonable if the total system memory is 32MB or 64MB.

Buffer Full Action

- **Stop Capture**
  The Packet Capture in-progress window will be stopped and packets captured will be listed when the capture buffer is full.

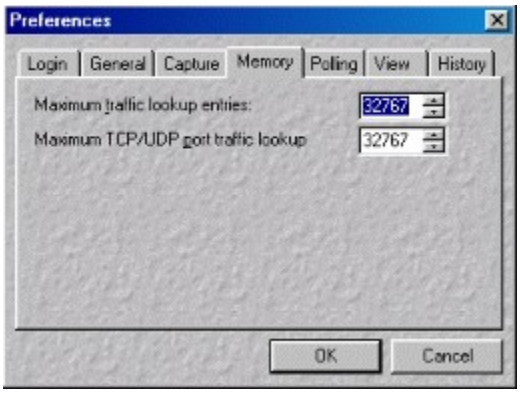
- **Wrap Around Buffer**
  The oldest packet in the buffer will be overridden by new captured packets when the capture buffer is full. The Packet Capture continues until the Stop Capture command is clicked.

Memory File

If the box is checked and the file name is specified, all captured packets will be saved to the file and can be retrieved later. Click the browse button to specify the file name.

Memory Preferences

Click the "Preferences" item of the Settings Menu, then click the "Memory" tab to change the Memory Preferences.



Maximum Traffic lookup entries

Maximum number of unique entries of Source and Destination Address can be used for Traffic Matrix and Host Table display purpose.

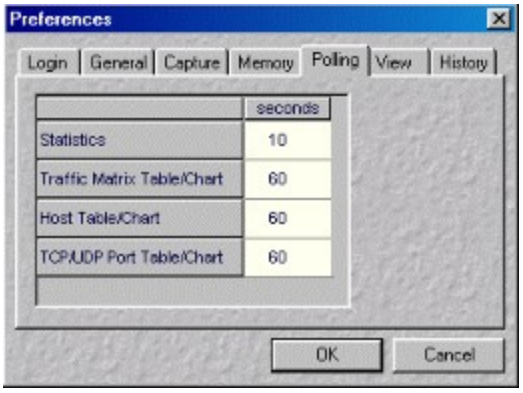
Maximum TCP/UDP port traffic lookup entries

Maximum number of unique entries of Source and Destination Port can be used for TCP/UDP Port Table/Chart display purpose.

Polling Frequencies

Click the "Preferences" item of the Settings Menu, then click the "Polling" tab to change the polling frequencies. Click any parameter cell and the spin buttons appears. Several ways to change parameters are described below.

- Press Backspace(s) to clear the value and type into a new value.
- Use the Up arrow to increase the value.
- Use the Down arrow to decrease the value.



Statistics

- Counter update in the Console Panel.
- Chart update in the Statistics Chart Windows.

Traffic Matrix Table/Chart

- Traffic Matrix Table update.
- Traffic Matrix Chart update.

Host Table/Chart

- Host Table update.
- Host Chart update.

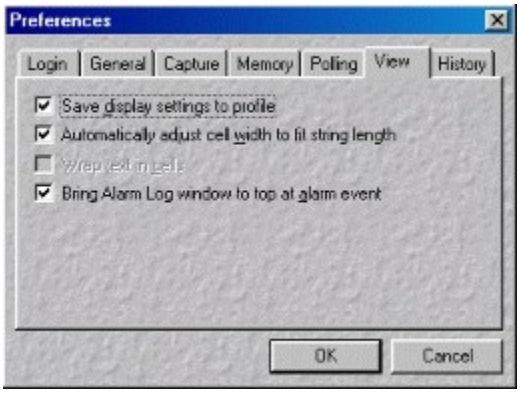
TCP/UDP Port Table/Chart

- TCP/UDP Port Table update.
- TCP/UDP Port Chart update.

Tip: Increase the polling frequency to reduce processing requirements for screen updates.
Tip: Use the Refresh button to force manual refreshes when needed.

View Options

Click the "Preferences" menu item of the File Menu then click the "View" tab to change the view options. You can check or uncheck any check box to enable or disable the feature.



Save display settings to profile

Settings will be reloaded in next session.

Automatically adjust cell width to fit string length / Wrap text in cell

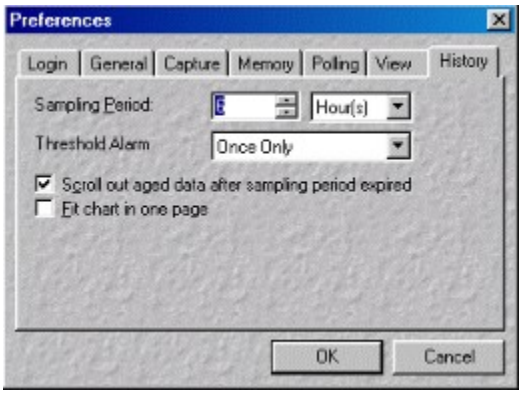
Cell width will be automatically adjusted to fit string length. If it is not checked, ‘‘Wrap text in cell’’ option can be checked to wrap text in cell.

Bring Alarm Log window to top at alarm event

This option allows you to see the alarm right away when it happens.

History Preferences

Click the "Preferences" item of the Settings Menu, then click the "History" tab to change the History Preferences. These preferences apply to all historical distribution and rate windows launched.



Sampling Period

Given minute(s), hour(s), day(s) or week(s) as long as the system memory available to record the statistics history. Default is 6 hours.

Threshold Alarm

Beep sound off, once only or continuously when threshold alarm has happened. Default is off at alarm event.

Scroll out aged data after sampling period expired

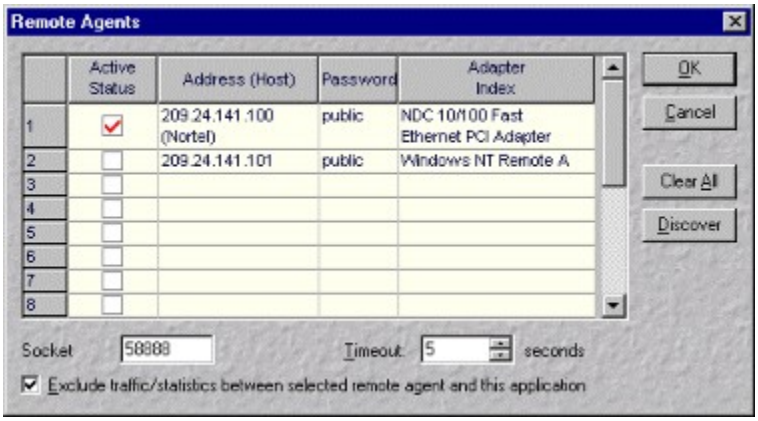
Stop the statistics history chart when sampling period has come to the end. Default is to continue log statistics history and drop the oldest statistics (scroll).

Fit chart in one page

There will be no scrolling bar available and everything will be seen in one page. Using this option may cause the time baseline display overlapped.

Connecting to a Remote Agent from LanExplorer

Click the "Remote Agents" item of the Setting Menu or the Remote Agents pane of the Status Bar to bring up the Remote Agents control window.



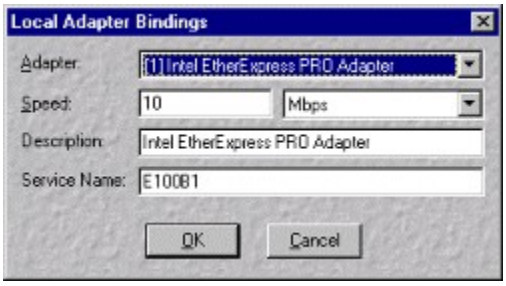
To connect to a Remote Agent, do the following steps:

- Enter the Remote Agent IP address.
- Enter the Remote Agent password (default is “public”)
- Enter the Remote Agent adapter index (0 base).
- Select Active Status.
- Click OK.

To discover Remote Agents in the same IP subnet of the LanExplorer application, click the Discover button. All Remote Agents will be discovered automatically by the LanExplorer. Socket port (default is 58888) for Remote Agents can be changed in the box at the bottom of the window.

Choosing Adapter to Use

If there is more than one LAN adapter in the system, you can switch to another adapter by clicking the "Local Adapter Bindings" item of the Settings Menu to launch the window and switch to another adapter.



Adapter for Modem/ISDN

For the 56K Modem/ISDN, select adapter ‘‘Remote Access WAN Wrapper.’’ Captured packets will be in Ethernet emulated form.

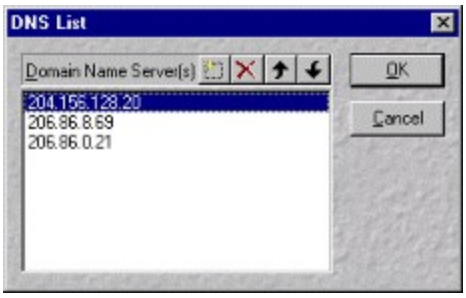
Setting Speed Option

Speed options for Ethernet are Auto Detection, 10 Mbps, 100 Mbps and 1000 Mbps.
Speed options for Token Ring are Auto Detection, 4 Mbps and 16Mbps.

The Speed option will be used to calculate the bandwidth utilization launched from the Statistics Task Panel. LanExplorer gets the wire speed from the network device (NDIS) driver if Auto Detection is selected. Due to some adapters not reporting the correct speed, you can set the speed in this dialog box if the wire speed is known.

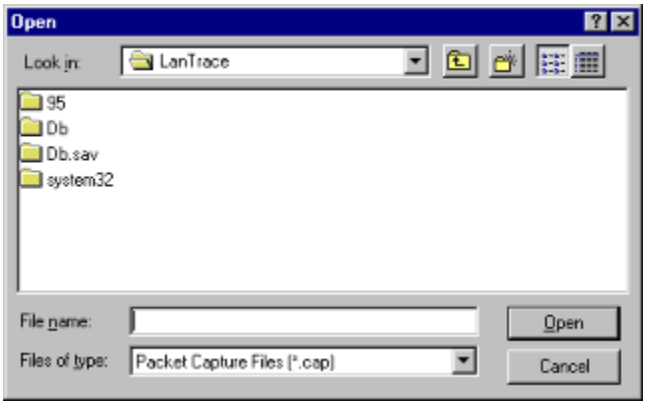
Choosing DNS Server for Lookup

Click the "DNS" item of the Setting Menu to bring up the DNS List window. DNS Server is used to resolve the Internet name of an IP address. By default, LanExplorer get from the current system setting. However, user can add a new DNS Server or delete an existing DNS server.



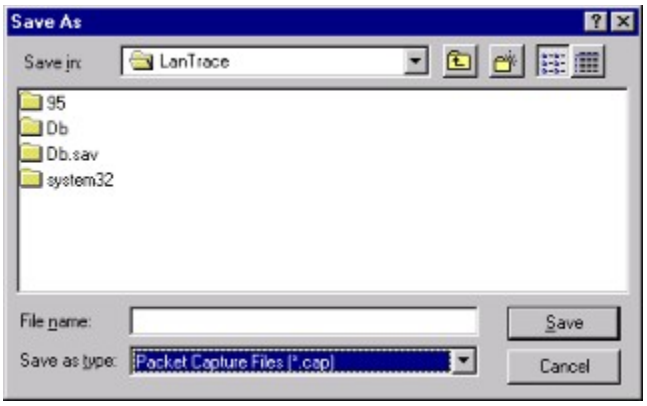
Opening a File

Click the "Open" menu item of the File Menu to launch the dialog box. For example, a Packet Capture file previously saving in the hard disk of another station can be opened and viewed on this station.



Saving to File

Click the "Save" menu item of the File Menu to launch the dialog box. Type a file name then click the Save button.



File Format

There are five file formats that you can save to the disk and the available formats depend on the active window you selected.

File Format	Available Window
Sniffer Non-compressed File (*.enc)	• Packet Capture
Packet Capture File (*.cap)	• Packet Capture
Printable Decode File (*.prn)	• Packet Capture • Protocol Decode
Tab-Delimited File (*.tab)	• Packet Capture • Traffic Matrix Table • Host Table • Alarm Log
Comma-Delimited File (*.cma)	• Packet Capture • Traffic Matrix Table • Host Table Table • Alarm Log
Windows Metafiles (*.wmf)	• Traffic Matrix Chart • Host Table Chart • Any Statistics Chart

Grid (Table) Window

Examples of Grid Window

- Packet Capture window
- Traffic Matrix Table
- Host Table
- Protocol Decode window
- Address Book
- Alarm Log

Summary of Display Options

- Click the right mouse button to show a popup menu for selected column(s) or cell(s).
- Resize the column width and row height dragging the line between columns or rows.
- Click the left mouse button to select a cell, column or row. To perform multiple selections, hold the control key while clicking the left mouse button.
- Change the column order by holding the column title and dragging to the new location.
- Print, save and copy if they are available.
- Click the "Toolbar" menu item of the View Menu to view the grid window toolbar.

Grid Window Toolbar

The grid window toolbar available for Packet Capture, Traffic Matrix and Host Table is described below. The property changed

by the grid window toolbar applies to the current window and does not affect the property of other grid windows.

Zoom In
Zoom 100%
Zoom Out
Format
Align Left
Align Center
Align Right
Bold
Italic
Underline
Strikeout

Display Settings

Move the mouse to the grid window and click the left mouse button once to select the active window. Click the Display Properties command in Toolbar or the Properties menu item of the View menu to launch the Display Settings window.

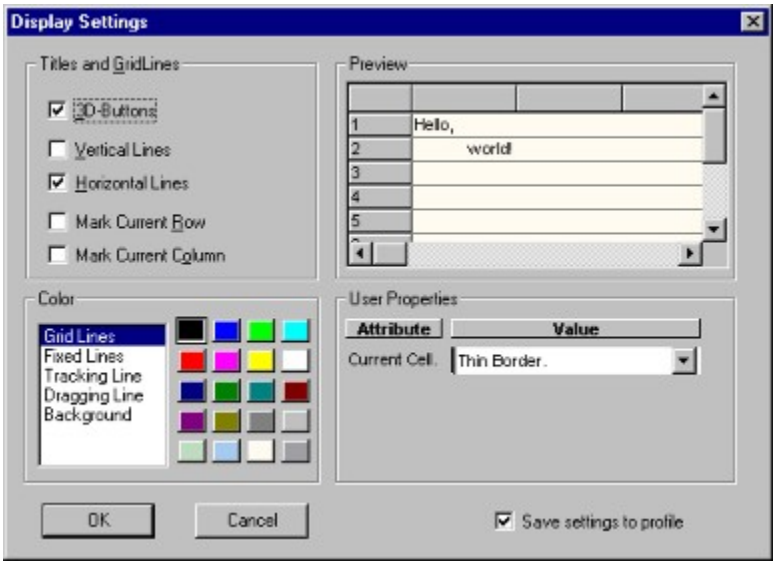


Chart Window

Examples of Chart Window

- Traffic Matrix Chart
- Host Chart
- Distribution Chart windows
- Rate Chart windows

Summary of Display Options

- Print, save and copy if they are available.
- Click the "Toolbar" menu item of the View Menu to view the chart window toolbar.

Chart Window Toolbar

The chart window toolbar available for any chart window is described below. The property changed by the chart window toolbar applies to the current window and does not affect the property of other chart windows.

Gallery type

Color palette

3D

Cluster option for 3D

Zoom in for selected area

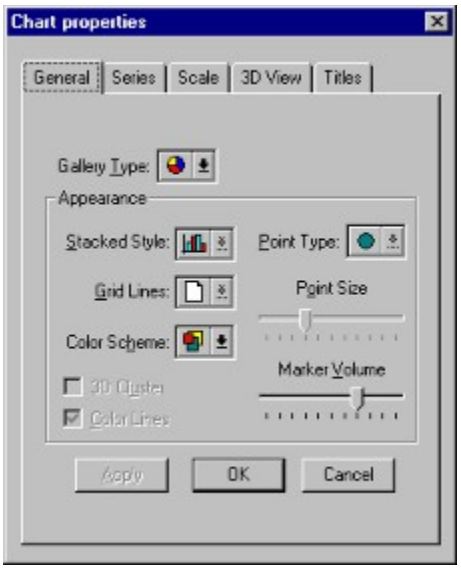
Vertical grid on/off

Horizontal grid on/off

Fonts

Chart Properties

Move the mouse to the chart window and click the left mouse button once to select the active window. Click the Display Properties command in Toolbar or the Properties menu item of the View menu to launch the Chart Properties window.



Gallery Type

Button	***Type***	***Description***
	Area	Shows the relative importance of values over a period of time.
	Lines	Shows trends or changes in data over a period of time.
	Horizontal Bars	Shows variation over a period of time.
	Pie	Shows the relationship or proportions of parts to a whole.
	Bars	Shows variation over a period of time.
	Points (Mark)	Similar to Lines except that its plots only the points or data markers.
	Doughnut	Same as Pie but a hole in the middle.
	Pareto	Same as Bars plus cumulative curve indicating the proportion accumulated by each column in the chart.
	Cubes	Shows the relative importance of values over a period of time. Instead of bars, cubes are the data markers.
	Spline (Curve)	Similar to Lines, only that the lines curve to pass through each point or data marker.
	Polar	Shows the relative importance of values over a period of time.

Remote Agent

Remote Agent is a remote probe running on Windows 95, 98, NT, or 2000 that LanExplorer can control just like any local adapter. LanExplorer application uses TCP/UDP over IP to communicate with the Remote agent. This chapter describes the installation, configuration and removal of the Remote agent. (Remote Agent also works with LanExplorer and LanTrend. In this manual section application will be referred to as LanExplorer.)

System Requirements

Please refer to Chapter 2 for system requirements. Note: Remote agent does not require a high resolution VGA monitor since all displays are done remotely.

Pre-installation

For Windows NT/2000, the Intellimax NT/2000 Service must be installed as a network service and the system must be restarted after installing the Service. Please refer to Part I, Chapter 2, for the installation of the Intellimax NT/2000 Service.

Installation

Install from a CD-ROM

- Get a valid Serial Number from the package you have received.
- Insert the LanExplorer CD-ROM into the CD-ROM drive.
- Double click My Computer.
- Double click the CD-ROM drive (e.g. d:\)
- Change to the Remote agent directory (e.g. d:\agent)
- Click the SETUP.EXE file.
- Follow the instructions to install the application.

Installation from a downloaded file

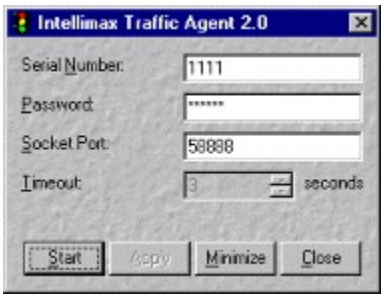
- Get a valid Serial Number emailing or calling Technical Support.
- Click the self-extracting file (e.g. AGENT.EXE).
- Follow the instructions to install the application.

Starting and Stopping Remote Agent

Restart the system after installation of the Remote Agent. The Remote Agent will be started automatically upon restarting the system.

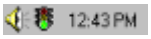
For Windows NT/2000, to launch the Remote Agent without restarting the system, do the following steps on the Desktop.

- Click the Desktop Start button.
- Move mouse to Programs.
- Move mouse to Intellimax.
- Click Remote Agent.
- A dialog box will be shown as below.
- Click the Start button to start the Remote Agent service.

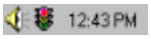


Minimizing or Closing Remote Agent on Desktop

Minimize the window by clicking the Minimize button. The traffic light icon in the Task Tray indicates the status of Remote Agent. A green light indicates the Remote Agent has been started. A red light indicates the Remote Agent has been stopped.



Remote Agent is started.



Remote Agent is stopped.

Close the window by clicking the Close button. For Windows NT/2000, closing the dialog box does not stop the Remote Agent service. You have to bring up the dialog box again or go to Services Control Panel Applet to stop the Remote Agent if you want to stop the service. For Windows 95/98, closing the dialog box will stop the Remote Agent service.

Configuring Remote Agent

Do the following steps on the Desktop to bring up the Remote Agent dialog box.

- Click the Desktop Start button.
- Move mouse to Programs.
- Move mouse to Intellimax.
- Click Remote Agent.
- Make sure the Start button is available (i.e. Remote Agent is currently stopped.)

Serial Number

Must be a valid serial number received when you purchased the software.

Password

Default password is ‘‘public’’. After changing the password, the remote LanExplorer application must use the new password to communicate with the agent.

Socket Port

Default socket (TCP/UDP) port is 58888. After changing the socket port, the remote LanExplorer application must use the new socket port to communicate with the agent. Both the remote agent and the client application must communicate over the same port.

Tip: If port 58888 is already in use, try using ports 71, 72, 73, or 74. These ports are generally used for remote services. Also, Firewalls may block communication to remote locations (outside the firewall). The communication port must be "open" by the firewall.

Restarting Remote Agent

Click the Start button to restart the Remote Agent after configuring it. An example is shown as below. When the Stop button is available, the Remote Agent is currently started.

Removing Remote Agent

Do the following steps on the Desktop to remove the Remote Agent.

- Click the Desktop Start button.
- Move mouse to Programs.
- Move mouse to Intellimax.
- Click Remote Agent unInstallShield.