

# LanExplorer User's Guide



---

Information in this document is subject to change without notice. No part of this publication may be reproduced, photocopied, stored in a retrieval system, transmitted, or translated into any language without the prior written permission of Intellimax Systems, Inc.

Copyright © 1997-2000 Intellimax Systems, Inc. All Rights Reserved.

TrafficMax, LanExplorer, LanTrend and Traffic Agent are registered trademarks of Intellimax Systems, Inc. Other brand and product names are trademarks or registered trademarks of their respective holders.

Printed in United States of America, January 2000

---

# License Agreement

## *Software License Agreement*

WARNING: INTELLIMAX SYSTEMS, INC. IS WILLING TO LICENSE THE ENCLOSED TrafficMax™, LanExplorer™, LanTrend™, and Remote Agent™ PROactive Monitoring & Reporting SOFTWARE (HEREINAFTER THE "SOFTWARE") AND USER DOCUMENTATION TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT.

PLEASE READ THE TERMS CAREFULLY BEFORE OPENING THIS PACKAGE OR CLICKING ON THE "YES" BUTTON, AS DOING SO WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN INTELLIMAX SYSTEMS, INC. IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNOPENED PACKAGE AND USER DOCUMENTATION TO THE PLACE FROM WHICH IT WAS ACQUIRED WITHIN THREE DAYS, AND YOUR MONEY WILL BE REFUNDED.

**LICENSE.** In consideration of your payment of the license fee, Intellimax Systems, Inc. grants to you a non-transferable and non-exclusive license to use the Software on a single computer.

**OWNERSHIP.** You own the physical diskette(s) containing the Software and user documentation. Intellimax Systems retains title to the Software. This agreement does not transfer title or ownership of the Software or any underlying proprietary rights, patents, copyrights, trademarks, or trade secrets. You may transfer all your license rights in the Software, the backup copy of the Software and a copy of this License to another party, provided the other party reads and agrees to accept the terms and conditions of this License.

**SCOPE OF GRANT.** You may:

- \* use the Software on any single computer;
- \* use the Software on a network, provided that each person accessing the Software through the network must have a copy licensed to that person;
- \* copy the Software for backup purposes, provided any copy must contain all of the original Software's proprietary notices.

**RESTRICTIONS.** You may not:

- \* permit other individuals to use the Software except under the terms listed above;
- \* permit concurrent use of the Software;
- \* modify, translate, reverse engineer, decompile, disassemble (except to the extent applicable laws specifically prohibit such restriction), or create derivative works based on the Software;
- \* copy the Software other than as specified above;
- \* rent, lease, grant a security interest in, or otherwise transfer rights to the Software; or
- \* remove any proprietary notices or labels on the Software.

**TERM.** The license granted that under this agreement is effective until terminated. You may terminate it at any time by destroying the Software together with all copies, modifications and merged portions in any form. This license will terminate immediately without notice from Intellimax Systems, Inc. if you fail to comply with any provisions of this License. You agree upon such termination to destroy the Software, together with all copies, modifications and merged portions in any form, and to certify to Intellimax Systems, Inc. that they have been destroyed. Upon termination there will be no refund of any monies or consideration paid by you.

**EXPORT LAW ASSURANCES.** You agree and certify that neither the Software nor any other technical data received from Intellimax Systems, Inc., nor the direct product thereof, will be shipped, transferred, or exported, directly or indirectly, outside the country within which the Software was purchased without the express written consent of Intellimax Systems, Inc.

---

**NO WARRANTIES.** Intellimax Systems expressly disclaims any warranty for the software product. The software product and any related documentation is provided "AS IS" without warranty of any kind, either express or implied, including, without limitation, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. The entire risk arising out of use or performance of the software product remains with you.

**LIMITATION OF LIABILITY.** To the maximum extent permitted by applicable law, in no event shall Intellimax Systems or its suppliers be liable for any special, incidental, indirect, or consequential damages whatsoever (including without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use the software product or the provision of or failure to provide support services, even if Intellimax Systems has been advised of the possibility of such damages. In any case, Intellimax Systems' entire liability under any provision of this Agreement shall be limited to the greater of the amount actually paid by you for the software product or US\$5.00; provided however, if you have entered into a Intellimax Systems Support Services Agreement, Intellimax Systems' entire liability regarding Support Services shall be governed by the terms of that agreement. Because some states and jurisdictions do not allow the exclusion or limitation of liability, the above limitation may not apply to you.

**HIGH RISK ACTIVITIES.** The Software is not fault-tolerant and is not designed, manufactured or intended for use or resale as on-line control equipment in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems, in which the failure of the Software could lead directly to death, personal injury, or severe physical or environmental damage ("High Risk Activities"). Licensor and its suppliers specifically disclaim any express or implied warranty of fitness for High Risk Activities.

**US GOVERNMENT END USERS.** This Agreement is not valid and shall not come into effect for any unit or agency of the United States government until the execution and delivery by both you and Intellimax Systems, Inc. of a RESTRICTED RIGHTS Government User Supplement in the form required by Intellimax Systems, Inc.

**MISCELLANEOUS.** If the copy of the Software you received was accompanied by a printed or other form of "hard-copy" End User License Agreement whose terms vary from this Agreement, then the hard-copy End User License Agreement governs your use of the Software. This Agreement represents the complete agreement concerning this license and may be amended only by a writing executed by both parties. **THE ACCEPTANCE OF ANY PURCHASE ORDER PLACED BY YOU IS EXPRESSLY MADE CONDITIONAL ON YOUR ASSENT TO THE TERMS SET FORTH HEREIN, AND NOT THOSE IN YOUR PURCHASE ORDER.** If any provision of this Agreement is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This Agreement shall be governed by California law (except for conflict of law provisions). The application the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded.

**COMPLETE AGREEMENT.** This License constitutes the entire agreement between the parties with respect to the use of the Software and related documentation, and supersedes all prior or contemporaneous understandings or agreements, written or oral, regarding such subject matter. No amendment to or modification of this License will be binding unless in writing and signed by a duly authorized representative of Intellimax Systems, Inc.

---

**TABLE OF CONTENTS**

<b>PURPOSE OF THIS MANUAL .....</b>	<b>9</b>
OBTAINING CUSTOMER TECHNICAL SUPPORT .....	9
AUDIENCE .....	10
ORGANIZATION OF THIS MANUAL .....	10
<b>PART I LANEXPLORER .....</b>	<b>11</b>
<b>CHAPTER 1: PRODUCT OVERVIEW .....</b>	<b>11</b>
<b>CHAPTER 2: INSTALLING LANEXPLORER.....</b>	<b>12</b>
SYSTEM REQUIREMENTS.....	12
PRE-INSTALLATION.....	12
<i>Intellimax NT Service - For Windows NT/2000 only.....</i>	<i>12</i>
INSTALLATION.....	13
<i>Install from a CD-ROM .....</i>	<i>13</i>
<i>Installation from a downloaded file .....</i>	<i>13</i>
POST-INSTALLATION.....	14
<i>Intellimax NT Service - For Windows NT only .....</i>	<i>14</i>
<i>Intellimax 2000 Service - For Windows 2000 only.....</i>	<i>15</i>
UNINSTALLING LANEXPLORER.....	16
<i>Uninstalling the LanExplorer application.....</i>	<i>16</i>
<i>Uninstalling Intellimax NT Service – Additional Procedure for Windows NT only.....</i>	<i>16</i>
<i>Uninstalling Intellimax 2000 Service – Additional Procedure for Windows 2000 only .....</i>	<i>16</i>
<b>CHAPTER 3: USING LANEXPLORER .....</b>	<b>17</b>
STARTING LANEXPLORER.....	17
<i>File Menu.....</i>	<i>18</i>
<i>Edit Menu.....</i>	<i>18</i>
<i>View Menu.....</i>	<i>18</i>
<i>Capture Menu.....</i>	<i>18</i>
<i>Tools Menu.....</i>	<i>19</i>
<i>Window Menu.....</i>	<i>19</i>
<i>Settings Menu.....</i>	<i>19</i>
<i>Profiles Menu.....</i>	<i>19</i>
TOOLBAR.....	20
STATUS BAR .....	20
<i>Packet Capture Trigger, Remote Agents .....</i>	<i>20</i>
TRAFFIC TASK PANEL .....	21
STATISTICS TASK PANEL .....	21
CONSOLE PANEL.....	23
<b>CHAPTER 4: TRAFFIC MONITORING.....</b>	<b>24</b>
LAUNCHING TRAFFIC MATRIX TABLE.....	24
TRAFFIC MATRIX TABLE OPTIONS.....	25
<i>Cell Options.....</i>	<i>25</i>
<i>Sorting Options.....</i>	<i>26</i>
<i>Traffic Matrix Sorting.....</i>	<i>26</i>
<i>Display Settings.....</i>	<i>27</i>
LAUNCHING TRAFFIC MATRIX CHART .....	28
TRAFFIC MATRIX CHART OPTIONS.....	29
<i>Chart Properties.....</i>	<i>29</i>
TRAFFIC MATRIX STATUS BAR .....	30
<i>Toggle MAC Window and IP Window.....</i>	<i>30</i>
<i>Changing Polling Interval.....</i>	<i>30</i>

---

<i>Toggle One-way and Two-way</i> .....	30
<i>Toggle Show-broadcast and No-broadcast</i> .....	31
<i>Changing Traffic Matrix Filter</i> .....	31
MORE SORTING OPTIONS.....	31
TABLE & CHART DISPLAY FILTERS.....	32
<i>Setting up Profiles</i> .....	32
<i>Select All and Clear All</i> .....	33
<i>Protocol Filter</i> .....	33
<i>Address Filter</i> .....	33
LAUNCHING HOST TABLE.....	34
HOST TABLE OPTIONS.....	34
<i>Cell Options</i> .....	34
<i>Host Table Sorting</i> .....	34
<i>Display Settings</i> .....	34
LAUNCHING HOST CHART.....	35
HOST CHART OPTIONS.....	35
<i>Chart Properties</i> .....	35
HOST WINDOW STATUS BAR.....	35
MORE SORTING OPTIONS.....	36
ADDRESS BOOK.....	37
<i>Address Book Commands</i> .....	38
<b>CHAPTER 5: NETWORK PROTOCOL ANALYSIS .....</b>	<b>39</b>
STARTING AND STOPPING PACKET CAPTURE.....	39
VIEWING PACKET CONTENTS.....	41
APPLYING PRE-CAPTURE OR POST-CAPTURE FILTER.....	42
<i>Layer 2 MAC Filter</i> .....	42
<i>Layer 2 VLAN Filter</i> .....	42
<i>Layer 2 Filter Example</i> .....	42
<i>Layer 2/3 Ethernet II Filter</i> .....	43
<i>Layer 2/3 LLC Filter</i> .....	43
<i>Layer 2/3 LLC SNAP Filter</i> .....	43
<i>Layer 2/3 Raw Filter</i> .....	43
<i>Layer 2/3 Filter Example</i> .....	43
<i>Layer 3+ IP/ARP Filter</i> .....	44
<i>Layer 3+ TCP/UDP Filter</i> .....	44
<i>Layer 3+ Filter Example</i> .....	44
<i>Address Filter</i> .....	45
<i>TCP/UDP Port Filter</i> .....	46
<i>Pattern Filter of Post-capture Filter</i> .....	47
SETTING UP PROFILE.....	48
<i>Select All and Clear All</i> .....	49
<i>TCP/UDP Port Definition</i> .....	49
PACKET CAPTURE TRIGGER.....	50
<i>Trigger to Start Packet Capture</i> .....	50
<i>Packet Capture Options</i> .....	50
<i>Trigger to Stop Packet Capture</i> .....	51
<i>Stop Trigger Options</i> .....	51
<b>CHAPTER 6: NETWORK S STATISTICS.....</b>	<b>52</b>
GENERAL.....	52
LAUNCHING ACCUMULATED OR HISTORICAL DISTRIBUTION.....	52
<i>MAC Layer Statistics</i> .....	53
<i>Protocol Statistics</i> .....	54
<i>TCP/UDP Statistics</i> .....	55
<i>Packet Size Statistics</i> .....	56
<i>Chart Properties</i> .....	56

USING THRESHOLD AND ALARM .....	57
<i>Setting up Threshold</i> .....	57
<i>Launching Rate Monitoring Windows</i> .....	58
ALARM LOG.....	59
<i>Unencrypted Password Alarm</i> .....	59
<b>CHAPTER 7: TRAFFIC GENERATOR.....</b>	<b>60</b>
SENDING PACKET FROM THE PACKET SENDS WINDOW .....	60
SENDING PACKETS FROM THE PACKET CAPTURE WINDOW .....	60
<i>Send Packet Option</i> .....	61
<i>Play Back Option</i> .....	61
<b>CHAPTER 8: SETTINGS .....</b>	<b>62</b>
ENFORCING LOGIN PROCEDURE.....	62
GENERAL PREFERENCES.....	63
<i>Enable promiscuous mode</i> .....	63
<i>Enable DNS lookup</i> .....	63
<i>Enable NetBIOS over TCP/IP on DNS lookup</i> .....	63
<i>Enable alarm of unencrypted password transactions</i> .....	63
<i>Count FTP passive mode packets</i> .....	63
<i>Automatically monitor statistics threshold alarm</i> .....	63
CAPTURING OPTIONS .....	64
<i>Buffer Size</i> .....	64
<i>Buffer Full Action</i> .....	64
<i>Memory File</i> .....	64
MEMORY PREFERENCES.....	65
<i>Maximum Traffic lookup entries</i> .....	65
<i>Maximum TCP/UDP port traffic lookup entries</i> .....	65
POLLING FREQUENCIES.....	66
<i>Statistics</i> .....	66
<i>Traffic Matrix Table/Chart</i> .....	66
<i>Host Table/Chart</i> .....	66
<i>TCP/UDP Port Table/Chart</i> .....	66
VIEW OPTIONS.....	67
<i>Save display settings to profile</i> .....	67
<i>Automatically adjust cell width to fit string length / Wrap text in cell</i> .....	67
<i>Bring Alarm Log window to top at alarm event</i> .....	67
HISTORY PREFERENCES.....	68
<i>Sampling Period</i> .....	68
<i>Threshold Alarm</i> .....	68
<i>Scroll out aged data after sampling period expired</i> .....	68
<i>Fit chart in one page</i> .....	68
CONNECTING TO A REMOTE AGENT FROM LANEXPLORER.....	69
CHOOSING ADAPTER TO USE .....	70
<i>Adapter for Modem/ISDN</i> .....	70
<i>Setting Speed Option</i> .....	70
CHOOSING DNS SERVER FOR LOOKUP .....	71
<b>CHAPTER 9: OPEN OR SAVE FILE.....</b>	<b>72</b>
SAVING TO FILE.....	72
OPENING A FILE.....	72
FILE FORMAT.....	73
<b>CHAPTER 10: DISPLAY PROPERTIES .....</b>	<b>74</b>
GRID (TABLE) WINDOW .....	74
<i>Examples of Grid Window</i> .....	74
<i>Summary of Display Options</i> .....	74

---

<i>Grid Window Toolbar</i> .....	74
<i>Display Settings</i> .....	75
CHART WINDOW .....	76
<i>Examples of Chart Window</i> .....	76
<i>Summary of Display Options</i> .....	76
<i>Chart Window Toolbar</i> .....	76
<i>Chart Properties</i> .....	76
<i>Gallery Type</i> .....	77
<b>QUICK START: LANEXPLORER.....</b>	<b>78</b>
<i>Network Protocol Analysis- Packet Capture and Protocol Decode</i> .....	78
<i>Traffic Generator- Send Packets and Playback Captured Packets</i> .....	80
<i>Network Traffic Monitoring - Network Statistics</i> .....	81
<i>Node to Node Traffic - IP Traffic Matrix and MAC Traffic Matrix</i> .....	82
<i>Identifying Network Nodes - Host Table, Host Chart and Address Book</i> .....	83
<b>PART II    REMOTE AGENT .....</b>	<b>84</b>
<b>REMOTE AGENT.....</b>	<b>84</b>
SYSTEM REQUIREMENTS.....	84
PRE-INSTALLATION.....	84
INSTALLATION.....	84
<i>Install from a CD-ROM</i> .....	84
<i>Installation from a downloaded file</i> .....	84
STARTING AND STOPPING REMOTE AGENT .....	85
MINIMIZING OR CLOSING REMOTE AGENT ON DESKTOP .....	85
CONFIGURING REMOTE AGENT .....	86
<i>Serial Number</i> .....	86
<i>Password</i> .....	86
<i>Socket Port</i> .....	86
RESTARTING REMOTE AGENT.....	86
REMOVING REMOTE AGENT.....	86
CONNECTING TO A REMOTE TRAFFIC AGENT .....	87

---

## Purpose of This Manual

This manual describes how to install and use LanExplorer and Remote Agent to analyze network traffic. Since many users prefer to learn through hands-on experience, the Getting Started chapter includes many examples that lead you through the basics of analyzing networks.

**LanExplorer** is an advanced, all-purpose analyzer that not only captures and decodes packets but also analyzes Internet access traffic from the local area network. LanExplorer provides a network management solution to let computer professionals troubleshoot network problems as well as monitor network activities in an efficient way.

**Remote Agent** is a background application that let the above Intellimax applications (i.e. TrafficMax, LanExplorer and LanTrend) to capture network traffic from a remote network segment. This product removes the limit of location to gather network data by application.

### *Obtaining Customer Technical 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](mailto:support@intellimax.com)

Web: <http://www.intellimax.com/support.htm>

Fax: (408) 588-9807

---

## ***Audience***

This manual is focused towards beginners and general users. Advanced users will find our software easy to use with the GUI Windows “look and feel,” and may want to skim through the manual after the installation sections.

## ***Organization of This Manual***

### Part I: LanExplorer

- Chapter 1: Product Overview
- Chapter 2: Installing LanExplorer
- Chapter 3: Using LanExplorer
- Chapter 4: Traffic Monitoring
- Chapter 5: Network Protocol Analysis
- Chapter 6: Network Statistics
- Chapter 7: Traffic Generator
- Chapter 8: Settings
- Chapter 9: Open or Save File
- Chapter 10: Display Properties
- Quick Start: LanExplorer

### Part II: Remote Agent

### Index

## Part I LanExplorer

### Chapter 1: 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 NIC.
- 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.

## Chapter 2: Installing LanExplorer

This chapter describes the system requirements and the installation procedures for LanExplorer.

### *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 "togglng" 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
- Oemsetup.inf

For 2000:

- Isproto2.sys
- 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**

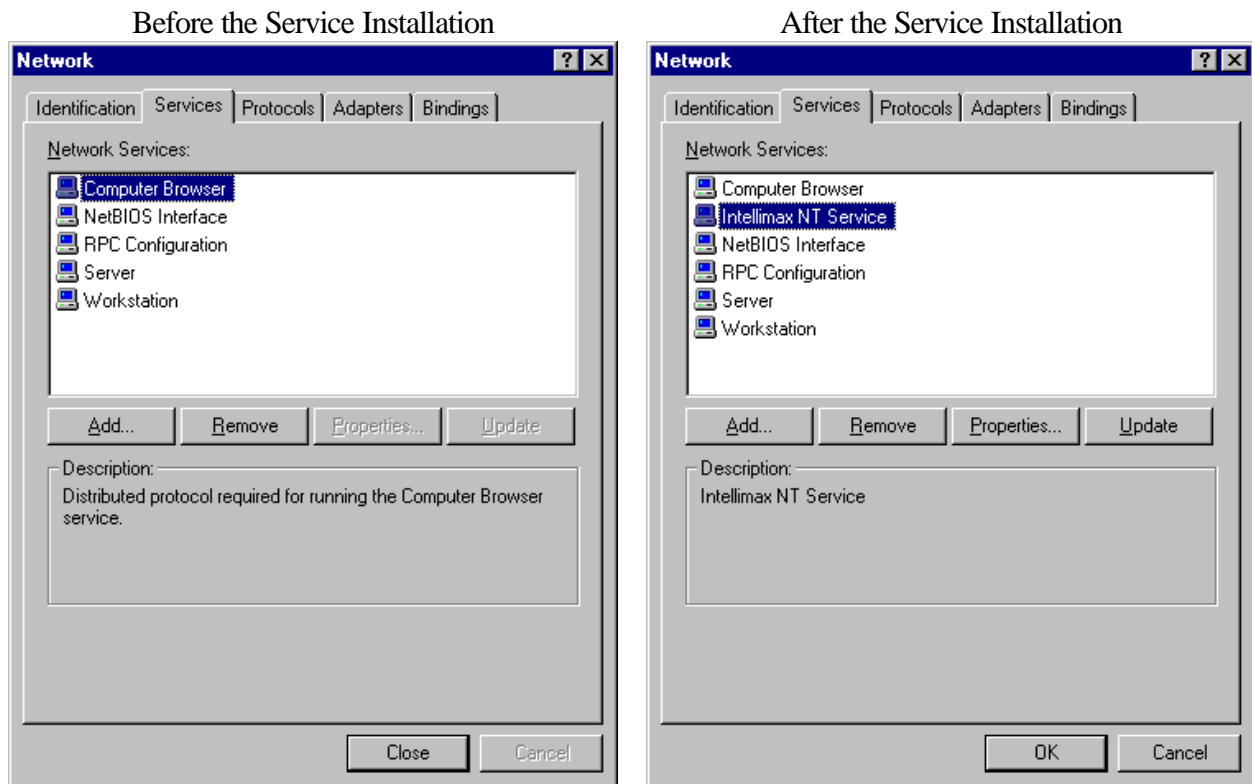
- Get a valid or temporary Serial Number by emailing or calling Technical Support.
- Click the self-extracting file (e.g. LANEXPLORER.EXE).
- Follow the instructions to install the application.

## *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.

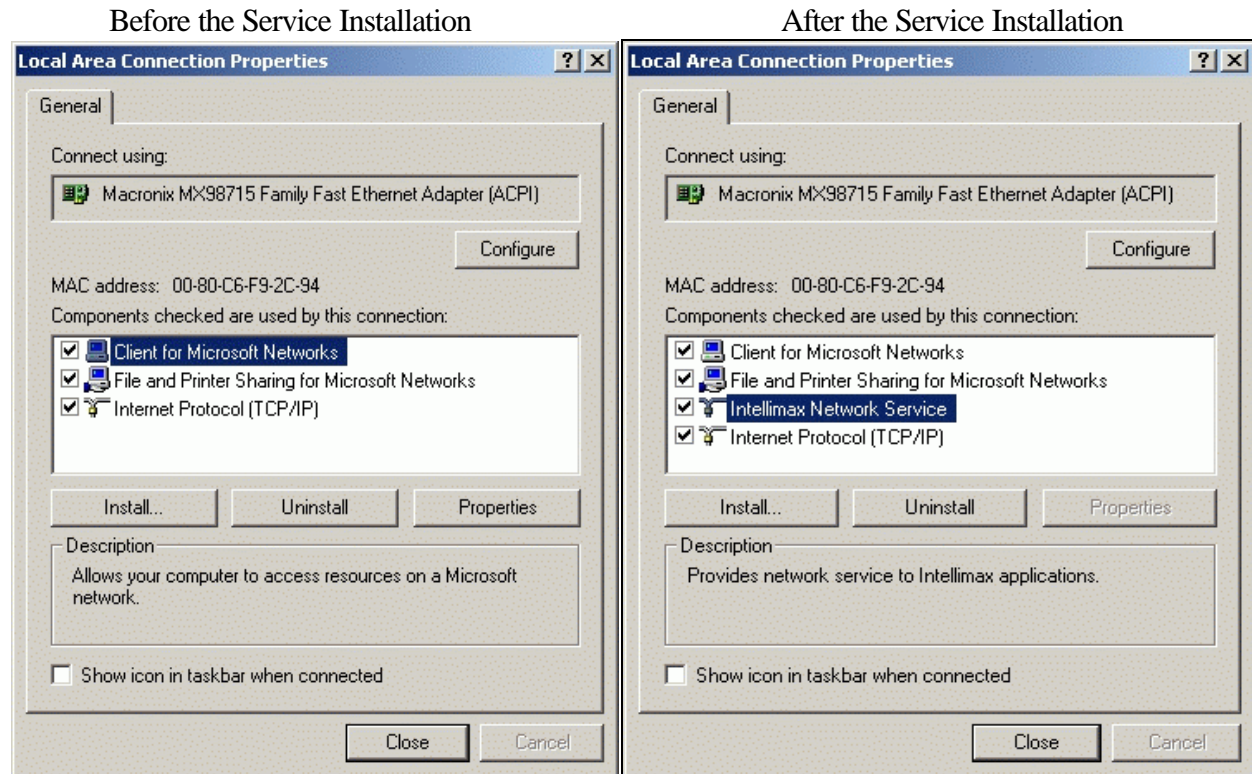
- Click the Services tab.
- Click the Add button.
- Click the Have Disk button.
- Enter the path for the Intellimax NT Service (ISPROTO.SYS and OEMSETUP.INF).
- Click the OK button.
- Click the OK button again.
- Follow the instructions to reboot your system.



## 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 (ISPROTO2.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.

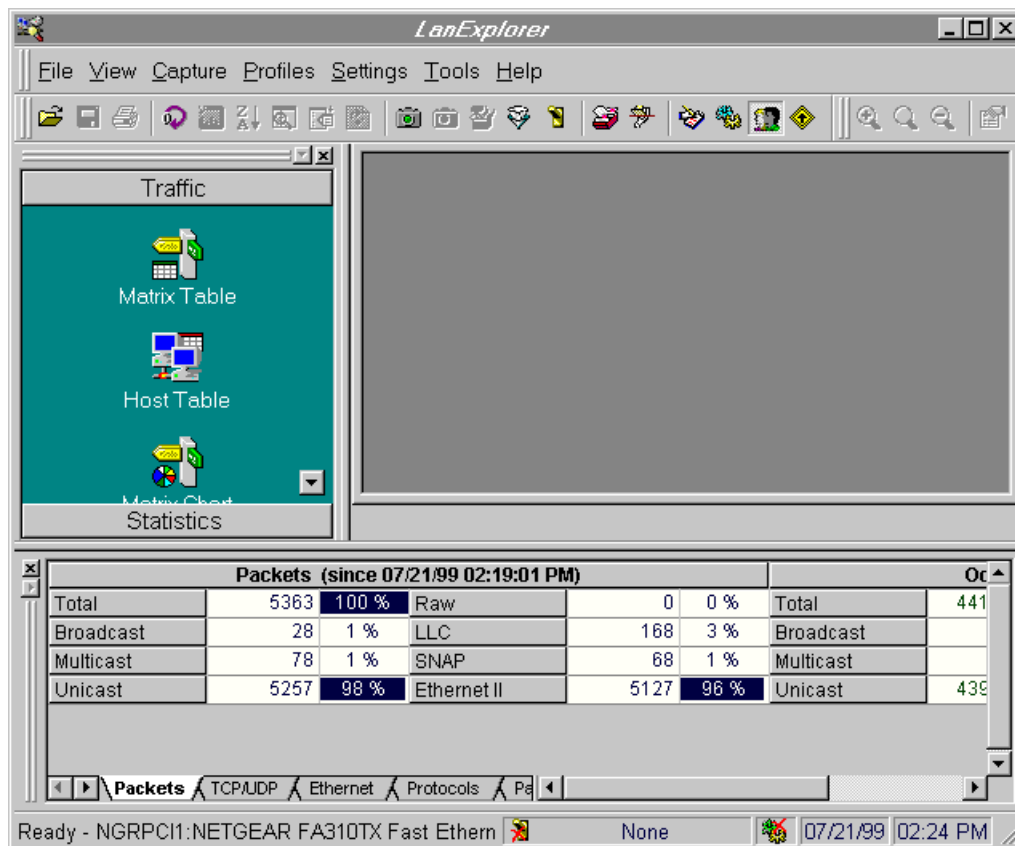
## Chapter 3: Using LanExplorer

### *Starting LanExplorer*

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

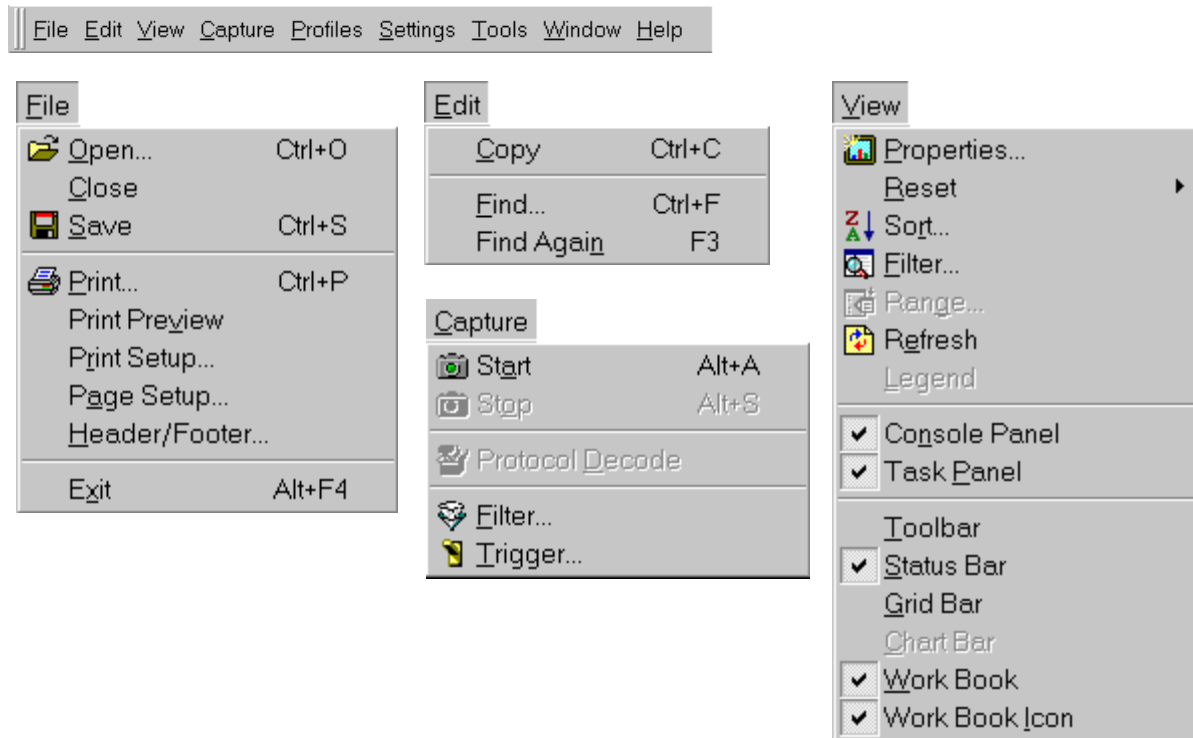
- Click the Desktop Start button.
- Move mouse to Programs.
- Move mouse to Intellimax.
- Click LanExplorer.

You can also create a shortcut of the LanExplorer application (probe.exe) on the Desktop and launch the application from the shortcut. The following window, the main window of LanExplorer, 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, print, and exit from LanExplorer.

### Edit Menu

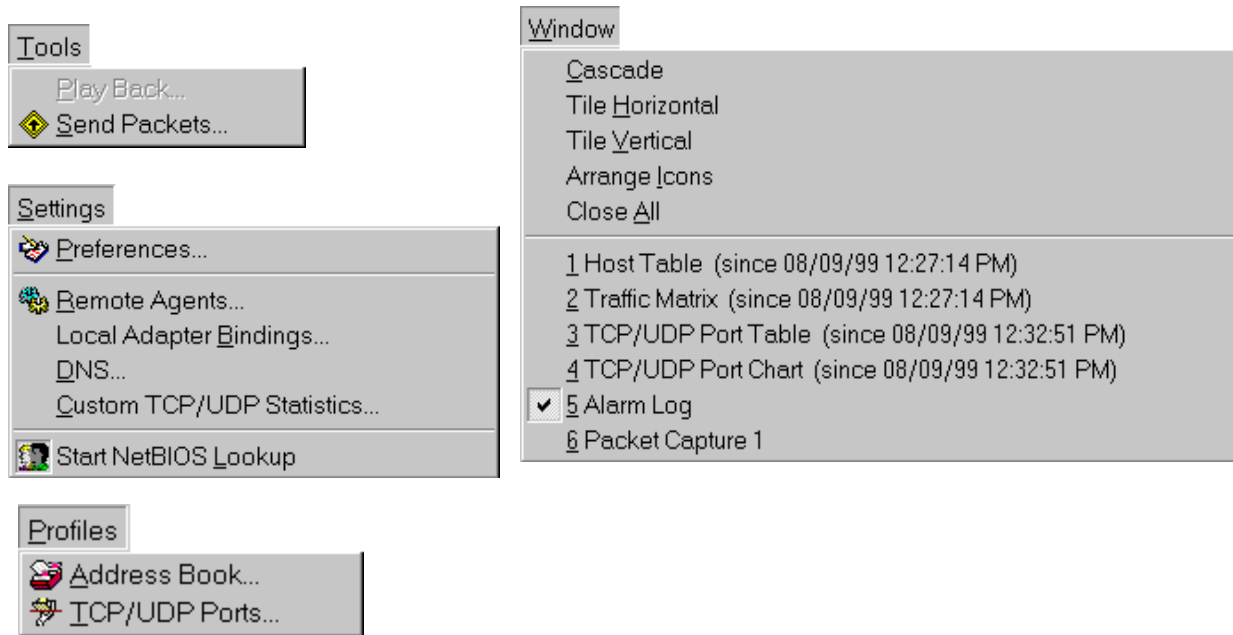
Edit Menu has commands to copy packets to Clickboard and find the name in the active window.

### 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.



### Tools Menu

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

### Window Menu

Window Menu has commands to manipulate LanExplorer windows.

### 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.



















### Profiles Menu

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

## ***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	 Show Protocol Decode
 Save	 Capture Filter
 Print	 Capture Trigger
 Reset Console Statistics	 Address Book
 Display Properties	 TCP/UDP Port Definition
 Sort	 Preferences
 Display Filter	 Remote Agent
 Refresh	 NetBIOS Lookup
 Start/Stop Packet Capture	 Send Packets

## ***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.

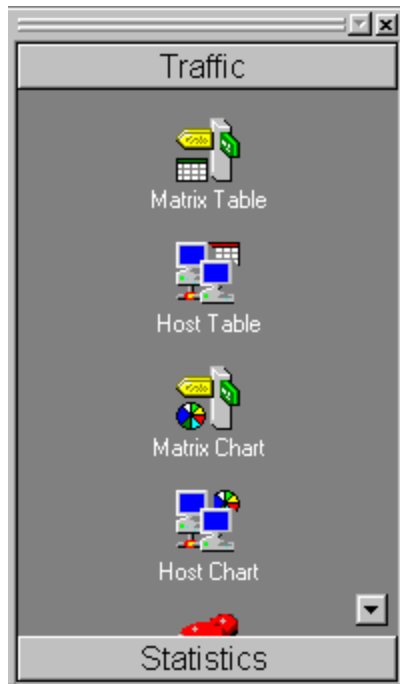
### **Packet Capture Trigger, Remote Agents**



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

in second	Type	Interval
MAC Layer	Packets	15
TCP/UDP	Packets	15
Protocol	Packets	15
Packet Size	Packets	15
TCP/UDP	Packets	15
Protocol	Packets	15
Packet Size	Packets	15

Distribution Statistics

in second	Threshold	Type	Interval
Utilization %	50	N/A	15
Total	5000	Packets	15
Broadcast	1000	Packets	15
Multicast	1000	Packets	15
Unicast	5000	Packets	15
ICMP	200	Packets	15
TCP SYNC	1000	Packets	15
64 Bytes	2000	Packets	15
65-127	2000	Packets	15
128-255	2000	Packets	15
256-511	2000	Packets	15

Rate Statistics

in second	Threshold	Type	Interval
FTP	5000	Packets	15
Telnet	5000	Packets	15
SMTP/POP/IMAP	5000	Packets	15
HTTP(S)	5000	Packets	15
NNTP	5000	Packets	15
NetBIOS	5000	Packets	15
SNMP	5000	Packets	15
Custom1	5000	Packets	15
Custom2	5000	Packets	15
Custom3	5000	Packets	15
Custom4	5000	Packets	15

TCP/UDP Statistics

## Console Panel

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

Packets (since 11/22/98 09:03:30 AM)						Octets	
Total	1469	100.00 %	Raw	0	0.00 %	Total	1683
Broadcast	49	3.34 %	LLC	255	17.36 %	Broadcast	60
Multicast	345	23.49 %	SNAP	326	22.19 %	Multicast	240
Unicast	1075	73.18 %	Ethernet II	888	60.45 %	Unicast	1382

Navigation tabs: Packets | TCP/UDP | Ethernet | Protocols

Click a tab at the bottom of the Console Panel to see different kinds of accumulated statistics (running totals). Available tabs are:

- Packets
- TCP/UDP
- Ethernet or Token Ring
- Protocol
- Packet size

## Chapter 4: Traffic Monitoring

### *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.

	Address	Address 2	Octets Ratio	Octets	Packets	Activ
1	Intmax2	fw.a2000.com	20 %	5872951	65061	
2	Intmax1	ppp04-1-215.cityline.ru	5 %	1419509	18072	
3	Intmax1	203.236.234.35	5 %	1399503	17811	
4	Intmax2	www.ifsw.uni-stuttgart.de	5 %	1334182	14798	
5	Intmax1	guy15-148.abo.wanadoo.fr	3 %	9206906	11679	
6	Intmax1	195.14.231.130	3 %	8895186	10504	
7	Intmax1	cable-195-162-193-32.customer.tvd.be	3 %	8414751	8755	
8	Intmax2	sfk1a-249.up.net	3 %	7979641	21657	
9	Intmax2	ns2.divi.com	3 %	7725690	9970	
10	Intmax1	val5-231.abo.wanadoo.fr	2 %	7181497	18527	
11	Intmax1	m7-43-ndf.dial-up.net	2 %	7109570	17833	
12	Intmax1	gate6-89.nordnet.fr	2 %	7035694	17705	
13	Intmax1	proxy.datacomm.ch	2 %	7026041	7797	
14	Intmax1	rt080na4.midsouth.rr.com	2 %	6970946	6919	

169 IP 10 sec. None Octets Ratio

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)
- URL group (Based on predefined or user defined groupings)
- 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.*

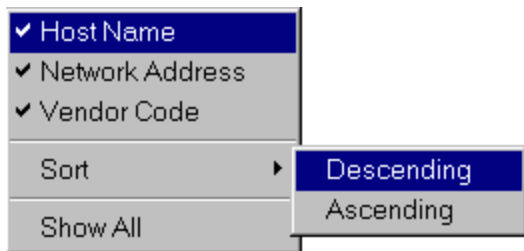
## Traffic Matrix Table Options

### 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.

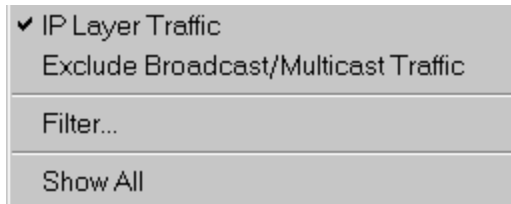


The menu gives you the following options:

- 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.

### Sorting Options

Click the right mouse button on any numbers cell in the leftmost column on the Traffic Matrix Table or the Host Table, and a popup menu will appear with sorting options.



The Sorting Options allow you to select IP or MAC Traffic Matrix, Exclude Broadcast/Multicast Traffic, Show All, and call up Filter window.

### 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	02FFFFFFFF	134	8576
2	Lockhaven	Broadcast	113	13470
3	02A0C95C56B1	02FFFFFFFF	76	4864
4	Lockhaven	01FFFFFFFF	72	4608
5	04A0C95C56B1	02FFFFFFFF	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	02FFFFFFFF	134	8576
4	02A0C95C56B1	02FFFFFFFF	76	4864
5	Lockhaven	01FFFFFFFF	72	4608
6	04A0C95C56B1	02FFFFFFFF	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	02FFFFFFFF	134	8576
4	02A0C95C56B1	02FFFFFFFF	76	4864
5	Lockhaven	01FFFFFFFF	72	4608
6	04A0C95C56B1	02FFFFFFFF	63	4032

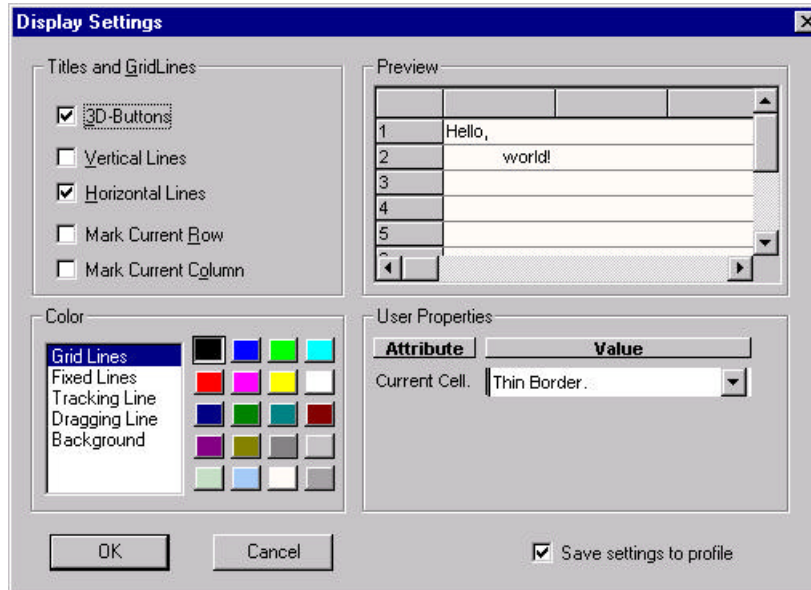
↑  
Before sorting Address2 ascending

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

↑  
After sorting Address2 ascending

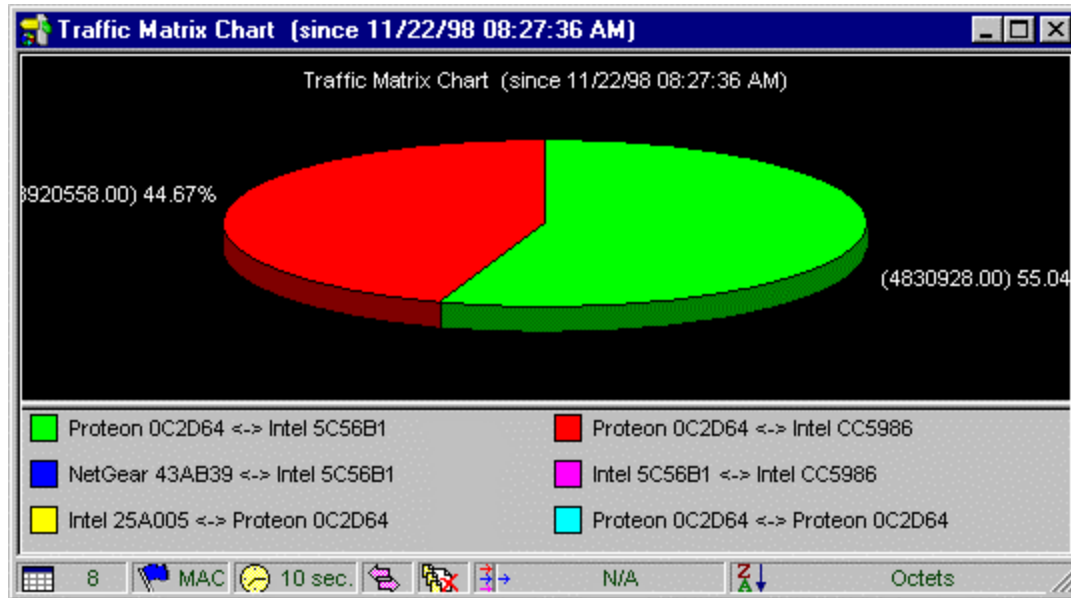
## Display Settings

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.*

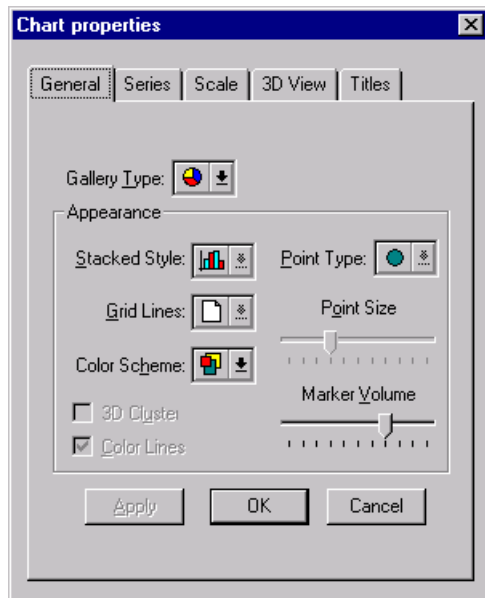
*Tip: Adjust the legend size by clicking anywhere in the legend.*

*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

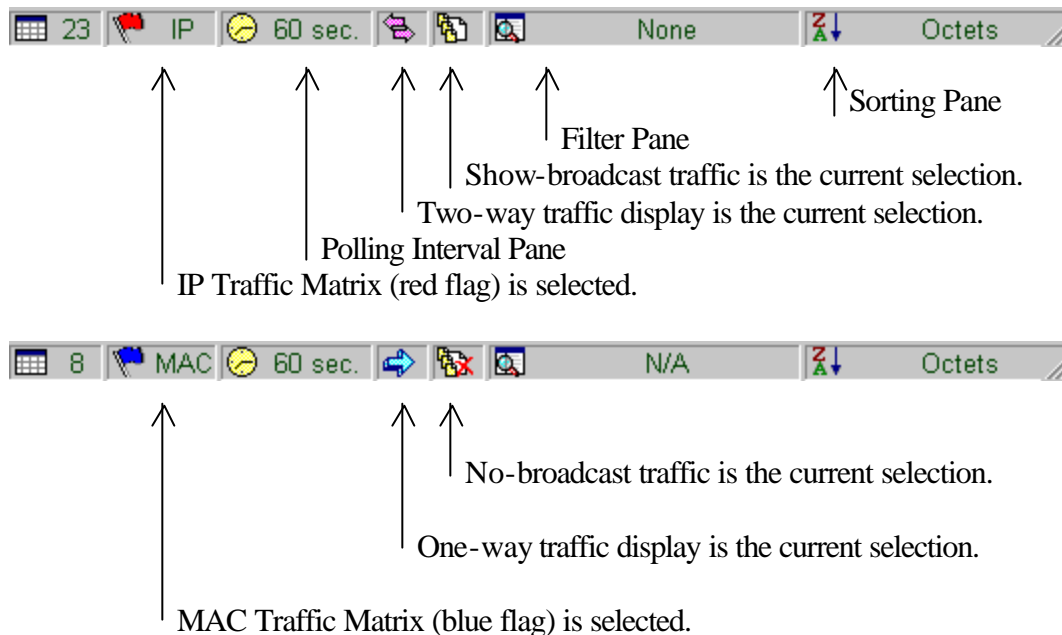
Click the left mouse button once on the Traffic Matrix Chart window to select the active window. Click the Display Properties command on the Toolbar or the Properties item of the View menu to launch the Chart Properties window. Please refer to the general information section of the Chart window for more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



*Tip: Many items on the charts are clickable or adjustable.*

## Traffic Matrix Status Bar

This section describes the Status Bar at the bottom of the Traffic Matrix Table and Traffic Matrix Chart windows. Each window has independent parameters for changing configurations, except the polling interval that can also be changed in Settings/Preferences. The changes apply 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 or displayed.

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

### Changing Polling Interval

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 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.

## 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.

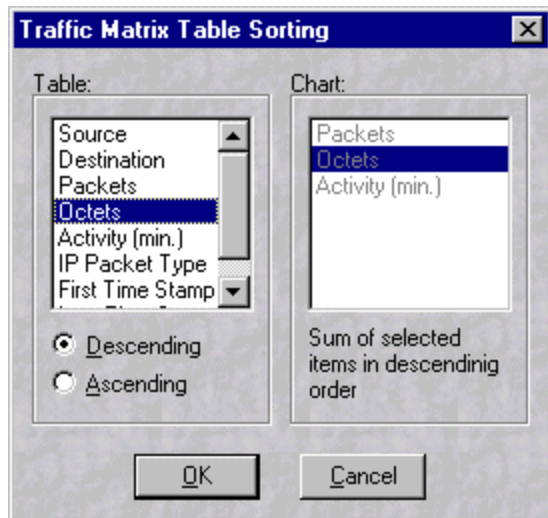
## Changing Traffic Matrix Filter

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

Click the sorting pane in the Traffic Matrix Status Bar or the Sort item of the View menu while Traffic Matrix is the active window to 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.

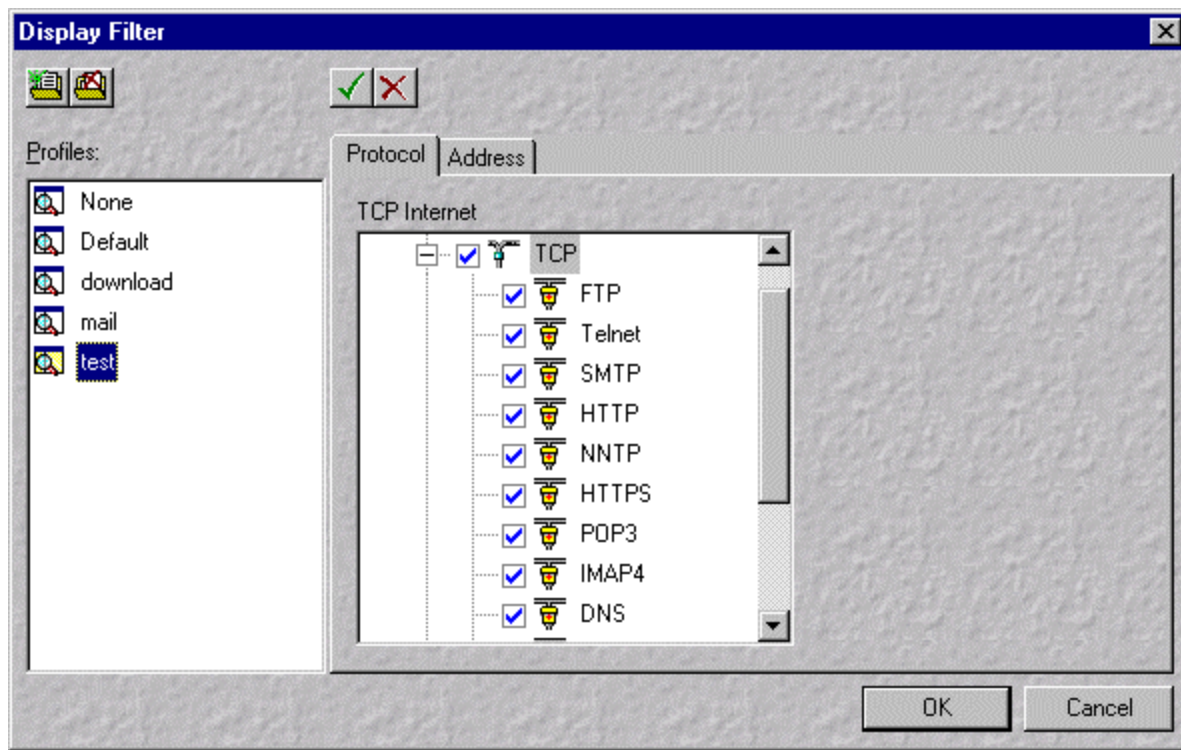
- Source address
- Destination address
- Octets Ratio
- Number of packets
- Number of octets
- Activity in minutes
- Hits/Calls
- IP Packet Type
- First Access Time Stamp
- Last Access Time Stamp
- URL Group

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 their 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. The 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

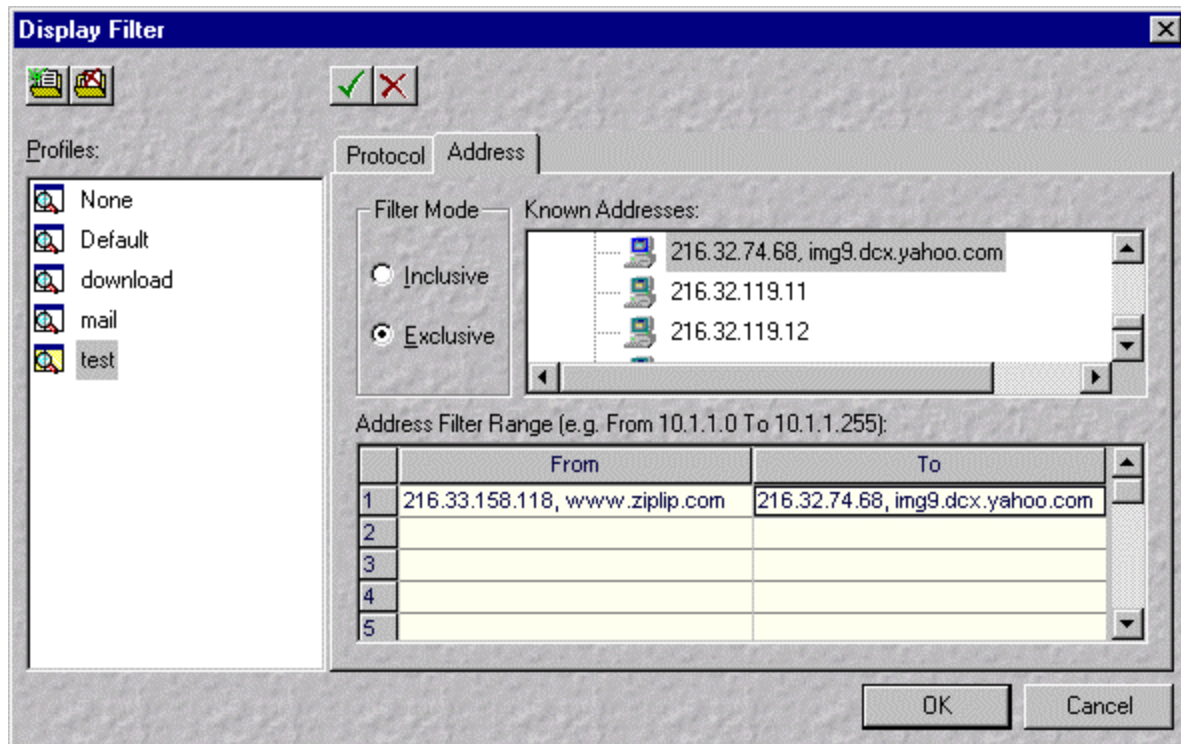
There are two buttons on the upper-center of the window to select all filter check boxes or clear all filter check boxes. If there are 20 check boxes selected and you want to delete 19 of them, the fastest way is to clear all, then check the one you want.

## 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 and MAC Host Table.

	Address	Octets Ratio	Total Octets	Total Packets	Act
1	Intmax1	25 %	149536722	217818	
2	Intmax2	24 %	141295508	186407	
3	fw.a2000.com	10 %	58729515	65061	
4	ppp04-1-215.cityline.ru	2 %	14258800	18247	
5	203.236.234.35	2 %	13997238	17828	
6	www.ifsw.uni-stuttgart.de	2 %	13341821	14798	
7	ct080na4.midsouth.rr.com	2 %	13296974	13216	
8	195.14.231.130	2 %	11557936	13687	
9	guy15-148.abo.wanadoo.fr	2 %	9206906	11679	
10	cable-195-162-193-32.customer.tvd.be	1 %	8414751	8755	
11	sfk1a-249.up.net	1 %	8034843	21863	
12	ns2.divi.com	1 %	7725690	9970	
13	val5-231.abo.wanadoo.fr	1 %	7181497	18527	
14	m7-43.pdf.dialun.net	1 %	7109570	17833	

119 IP 10 sec. None Octets Ratio

In Host Table, the following information is displayed.

- Address
- Octets Ratio
- Total octets
- Total packets
- URL Group
- 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

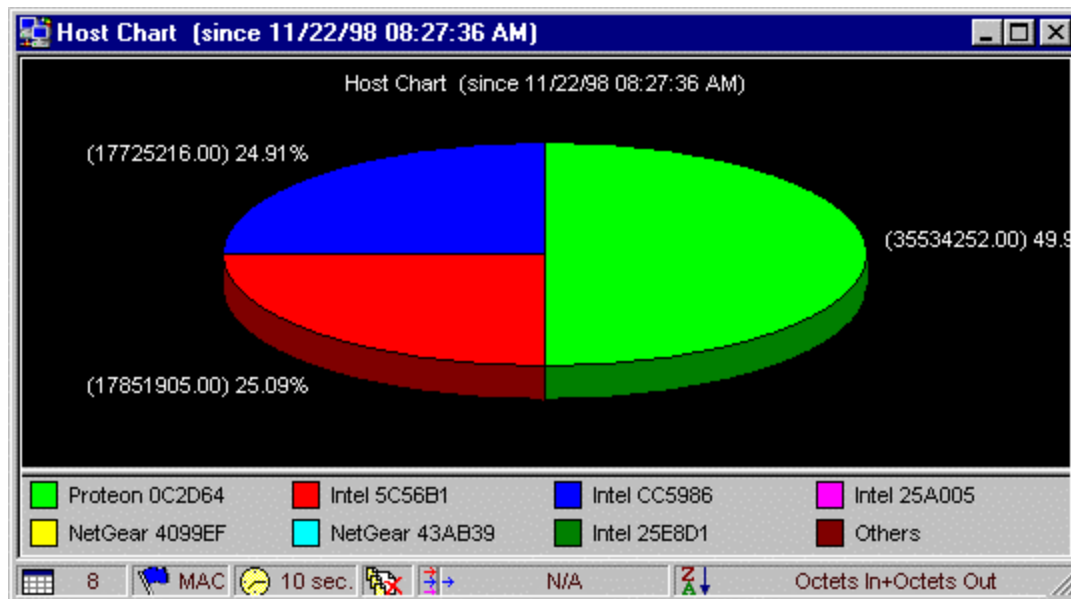
### Host Table Sorting

### Display Settings

See *Traffic Matrix Table Options*, for instructions.

## 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



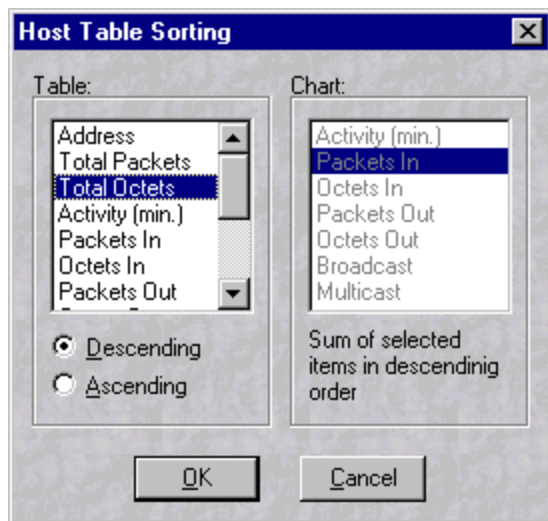
Please refer to Traffic Matrix Status Bar in this Chapter for status bar options on:

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

## More Sorting Options



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.

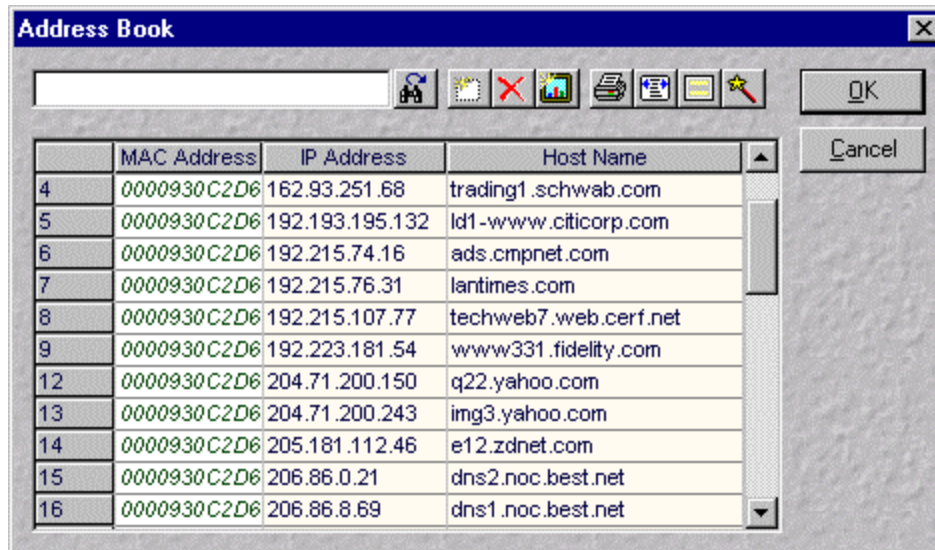
- Address
- Octets Ratio
- Total packets
- Total octets
- Activity in minutes
- Hits/Calls
- Number of packets in
- Number of octets in
- Number of packets out
- Number of octets out
- Number of broadcast packets
- Number of multicast packets
- IP Packet Type
- First Access Time Stamp
- Last Access Time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

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

<i>Button</i>	<i>Type</i>	<i>Description</i>
	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.*

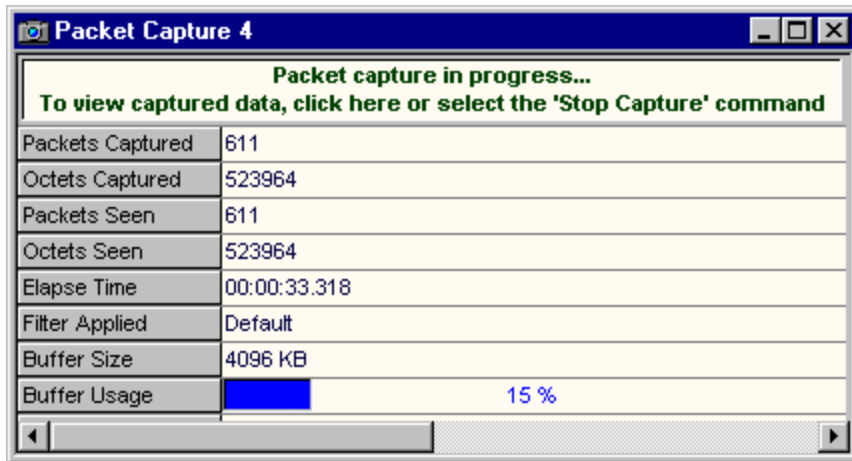
*Tip: If domain names are not displaying (e.g. due to a DNS failure on the first pass), use the DNS Lookup button to start a new lookup.*

*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.*

## Chapter 5: Network Protocol Analysis

### *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.

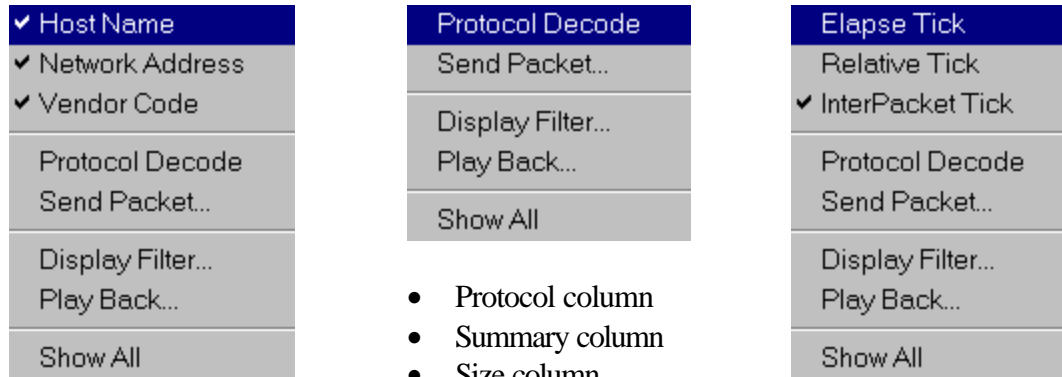
The screenshot shows a window titled "Packet Capture 3" displaying a list of captured packets. The table below represents the data shown in the window:

	Destination	Source	Protocol
13	210.77.224.110	Intmax1	TCP
14	Intmax1	Intmax2	NetBIOS
15	Intmax2	Intmax1	NetBIOS
16	Intmax2	zeve242.info.net	TCP
17	zeve242.info.net	Intmax2	TCP
18	zeve242.info.net	Intmax2	TCP
19	Intmax2	sprinter.millenniumit.com	TCP
20	Intmax2	Fremont	TCP
21	sprinter.millenniumit.com	Intmax2	TCP
22	Fremont	Intmax2	TCP
23	Intmax2	Fremont	TCP
24	Fremont	Intmax2	TCP

At the bottom of the window, there is a toolbar with icons for "Default", "252", "None", and "252".

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 enables you to 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.

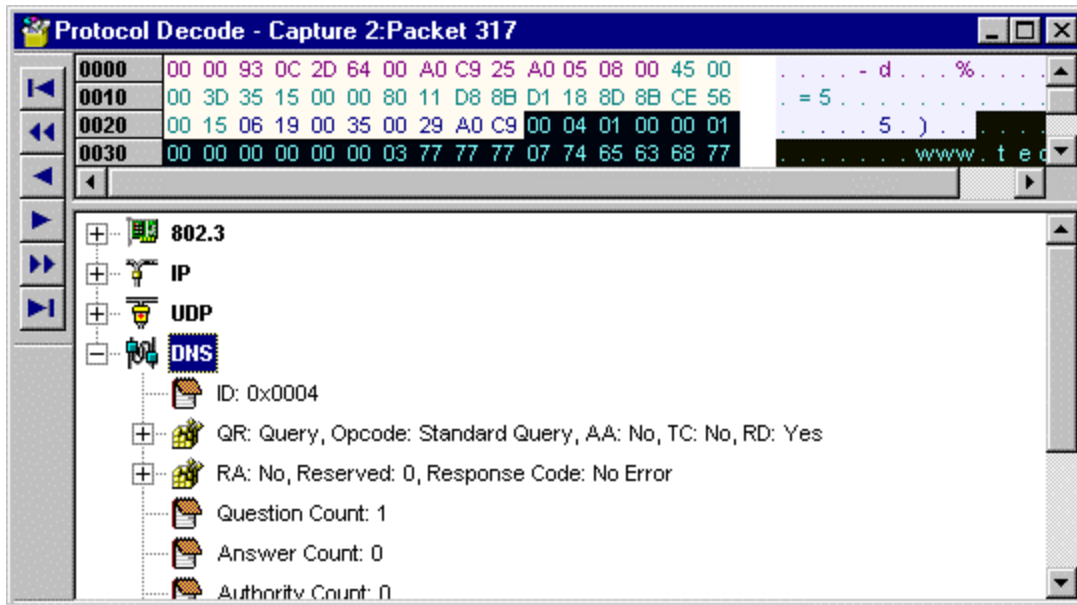
InterPacket – measures the time between the capture of each packet, relative to the previous packet.

## 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.

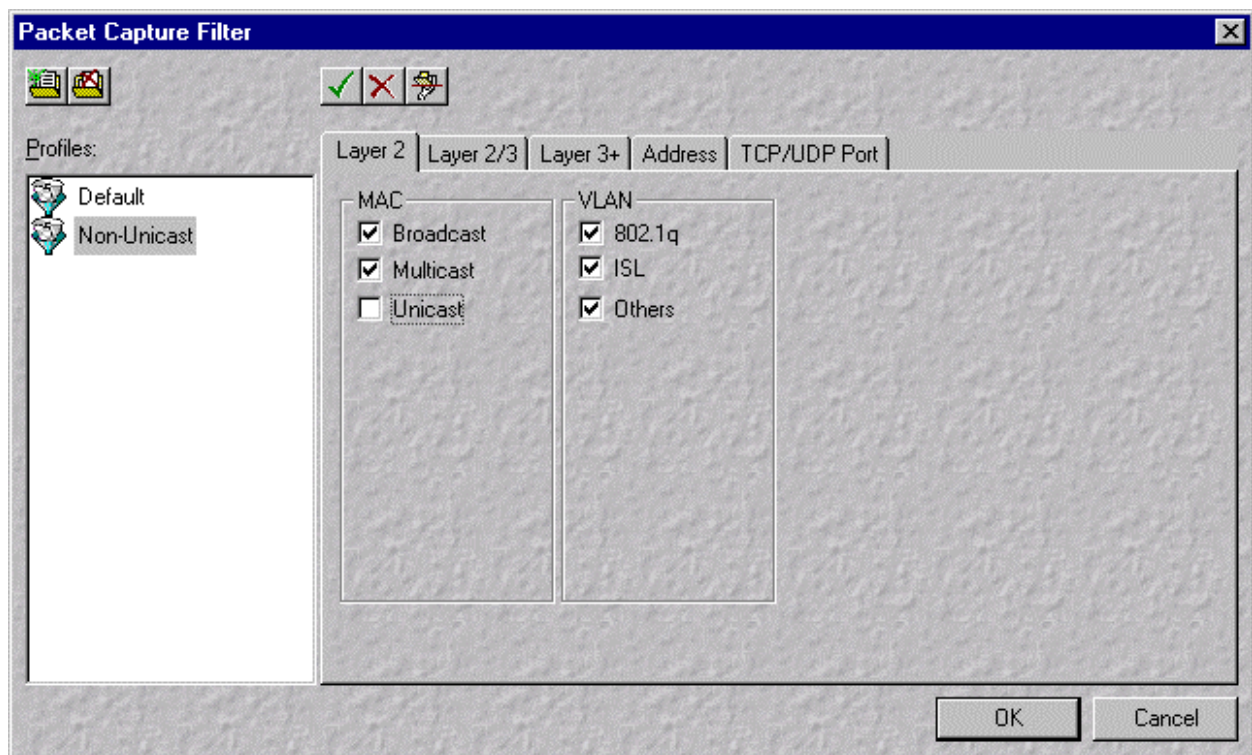
### **Layer 2 MAC Filter**

- 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

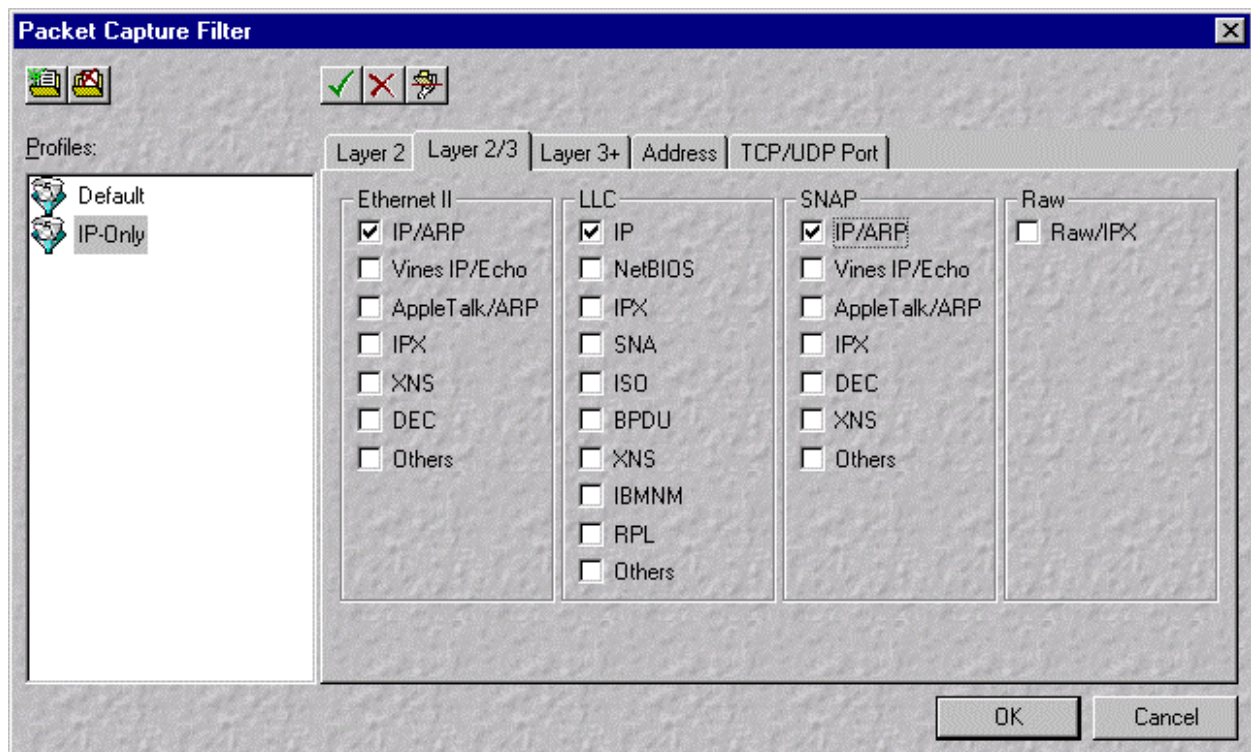
**Layer 2/3 LLC SNAP Filter**

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

**Layer 2/3 Raw Filter**

- Raw XNS/IPX

**Layer 2/3 Filter Example**



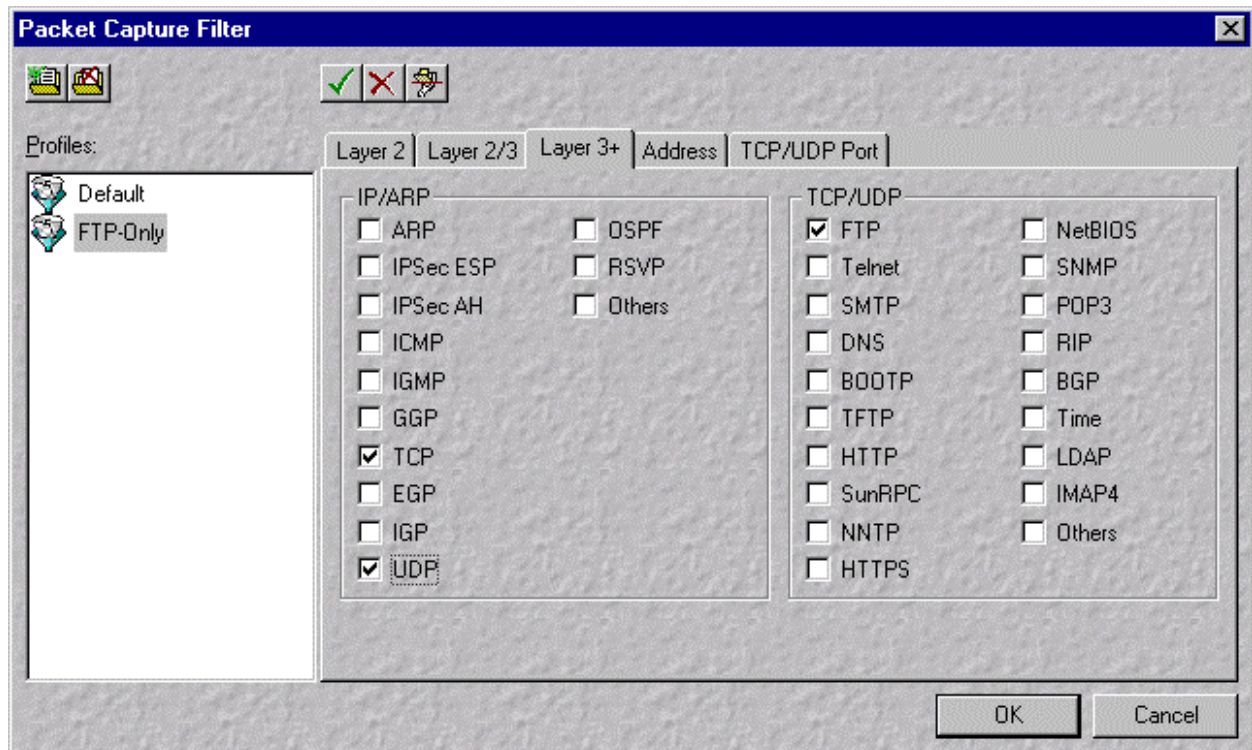
### Layer 3+ IP/ARP Filter

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

### Layer 3+ TCP/UDP Filter

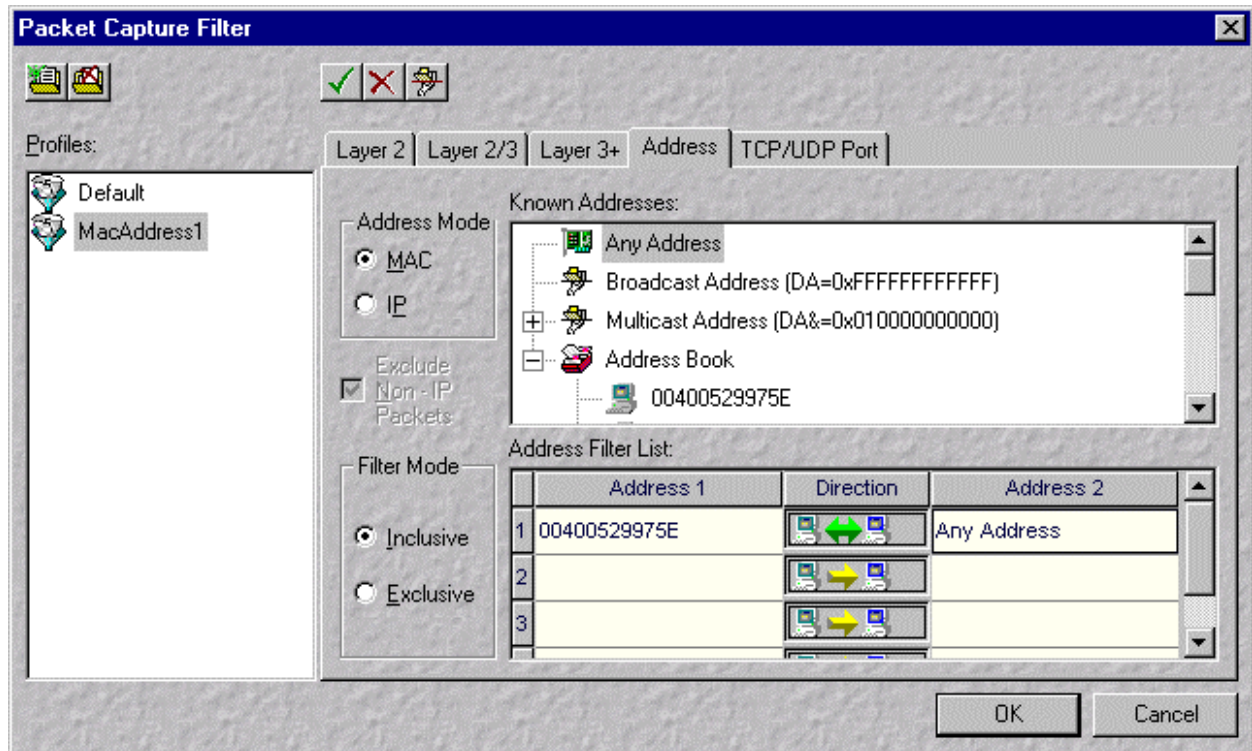
- FTP
- Telnet
- SMTP
- DNS
- BOOTP
- TFTP
- HTTP
- SunRPC
- NNTP
- HTTPS
- NetBIOS
- SNMP
- POP3
- RIP
- BGP
- Time
- LDAP
- IMAP4
- Others

### 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.

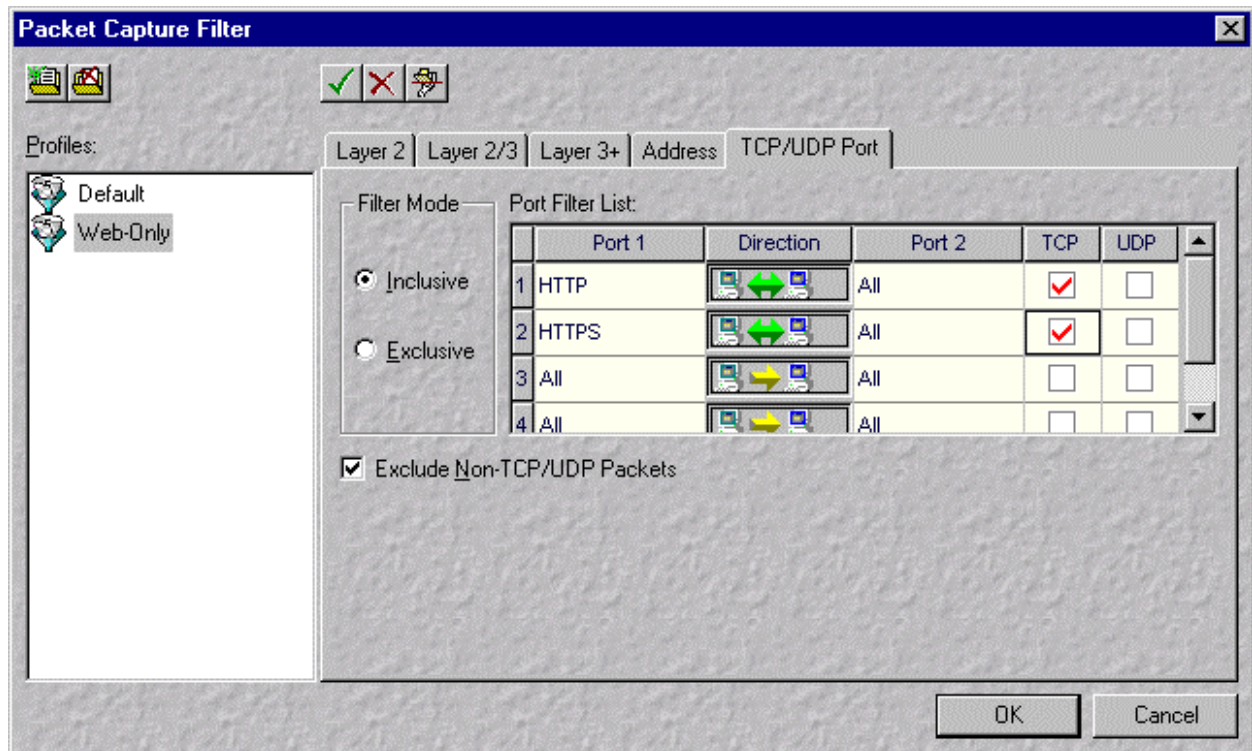
- **Direction**

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**

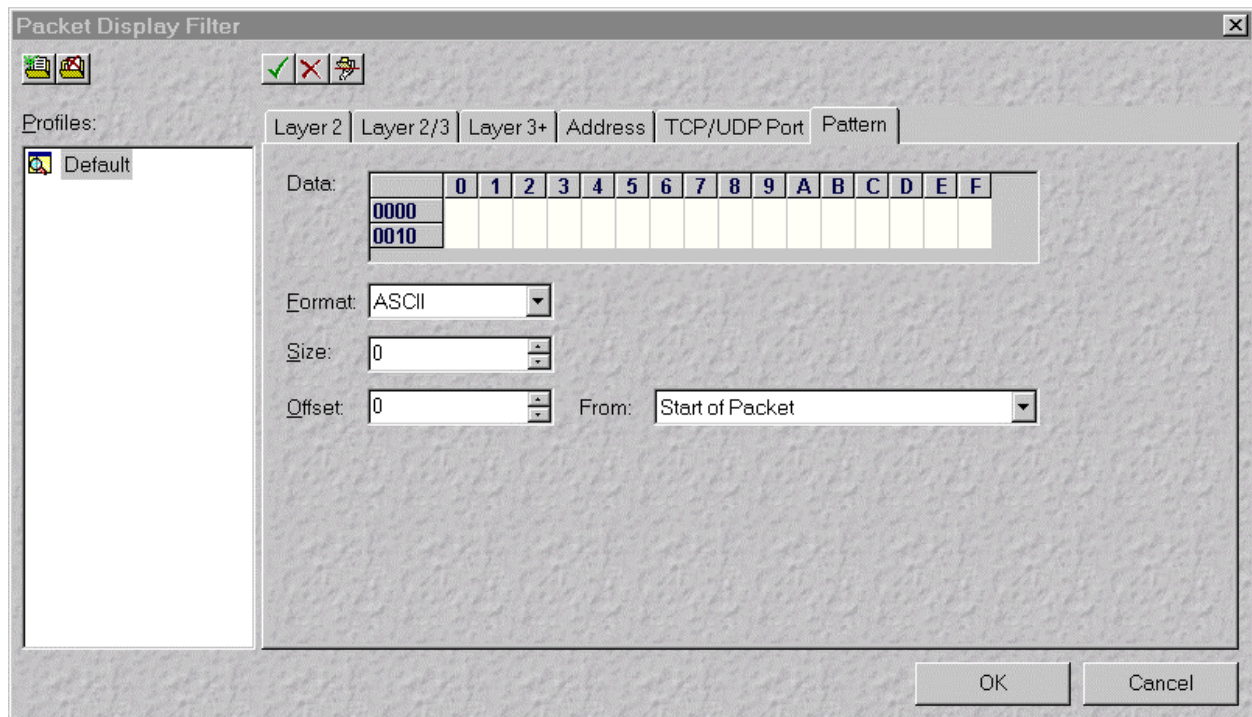
Clicking a direction box between Port1 and Port2 will let you select three different ways of traffic between the two ports.

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 15<sup>th</sup> and 16<sup>th</sup> byte offsets will be passed through the Pattern Filter.



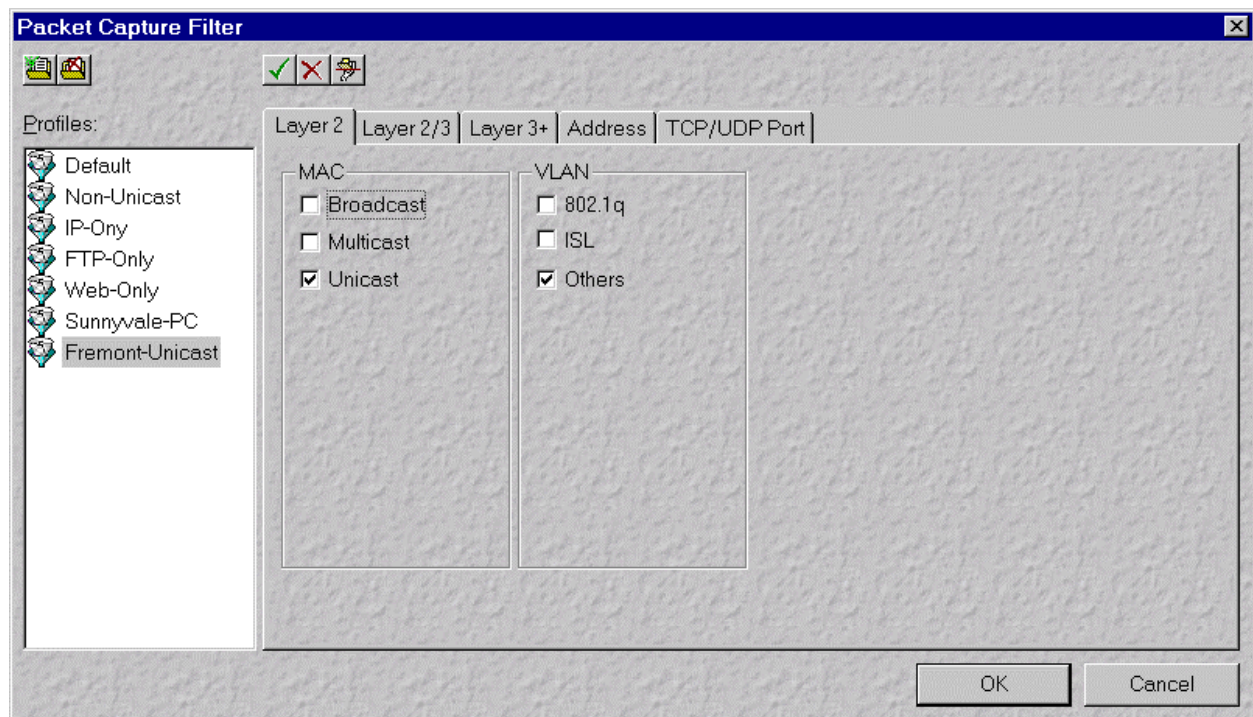
## Setting up Profile

 New profile

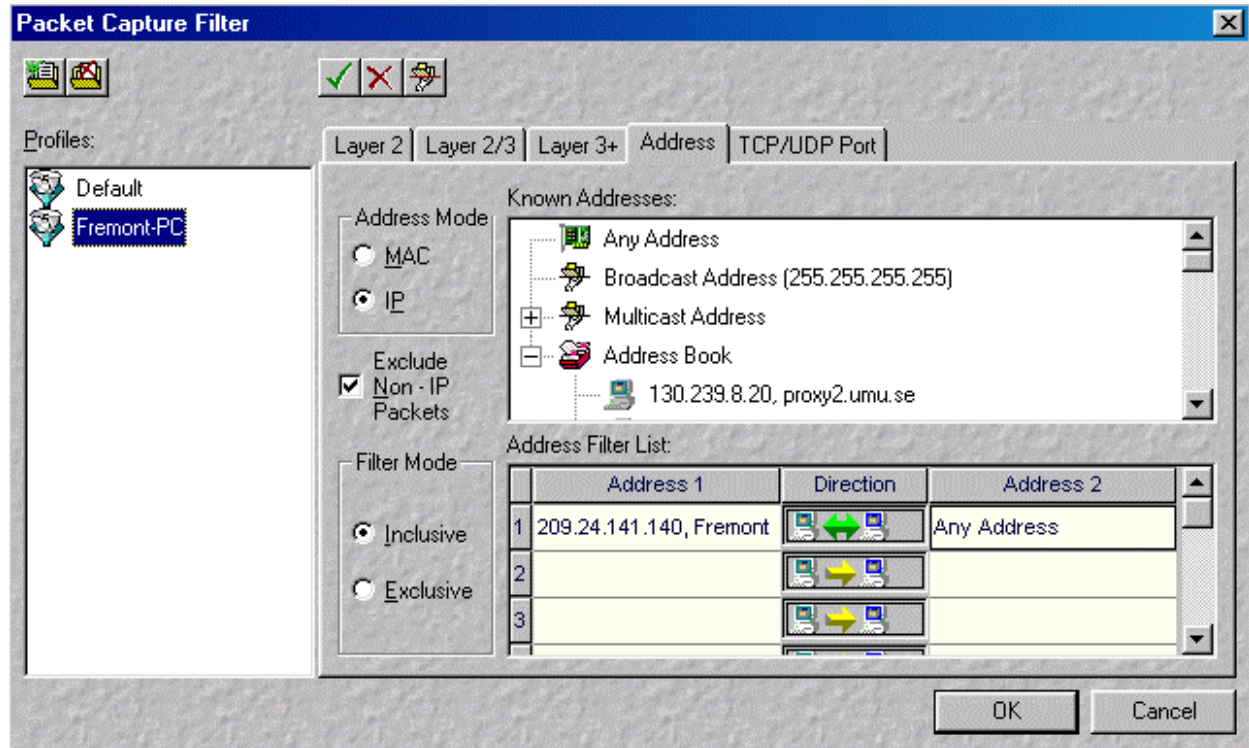
 Delete Profile

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.

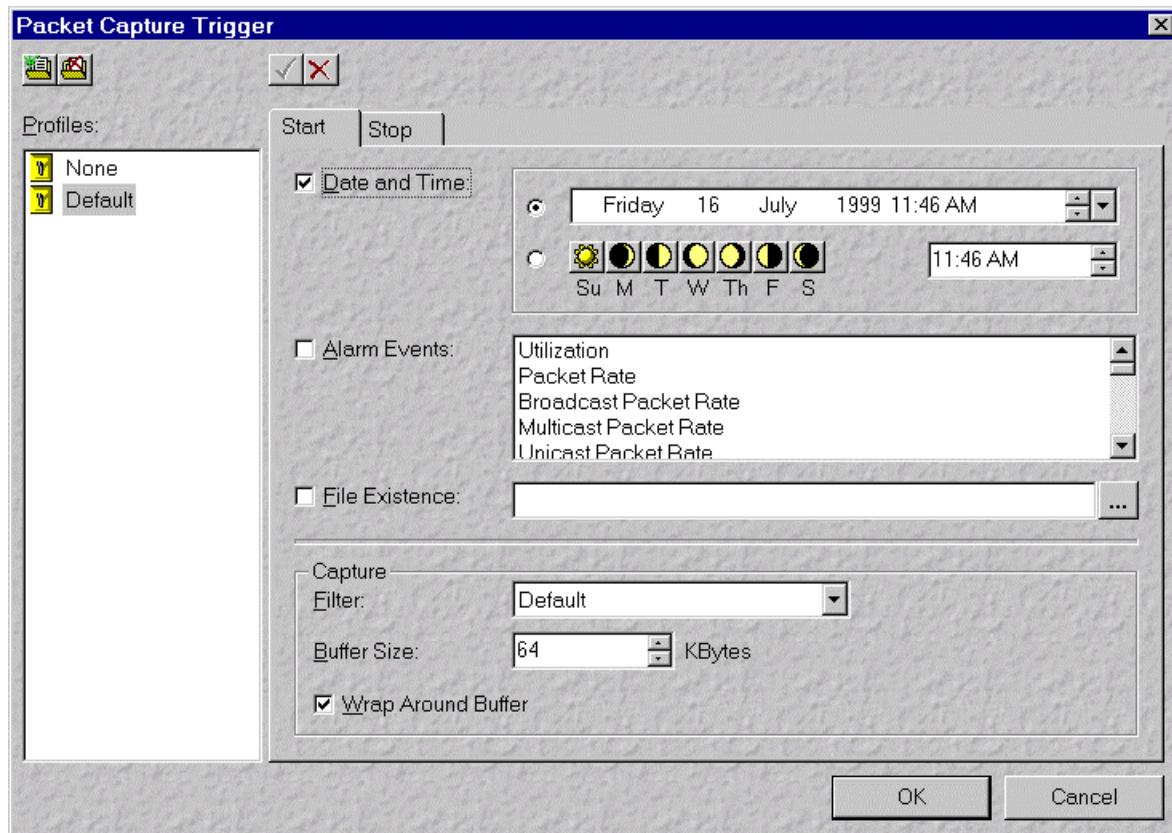
## Packet Capture Trigger

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.



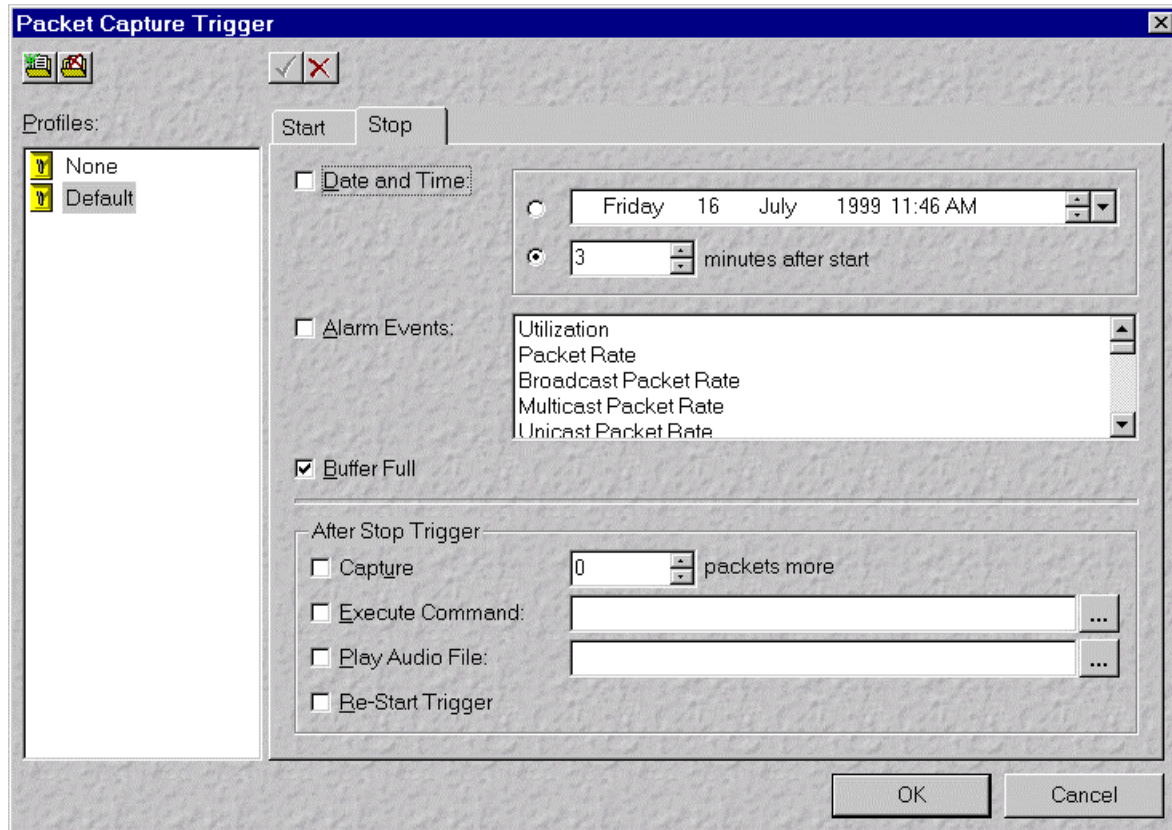
### Packet Capture Options

- 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



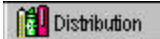

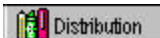

There are options after stopping Packet Capture.

- 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.

## Chapter 6: Network Statistics

### General

Use Network Statistics to understand 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		Rate charts	Shows traffic as a "rate" over time - integrated with (threshold) alarms and useful for monitoring
 Distribution		Historical distribution	Shows traffic as a percentage of total traffic - for understanding overall traffic patterns
 Distribution		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

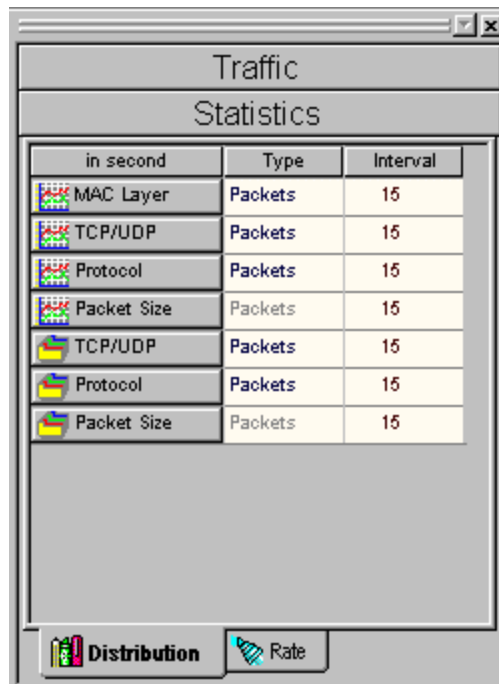
Each accumulated or historical distribution has an icon associated with the name. Click the button of accumulated or historical distribution such as "MAC Layer" in the Distribution category of the Statistics Task Panel to launch the distribution window.

Available historical distributions are:

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

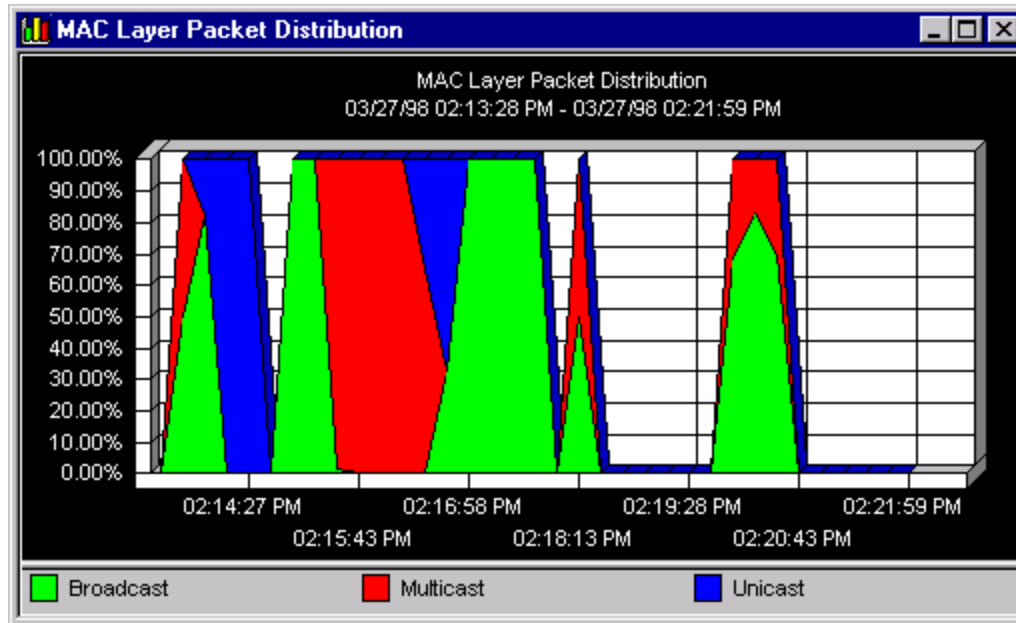
Available accumulated distributions are:

- 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.



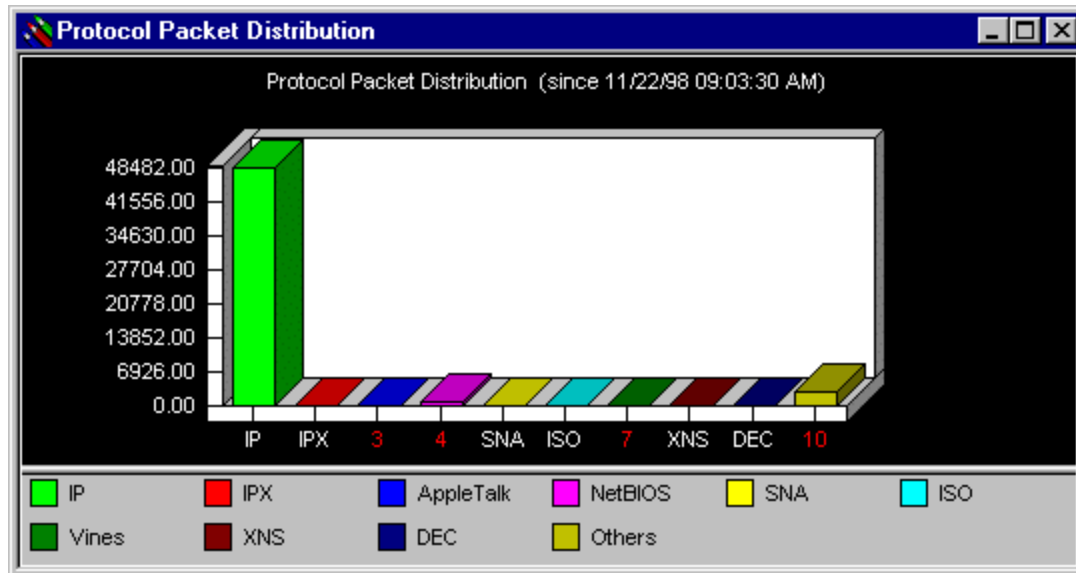
The MAC Layer distribution consists of the following members.

- 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.



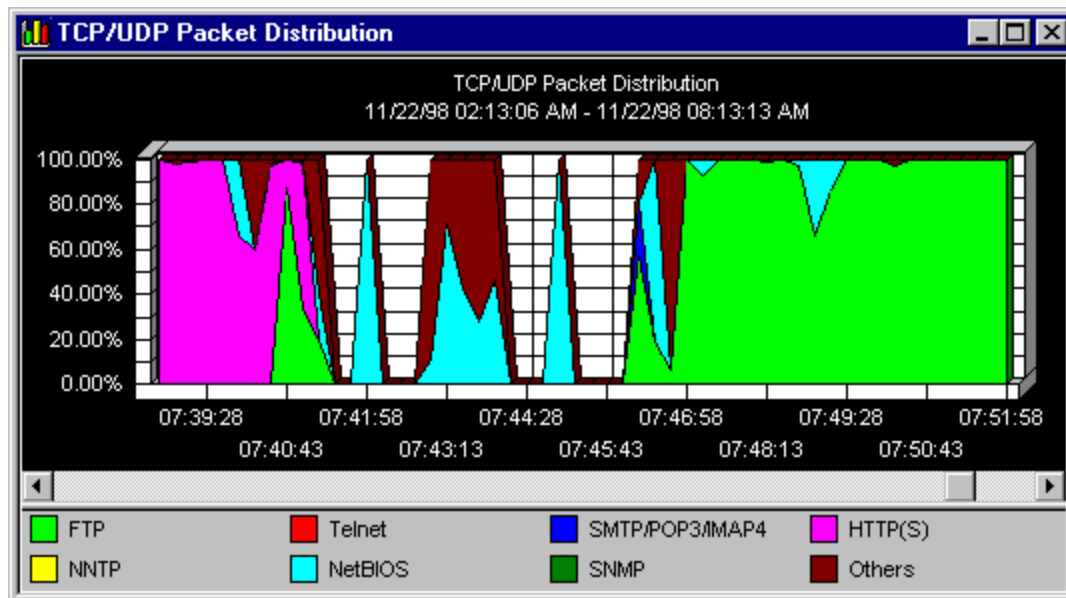
The Protocol distribution consists of the following members.

- 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.



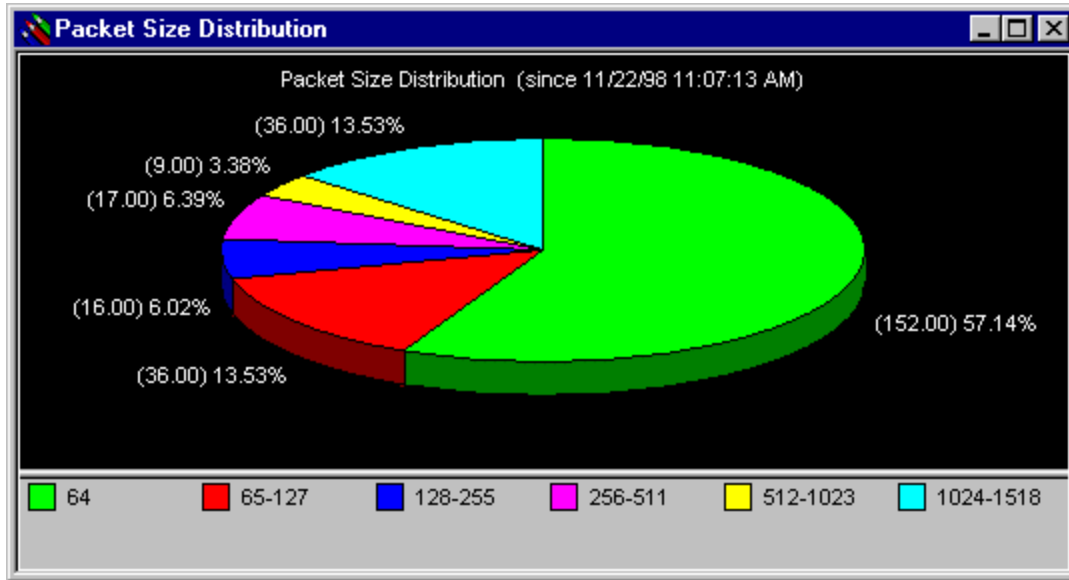
The TCP/UDP distribution consists of the following members.

- FTP packets (download protocol)
- Telnet packets
- SMTP/POP3/IMAP4 packets (Mail protocols)
- HTTP/HTTPS packets (Web protocols)
- NNTP packets (News protocol)
- NetBIOS packets
- SNMP packets (Network 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

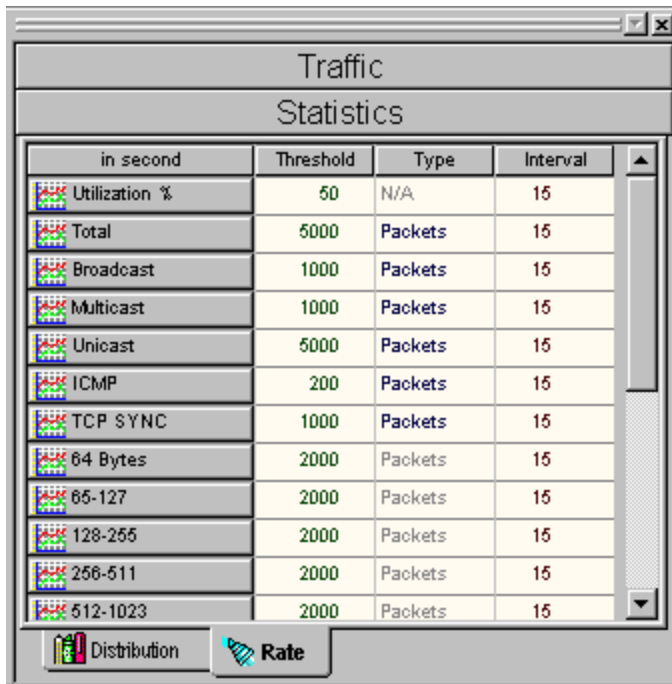
Click the Display Properties command in Toolbar or the Properties item of the View menu to launch the Chart Properties window for the active statistics window. Please refer to the section on Display Properties for additional information.

## 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.

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



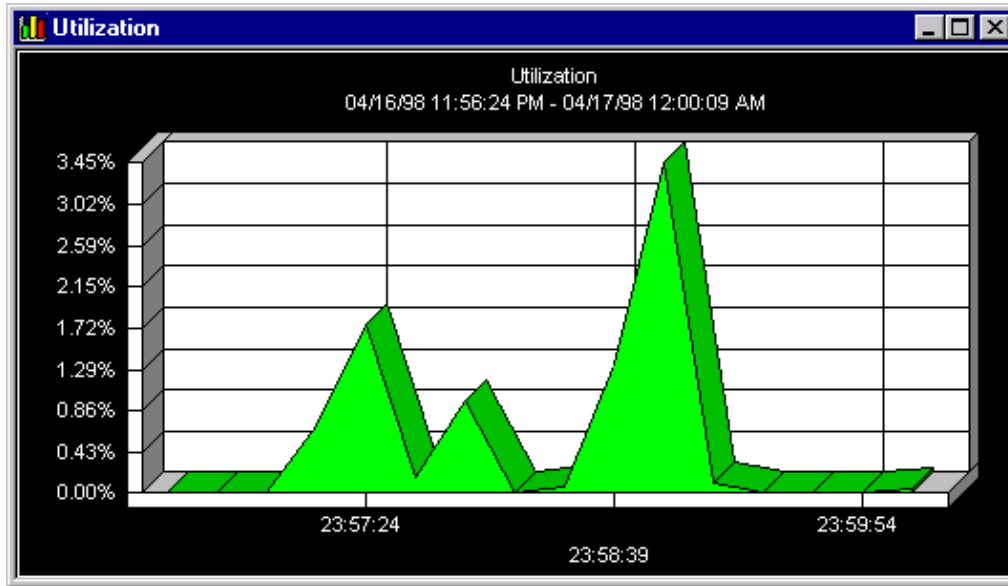
in second	Threshold	Type	Interval
Utilization %	50	N/A	15
Total	5000	Packets	15
Broadcast	1000	Packets	15
Multicast	1000	Packets	15
Unicast	5000	Packets	15
ICMP	200	Packets	15
TCP SYNC	1000	Packets	15
64 Bytes	2000	Packets	15
65-127	2000	Packets	15
128-255	2000	Packets	15
256-511	2000	Packets	15
512-1023	2000	Packets	15

Available rate items are listed below:

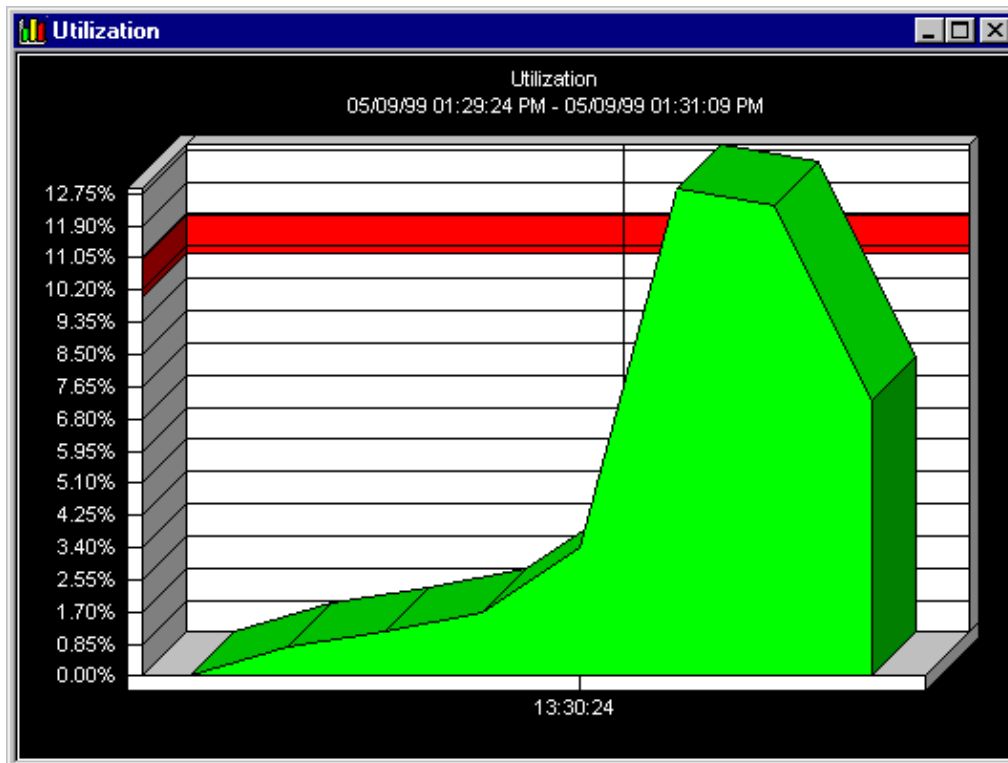
- Utilization
- Errors
- Total packets
- Broadcast packets
- Multicast packets
- Unicast packets
- ICMP (Ping) packets
- TCP SYNC (Session Start) packets
- Packet size 64-byte packets
- Packet size 65-byte to 127-byte packets
- Packet size 128-byte to 255-byte packets
- Packet size 256-byte to 511-byte 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.



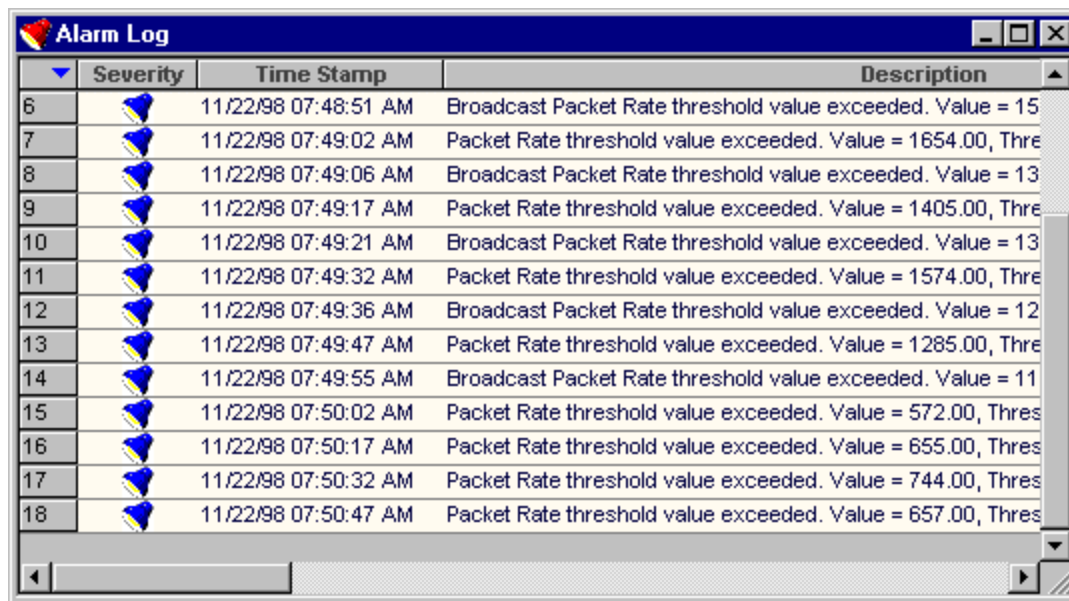
In this second example for the utilization table, a red bar appears across the 10% marker. The red bar indicates the threshold level that was specified for an alarm event.



## Alarm Log

If a "Rate" being monitoring from the Statistics Task Panel exceeds 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 logged events, or the Alarm Log window will be automatically launched once there is an event to report during runtime. Color scheme of the alarm is described below:

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



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

A popup menu will be shown as below if you click the right mouse button in the Alarm Log window. You can delete 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

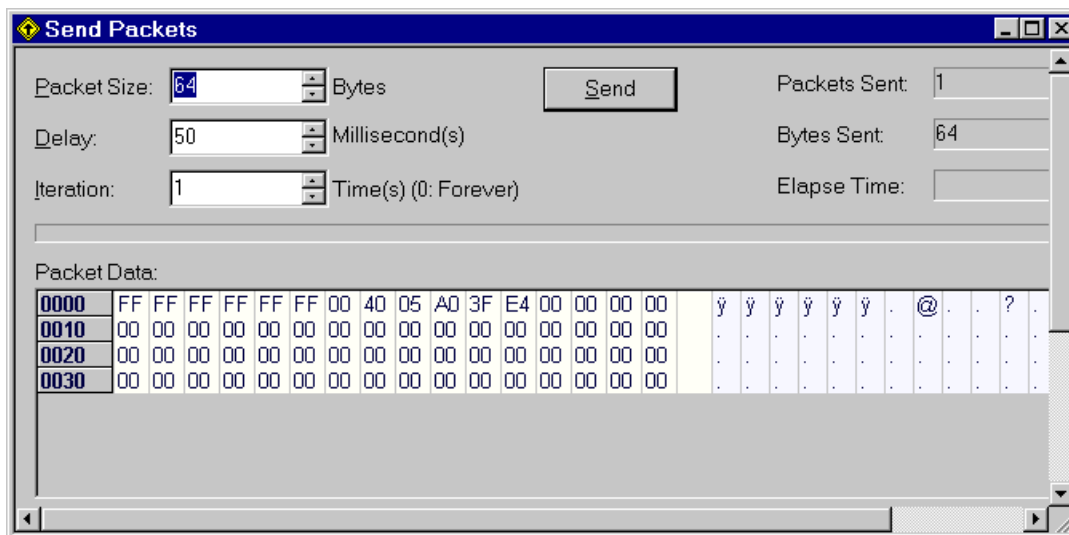
Alarm Log captures and records successful and failed FTP logins - except logins with the user name "anonymous." POP3 logins are recorded in the Alarm Log window as well. Destination (IP address or site name), source (IP address or site name) and user name of each FTP/POP3 transaction are displayed in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

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

## Chapter 7: Traffic Generator

### *Sending Packet from the Packet Sends window*

Click 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 and 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.



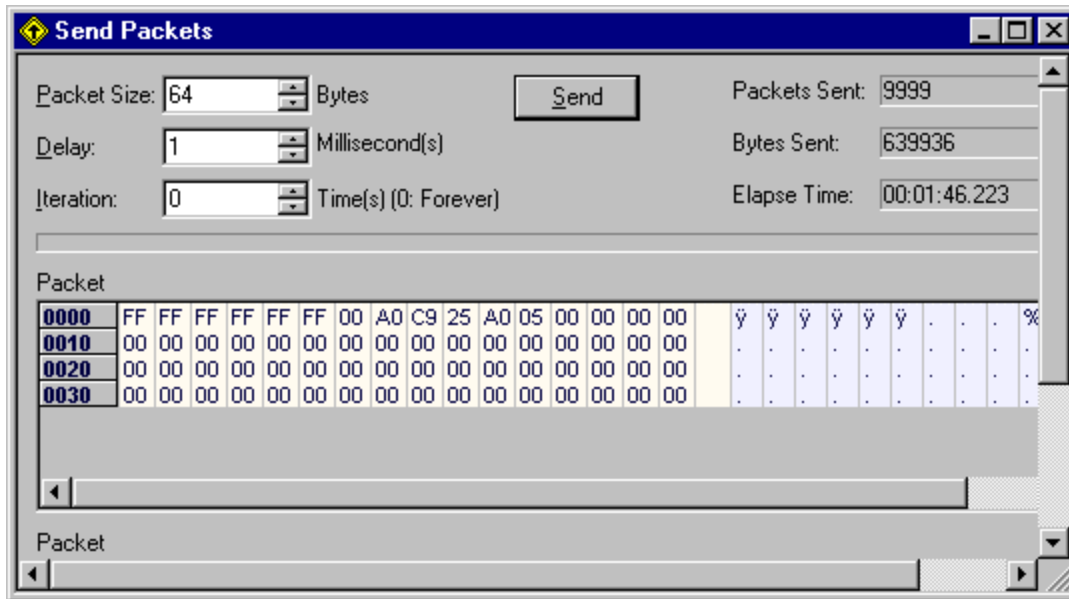
### *Sending Packets from the Packet Capture window*

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.



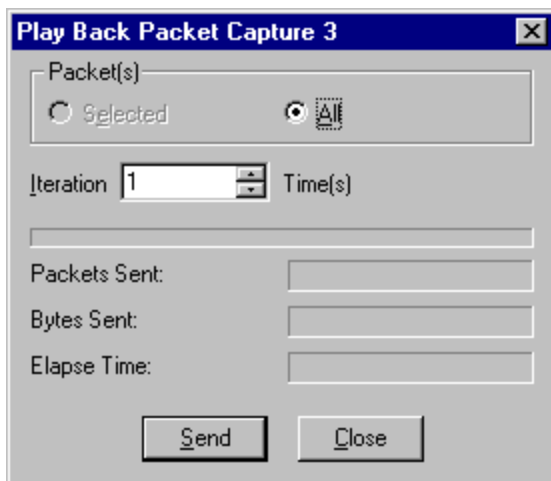
### Send Packet Option

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 mentioned in the previous section.



### Play Back Option

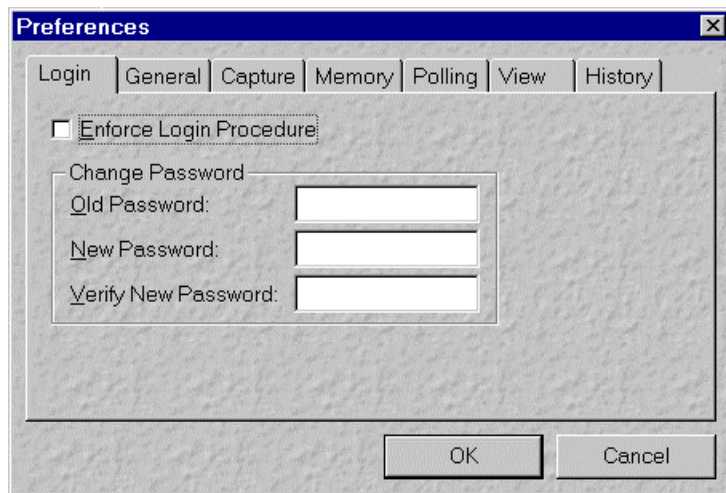
The Play Back option sends packets back to the network without editing the packet content. User can send multiple selected or all packets in the capture buffer from the Packet Capture window back to the network and with as many iterations as you wish.



## Chapter 8: Settings

### *Enforcing Login Procedure*

Click the "Preferences" menu item of the Settings 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 in to LanExplorer.



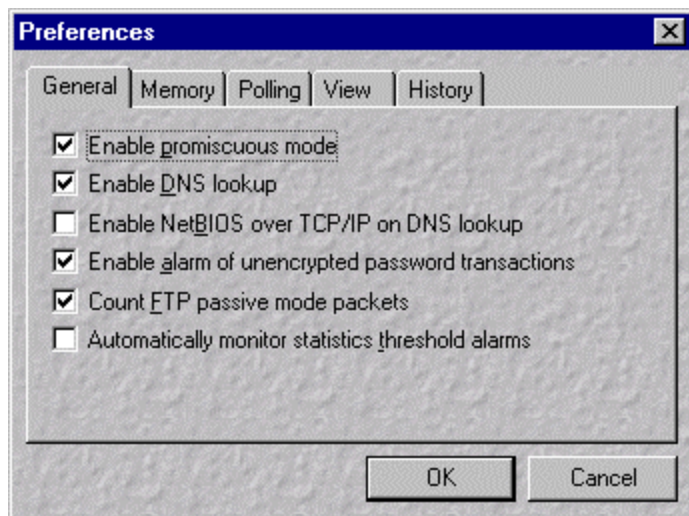
Follow these steps to change the password:

1. Check the Enforce Login Procedure check box.
2. Enter the Old Password or leave it blank if it was not set before.
3. Enter the New password.
4. 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 packets sent to this station will be captured. When 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

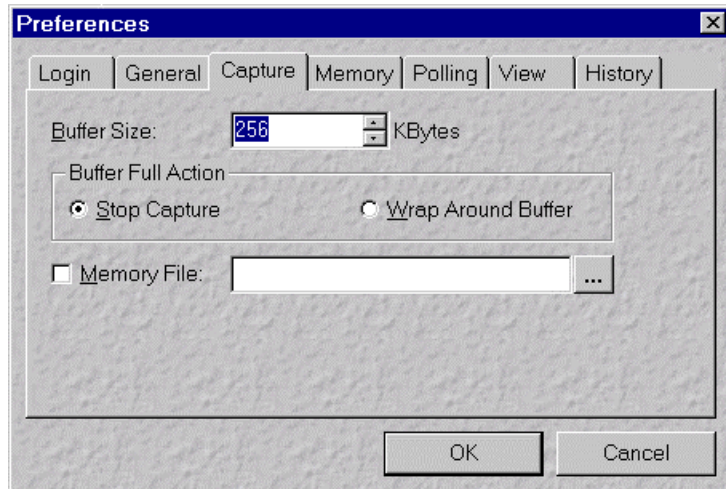
FTP Passive Mode packets will not count as FTP packets if this option is not checked.

### 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

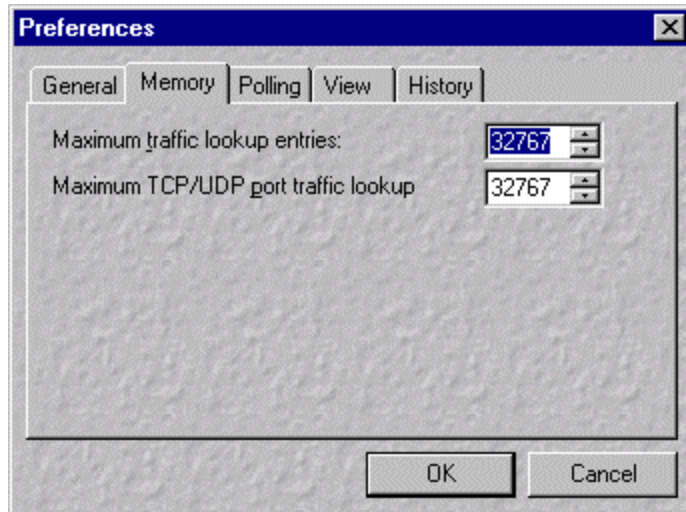
- **Stop Capture**  
The Packet Capture in-progress window will be stopped and packets captured will be listed when the capture buffer is full.
- **Wrap Around Buffer**  
The oldest packet in the buffer will be overridden by new captured packet when the capture buffer is full. The Packet Capture continues 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 that can be used for Traffic Matrix and Host Table display purpose.

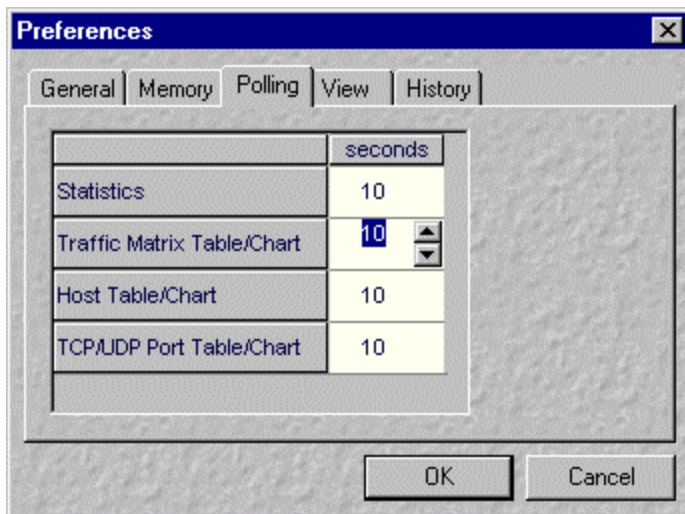
### **Maximum TCP/UDP port traffic lookup entries**

Maximum number of unique entries of Source and Destination Port that 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.

1. Press Backspace(s) to clear the value and type into a new value.
2. Use the Up arrow to increase the value.
3. 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**

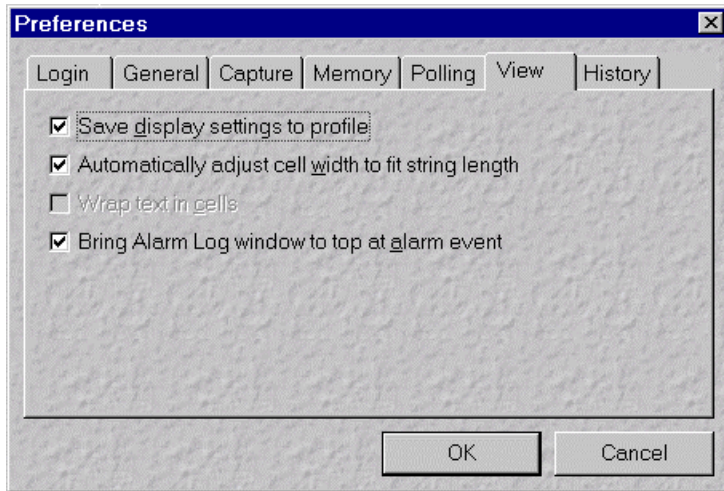
- TCP/UDP Port Table update.
- TCP/UDP Port Chart update.

*Tip: Increase the polling frequency to reduce processing requirements for screen updates. The minimum frequency is 10 seconds. Setting polling frequency at 300 seconds is recommended.*

*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

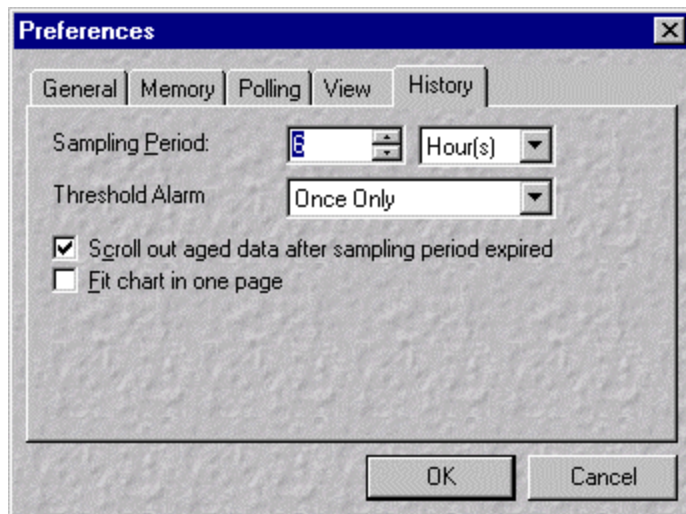
Cell width will be automatically adjusted to fit string length. If it is not checked, "Wrap text in cell" option can be checked to wrap text in cell.

### 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**

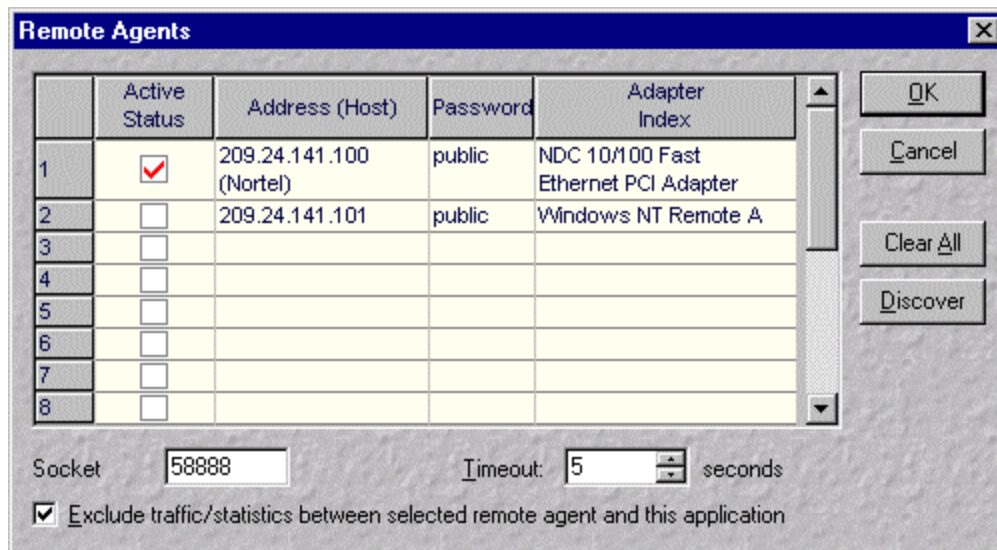
Stop the statistics history chart when sampling period has come to the end. Default is to continue log statistics history and drop the oldest statistics (scroll).

### **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 to overlap.

## 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.



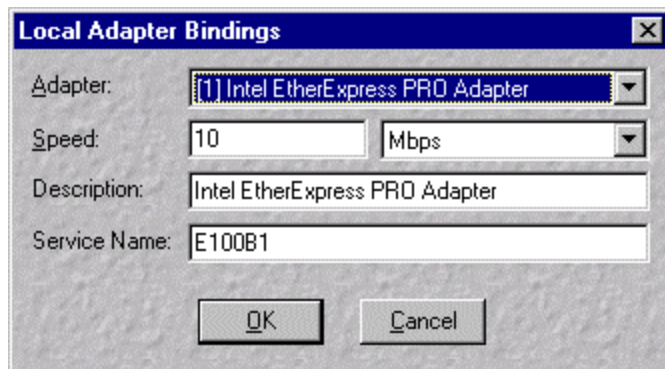
To connect to a Remote Agent, do the following steps:

- 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.

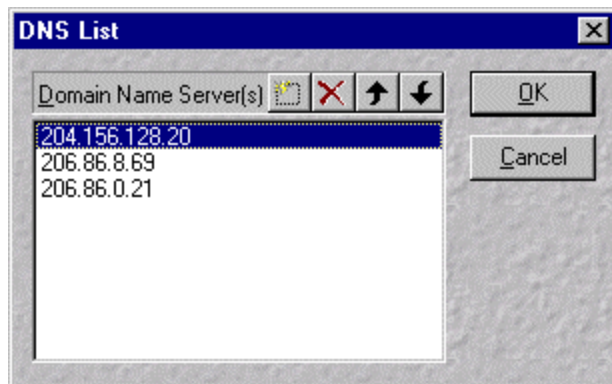
### **Setting Speed Option**

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*

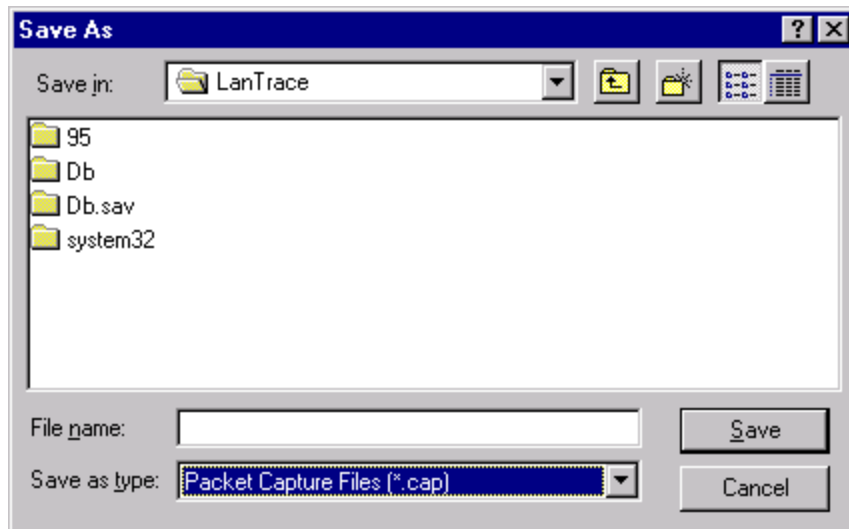
Click the "DNS" item of the Setting Menu to bring up the DNS List window. DNS Server is used to resolve the Internet name of an IP address. By default, LanExplorer uses the current system setting. However, user can add a new DNS Server or delete an existing DNS server.



## Chapter 9: Open or Save File

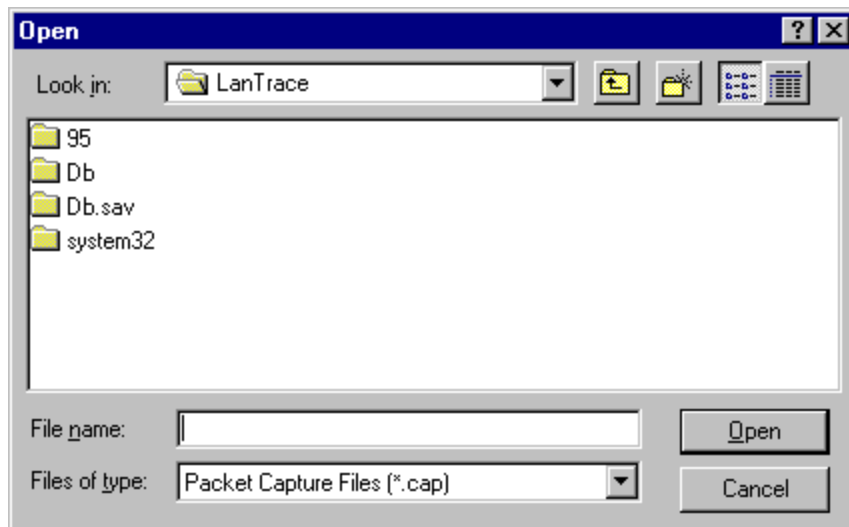
### *Saving to File*

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



### *Opening a File*

Click the "Open" 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.



## ***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.

<b>File Format</b>	<b>Available Window</b>
Tab Separated Value File (*.tsv)	<ul style="list-style-type: none"> <li>• Traffic Matrix Table</li> <li>• Host Table</li> <li>• TCP/UDP Port Table</li> <li>• Alarm Log</li> </ul>
Comma Separated Value File (*.csv)	<ul style="list-style-type: none"> <li>• Traffic Matrix Table</li> <li>• Host Table</li> <li>• TCP/UDP Port Table</li> <li>• Alarm Log</li> </ul>
JPEG File (*.jpg)	<ul style="list-style-type: none"> <li>• Traffic Matrix Table</li> <li>• Host Table</li> <li>• TCP/UDP Port Table</li> <li>• Alarm Log</li> <li>• Traffic Matrix Chart</li> <li>• Host Chart</li> <li>• TCP/UDP Port Chart</li> <li>• Any Statistics Chart</li> </ul>
Bitmap File (*.bmp)	<ul style="list-style-type: none"> <li>• Traffic Matrix Table</li> <li>• Host Table</li> <li>• TCP/UDP Port Table</li> <li>• Alarm Log</li> <li>• Traffic Matrix Chart</li> <li>• Host Chart</li> <li>• TCP/UDP Port Chart</li> <li>• Any Statistics Chart</li> </ul>
Windows Metafiles (*.wmf)	<ul style="list-style-type: none"> <li>• Traffic Matrix Chart</li> <li>• Host Chart</li> <li>• TCP/UDP Port Chart</li> <li>• Any Statistics Chart</li> </ul>

Saving a chart in one of the text formats - either Tab Separated Value File (\*.tsv) or Comma Separated Value File (\*.csv) - saves the underlying data statistics instead of the actual picture. This option is available on most of the charts.

## Chapter 10: Display Properties

### *Grid (Table) Window*

#### Examples of Grid Window












- Traffic Matrix Table
- Host Table
- TCP/UDP Port Table
- 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" item of the View Menu to view the grid window toolbar.

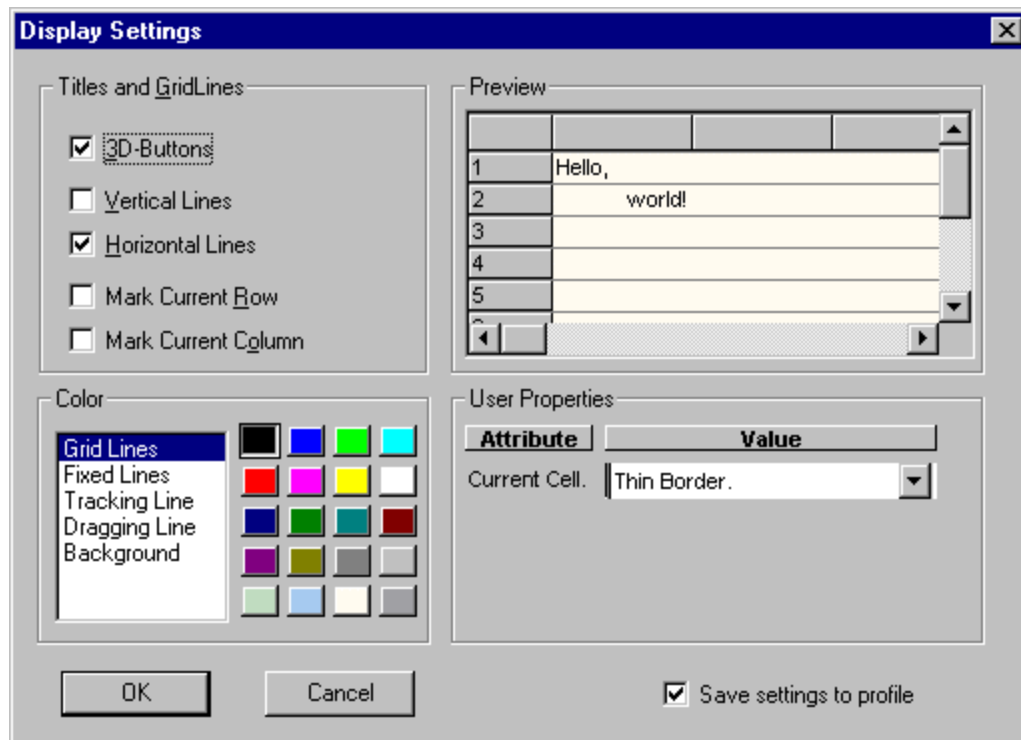
#### Grid Window Toolbar

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

## 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 item of the View menu to launch the Display Settings window.



## ***Chart Window***

### **Examples of Chart Window**

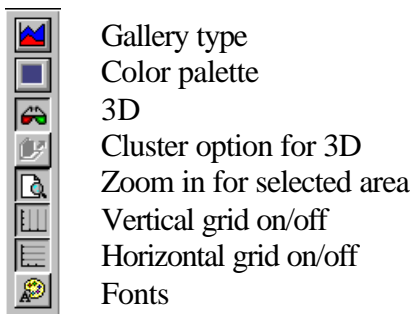
- Traffic Matrix Chart
- Host Chart
- TCP/UDP Port Chart
- Distribution Chart windows
- Rate Chart windows

### **Summary of Display Options**

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

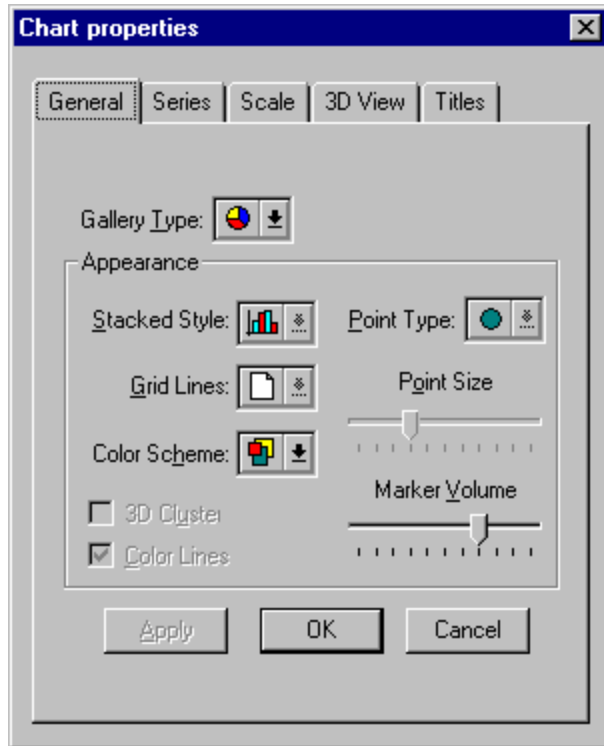
### **Chart Window Toolbar**

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.














### **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 item of the View menu to launch the Chart Properties window.

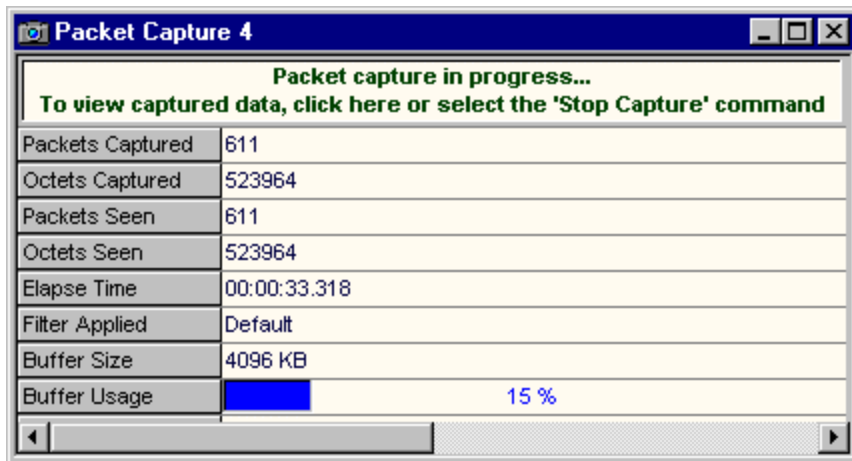


### Gallery Type

<i>Button</i>	<i>Type</i>	<i>Description</i>
	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.

## Quick Start: LanExplorer

### Network Protocol Analysis- Packet Capture and Protocol Decode



Capturing every data packet is 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 when a complex problem needs a 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 number of available packets - is 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).

**Packet Capture 2**

	Destination	Source	Protocol
318	www.intellimax.com	www.intellimax.com	Racal-Interlan
319	sanjose	dns2.noc.best.net	Domain Name Server
320	192.215.17.2	sanjose	World Wide Web HTTP
321	sanjose	192.215.17.2	World Wide Web HTTP
322	192.215.17.2	sanjose	World Wide Web HTTP
323	192.215.17.2	sanjose	World Wide Web HTTP
324	dns2.noc.best.net	209.24.141.131	Domain Name Server
325	209.24.141.131	dns2.noc.best.net	Domain Name Server
326	dns2.noc.best.net	209.24.141.131	Domain Name Server
327	209.24.141.131	dns2.noc.best.net	Domain Name Server
328	209.24.141.131	slip-129-37-101-134.ri.br.ibm.net	TCP
329	slip-129-37-101-134.ri.br.ibm.net	209.24.141.131	TCP
330	dns2.noc.best.net	209.24.141.131	Domain Name Server
331	209.24.141.131	202.180.58.int.ad.com	TCP

Default 6652 None 6652

**Protocol Decode - Capture 2:Packet 317**

```

0000 00 00 93 0C 2D 64 00 A0 C9 25 A0 05 08 00 45 00  . . . . - d . . . % . . . .
0010 00 3D 35 15 00 00 80 11 D8 8B D1 18 8D 8B CE 56  . = 5 . . . . . . . . . .
0020 00 15 06 19 00 35 00 29 A0 C9 00 04 01 00 00 01  . . . . 5 . ) . . . . .
0030 00 00 00 00 00 00 03 77 77 77 07 74 65 63 68 77  . . . . . www . t e c
    
```

- 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**

Network monitoring is a simple way to read network performance at different levels. LanExplorer provides various charts and counters for understanding 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 are very useful features 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
- TCP Sync and ICMP Rate Counter
- Accumulated and Historical Statistics
- Threshold and Alarm

### 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 the network, the parties are two IP addresses. To receive information from the Internet, the local computer (1<sup>st</sup> party) normally sends out request packets and the Internet site (2<sup>nd</sup> party) 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 on the Traffic Matrix window.

In addition to the IP Traffic Matrix, a MAC Traffic Matrix is also available for viewing 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.

	Address 1	Address 2	Octets Ratio	Octets	Packets	UF
1	Intmax1	209.154.191.11	37 %	737933	935	
2	Intmax2	tntbrs11-237.abo.wanadoo.fr	29 %	572056	581	
3	Intmax2	dialup3.cb.cesnet.cz	26 %	519379	645	
4	Intmax1	195.235.120.61	7 %	139906	346	
5	209.24.141.135	Nortel	1 %	21792	132	
6	epic8.Stanford.EDU	Santaclara	0 %	6634	94	
7	news1.best.com	Santaclara	0 %	1374	13	
8	Intmax1	Intmax3	0 %	560	7	
9	Broadcast	Jacob Hsu	0 %	261	1	
10	dns1.noc.best.net	Santaclara	0 %	246	2	
11	alukacs3.albacomp.hu	Intmax2	0 %	120	2	

At the bottom of the window, there is a toolbar with icons for a calendar (11), a red flag (IP), a clock (60 sec.), a refresh icon, a document icon, a magnifying glass icon, a dropdown menu (None), a sort icon (Z↓), and a dropdown menu (URL Group).

## Identifying Network Nodes - Host Table, Host Chart and Address Book

To find active stations in the network and their traffic statistics, the Host Table and Host Chart display 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 in the Address Book is obtained from DNS query and NetBIOS name auto-discovery by LanExplorer.

	Address	Octets Ratio	Total Octets	Total Packets	URL G
1	Intmax2	28 %	1610183	1798	
2	Intmax1	21 %	1241922	1794	
3	209.154.191.11	19 %	1090029	1375	
4	tntbrs11-237.abo.wanadoo.fr	15 %	873190	885	
5	dialup3.cb.cesnet.cz	13 %	736873	911	
6	195.235.120.61	2 %	141736	350	
7	209.24.141.135	1 %	32688	198	
8	Nortel	1 %	32688	198	
9	Intmax3	0 %	10065	68	
10	Santaclara	0 %	8848	115	
11	epic8.Stanford.EDU	0 %	6634	94	
12	news1.best.com	0 %	1968	19	
13	Broadcast	0 %	721	6	
14	Jacob Hsu	0 %	261	1	

16 IP 60 sec. None Octets Ratio

## **Part II Remote Agent**

### **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.

#### ***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**

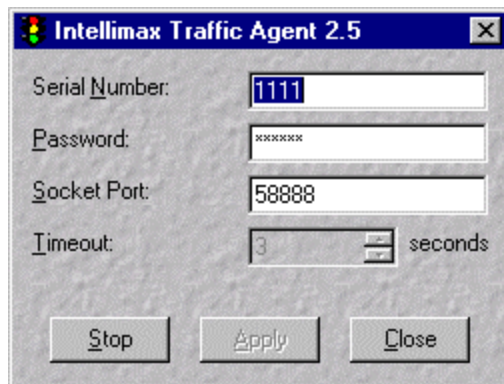
- Get a valid Serial Number emailing or calling Technical Support.
- Click the self-extracting file (e.g. AGENT.EXE).
- Follow the instructions to install the application.

## *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.

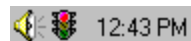


## *Minimizing or Closing Remote Agent on Desktop*

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. When the Stop button is available, the Remote Agent is currently started.

## ***Removing Remote Agent***

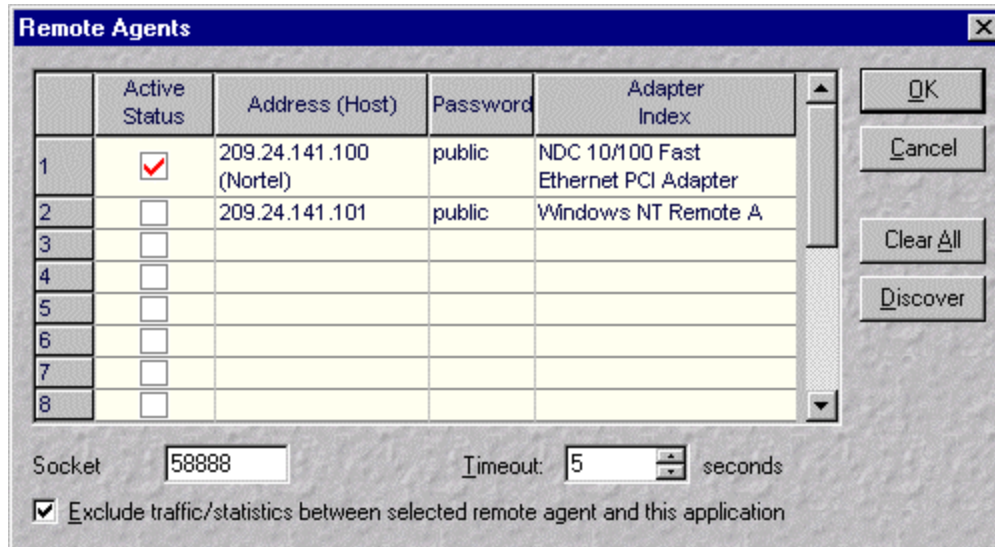
Do the following steps on the Desktop to remove the Remote Agent.

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

Follow additional uninstalling procedures for Windows NT 4.0 and Windows 2000, as described in Part I, *LanExplorer*, Chapter 2: Installing LanExplorer.

## Connecting to a remote Traffic Agent

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



To connect to a remote Traffic Agent, follow these steps:

- Enter the remote Traffic Agent IP address.
- Enter the remote Traffic Agent password (default is "public")
- Enter the remote Traffic Agent adapter index.
- Select Active Status.
- Click OK.

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

---

Address Book.....	37, 83	Installation	
Alarm.....	57	Install from a CD-ROM .....	12
Unencrypted Password Alarm.....	59	Installation from a downloaded file .....	12
Viewing Alarm Log.....	59	Post-Installation	
Console Panel.....	23	Intellimax 2000 Service- For Windows 2000	
Customer Support.....	9	only .....	15
Display Filters .....	32	Intellimax NT Service- For Windows NT only	
Address Filter.....	33	.....	14
Exclusive option.....	33	Winsock2 Component- For Windows 95 only .	12
Inclusive option.....	33	Pre-installation .....	12
Protocol Filter .....	33	Intellimax 2000 Service- For Windows 2000	
Select All and Clear All .....	33	only .....	12
Setting up Profiles .....	32	Intellimax NT Service- For Windows NT only	
Display Properties .....	74	.....	12
Chart Properties.....	76	System Requirements .....	12
Chart Window.....	76	IP Traffic Matrix.....	82
Chart Window Toolbar.....	76	LanExplorer.....	11
Display Settings.....	75	Launching Traffic Matrix Table .....	24
Gallery Type .....	77	MAC Layer Statistics.....	53
Grid (Table) Window .....	74	MAC Traffic Matrix.....	82
Grid Window Toolbar .....	74	Memory Preferences .....	65
Display Settings.....	27	Menu Bar .....	18
DNS Server for Lookup .....	71	Capture Menu .....	18
File		Edit Menu .....	18
Open or Save .....	72	File Menu.....	18
File Format .....	73	Profiles Menu.....	19
Filter		Settings Menu .....	19
Address .....	45	Tools Menu .....	19
Layer 2 .....	42	View Menu.....	18
Layer 2 MAC.....	42	Window Menu .....	19
Layer 2 VLAN.....	42	Network Protocol Analysis .....	39
Layer 2/3.....	43	Network Statistics .....	52, 81
Layer 2/3 Ethernet.....	43	Chart Properties .....	56
Layer 2/3 LLC .....	43	Launching Accumulated or Historical Distribution	
Layer 2/3 LLC SNAP.....	43	.....	52
Layer 2/3 Raw.....	43	Monitoring MAC Layer Statistics .....	53
Layer 3+.....	44	Monitoring Packet Size Statistics .....	56
Layer 3+ IP/ARP .....	44	Monitoring Protocol Statistics .....	54
Layer 3+ TCP/UDP .....	44	Network Statistics	
Pattern Filter of Post-capture.....	47	Monitoring TCP/UDP Statistics .....	55
TCP/UDP.....	46	Network Traffic Monitoring - .....	81
Filter Profile .....	48	Node to Node Traffic .....	82
General Preferences .....	63	Open File .....	72
History Preferences .....	68	Packet Capture	
Host Chart .....	35, 83	Changing Options.....	64
Host Chart Options		Changing Packet Options	
Chart Properties .....	35	Buffer Full Action .....	64
Host Table.....	34, 83	Buffer Size .....	64
Host Table Options		Memory File .....	64
Cell Options .....	34	Options.....	50
Display Settings.....	34	Pre-capture or Post-capture Filter.....	42
Host Table Sorting .....	34	Starting and Stopping.....	39
Host Window Status Bar .....	35	Stop Trigger Options .....	51
Identifying Network Nodes .....	83	Trigger to Start.....	50
Installing LanExplorer		Trigger to Stop.....	51

---

Viewing Packet Contents.....	41	Enable NetBIOS over TCP/IP on DNS lookup	63
Packet Size Statistics.....	56	Enable promiscuous mode.....	63
Polling Frequencies.....	66	View Options.....	67
Protocol Statistics.....	54	Sorting Options.....	31, 35
Remote Agent.....	84	Starting LanExplorer.....	17
Choosing Adapter to Use.....	70	Statistics Task Panel.....	21
Configuring Remote Agent.....	86	Status Bar.....	20
Connecting to a Remote Agent from LanExplorer		TCP/UDP Statistics.....	55
.....	69	Threshold and Alarm.....	57
Connecting to a remote Traffic Agent from		Launching Rate Monitoring Windows.....	58
LanExplorer.....	87	Setting up Threshold.....	57
Installation.....	84	Toolbar.....	20
Minimizing or Closing Remote Agent on Desktop		Traffic Generator.....	60
.....	85	Play Back Option.....	61
Pre-installation.....	84	Send Packet Option.....	61
Removing Remote Agent.....	86	Sending Packet.....	60
Restarting Remote Agent.....	86	Traffic Generator- Send Packets and Playback	
Starting and Stopping Remote Agent.....	85	Captured Packets.....	80
System Requirements.....	84	Traffic Matrix Chart.....	28
Save File.....	72	Traffic Matrix Chart Options	
Sending Packets.....	60	Chart Properties.....	29
Settings.....	62	Traffic Matrix Sorting.....	26
Capturing Options.....	64	Traffic Matrix Status Bar.....	30
Changing History Preferences.....	68	Changing Polling Interval.....	30
Changing Memory Preferences.....	65	Changing Traffic Matrix Filter.....	31
Maximum TCP/UDP port traffic lookup entries		Toggle MAC Window and IP Window.....	30
.....	65	Toggle One-way and Two-way.....	30
Maximum Traffic lookup entries.....	65	Toggle Show-broadcast and No-broadcast.....	31
Changing Polling Frequencies.....	66	Traffic Matrix Table.....	24
Host Table/Chart.....	66	Traffic Matrix Table Options	
Statistics.....	66	Cell Options.....	25
TCP/UDP Port Table/Chart.....	66	Display Settings.....	27
Traffic Matrix Table/Chart.....	66	Sorting Options.....	26
Enforcing Login Procedure.....	62	Traffic Matrix Sorting.....	26
General Preferences.....	63	Traffic Monitoring.....	24
Automatically monitor statistics threshold alarm		Traffic Task Panel.....	21
.....	63	Uninstalling LanExplorer.....	16
Count FTP passive mode packets.....	63	Uninstalling Intellimax 2000 Service – Additional	
Enable alarm of unencrypted password		Procedure for Windows 2000 only.....	16
transactions.....	63	Uninstalling Intellimax NT Service – Additional	
Enable DNS Lookup.....	63	Procedure for Windows NT only.....	16