Etherman Version 1.2

A Network Manager's Workbench Application

Gary Ratterree • Udo Pooch, Ph.D., P.E. • Willis Marti
(garyr@cs.tamu.edu, pooch@cs.tamu.edu, willis@cs.tamu.edu)
Version 1.1a by Curtin University

April 1995

Abstract. *The Network Manager's Workbench is a set of tools that addresses many different aspects of network management. The Netman tools are a set of network monitoring and packet analysis tools that are one component of the Network Manager's Workbench. Etherman is one of three tools in the Netman tool set. Etherman provides a real time graphical display of network traffic on an Ethernet network. Etherman color codes network connections to show the dominant protocol that is being used. The amount of traffic between hosts is shown in Etherman by changing the size of the lines connecting hosts. This document is a comprehensive user's guide covering the capabilities and use of the Etherman network monitoring tool.*

Key Words. Network Monitoring, TCP/IP, Network Management, Ethernet.

1.0 General Disclaimer

This program bears a copyright notice to prevent rights from being claimed by any other party. Texas A&M University intends that the executable version of this program be placed into the public domain and grants permission for its restricted use and distribution, provided that:

1) the source code, when provided, is distributed without changes (source code distribution is limited under agreement from Curtin University and is not in the public domain),
2) this copyright notice is retained in all copies of the source code, and
3) the program is distributed free of charge, and is not sold without written approval from Texas A&M University -- Department of Computer Science and Curtin University.

The program is distributed "as is". TEXAS A&M UNIVERSITY DOES NOT WARRANT THAT THE OPERATION OF THE PROGRAM WILL BE UNINTERRUPTED OR ERROR-FREE, AND MAKES NO REPRESENTATIONS OR OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. WE ARE NOT RESPONSIBLE AND CANNOT BE HELD LIABLE FOR DAMAGE CAUSED TO NETWORK SERVERS OR TO NETWORKS BY THIS PRODUCT. No support service will be provided unless special arrangements have been made to do so. Certain manufacturers and trade names are mentioned in this code for the purpose of describing their communications protocol. Such reference does not constitute an endorsement or recommendation of such equipment, but is provided for informational purposes only.

Earlier versions of Etherman are Copyright 1993 by Curtin University. The source code for any version of Etherman (including this version) may not be distributed without written permission from Curtin University.

2.0 Table Of Contents

3.0 List of Figures

4.0 History of Etherman

The Etherman application was originally developed at Curtin University. Version 1.2 was developed at Texas A&M University. Etherman is a passive network monitoring tool that monitors all types of packets on an Ethernet network. Packet types are coded by color and traffic density is shown by line thickness for easy observation of network activity.

4.1 Version 1.1a

Etherman Version 1.1 was developed in 1991 at Curtin University by George Benko, Mike Schulze, and Craig Farrell as part of the *Netman* project. This version was created for *Irix 4.x*, *Ultrix 4.x* and *SunOS* 4.x, and *Solaris 2.x*.

4.2 Version 1.2

Version 1.2 was developed at Texas A&M University by Gary Ratterree, Udo Pooch, Ph.D., P.E., and Willis Marti. This version includes several modifications to the user interface to make the program easier to use. Command line parameters were added to the program to allow it to be used from shell scripts and other automated programs. A secure mode of operation has also been added, allowing the program to be used for classroom instruction without compromising the security of the network. Version 1.2 runs under *Irix 4.x*, *SunOS* 4.x, *Ultrix 4.x*, and *Solaris* 2.x. A launch application for Etherman written in Tcl/Tk is also provided with the version 1.2 distribution.

5.0 Using Etherman

5.1 Requirements for Use

Version 1.2 of Etherman requires a X11R4 or higher installation on one of the following operating systems: *Irix 4.x*, *SunOS 4.1.x*, *Ultrix 4.x*, and *Solaris 2.x*. Etherman will not function on workstations with network devices that do not support a promiscuous capture mode. On all systems but *Ultrix*, the program must be run either by root or be Set User ID root in order to capture packets in promiscuous mode. In *Ultrix*, the root user may give other users promiscuous mode access to the network device. Users without permission to access the network device in promiscuous mode will not be able to run Etherman. When the program is run Set User ID root by another user, it automatically enters a secure operating mode. Secure mode censors incoming data and restricts certain operations to prevent sensitive material from being revealed to non-privileged users. Only the root user can use Etherman in its non-secure mode, all other users are restricted to secure mode. All program functions are available to the root user in the non-secure mode of operation.

Etherman places the workstation's network device in promiscuous mode and uses it to monitor all traffic on the network. This can place a heavy processing load on the workstation. For this reason, Etherman should not be run on multi-user machines or machines that are being used as servers. If Etherman is run on such a machine, it will cause an unacceptable loss in performance to other users. Excessive loads or a slow machine can cause Etherman to lose or "drop" packets. This packet dropping can cause problems with the accuracy of the network monitoring. Etherman may not be able to provide a warning when this occurs. The ideal environment for Etherman is a fast, dedicated workstation.

Etherman requires a special set of X-Windows fonts from the Hershey font library for its display. This font library must be present in the same directory as the Etherman executable. These fonts are included with the Etherman binary distribution.

5.2 Starting Etherman

Start Etherman by executing the command `etherman` at the command prompt. Be sure to set the X-Windows DISPLAY environment variable, if necessary, before running Etherman. Etherman will not run on remote X-Windows displays in secure mode. Only the root user may run Etherman remotely. Etherman supports a large number of command line options that can be set at startup. These options are described in the next section. All of these options (except -I) can also be changed from menus after Etherman is started. Etherman requires one configuration file in order to execute correctly. The `manf.codes` configuration file must be in the current directory or the environment variable ETHERMAN_HOME must be set to this file's current location before Etherman can be started.

A Tcl/Tk launch script is also provided with Etherman to start the program. The Tcl/Tk launch script is started by typing the command `netman` at the command prompt. This script provides a convenient graphical user interface (GUI) that allows the user to set many of Etherman's command line options. It is not necessary to use this script to launch Etherman; however, it provides a convenient way to set many options.

5.2.1 Command Line Switches

Etherman supports a wide variety of options that can be used to customize the operation of the program. For convenient use of Etherman from a shell script or other automated programs, a large number of command line switches are provided to set these options before launching Etherman. All of these options except -I can be changed from the internal menus once Etherman is started.

Because several of the command line switches operate functions that can violate system security; their use is restricted in secure mode. The following figure summarizes the command line switches that are available in secure mode (all functions are available to root users running in non-secure mode):

Command Line Switch	Available in Secure Mode?
-I interface	yes
-L link layer filter	yes
-E ethernet frame #	yes
-N network filter	yes
-A application filter	yes
-U port #	yes
-P port #	yes
-H and -?	yes

Figure 5.2.1.1. Command Line Switches Available in Secure Mode.

5.2.1.1 -I interface

Specify the hardware network interface (le0, etc.) that Etherman will use to capture packets. This command line switch allows the user to override Etherman's default choice of the hardware network interface to open for promiscuous mode packet capture. Etherman will attempt to open the first Ethernet interface by default. In most environments this will be sufficient; however, this override is provided for special situations. The network interface selection is the only command line switch that cannot be changed once the program has started. The following figure lists the default choices:

Operating System	Default Interface
SunOS 4.x and Solaris 2.x	le0
Ultrix 4.x	ln0
Irix 4.x	ec0
BSD Packet Filter (if available)	bpf0

Figure 5.2.1.1.1. Default Packet Filter Choice.

The interface that is selected with this command line switch must be able to handle promiscuous mode packet captures. Interfaces that do not support promiscuous mode packet capturing are not supported in this version of Etherman. Etherman will not start unless it can open the interface in promiscuous capture mode.

The -I command line switch may be used in secure mode; however, Etherman must have permission to use the specified interface in promiscuous capture mode.

5.2.1.2 -L link layer filter

Specify a data link layer packet filter. This command line switch allows the user to select one of Etherman's built in link layer packet filters. Only one of these filters may be selected at a time. All packets that do not match the filter are rejected by Etherman. The filter is specified by typing its code after the -L. Enter the codes in uppercase exactly as shown in the list.

Filter Code	Type of Packet Accepted by Filter
IP	IP (ARPA TCP/IP) Packets only
DEC	DECNet Packets only
LAT	LAT Packets only
ICMP	ICMP (ARPA TCP/IP) Packets only
APPLE	AppleTalk Packets only
IPX	Novell (SPX/IPX) Packets only

Figure 5.2.1.2.1. Link Layer Filters.

The following example sets Etherman to only capture AppleTalk packets:

```
etherman –L APPLE
```

5.2.1.3 -E ethernet frame #

Specify a custom Ethernet frame filter. This command line switch allows the user to filter for specific Ethernet frame types. Several common frame types are provided as link layer filters (see section 5.2.1.2). This switch allows the user to capture packets not selected by the provided filter set. Figure 5.2.1.3.1 shows a partial list of common Ethernet frame numbers [1]. The frame ID number must be specified in base 10. Only one custom frame filter may be entered at a time. The following example show how to set Etherman to capture only Ethernet packets with a frame type of 2048 (Ethernet frame type 2048 selects only ARPA IP packets):

```
Etherman –E 2048
```

Decimal Frame Number	Description
000	IEEE802.3 Length Field
257	Experimental
2048	DOD IP (ARPA TCP/IP)
2049	X.75 Internet
2050	NBS Internet
2051	ECMA Internet
2052	Chaosnet
2053	X.25 Level 3
2054	ARP
24580	DEC LAT
32788	SGI network games
32821	Reverse ARP
32923	AppleTalk
33079	Novell, Inc.

Figure 5.2.1.3.1. Ethernet Frame Types.

5.2.1.4 -N network filter

Specify a network level packet filter. This command line switch allows the user to select one of Etherman's built in network layer packet filters. Only one of these filters may be selected at a time. All packets that do not match the filter are rejected by Etherman. The filter is specified by typing its code after the -N. Enter the codes in uppercase exactly as shown in the list.

Filter Code	Type of Packet Accepted by Filter
TCP	TCP (TCP/IP) Packets only
UDP	UDP (UDP/IP) Packets only

Figure 5.2.1.4.1. Network Layer Filters.

The following example shows how to set Etherman to capture only TCP packets:

```
etherman -N TCP
```

5.2.1.5 -A application filter

Specify an application level packet filter. This command line switch allows the user to select one of Etherman's built in application layer packet filters (not all of these application filters are in the OSI Application layer; however, they are grouped here for convenience). Only one of these filters may be selected at a time. All packets that do not match the filter are rejected by Etherman. The filter is specified by typing its code after the -A. Enter the codes in uppercase exactly as shown in the list.

Filter Code	Type of Packets Accepted by Filter
FTP	FTP Packets (FTP/TCP/IP) only
TELNET	Telnet Packets (Telnet/TCP/IP) only
TRPC	TCP Sun Remote Procedure Call Packets only
URPC	UDP Sun Remote Procedure Call Packets only
FINGER	Finger Packets (Finger/TCP/IP) only
NNTP	News Packets (News/TCP/IP) only
SMTP	Mail Packets (Mail/TCP/IP) only
X400	OSI X400 Packets (X400/TCP/IP) only
LPD	Line Printer Daemon Packets (LPD/TCP/IP) only

NFS	Network File System Packets (NFS/UDP/IP) only
DNS	Domain Name Service Packets (DNS/UDP/IP) only
TFTP	Trivial FTP Packets (TFTP/UDP/IP) only
RWHO	Remote Who Packets (RWHO/UDP/IP) only
SYSLOG	Syslogd Packets (SYSLOGD/UDP/IP) only
TALK	Talk Packets (TALK/UDP/IP) only
NTALK	NTalk Packets (NTALK/UDP/IP) only
WWW	World Wide Web Packets (WWW/TCP/IP) only
GOPHER	Gopher Packets (Gopher/TCP/IP) only

Figure 5.2.1.5.1. Application Layer Filters.

The following example sets Etherman to capture only telnet packets:

```
etherman –A TELNET
```

5.2.1.6 -U port #

Specify a custom UDP port number. This command line switch is used to filter for packets based on a custom distinguished UDP port number. Figure 5.2.1.6.1 gives a partial listing of common UDP port numbers [1]. Etherman looks at both the source and destination port of the packet to match it to a port filter. If either the source or destination port matches the filter number, the packet is allowed through. Usually, only one port will match a filter. If both ports match a filter, Etherman will still allow the packet through, but it may not be decoded correctly. The following example sets Etherman to filter for UDP port 2049 (port 2049 is used by the NFS protocol):

```
etherman –U 2049
```

UDP Port Number	Description
0	Reserved
1	TCP Port Service Multiplexer
2	Management Utility
3	Compression Process
5	Remote Job Entry

7	Echo
9	Discard
11	Active Users
13	Daytime
17	Quote of the day
53	Domain Name Service
69	Trivial FTP
123	Network Time Protocol
513	Who
517	Talk
518	NTalk
750	Kerberos
2049	Network File System

Figure 5.2.1.6.1. Common UDP Port Numbers.

5.2.1.7 -P port #

Specify a custom TCP port number. This command line switch is used to filter for packets based on a custom distinguished TCP port number. Figure 5.2.1.7.1 gives a partial listing of TCP port numbers [1]. Etherman looks at both the source and destination port to match a port filter. If either the source or destination port matches the filter number, the packet is allowed through. Usually, only one port will match a filter. If both ports match a filter, Etherman will still allow the packet through, but it may not be decoded correctly. The following example sets Etherman to filter for TCP port 23 (port 23 is used by the Telnet application):

```
etherman -P 23
```

TCP Port Number	Description
0	Reserved
21	File Transfer Protocol (FTP)
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)

43	Whois
53	Domain Name Service
79	Finger
110	Post Office Protocol Ver. 3 (POP)
113	User Authentication (identd)
513	Login
514	Shell
515	Printer

Figure 5.2.1.7.1. Common TCP Port Numbers.

5.2.1.8 -H and -?

Print Etherman options help. This command line switch prints a list of all available command line switches and a short summary of their use. This is useful to quickly look up the syntax of one of these switches. This switch prints the list of options and causes Etherman to exit, so it should not be used in combination with any other command line switches.

5.2.2 Etherman Launch Application

The Etherman launch utility is a Tcl/Tk script that allows the user to set Etherman's command line switches with a graphical user interface. Most of the command line options can be specified with this tool. To start the Etherman launch utility, type `netman` at the command line to start the Netman launch utility. The Netman launch application allows you to start any of the Netman tools (the launch programs for Interman, Etherman, and Packetman can be started from this utility). Figure 5.2.1.1 shows the Netman launch utility program.

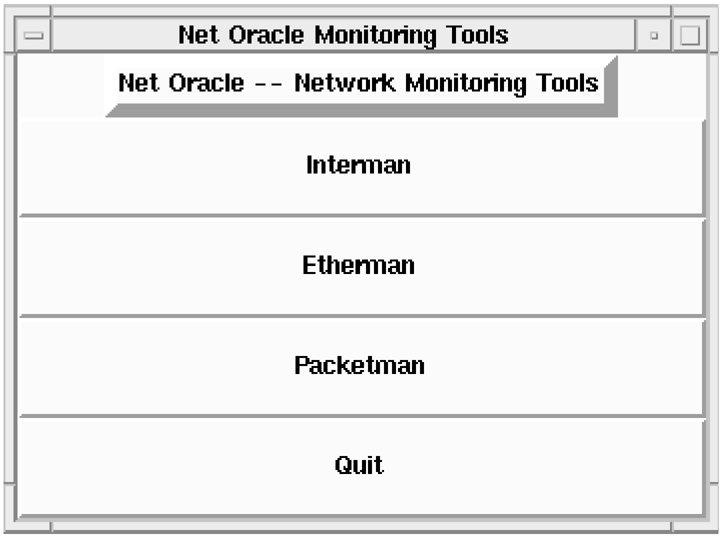


Figure 5.2.2.1. Netman Launch Utility.

Click on the Etherman button to start the Etherman launch utility. Figure 5.2.2.2 shows the Etherman launch utility user interface.

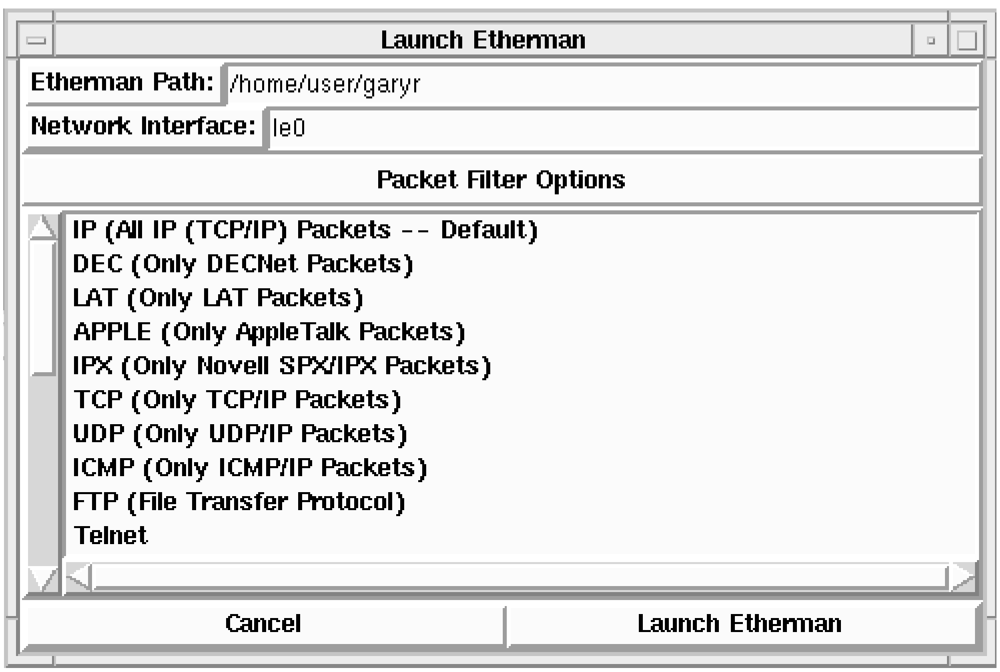


Figure 5.2.2.2. Etherman Launch Application.

5.2.2.1 Etherman Path

This field specifies the location of the Etherman executable file. The default location of this file should have been set by the site's system administrator; however, it can be changed with this setting.

5.2.2.2 Network Interface

This text box allows the user to override Etherman's choice of the workstation's network interface to open for promiscuous mode packet capture. Etherman will attempt to open the first Ethernet interface by default. In most environments this will be sufficient; however, this override is provided for special situations. The network interface selection is the only command line switch that cannot be changed once the program has started. The following figure lists the default choices:

Operating System	Default Interface
SunOS 4.x and Solaris 2.x	le0
Ultrix 4.x	ln0
Irix 4.x	ec0
BSD Packet Filter (if available)	bpf0

Figure 5.2.2.2.1. Default Packet Filter Choice.

The interface that is selected with this option must be able to handle promiscuous mode packet captures. Interfaces that do not support promiscuous mode are not supported in this version of Etherman. Etherman will not start if it cannot open the network interface in promiscuous mode.

This option may be used in secure mode; however, Etherman must have permission to use the specified interface in promiscuous capture mode.

5.2.2.3 Packet Filter Options

This list box allows the selection of one of the link layer, network layer, or application layer filters. In this version of the Etherman launch utility, there is a limit of one filter selection per session. Custom filter selections are not supported in this version of the launch utility.

5.2.2.4 Cancel

Pressing this button with the left mouse button will exit the Etherman launch utility without starting Etherman. All of the Etherman launch utilities' settings will be lost.

5.2.2.5 Launch Etherman

Pressing this button with the left mouse button will create a set of command line switches corresponding to the selections in the launch utility and start Etherman with them. The Etherman launch utility will automatically exit when Etherman is started.

5.3 The Etherman Menu

The Etherman main menu is located along the top of the program's main window. Some menu items operate as simple buttons. These choices are activated by clicking on them with the left mouse button. Other menu items have sub-menus under them. Access the sub-menus by pressing and holding the left mouse button over the menu button on the screen. Move the mouse to the menu item to be selected and release the left button. Figure 5.3.2 shows the Etherman menu bar.

Figure 5.3.1. Etherman Menu Bar.

Because several of the menu items activate operations that might violate system security, their operation is restricted in secure mode. The following figure summarizes the operations that are available in secure mode (all operations are available to the root user when running in non-secure mode):

Menu Item	Available in Secure Mode?
Quit	yes
Filter	yes
Traffic	yes
Misc	yes

Hosts	yes
Statistics	yes

Figure 5.3.2. Menu Items Available in Secure Mode.

5.3.1 Quit

Single clicking on this menu item with the left mouse button will cause Etherman to exit immediately. All of the statistical information that has been gathered will be lost. Use the Protocol Summary menu item to save this information before exiting. A Postscript dump of the screen may be printed before exiting to save the information on the network display.

5.3.2 Filter

Pressing and holding the left mouse button on the filter menu button will drop down a sub-menu of filter choices. Only one of the filters under this menu should be selected at a time. Always select the All menu item to clear the current filter selection before selecting another packet filter. Some filters may work together, but the results of other filter selections may be unpredictable (or lead to a situation where no packets can meet the filter criteria). Selecting the All menu item will always clear all of the packet filters. A check mark will appear on the menu next to each selected filter to show which filters are active.

5.3.2.1 All

Selecting the All filter menu item will clear all of the currently selected filters and allow all types of packets to be captured. This menu item will also clear any custom filters that have been set. The All menu item may be selected when there are no active filters.

5.3.2.2 IP

Selecting the IP filter menu item will only allow Internet Protocol (IP from the ARPA TCP/IP set of protocols) packets to be captured.

5.3.2.3 DecNet

Selecting the DecNet filter menu item will only allow DecNet packets to be captured.

5.3.2.4 LAT

Selecting the LAT filter menu item will only allow Digital Local Area Transport packets to be captured.

5.3.2.5 AppleTalk

Selecting the AppleTalk filter menu item will only allow Apple AppleTalk packets to be captured.

5.3.2.6 Novell

Selecting the Novell filter menu item will only allow Novell Netware (SPX/IPX) packets to be captured.

5.3.2.7 ICMP

Selecting the ICMP filter menu item will only allow Internet Control Message Protocol (ICMP from the ARPA TCP/IP set of protocols) packets to be captured.

5.3.2.8 UDP

Selecting the UDP filter menu item with the left mouse button will show a sub-menu of filters that only allow certain types of User Datagram Protocol (UDP from the ARPA TCP/IP set of protocols) packets to be captured.

5.3.2.8.1 All UDP

Selecting the All UDP filter menu item will allow all types of User Datagram Protocol (UDP from the ARPA TCP/IP set of protocols) packets to be captured. All other packets that are not based on the UDP protocol will be rejected.

5.3.2.8.2 NFS

Selecting the NFS filter menu item will only allow Network File System (NFS/UDP/IP) packets to be captured. This also selects UDP and IP filtering.

5.3.2.8.3 DNS

Selecting the DNS filter menu item will only allow Domain Name System (DNS/UDP/IP) packets to be captured. This also selects UDP and IP filtering.

5.3.2.8.4 Sun RPC

Selecting the Sun RPC filter menu item will only allow UDP based Sun Remote Procedure Call (Sun RPC/UDP/IP) packets to be captured. This also selects UDP and IP filtering.

5.3.2.8.5 tftp

Selecting the tftp filter menu item will only allow trivial file transfer protocol (tftp/UDP/IP) packets to be captured. This also selects UDP and IP filtering.

5.3.2.8.6 rwho

Selecting the rwho filter menu item will only allow remote who (rwho/UDP/IP) packets to be captured. This also selects UDP and IP filtering.

5.3.2.8.7 syslog

Selecting the syslog filter menu item will only allow system logging (syslog/UDP/IP) packets to be captured. This also selects UDP and IP filtering.

5.3.2.8.8 talk

Selecting the talk filter menu item will only allow talk (talk/UDP/IP) packets to be captured. This also selects UDP and IP filtering.

5.3.2.8.9 ntalk

Selecting the ntalk filter menu item will only allow ntalk (ntalk/UDP/IP) packets to be captured. This also selects UDP and IP filtering.

5.3.2.8.10 Custom UDP Port

The Custom UDP port menu item allows the user to create a custom UDP port filter. Selecting this menu item causes a dialog box to appear as shown in Figure 5.3.2.8.9.1. A base 10 number should be entered in this dialog box to indicate the port to be used as the filter criteria.

Only one custom port filter may be set at a time. This filter also selects UDP and IP filtering. Figure 5.2.1.6.1 gives a list of custom UDP ports for many common applications.

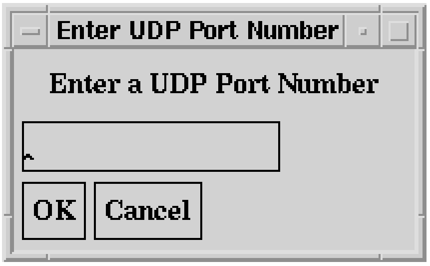


Figure 5.3.2.8.9.1. Enter UDP Port Number.

The Custom UDP filter will capture any UDP/IP based packet that has either the same source or destination port number as the custom filter port number. Usually only one of the ports will match a filter, so this approach is fairly efficient. Under some circumstances, the system may not properly decode a packet if more than one UDP port filter is selected at a time.

5.3.2.9 TCP

Selecting the TCP filter menu item with the left mouse button will show a sub-menu of filters that only allow only certain types of Transmission Control Protocol (TCP from the ARPA TCP/IP set of protocols) packets to be captured.

5.3.2.9.1 All TCP

Selecting the All TCP filter menu item will allow all types of Transmission Control Protocol (TCP from the ARPA TCP/IP set of protocols) packets to be captured. All other packets that are not based on the TCP protocol will be rejected.

5.3.2.9.2 FTP

Selecting the FTP filter menu item will only allow File Transfer Protocol (FTP/TCP/IP) packets to be captured. This also selects TCP and IP filtering.

5.3.2.9.3 telnet

Selecting the telnet filter menu item will only allow telnet protocol (telnet/TCP/IP) packets to be captured. This also selects TCP and IP filtering.

5.3.2.9.4 Sun RPC

Selecting the Sun RPC filter menu item will only allow Sun Remote Procedure Call (Sun RPC/TCP/IP) packets that are using TCP to be captured. This also selects TCP and IP filtering.

5.3.2.9.5 finger

Selecting the finger filter menu item will only allow finger protocol (finger/TCP/IP) packets to be captured. This also selects TCP and IP filtering.

5.3.2.9.6 NNTP

Selecting the NNTP filter menu item will only allow Network News Transport Protocol (NNTP/TCP/IP) packets to be captured. This also selects TCP and IP filtering.

5.3.2.9.7 SMTP

Selecting the SMTP filter menu item will only allow Simple Mail Transfer Protocol (SMTP/TCP/IP) packets to be captured. This also selects TCP and IP filtering.

5.3.2.9.8 X400

Selecting the X400 filter menu item will only allow OSI X400 (X400/TCP/IP) packets to be captured. This also selects TCP and IP filtering.

5.3.2.9.9 lpd

Selecting the lpd filter menu item will only allow Line Printer Daemon (lpd/TCP/IP) packets to be captured. This also selects TCP and IP filtering.

5.3.2.9.10 WWW

Selecting the WWW filter menu item will only allow World Wide Web (WWW/TCP/IP) packets to be captured. This also selects TCP and IP filtering.

5.3.2.9.11 gopher

Selecting the gopher filter menu item will only allow Gopher (gopher/TCP/IP) packets to be captured. This also selects TCP and IP filtering.

5.3.2.9.12 Custom TCP Port

The Custom TCP port menu item allows the user to create a custom TCP port filter. Selecting this menu item causes a dialog box to appear as seen in Figure 5.3.2.9.10.1. Enter a base 10 number in this dialog box for the TCP port to filter on. Only one custom port filter may be set at a time. This filter also selects TCP and IP filtering. Figure 5.2.1.7.1 gives a list of TCP port numbers for many common applications.

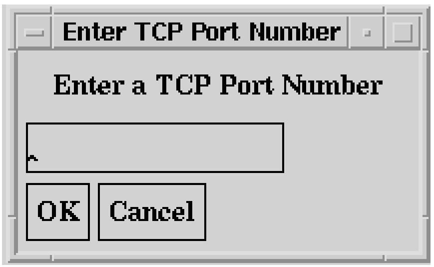


Figure 5.3.2.9.10.1. Enter TCP Port Number.

The Custom TCP filter will pass any TCP/IP packet that has either the same source or destination port number as the custom filter port number. Usually only one of the ports will match a filter, so this approach is fairly efficient. Under some circumstances, the system may not properly decode a packet if more than one custom TCP filter is selected at a time.

5.3.2.10 Custom

The Custom filter menu item allows the user to create a filter for any Ethernet frame type. Selecting this menu item with the left mouse button will display the Custom Frame ID dialog box as shown in Figure 5.3.2.10.1. Enter the custom Ethernet frame number in this dialog box in base 10. Figure 5.2.1.3.1 gives a list of common Ethernet frame types. Only one custom filter may be entered at a time. Use the All filter menu item to clear the current custom filter before creating another one.

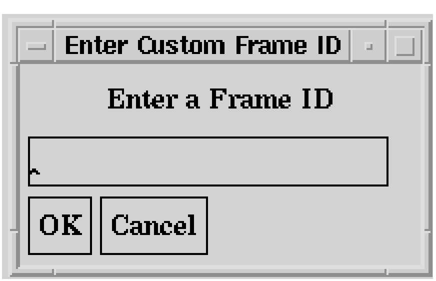


Figure 5.3.2.10.1. Enter Custom Frame ID.

5.3.3 Traffic

Pressing and holding the left mouse button on the Traffic menu will display the Traffic sub-menu. This menu allows the user to change the way Etherman displays traffic on the network.

5.3.3.1 Packets

The Packets menu item toggles the display to show network traffic as the number of packets that are being transmitted between hosts. Etherman will increase the size of the links and hosts on the screen based on the number of packets that are being transmitted. A check mark will appear next to this menu item when it is selected. Selecting this menu item will automatically turn off (uncheck) the Bytes menu item.

5.3.3.2 Bytes

The Bytes menu item toggles the display to show network traffic as the number of bytes that are being transmitted between hosts. Etherman will increase the size of the links and hosts on the screen based on the number of bytes that are being transmitted. A check mark will appear next to this menu item when it is selected. Selecting this menu item will automatically turn off (uncheck) the Packets menu item.

5.3.4 Misc

Pressing and holding the left mouse button on the Misc menu button will display the miscellaneous functions sub-menu. This sub-menu has options for several different types of actions that are not related.

5.3.4.1 Postscript Dump

The Postscript Dump menu item will save a snapshot of the current screen display to a file in Postscript format. This Postscript file is suitable for sending directly to a Postscript printer for printing. Enter the name of the file in the text box and press the Start button to save the Postscript screen dump. Pressing the Cancel button removes the dialog box and does not save the file. A path to the file may also be entered in the text box. By default, the file is created in the current directory.

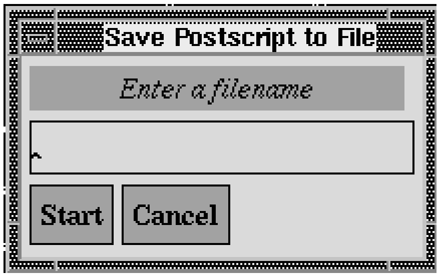


Figure 5.3.4.1.1. Save Postscript to File.

5.3.4.2 Protocol Summary

The Protocol Summary menu item will save a report detailing all activity that has been seen on the network to a file in ASCII format. This ASCII file is suitable for editing or sending to a text printer for printing. Enter the name of the file in the text box and press the Start button to save the protocol summary information. Pressing the Cancel button removes the dialog box and does not save the file. A path to the file may also be entered in the text box. By default, the file is created in the current directory.

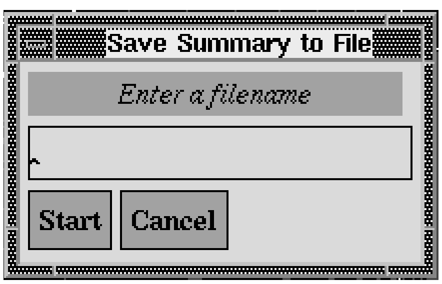


Figure 5.3.4.2.1. Save Summary to File.

5.3.4.3 Short Protocol Summary

The Short Protocol Summary menu item will save an abbreviated report detailing all activity that has been seen on the network to a file in ASCII format. This ASCII file is suitable for editing or sending to a text printer for printing. Enter the name of the file in the text box and press the Start button to save the protocol summary information. Pressing the Cancel button removes the dialog box and does not save the file. A path to the file may also be entered in the text box. By default, the file is created in the current directory.

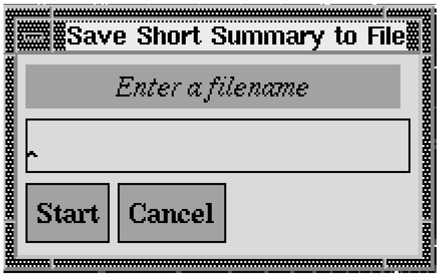


Figure 5.3.4.3.1. Save Short Summary to File..

5.3.4.4 Network Load Summary

The Network Load Summary will save the load values seen on the network to a file in ASCII format. This ASCII file is suitable for editing or sending to a text printer for printing. The load values are the same numbers that are used to make the network utilization strip chart at the top of the Etherman display. Enter the name of the file in the text box and press the Start button to save the protocol summary information. Pressing the Cancel button removes the dialog box and does not save the file. A path to the file may also be entered in the text box. By default, the file is created in the current directory.

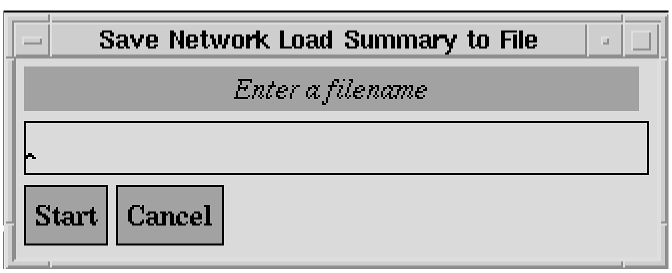


Figure 5.3.4.4.1. Save Network Load Summary to File.

5.3.4.5 Reset Counters

The Reset Counters menu item clears the current display and all of the protocol counters. Use this menu option to reduce screen clutter and to start a new capturing run after saving protocol summary information to disk. All of the program's information is lost when this option is selected, so be sure to save the protocol summary information or the postscript screen dump to a disk file first. This menu item is the same as the Clear Screen button on the button bar (see section 5.4.4).

5.3.4.6 Show Broadcasts

The Show Broadcasts menu item turns on capturing of broadcast packets. This item will have a check mark next to it when it is selected. When this item is checked, Etherman shows and counts Broadcast packets. When this item is not checked, Etherman will not show or count these packets. This item is on (checked) by default.

5.3.5 Hosts

Pressing and holding the left mouse button on the hosts menu will display the hosts sub-menu. This menu allows the user to specify how host labels are shown on the display.

5.3.5.1 Ethernet Address

The Ethernet Address menu item sets the display to show hosts by their alphanumeric Ethernet address. This menu item will have a check mark next to it when it is selected. Use the Local Name menu item to show the local name of each host. Selecting the Ethernet Address menu item will automatically turn off the Local Name and IP Address menu items. This menu item is off (not checked) by default.

5.3.5.2 IP Address

The IP Address menu item sets the display to show hosts by their numeric IP address (ARPA TCP/IP address) if they have one. Hosts that do not have an IP address are shown with their Ethernet address. This menu item will have a check mark next to it when it is selected. Use the Local Name menu item to show the local name of each host. Selecting the IP Number menu item will automatically turn off the Local Name and Ethernet Address menu items. This menu item is off (not checked) by default.

5.3.5.3 Local Name

The Name menu item sets the display to show hosts by their name and domain. Hosts that cannot be identified by name are shown with their numeric Ethernet address. This menu item will have a check mark next to it when it is selected. An /etc/ethers file or a NIS ethers map must be present on the workstation for Etherman to resolve Ethernet addresses into host names. Selecting the Local Name menu item will automatically turn off the IP Address and Ethernet Address menu items. This menu item is on (checked) by default.

5.3.5.4 Manufacturer's Code

The Manufacturer's Code menu item sets the display to show the name of the manufacturer of the Ethernet card in the host. This menu item will have a check mark next to it when it is selected. This menu item may be used in conjunction with the Local Name, IP Address, and Ethernet Address menu items. This menu item is off (not checked) by default.

5.3.6 Statistics

Pressing and holding the left mouse button on the Statistics menu item will display the Statistics sub-menu. This menu allows the user to display the hosts and links on the screen either cumulatively or dynamically.

5.3.6.1 Dynamic

The Dynamic menu item sets the display to show only the hosts and connections that are currently active on the network. This menu item will have a check mark next to it when it is selected. The amount of time that elapses before a host or connection is declared non-active and removed may be set from the Etherman Settings Panel. See section 5.5 for more information about how to change the time-out settings. Selecting this menu item will automatically turn off (uncheck) the Cumulative menu item. This menu item is on (checked) by default.

5.3.6.2 Cumulative

The Cumulative menu item sets the display to show all hosts and connections that have been seen on the network since Etherman was started or since the Reset Counters menu item was selected. In cumulative mode, the host time-out settings have no effect. Selecting this menu item will automatically turn off (uncheck) the Dynamic menu item. This menu item is off (unchecked) by default.

5.4 The Etherman Button Bar

The Etherman button bar provides a convenient way to rapidly access some of Etherman's more common functions. These buttons are activated by clicking once on the button with the left mouse button. Several of these buttons execute Unix commands (Finger, Telnet, and Ping). These commands must be on the user's path or Interman will not be able to find them.

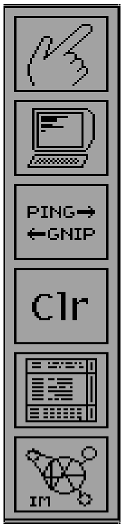
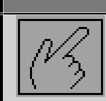
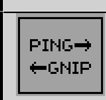
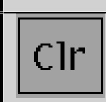


Figure 5.4.1. Etherman Button Bar.

Figure 5.4.1 shown the layout of the buttons on the button bar. Several of these buttons are disabled in secure mode because they might compromise system security. Figure 5.4.2 summarizes the buttons that are not available in secure mode (all buttons are available to the root user in non-secure mode).

Button	Available in Secure Mode?
 **Finger**	no
 **Telnet**	no
 **Ping**	no
 **Clear Screen**	yes

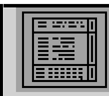
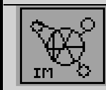
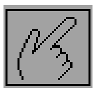
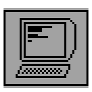
 **Packetman**	yes
 **Interman**	yes

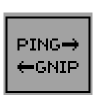
Figure 5.4.2. Buttons Available in Secure Mode.

5.4.1  Finger

The finger button allows the user to run the Unix finger command on a remote computer. First, click on the finger button with the left mouse button. Next, click on the host's label to finger with the middle mouse button. The host's label will briefly turn yellow to indicate that it has been selected. A window will appear with the finger information in it. Pressing Control-C in the window will remove it immediately. The window will automatically disappear after one minute if no action is taken.

5.4.2  Telnet

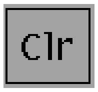
The telnet button allows the user to run the Unix telnet command to a remote computer. First, click on the telnet button with the left mouse button. Next, click on the host's label that is the telnet destination with the middle mouse button. The host's label will briefly turn yellow to indicate that it has been selected. A X-term window will appear with the telnet session in it. The window will automatically disappear when the telnet session is ended.

5.4.3 

Ping

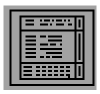
The ping button allows the user to run the Unix ping command on a remote computer. First, click on the ping button with the left mouse button. Next, click on the host's label to ping with the middle mouse button. The host's label will briefly turn yellow to indicate that it has been selected. A window will appear with the ping information in it. Pressing Control-C in the window will remove it immediately. The window will automatically disappear after one minute if no action is taken.

5.4.4 Clear Screen



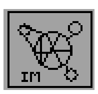
The clear screen button clears the screen and empties all of the host and link counters. All of the information that has been captured will be lost, so be sure to save the protocol summary information to disk first. Click on this button with the left mouse button to clear the screen and empty the counters. This button is the same as the Reset counters menu item.

5.4.5 Packetman



The Packetman button allows the launch of the Packetman program from inside Etherman. First, click on the Packetman button with the left mouse button. Next click on the two hosts to be examined in Packetman with the middle mouse button. The host's labels will briefly turn yellow to indicate that they have been selected. Etherman will launch Packetman and set its Ethernet host filters to the hosts that were selected.

5.4.6 Interman



The Interman button allows the launch of the Interman program from inside Etherman. Clicking on the Interman button with the left mouse button will launch Interman to examine the local TCP/IP network.

5.5 Etherman Settings Panel

The Etherman Settings Panel allows the user to modify several parameters that change the way the display is updated. It allows the user to change the scale and maximum size of links and host nodes. As the scale is increased, Etherman is more sensitive to small changes in the number of packets or bytes transmitted. Decrease the scale if there is a lot of traffic to make Etherman less sensitive. The maximum radius settings determine how large the host and link icons expand. Decrease the maximum width if the display is becoming very cluttered. The node time-out and link time-out settings change the amount of time before a link or host is removed from the display. These functions only work when Etherman is in Dynamic display mode. See section 5.3.6 for information about how to change Etherman's display mode.

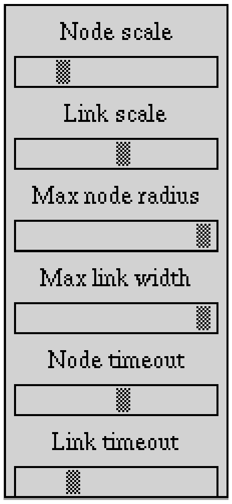


Figure 5.5.1. Etherman Settings Panel.

The setting scroll bars are changed by pressing and holding the middle mouse button while moving the scroll bar. Move the scroll bars to the left to decrease the setting or move the scroll bars to the right to increase the setting. All of these settings may be changed in secure mode.

5.6 Etherman Statistics Panel

The Etherman Statistics Panel shows information about the current utilization of the network. These numbers may be used as a rough guide of the current performance of the network. Each of these parameters is measured over a one second interval. The average load is reported as the average of the network utilization from the time that Etherman was started or the counters were last cleared. The peak load is the highest one second load (utilization) that Etherman has seen since it was started or the counters were cleared. Current packets per second and bytes per second display the amount of traffic currently on the network. The Dropped counter is an indication of how many packets the workstation was unable to monitor. Large numbers of dropped packets indicate that the workstation is not able to keep up with the network load. Some workstations may not give an accurate count of dropped packets.

Figure 5.6.1. Etherman Statistics Panel.

Etherman statistics are displayed in secure mode.

5.7 The Etherman Display

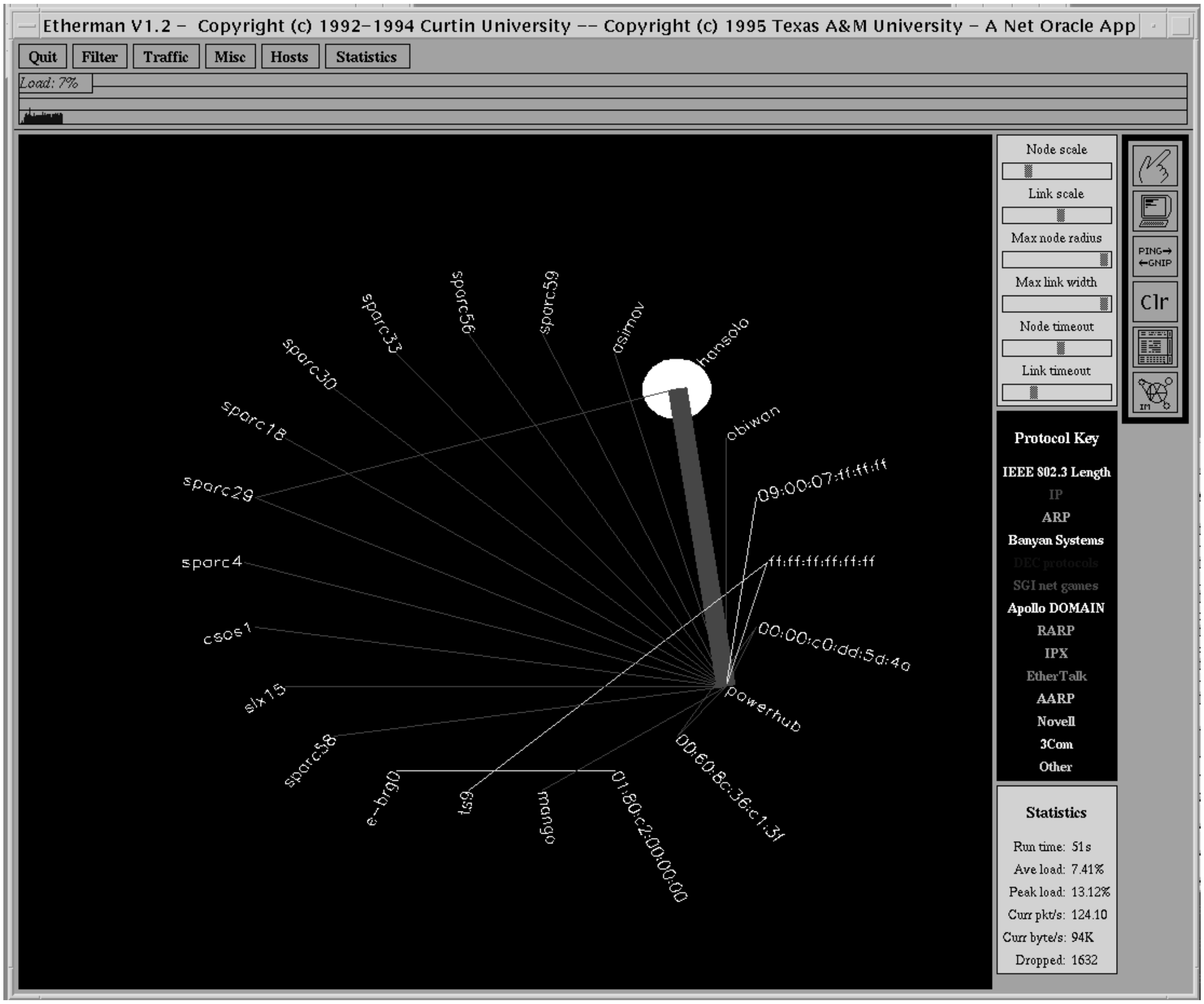


Figure 5.7.1. The Etherman Display.

Etherman displays the network as a large circle with the hosts arranged along the outside edge. Hosts that are communicating with each other are connected with lines. The color of the line is determined by the most frequent protocol being used between the hosts. The size of the hosts and the lines connecting hosts increases as the amount of traffic increases. A protocol key at the right of the screen shows the colors being used for the links.

At the top of the display, a strip chart shows the utilization of the Ethernet network. This is a quick way to check the current performance of the network. This chart is updated once a second to show the current network utilization. The menu buttons for Etherman are located directly above the strip chart. These menus are described in section 5.3.

5.8 Exiting Etherman

To exit from Etherman, click on the Quit menu button with the left mouse button. Quitting Etherman deletes all network information that has been gathered during this session. Use the Protocol Summary and Postscript Dump menu items to save this information to disk before exiting.

6.0 Known Limitations and Suggestions for Improvement

The following are known limitations of Etherman and suggestions for improvement. These items should be fixed in some future version. However, this is not a guarantee that these items can or will be fixed in a future version.

- Etherman causes an extremely heavy load on the workstation that it is running on. Workstations that are being used for other operations or slower workstations may not be able to accurately monitor all of the traffic on the network. Packets that are lost because the workstation is too slow to respond will not be seen by Etherman, and no warning will be given (the workstation never realizes that it has not seen the packets). Because of this, the numbers reported by Etherman should be taken as only a rough estimate of network traffic. This is especially true when network utilization is over 50%. Dedicated network monitoring hardware should be used when extreme precision is required.

7.0 References

1. Reynolds, J. and Postel, J. Assigned Numbers. *Internet Request for Comments 1340*, July 1992.

