Packetman 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 1.1 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. Packetman is one of three tools in the Netman tool set. Packetman provides the network manager with a tool that can capture and analyze packets on an Ethernet network. Packetman is capable of capturing and decoding packets from several network protocols. This document is a comprehensive user's guide covering the capabilities and use of the Packetman network monitoring tool.*

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

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 the 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 Packetman are Copyright 1991, 1993, and 1993 by Curtin University. The source code for any version of Packetman (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 Packetman

4.1 Version 1.0

Packetman Version 1.0 was originally developed in 1992 at Curtin University by George Benko, Mike Schulze, and Craig Farrell as part of the *Netman* project. This version was created for *Ultrix 4.x* and *SunOS* 4.x.

4.2 Version 1.1

Packetman Version 1.1 was also developed at Curtin University by Gregory Barron, Mike Schulze, and Craig Farrell. This version included several significant changes to the user interface to make the program easier to use. The ability to decode ICMP, NFS and RPC packets was also added. Version 1.1 runs under *Irix 4.x*, *SunOS* 4.x, and *Ultrix 4.x.*

4.3 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 additional 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 Packetman written in Tcl/Tk is also provided with the version 1.2 distribution.

5.0 Using Packetman

5.1 Requirements for Use

Version 1.2 of Packetman 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.* Packetman 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 either run by root or have the Set User ID bit set to give root permission 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 Packetman. When the program is run Set User ID root by an user other than root, it automatically enters a secure operating mode. Secure mode censors incoming data to prevent sensitive material from being revealed to non-privileged users. Secure mode also limits the commands that are available to the user. Only the root user can use Packetman in its non-secure mode, all other users are limited to secure mode. All of Packetman's functions are available when running as root in non-secure mode.

Packetman 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, Packetman should not be run on multi-user machines or machines that are being used as servers. If Packetman 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 Packetman to lose or "drop" packets. This packet dropping cause problems with the accuracy of the packet captures. Packetman may not be able to provide a warning when this occurs. The ideal environment for Packetman is a fast, dedicated workstation.

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

5.2 Starting Packetman

Start Packetman by executing the command `packetman` at the command prompt. Be sure to set the X-Windows DISPLAY environment variable, if necessary, before running Packetman. Packetman will not run on remote X-Windows displays in secure mode. Only the root user may run Packetman remotely. Packetman 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 Packetman is started.

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

5.2.1 Command Line Switches

Packetman supports a wide variety of options that can be used to customize the operation of the program. For convenient use of Packetman from a shell script or other automated program, a large number of command line switches are provided to set these options before launching Packetman. All of these options except -I can be changed from the internal menus once Packetman is started. The command line switches also allow Packetman to be used in a background mode as a simple packet capture tool. Captured packets are saved to a file in this mode for later analysis with Packetman or some other packet analysis tool.

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 the root user in non-secure mode):

Command Line Switch	Available in Secure Mode?
-I interface	yes
-S source host	yes
-D destination host	yes
-X IP source host	yes
-Y IP destination host	yes
-F filename	no
-R filename	yes
-C number	yes (but not with -T)
-T	no
-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.). This command line switch allows the user to override Packetman's choice of the workstation's network interface to open for promiscuous mode packet capturing. By default, Packetman will attempt to open the first Ethernet interface on the workstation. In most environments this will be sufficient, however, this command line 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 option 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 Packetman. Packetman will not start if it cannot open a network interface in promiscuous mode.

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

5.2.1.2 -S source host

Specify an Ethernet source host filter. This command line switch allows the user to specify a Ethernet address level host filter. An Ethernet host filter rejects all packets whose

Ethernet addresses do not match those specified by the filters. The source filter must always be paired with a corresponding Ethernet destination filter. For instance the pair "-S *hansolo* -D *obiwan*" allows only traffic that originates at *hansolo* (source host) and is sent to *obiwan* (destination host) to be seen. In order to filter for traffic going both ways between two machines, two different filter pairs must be set. The following command line would set the filter to collect traffic going both ways between *obiwan* and *hansolo*:

```
packetman -S obiwan -D hansolo -S hansolo -D obiwan
```

Since Ethernet addresses cannot cross routers or gateways, both of the hosts to be filtered must be on the same Ethernet network. Use the Ethernet address of the network's router or gateway to capture packets coming from other networks (or use the TCP/IP host filters if this protocol is being examined).

Packetman allows multiple host filters to be specified on the command line, however, the source and destination filters must match in pairs as in the above example. A -S must follow a -D before another -D can be issued or a -D must follow a -S before another -S can be issued. The following command line shows an example of an ***illegal*** combination:

```
packetman -S obiwan -S hansolo -D hansolo -D obiwan
```

In this example, Packetman would be unable to determine which destination host matched with each source host. Packetman will print an error message and exit if source and destination filters are paired incorrectly as in the above example.

The filter uses the Ethernet address of the host to determine which packets to capture. An /etc/ethers file or an NIS Ethernet address map must be present for Packetman to map host names to Ethernet addresses. If Packetman cannot resolve a host name to an Ethernet address, it will print an error message and exit. The filter may also be set with the six octet Ethernet address of the host in the following format: xx:xx:xx:xx:xx:xx. If a valid Ethernet address is specified, Packetman will use it without performing any checking to see if a host with that address is present on the network. If packets are not being captured, make sure that the addresses have been entered correctly. Mixing the two methods is also allowed. The following command line shows an example of mixing host names and Ethernet addresses:

```
packetman -S 00:00:ae:dc:f8:9f -D hansolo
```

The -S and -D command line switches may be combined with the -X and -Y IP host filter switches (see sections 5.2.1.4 and 5.2.1.5), however packets will not be captured unless they match at least one entry in both sets of filters.

5.2.1.3 -D destination host

Specify an Ethernet destination host filter. This command line switch is used in conjunction with the -S switch to specify an Ethernet host filter pair. An Ethernet host filter rejects all packets whose Ethernet addresses do not match those specified by the filters. See section 5.2.1.2 for a discussion of the rules for specifying filter pairs.

Like the -S switch, the -D switch can be entered as a host name or as an Ethernet address in the form xx:xx:xx:xx:xx:xx. The following command line shows an example of setting an Ethernet host filter:

```
packetman -S 00:00:ae:dc:f8:9f -D hansolo -S hansolo -D 00:00:ae:dc:f8:9f
```

Please see section 5.2.1.2 for more information and for cautions about using the -S and -D switches in conjunction with the -X and -Y IP host filters.

5.2.1.4 -X IP source host

Specify an IP (ARPA TCP/IP) source host filter. This command line switch allows the user to specify an Internet Protocol (IP) address level host filter. An IP host filter rejects all packets whose IP addresses do not match those specified by the filters. The source filter must always be paired with an IP destination filter. For instance the pair "-X *hansolo* -Y *obiwan*" allows only TCP/IP traffic that originates at *hansolo* (source host) and is sent to *obiwan* (destination host) to be seen. In order to filter for traffic going both ways between two machines, two different filter pairs must be set. The following command line would set the filter to collect traffic going both ways between *obiwan* and *hansolo*:

```
     packetman -X obiwan -Y hansolo -X hansolo -Y obiwan
```

Packetman allows multiple host filters to be specified on the command line, however, the source and destination filters must match in pairs as in the above example. A -X must follow a -Y before another -Y can be issued or a -Y must follow a -X before another -X can be issued. The following command line shows an example of an ***illegal*** combination:

```
     packetman -X obiwan -X hansolo -Y hansolo -Y obiwan
```

In this example, Packetman would be unable to determine which destination host matched with each source host. Packetman will print an error message and exit if source and destination filters are paired incorrectly as in the above example.

The filter uses the IP address of the host to determine which packets to capture. An /etc/hosts file, NIS hosts map, or a pointer to a Domain Name Service (DNS) server (usually in /etc/resolv.conf) must be present on the workstation for Packetman to map host names to IP addresses. If Packetman cannot resolve a host name to an IP address, it will print an error message and exit. Fully qualified host names do not have to be entered if the workstation understands domain names (i.e. *hansolo* instead of *hansolo.cs.tamu.edu*). The IP filter may also be set with the numeric IP address of the host in the following format: 123.123.123.123. If a valid IP address is specified, Packetman will use it without performing any checking to see if the host is present on the network. If no packets are being captured, make sure that the addresses have been entered correctly. Mixing the two methods is also allowed. The following command line shows an example of mixing host names and IP addresses:

```
      packetman -X 128.194.18.1 -Y hansolo
```

The -X and -Y IP host filter command line switches may be combined with the -S and -D Ethernet host filter switches (see sections 5.2.1.2 and 5.2.1.3), however packets will not be captured unless they match at least one entry in both sets of filters.

5.2.1.5 -Y IP source host

Specify an IP (ARPA TCP/IP) destination host filter. This command line switch is used in conjunction with the -X switch to specify an IP host filter pair. An IP host filter rejects all packets whose IP addresses do not match those specified by the filters. See section 5.2.1.4 for a discussion of the rules for specifying filter pairs.

Like the -X switch, the -Y switch can be entered as a host name or as a numeric IP address in the form 123.123.123.123. The following command line shows an example of setting an IP host filter:

```
packetman -S 128.194.18.1 -D hansolo -S hansolo -D 128.194.18.1
```

Please see section 5.2.1.4 for more information and for cautions about using the -X and -Y host filter switches in conjunction with the -S and -D Ethernet host filters.

5.2.1.6 -F filename

Specify a filename for a file to contain saved packets. This command line switch specifies the default location to save packet files. The Save to File dialog box will show the filename that is entered with this switch. The filename may be changed in the dialog box by the user if desired. The filename may be entered with a complete path giving its location. By default, files are stored in the same directory as Packetman (if no path is specified). Files are always stored in the Network General *Sniffer* format. The following example shows the use of this switch:

```
packetman -F /user/garyr/packets.out
```

This command line switch is also used to give the filename that packets are saved in when performing an automated capture. See section 5.2.1.9 for more information about using Packetman to perform automated packet captures.

5.2.1.7 -R filename

Read packets from filename at startup. This command line switch specifies the name of a packet file to read when Packetman is started. Packetman will automatically load all the packets from this file and display their contents in the packet list section at startup. A packet file must be in the Network General *Sniffer* format in order to be read correctly. The filename may be entered with a complete path giving its location. By default, files are read from the same directory as Packetman. See sections 5.2.1.6 and 5.3.5 for more information about saving packet files. The following example shows the use of this command line switch to read a packet file named packets.save from the directory /user/garyr:

```
packetman -R /user/garyr/packets.save
```

5.2.1.8 -C number

Capture *number* of packets immediately at startup. This command line switch causes Packetman to capture packets beginning immediately upon startup. The number specifies the number of packets to be captured. The number of packets to capture must be greater than zero and less than 10,000. This command line switch is most often used with the automated packet capture facility in Packetman. See section 5.2.1.9 for more information about the automated packet capture facility.

The following example shows the use of this command line switch to automatically capture fifty packets at startup:

```
packetman -C 50
```

5.2.1.9 -T

Runs Packetman in non-interactive text mode for packet capture. This automated packet capture facility allows the user to capture packets from the command line and save them to a file. The X-Windows display is not invoked when this option is used. Packetman does not have to be running in X-Windows to use this mode. The -C and -F command line switches must always be used with the -T switch. The -C switch indicates the number of packets to capture and the -F switch indicates the file name to save the packets in. See sections 5.2.1.8 and 5.2.1.6 for more information about these switches. If the -C and -F switches are not specified when the -T switch is used, Packetman will exit with an error message. The packet file that is generated is saved in the Network General *Sniffer* format. The following example shows how to capture 50 packets in the background and save them to the file packets.out located in the directory /user/garyr:

```
packetman -C 50 -F /user/garyr/packets.out -T &
```

5.2.1.10 -L link layer filter

Specify a data link layer packet filter. This command line switch allows the user to select one of Packetman'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 Packetman. The link layer filters may be used in conjunction with the Ethernet and IP host filters. The filter is specified by typing its code after the -L. The codes must be entered in uppercase exactly as shown in the list.

Filter Code	Type of Packet Accepted by Filter
IP	IP (ARPA TCP/IP) Packets only
ICMP	ICMP (ARPA ICMP) Packets only
DEC	DECNet Packets only
LAT	LAT Packets only

APPLE	AppleTalk Packets only
IPX	Novell (SPX/IPX) Packets only

Figure 5.2.1.10.1. Link Layer Filters.

The following example sets Packetman to only capture AppleTalk packets:

```
packetman -L APPLE
```

5.2.1.11 -E ethernet frame #

Specify a custom Ethernet frame filter. This command line switch allows the user to capture packets based on a custom Ethernet frame type. Several common frame types are provided as link layer filters (see section 5.2.1.10). This switch allows the user to capture packets not selected by the provided filter set. Figure 5.2.1.11.1 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. This filter may be used in conjunction with the Ethernet and IP host filters.

The following example show how to set Packetman to capture only Ethernet packets with a frame type of 2048 (ARPA IP packets have a Ethernet frame type of 2048):

```
packetman -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 5.2.1.11.1. Ethernet Frame Types.

5.2.1.12 -N network filter

Specify a network level packet filter. This command line switch allows the user to select one of Packetman'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 Packetman. The network layer filters may be used in conjunction with the Ethernet and IP host filters. The filter is specified by typing its code after the -N. The codes must be entered 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 5.2.1.12.1. Network Layer Filters.

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

```
packetman –N TCP
```

5.2.1.13 -A application filter

Specify an application level packet filter. This command line switch allows the user to select one of Packetman's built in application layer packet filters (not all of these programs operate 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 Packetman. The application layer filters may be used in conjunction with the Ethernet and IP host filters. The filter is specified by typing its code after the -A. The codes must be entered 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 5.2.1.13.1. Application Layer Filters.

The following example sets Packetman to capture only telnet packets:

```
packetman -A TELNET
```

5.2.1.14 -U port #

Specify a custom UDP port number. This command line switch is used to filter for a custom distinguished UDP port number. Figure 5.2.1.14.1 gives a partial listing of common UDP port numbers [1]. Packetman looks at both the source and destination port to match a port filter with a packet. 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, Packetman will still allow the packet through, but it may not be decoded correctly. The custom UDP port filter may be used in conjunction with the -S and -D Ethernet host filters and the -X and -Y IP host filters.

The following example sets Packetman to filter for UDP port 2049 (UPD port 2049 matches NFS packets):

```
packetman -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 5.2.1.14.1. Common UDP Port Numbers.

5.2.1.15 -P port #

Specify a custom TCP port number. This command line switch is used to filter for a custom distinguished TCP port number. Figure 5.2.1.15.1 gives a partial listing of TCP port numbers [1]. Packetman looks at both the source and destination port to match a port filter to a packet. 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, Packetman will still allow the packet through, but it may not be decoded correctly. The custom TCP port filter may be used in conjunction with the -S and -D Ethernet host filters and the -X and -Y IP host filters.

The following example sets Packetman to filter for TCP port 23 (TCP port 23 matches Telnet packets):

```
packetman –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 5.2.1.15.1. Common TCP Port Numbers.

5.2.1.16 -H and -?

Print Packetman 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 Packetman to exit, so it should not be used in combination with any other command line switches.

5.2.2 Packetman Launch Utility

The Packetman launch utility is a Tcl/Tk script that allows the user to set Packetman's command line switches and start Packetman with a graphical user interface. Most of the command line options can be specified with this tool. To start the Packetman 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.

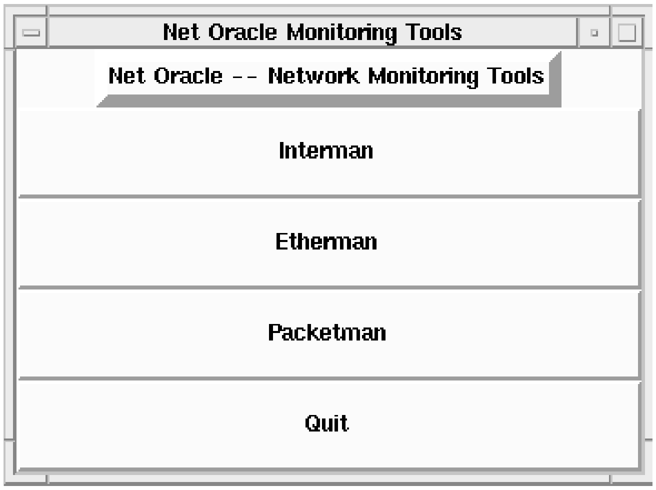
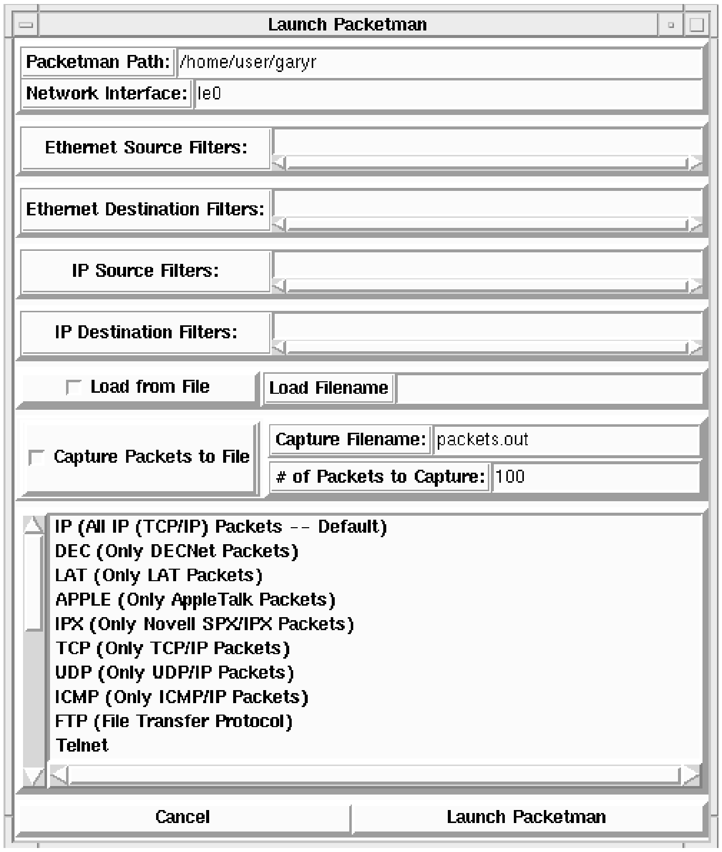


Figure 5.2.2.1. Netman Launch Utility.

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



Packetman Path: /home/user/garyr
Network Interface: le0
Capture Filename: packets.out
# of Packets to Capture: 100

Figure 5.2.2.2. Packetman Launch Utility.

Because several of the Packetman Launch Utility's functions activate operations that might violate system security, they are restricted in secure mode. The following figure summarizes the operations that are available in secure mode (all operations are available to the root user in non-secure mode):

Function	Available in Secure Mode?
Packetman Path	yes
Network Interface	yes
Ethernet Source Filters	yes
Ethernet Destination Filters	yes
IP Source Filters	yes
IP Destination Filters	yes
Load from File	yes
Capture Packets to File	no

Filter	yes
Cancel	yes
Launch Packetman	yes

Figure 5.2.2.2. Launch Utility Functions Available in Secure Mode.

5.2.2.1 Packetman Path

This field allows the user to specify the location of the Packetman executable file. The default location of this file should have been set by the system administrator; however, the user can change it with this setting.

5.2.2.2 Network Interface

This text box allows the user to override Packetman's choice of the workstation's network interface to open for promiscuous mode packet capture. By default, Packetman will attempt to open the first Ethernet interface. 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 Packetman. Packetman will not start if it cannot open the network interface in promiscuous mode.

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

5.2.2.3 Ethernet Source Filters

This text box allows the user to set Ethernet source host filters for packet capturing. Both source and destination filters must be specified in order to correctly setup a filter. The host names or addresses that are to be used as the filter criteria may be entered separated by spaces, commas, or semi-colons. Either the host name or the Ethernet address of the host may be entered (use the form xx:xx:xx:xx:xx:xx for Ethernet addresses). The Packetman launch utility will automatically build -S and -D command line parameters in the order that the hosts are specified. There must be the same number of source and destination hosts listed. The Packetman launch utility will give an error message if the number of source and destination hosts differ. Any number of host pairs may be entered.

These filters operate only one way. If the source filter is set to *hansolo* and the destination filter is set to *obiwan*, then only packets traveling from *hansolo* to *obiwan* will be captured. Packets from traveling *obiwan* to *hansolo* will not be captured. Pairs of hosts may be entered in both directions to capture traffic traveling both ways.

The following example shows how to set the Ethernet host filter to capture all packets between *hansolo* and *obiwan* in both directions:

```
Ethernet Source Filters:  obiwan, hansolo
Ethernet Destination Filters:  hansolo, obiwan
```

This example would be equivalent to the following command line for launching Packetman:

```
packetman -S obiwan -D hansolo -S hansolo -D obiwan
```

This command line will be created automatically by the Packetman launch program and will be executed when the Launch Packetman button is pressed.

5.2.2.4 Ethernet Destination Filters

This text box allows the user to set Ethernet destination host filters for packet capturing. Both source and destination filters must be specified in order to correctly setup an Ethernet host filter. The host names and addresses that are to be used to filter packets may be entered separated by spaces, commas, or semi-colons. Either the host name or the Ethernet address of the host may be entered (use the form xx:xx:xx:xx:xx:xx for Ethernet addresses). The Packetman launch utility will build -S and -D command line parameters in the order that the hosts are specified. Any number of pairs may be entered, but there must be the same number of source and destination hosts listed. These filters operate in only one direction. If the source filter is set to *hansolo* and the destination filter is set to *obiwan*, then only packets traveling from *hansolo* to *obiwan* will be captured. Packets traveling from *obiwan* to *hansolo* will not be captured. Pairs of hosts may be entered in both directions to capture traffic traveling in both ways.

The following example shows how to set the Ethernet host filter to capture all packets between *hansolo* and an Ethernet address in both directions:

```
Ethernet Source Filters:  obiwan, 00:00:c0:de:8f:b0
Ethernet Destination Filters:  00:00:c0:de:8f:b0, obiwan
```

This example would be equivalent to the following command line for launching Packetman:

```
packetman -S obiwan -D 00:00:c0:de:8f:b0 -S 00:00:c0:de:8f:b0 -D obiwan
```

This command line will be created automatically by the program and executed when the Launch Packetman button is pressed.

5.2.2.5 IP Source Filters

This text box allows the user to set IP source host filters for packet capturing. Both source and destination filters must be specified in order to correctly setup an IP host filter. The host name or addresses that are to be used as filters may be entered separated by spaces, commas, or semi-colons. Either the host name or the IP address of the host may be entered (use the form 123.123.123.123 for IP addresses). The Packetman launch utility will build -X and -Y command line parameters automatically in the order that the hosts are specified. There must be the same number of source and destination filters listed. The Packetman launch utility will give an error message if the number of source and destination hosts differ. As many pairs of hosts as needed may be entered.

These filters operate in only one direction. If the source filter is set to *hansolo* and the destination filter is set to *obiwan*, then only packets traveling from *hansolo* to *obiwan* will be captured. Packets traveling from *obiwan* to *hansolo* will not be captured. Pairs of hosts may be entered in both directions to capture traffic traveling both ways.

The following example shows how to set the IP host filter to capture all packets between *hansolo* and *obiwan* in both directions:

```
IP Source Filters:  obiwan, hansolo
```

```
IP Destination Filters:  hansolo, obiwan
```

This example would be equivalent to the following command line for launching Packetman:

```
packetman -X obiwan -Y hansolo -X hansolo -Y obiwan
```

This command line will be created automatically by the program and executed when the Launch Packetman button is pressed.

5.2.2.6 IP Destination Filters

This text box allows the user to set IP destination host filters for packet capturing. Both source and destination filters must be specified in order to correctly setup a filter. The host names and addresses that are to be filtered on may be entered separated by spaces, commas, or semi-colons. The host name or the IP address of the host may be entered (use the form 123.123.123.123 to enter IP addresses). The Packetman launch utility will build -X and -Y command line parameters automatically in the order that the hosts are specified. There must be the same number of source and destination filters listed. The Packetman launch utility will give an error message if the number of source and destination hosts differ. There is no limit to the number of hosts that may be entered.

These filters operate only in one direction. If the source filter is set to *hansolo* and the destination filter is set to *obiwan*, then only packets traveling from *hansolo* to *obiwan* will be captured. Packets traveling from *obiwan* to *hansolo* will not be captured. Pairs of hosts may be entered in both directions to capture packets traveling both ways.

The following example shows how to set the IP host filter to capture all packets between *hansolo* and an IP address in both directions:

```
IP Source Filters:  obiwan, 128.194.18.1
IP Destination Filters:  128.194.18.1, obiwan
```

This example would be equivalent to the following command line for launching Packetman:

```
packetman -X obiwan -Y 128.194.18.1 -X 128.194.18.1 -Y obiwan
```

This command line will be created automatically by the program and executed when the Launch Packetman button is pressed.

5.2.2.7 Load from File

This checkbox instructs Packetman to load a packet file and display its contents at startup. This option corresponds to the -R command line switch. If a filename for a Network General *Sniffer* format packet file is specified in the Load Filename text box, Packetman will load this file at startup. If a valid filename is not specified, Packetman will ignore this option.

5.2.2.7.1 Load Filename

This text box specifies the name of a Network General *Sniffer* file to load at startup. The Load From File checkbox must be checked to use this option. The full path to the file may be specified in this box. By default, the file is loaded from the current directory.

5.2.2.8 Capture Packets to File

The capture packets to file checkbox places Packetman into the non-interactive text mode for automated packet capturing. The checkbox corresponds to the -T command line switch. The number of packets to capture and a file name to save the packets to must be specified in the adjacent text boxes. Packetman does not need to be running in X-Windows to use this mode (use the command line switches if Packetman is not running in X-Windows).

5.2.2.8.1 Capture Filename

The text box specifies the filename that the captured packets will be saved in. This file will be written in the Network General *Sniffer* file format. The complete path to the file may be entered as well as the filename. By default, Packetman stores the file in the current directory.

5.2.2.8.2 # of Packets to Capture

This text box specifies the number of packets to capture. The number must be greater than zero and less than 10,000.

5.2.2.9 Select Filter

This list box allows the user to select from one of the link layer, network layer, or application layer filters. This version of the Packetman launch utility is limited to only one filter selection. All of these filters may be used in conjunction with the Ethernet host filters and the IP host filters.

5.2.2.10 Cancel

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

5.2.2.11 Launch Packetman

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

5.3 The Packetman Menu:

The Packetman 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. The sub-menus are accessed by pressing and holding the left mouse button over the menu button on the screen. Move the mouse to the sub-menu item that is to be selected and release the left button. Figure 5.3.1 shows the Packetman menus.

Figure 5.3.1. Packetman Menus.

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 running in non-secure mode):

Menu Item	Available in Secure Mode?
Quit	yes
Filter	yes
Hosts	yes

Capture	yes
Save	no
Load	yes
Clear	yes
Print	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 Packetman to exit immediately. All of the packets that have been captured into memory will be lost. Use the Save menu button to save the packets that are in memory before exiting.

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. The All menu item should always be selected 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. Selecting this menu item does not clear any Ethernet host filters or IP host filters that have been set. The All filter menu item can be safely used 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 seen in figure 5.3.2.8.10.1. A base 10 number should be entered in this dialog box to indicate the port to be used as the filter criteria.

Figure 5.2.1.14.1 gives a list of common UDP port numbers. Only one custom port filter can be entered at a time. This filter also selects UDP and IP filtering.

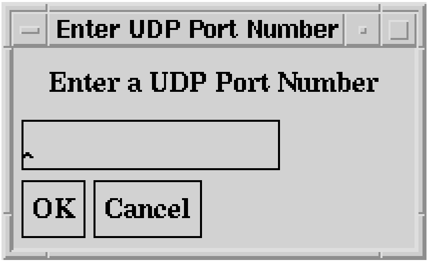


Figure 5.3.2.8.10.1. Enter UDP Port Number.

The Custom UDP filter will pass any 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 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 running over TCP/IP 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. A base 10 number should be entered in this dialog box to indicate the TCP port that is to be used as the filter criteria. Figure 5.2.1.15.1 gives a list of common TCP port numbers. Only one custom port filter may be selected at a time. Activating this filter also selects TCP and IP filtering.

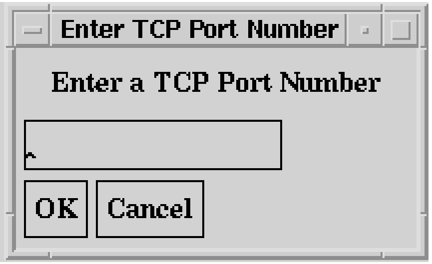


Figure 5.3.2.9.10.1. Enter TCP Port Number.

The Custom TCP filter will pass any packet that has either that 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 packet 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 a custom Ethernet frame number in this dialog box in base 10. Figure 5.2.1.11.1 gives a list of common Ethernet frame types. Only one custom filter may be entered at a time.

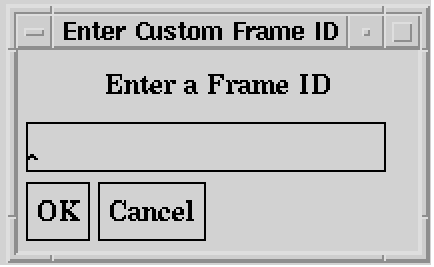


Figure 5.3.2.10.1. Enter Custom Frame ID.

5.3.3 Hosts

Pressing and holding the Hosts button with the left mouse button will display the hosts filter sub-menu. These menus allow the user to set both Ethernet and IP (ARPA TCP/IP) host filters. These host filters may be used in combination with the protocol filters under the filter menu item. While the Ethernet and IP host filters may be used in combination, it is usually not necessary to do so.

5.3.3.1 Ethernet Host Filter

Selecting the Ethernet Host Filter menu item allows the user to filter packets based on their source and destination address. The Ethernet address of the source and destination host is used as the basis of the filtering. When the menu item is selected, a dialog box will be displayed as shown in Figure 5.3.3.1.1. Enter the source host followed by the destination host. The two names should be separated by a space. Pressing the Enter key or the Add button will add the filter. There is no limit to the number of host pairs that can be entered. Pressing the Clear All button clears all of the Ethernet Host Filters that have been added. Press the Done button when finished to close the dialog box.

These filters operate in one direction only. Entering the pair *obiwan hansolo* will show only packets traveling from *obiwan* to *hansolo*. Packets traveling in the other direction are not shown. Enter the pair twice (*obiwan hansolo* and *hansolo obiwan*) to filter in both directions.

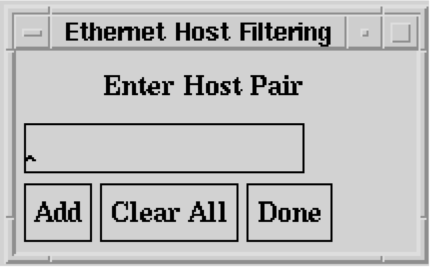


Figure 5.3.3.1.1. Ethernet Host Filtering.

The hosts may be entered either by name or by Ethernet address in the form xx:xx:xx:xx:xx:xx. The Packetman program uses the file /etc/ethers and the NIS Ethernet address map to resolve host names to Ethernet addresses. If these files are not present or the name is not located, Packetman will display an error message.

5.3.3.2 IP Host Filter

Selecting the IP Host Filter menu item allows the user to filter packets based on their IP source and destination address. The IP (ARPA TCP/IP) address of the source and destination host is used as the basis of the filtering. When the menu item is selected, a dialog box will be displayed as shown in Figure 5.3.3.2.1. The source host should be entered followed by the destination host. The two names should be separated by a space. Pressing the Enter key or the Add button will add the filter. There is no limit to the number of pairs of hosts that can be entered. Pressing the Clear All button clears all of the IP Host Filters that have been added. Press the Done button when finished to close the dialog box.

These filters operate in one direction only. Entering the pair *obiwan hansolo* will show only packets traveling from *obiwan* to *hansolo*. Packets traveling in the other direction are not shown. Enter the pair twice (*obiwan hansolo* and *hansolo obiwan*) to filter in both directions.

Figure 5.3.3.2.1. IP Host Filtering.

The hosts that are to be filtered on may be entered either by name or by IP address in the form 123.123.123.123. The fully qualified domain name does not have to be entered for hosts in the local domain. The Packetman program uses the file /etc/hosts, a NIS hosts map, and any domain name servers known by the workstation to resolve host names to IP addresses. If these files are not present or the name is not located, Packetman will display an error message.

5.3.4 Capture

The Capture menu item is used to capture packets into the Packetman program. When the Capture menu item is selected, a dialog box as shown in Figure 5.3.4.1 is displayed. Enter the number of packets to capture in the text box and press Start to begin the capture. A number between 1 and 10,000 must be entered. Pressing the Cancel button removes the dialog box without capturing any packets.

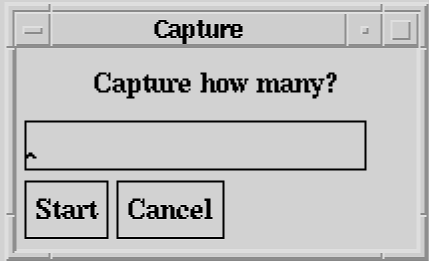


Figure 5.3.4.1. Capture.

After starting a capture, the number of packets that have been captured will be displayed in the upper right corner of the Packetman display. The Start button will turn into a Stop button while that capture is taking place. Pressing the Stop button will abort the capture. Any packets that have been captured to the point that Stop is pressed will be retained in memory.

5.3.5 Save

Selecting the Save menu button with the left mouse button allows the user to save a set of packets to file in Network General *Sniffer* format. When this menu button is pressed, a dialog box as shown in Figure 5.3.5.1 is displayed. Enter the name of the file to save packets into and press the Start button to begin the save. Pressing the Cancel button removes the dialog box without saving any packets. A complete path for the file may be entered along with its filename. By default, files are saved in the current directory.

Figure 5.3.5.1. Save to File.

Saving large amounts of packets to a file may require several seconds. The Start button will turn into a Stop button as soon as the save is started. The save may be stopped at any time by clicking on the Stop button. The packet file will not be created correctly if the save operation is stopped before it is finished. Do not depend on being able to read any file that has not been allowed to complete saving.

5.3.6 Load

Selecting the Load menu button with the left mouse button allows the user to load a set of packets from a file that was saved in Network General *Sniffer* format. When this menu button is pressed, a dialog box as shown in Figure 5.3.6.1 is displayed. Enter the name of the file to load packets from and press the Start button to begin the load. Pressing Cancel removes the dialog box without loading any packets. A complete path to the file may be entered along with its filename. By default, files are loaded from the current directory.

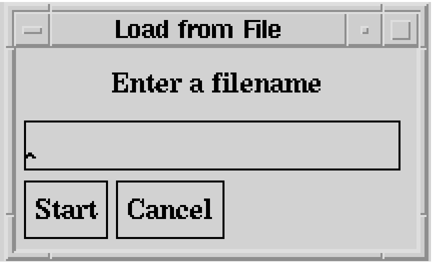


Figure 5.3.6.1. Load from File.

Loading large amounts of packets to a file may require several seconds. The Start button will turn into a Stop button as soon as the load is started. The load may be stopped at any time by clicking on the Stop button. All the packets that have been completely loaded before the Stop button is pressed will be displayed.

5.3.7 Clear

This menu item clears the packet capture buffer and deletes all the captured packets from memory. There is no undo command, so be careful not to delete any packets that have not been saved to disk. Use the Save menu item to permanently write out packets to a disk file in *Sniffer* format.

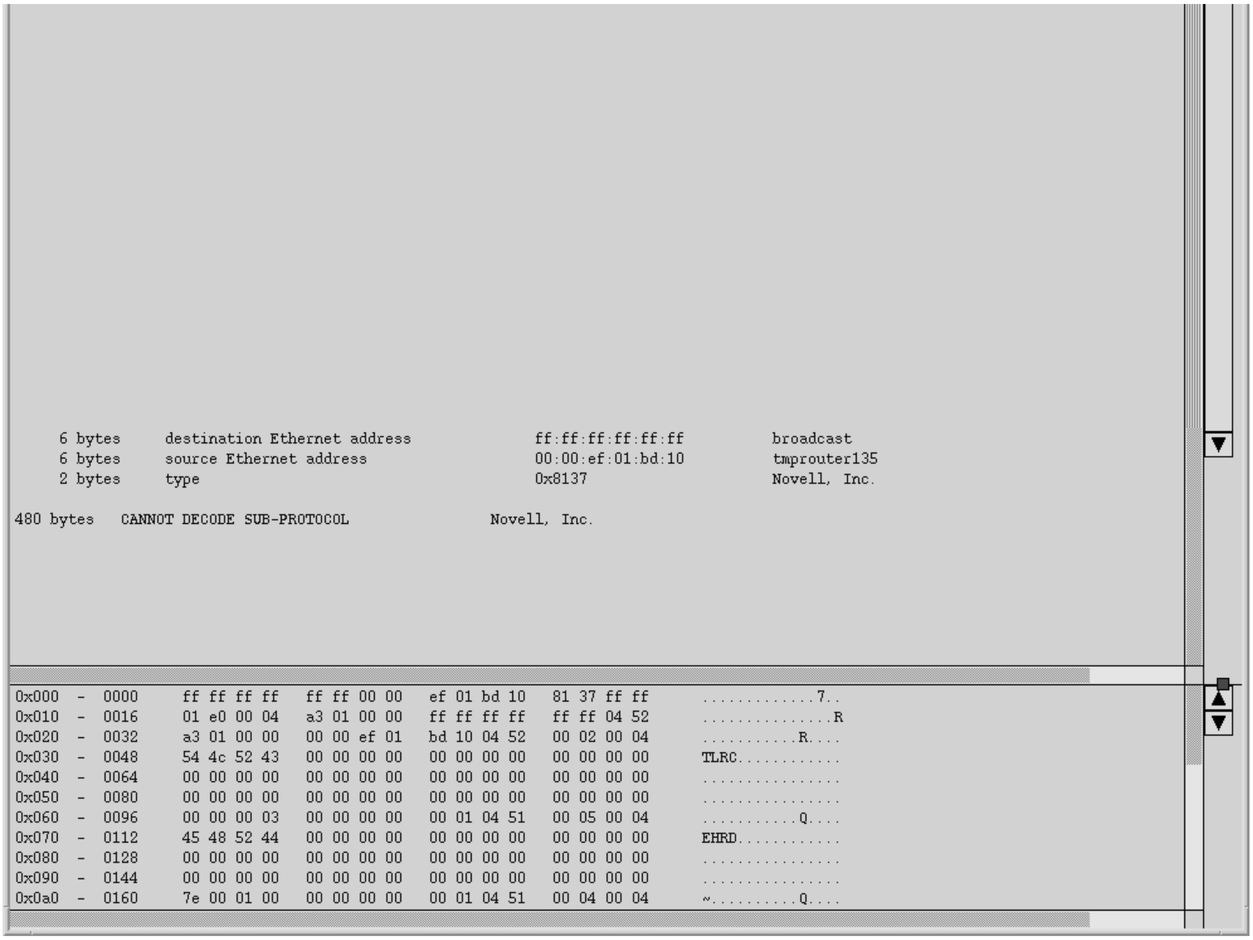
5.3.8 Print

Selecting the Print menu button with the left mouse button will print the ASCII text of the current packet that is being decoded to a file. When the menu button is pressed, a dialog box will be displayed as shown in Figure 5.3.8.1. Enter the filename of the file to save the text into in the text box and press the Start button to begin the print operation. Pressing the Cancel button removes the dialog box without printing any packets. The complete path to the file may be entered along with the filename in the text box. By default, files are saved in the current directory.

Figure 5.3.8.1. Print to File.

A packet must be selected in the top Packetman pane and packet decoding information must be showing in both of the bottom panes to use the Print menu item. Packetman will display an error message if no packet is selected. In secure mode, the same censored information that is shown on the display is also printed to the file.

5.4 Using the Packetman Packet Display



```
     6 bytes     destination Ethernet address            ff:ff:ff:ff:ff:ff         broadcast
     6 bytes     source Ethernet address                 00:00:ef:01:bd:10         tmprouter135
     2 bytes     type                                    0x8137                    Novell, Inc.

480 bytes   CANNOT DECODE SUB-PROTOCOL               Novell, Inc.
```

```
0x000  -  0000     ff ff ff ff   ff ff 00 00   ef 01 bd 10   81 37 ff ff      .............7..
0x010  -  0016     01 e0 00 04   a3 01 00 00   ff ff ff ff   ff ff 04 52      ...............R
0x020  -  0032     a3 01 00 00   00 00 ef 01   bd 10 04 52   00 02 00 04      ...........R....
0x030  -  0048     54 4c 52 43   00 00 00 00   00 00 00 00   00 00 00 00      TLRC............
0x040  -  0064     00 00 00 00   00 00 00 00   00 00 00 00   00 00 00 00      ................
0x050  -  0080     00 00 00 00   00 00 00 00   00 00 00 00   00 00 00 00      ................
0x060  -  0096     00 00 00 03   00 00 00 00   00 01 04 51   00 05 00 04      ...........Q....
0x070  -  0112     45 48 52 44   00 00 00 00   00 00 00 00   00 00 00 00      EHRD............
0x080  -  0128     00 00 00 00   00 00 00 00   00 00 00 00   00 00 00 00      ................
0x090  -  0144     00 00 00 00   00 00 00 00   00 00 00 00   00 00 00 00      ................
0x0a0  -  0160     7e 00 01 00   00 00 00 00   00 01 04 51   00 04 00 04      ~..........Q....
```