Interman 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. Interman is one of three tools in the Netman tool set. Interman provides a graphical display of TCP/IP network connections in real time. Each connection is color coded to show the dominant protocol that is being used. Interman also provides a set of tools for collecting information from TCP/IP hosts. This document is a comprehensive user's guide covering the capabilities and use of the Interman network monitoring tool.*

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

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

The Interman application was originally written at Curtin University in Western Australia. Version 1.2 of Interman was written at Texas A&M University in College Station, Texas. Interman is a graphical network discovery tool that shows real time TCP/IP communications between hosts on the Internet (or any other TCP/IP network).

4.1 Version 1.1

Interman 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 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 Interman written in Tcl/Tk is also provided with the version 1.2 distribution.

5.0 Using Interman

5.1 Requirements for Use

Version 1.2 of Interman 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*. Interman 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 Set User ID to 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 Interman. When the program is run Set User ID to 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 Interman in its non-secure mode, all other users are restricted to the secure mode of operation. All of the program's functions are available to the root user when running in non-secure mode. Only the secure mode of operation limits the functions that are available.

Interman 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, Interman should not be run on multi-user machines or machines that are being used as servers. If Interman is run on such a machine, it will cause an unacceptable loss in performance to other users. Excessive load or a slow machine will cause Interman to lose or "drop" packets. This packet dropping can cause problems with the accuracy of the network monitoring. Interman may not be able to provide a warning to the user when this occurs. The ideal environment for Interman is a fast, dedicated workstation with a color display.

Interman 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 Interman executable. These fonts are included with the Interman binary distribution.

5.2 Starting Interman

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

A Tcl/Tk launch script also is provided with Interman 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 Interman's command line options. It is not necessary to use this script to launch Interman; however, it provides a convenient way to set many options.

5.2.1 Command Line Switches

Interman supports a wide variety of options that can be used to customize the operation of the program. For convenient use of Interman from a shell script or other automated program, a large number of command line switches are provided to set these options before launching Interman. All of these options except -I can be changed from the internal menus once Interman 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 of these functions are available to a root user 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.). This command line switch allows the user to override Interman's choice of the workstation's network interface to open for promiscuous mode packet capture. Interman 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 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 Interman. Interman will not start if it cannot open the 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 -L link layer filter

Specify a data link layer packet filter. This command line switch allows the user to select one of Interman'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 Interman. 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
ICMP	ICMP (ARPA TCP/IP) Packets only
IP	IP (ARPA TCP/IP) Packets only

Figure 5.2.1.2.1. Link Layer Filters.

The following example sets Interman to only capture IP packets:

```
interman -L IP
```

5.2.1.3 -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 5.2.1.2). This switch allows the user to capture packets that are 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 Interman to capture only Ethernet packets with a frame type of 2048 (type 2048 will capture ARPA IP packets):

```
interman -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 Interman'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 Interman. 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 Interman to capture only TCP packets:

```
interman -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 Interman's built in application layer packet filters (some of these applications are not 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 Interman. 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
LPD	Line Printer Daemon Packets (LPD/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

WAIS	WAIS Packets (WAIS/TCP/IP) only
GOPHER	Gopher Packets (Gopher/TCP/IP) only
WWW	World Wide Web Packets (WWW/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

Figure 5.2.1.5.1. Application Layer Filters.

The following example sets Interman to capture only telnet packets:

```
interman -A TELNET
```

5.2.1.6 -U port #

Specify a custom UDP port number. This command line switch is used to capture 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]. Interman 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, Interman will still allow the packet through, but it may not be decoded correctly. The following example sets Interman to filter for UDP port 2049 (Port 2049 is used by the NFS protocol):

```
interman -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 capture packets based on a custom distinguished TCP port number. Figure 5.2.1.7.1 gives a partial listing of TCP port numbers [1]. Interman 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, Interman will still allow the packet through, but it may not be decoded correctly. The following example sets Interman to filter for TCP port 23 (Port 23 is used by the Telnet application):

```
interman -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 Interman 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 Interman to exit, so it should not be used in combination with any other command line switches.

5.2.2 Interman Launch Application

The Interman launch utility is a Tcl/Tk script that allows the user to set Interman's command line switches and start Interman with a graphical user interface. Most of the command line options can be specified with this tool. To start the Interman 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 5.2.2.1 shows the Netman launch utility program.

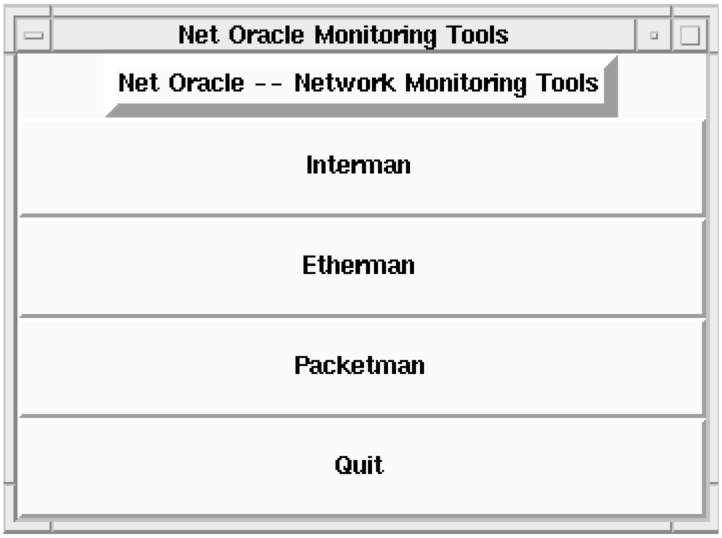

Figure 5.2.2.1. Netman Launch Utility.

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