PROBEwatch for Windows

User Manual

Part Number: AA–Q24FA–TE

June 1994

This manual describes how to install and operate PROBEwatch for Windows.

Revision/Update:	This is a new manual.
Operating System:	Microsoft Windows, Version 3.1 or higher
Software Version	PROBEwatch for Windows, Version 1.0

Digital Equipment Corporation
Maynard, Massachusetts

First Edition, June 1994

Digital Equipment Corporation makes no representations that the use of its products in the manner described in this publication will not infringe on existing or future patent rights, nor do the descriptions contained in this publication imply the granting of licenses to make, use, or sell equipment or software in accordance with the description.

This document was prepared using VAX DOCUMENT Version 2.1.

Contents

1 Introduction

2 Installation

3 Getting Started

4 Fundamentals of Operation

5 Domain View

6 Data Capture

7 Protocol Decode

8 Tools

9 Traps

A Running PROBEwatch for Windows with the SLIP Protocol

B MIB Groups and Communities

C Running PROBEwatch for Windows with a PATHWORKS Network

D Default Names

E PROBEwatch for Windows Troubleshooting

Index

Figures

Tables

Preface

This manual describes the installation and operation of PROBEwatch for Windows, a network diagnostic application that provides network users with the capability to collect performance data and to identify and isolate fault conditions in data communications networks.

Document Organization

This manual is comprised of the following:

- Chapter 1—Provides an introduction to PROBEwatch network diagnostic devices. Also provides information about the operational environment of PROBEwatch.
- Chapter 2—Provides information on installing PROBEwatch.
- Chapter 3—Provides information on getting started and using the top-level screen menu operations.
- Chapter 4—Addresses control entries and symbolic names used with PROBEwatch.
- Chapter 5—Explains how Domain View is a PROBEwatch function that provides all the power of the RMON–MIB standard while masking the details of the standard from the user.
- Chapter 6—Describes how the Data Capture utility sets up a DECpacketprobe agent to capture packets in a selective manner.
- Chapter 7—Defines Protocol Decode and shows how to use it.
- Chapter 8—Describes the PROBEwatch management tool called Discovery.
- Chapter 9—Defines traps and their uses.
- Appendix A—Describes how to run PROBEwatch for Windows with the SLIP protocol.
- Appendix B—Contains descriptions for each object within the RMON–MIB.

- Appendix C—Contains instructions for using PROBEwatch with a PATHWORKS network.
- Appendix D—Contains the default names and their related IDs for the network protocols that PROBEwatch recognizes.
- Appendix E—Contains instructions for troubleshooting PROBEwatch with a PATHWORKS network.

Conventions

This manual uses the following conventions:

<table>
<tr><th>Convention</th><th>Meaning</th></tr>
<tr><td>Return</td><td>A key name enclosed in a box indicates that you press that key. In this example, you would press the Return key only.</td></tr>
<tr><td><b>For Mouse Users</b></td><td></td></tr>
<tr><td>MB1</td><td>Mouse button one. Most operations relating to PROBEwatch for Windows are accomplished using MB1.</td></tr>
<tr><td>Click on</td><td>To press and release the mouse button when the pointer is positioned on an active object.</td></tr>
<tr><td>Drag</td><td>To press and hold the mouse button, move the mouse, and then release the button.</td></tr>
<tr><td><b>For Keyboard Users</b></td><td></td></tr>
<tr><td>Underline</td><td>Indicates the underlined letter on the screen menu item or option. These are designed for you to use if you do not have a mouse or do not want to use a mouse for accessing menu items. To access menu items without using a mouse, do the following:
<table>
<tr><th>To . . .</th><th>Press . . .</th></tr>
<tr><td>Access menu items</td><td>Alt and the underlined letter</td></tr>
<tr><td>Access options</td><td>Shift and the underlined letter</td></tr>
</table>
</td></tr>
</table>

Related Documentation

You can order the following documents from Digital:

Document Title	Part Number
Open DECconnect Building Wiring Components and Application Catalog	EB–K2407–42
DECconnect System Planning and Configuration Guide	EK–DECSY–CG
DECpacketprobe 90 User’s Guide	EK–DERMN–UM
Network Manager 200	QA–VM9AA–GZ

1

Introduction

PROBEwatch for Windows is a network diagnostic application that is compatible with the Remote Monitoring Management Information Base (RMON–MIB) standard. This client application is designed for use as a centralized network management station on a PC running Microsoft Windows, Version 3.1 or higher.

The PROBEwatch client operates in a distributed heterogeneous network with DECpacketprobe agents. These RMON–MIB agents collect and store statistical and message data on their network segments for use in PROBEwatch operations.

1.1 Function

With the DECpacketprobe agent, the PROBEwatch client provides support for:

- Nine Ethernet RMON–MIB groups
- Seven-layer protocol analysis

As a distributed system, the PROBEwatch client (with a DECpacketprobe agent) can:

- Collect a wide range of statistical data
- Display captured and fully decoded network traffic
- Set user-defined alarm conditions
- Obtain real-time updates from all segments of a widely dispersed internetwork from a centralized SNMP-compatible network management station

1.2 Standards

The PROBEwatch client is based on standards that enable operation in heterogeneous networks made up of multiprotocol, multitopology, and multivendor environments. PROBEwatch is based on the following standards:

Standard	Definition
Simple Network Management Protocol (SNMP)	Defines the protocol for all intercommunications between PROBEwatch and DECpacketprobe.
Remote Monitoring Management Information Base (RMON–MIB)	Defines the type of information that is to be gathered and made available to you for each network segment.

Also, the PROBEwatch client incorporates a variety of additional capabilities that are highly useful for network diagnostics but which have not yet been fully defined and accepted as network standards. These capabilities will be modified to correspond to generally accepted standards as the standards are developed and approved.

1.3 Basic Terms

You need to be familiar with the following basic terms to use PROBEwatch for Windows:

Term	Definition
DECpacketprobe Agent	A hardware/software device that is physically attached to a network segment. The agent accumulates statistical information regarding all packets that are on that segment. When commanded, the agent records and stores selected data traffic for further analysis. The agent provides complete statistical data regarding nodes on that segment. It provides partial or no information for nodes that reside on other network segments. For total coverage of all nodes, an agent must be installed on each segment.
Domain	A collection of one or more manageable entities (protocols). These entities include the industry-standard protocols listed in Section 1.6.1 or any user-defined protocols.
Ethernet	A LAN incorporating bus topology. Ethernet is based on IEEE standard 802.3.

Term	Definition
IP Address	An IP address is the four-byte address convention that uniquely identifies each node under SNMP. SNMP is the underlying protocol used for PROBEwatch communications.
IP Address Format	The format of the IP address is *X.X.X.X*, where *X* is one byte with a decimal value of 0 to 255. You must define the conventions for determining the IP address for the network or internetwork under your control.
Network	A network is a group of interconnected nodes that may communicate with one another and that use the same network addressing scheme. Multiple networks may be connected to form an internetwork. Data is passed from network to network by devices such as bridges, routers, and gateways on the basis of individual network addresses.
Node	A node is an individually addressable location on a data communications network. In RMON–MIB terminology, a *host* and a *node* are the same. A node may be any number of physical devices including personal computers, a larger scale server computer, a printer, and so on. A physical device may have multiple connections to a network and, therefore, may constitute multiple nodes.
PROBEwatch Client	A software application that implements the user interface function for retrieving and displaying all network and statistical data gathered by DECpacketprobe agents.
Segment	A segment is a network or subnet where all nodes are physically and logically connected in such a way that they receive all data traffic seen by all other nodes on the segment. A segment may be one of the following: One physical bus Nodes interconnected by repeaters The data traffic passes through the segment. All traffic does not pass through bridges, routers, or gateways because these devices logically separate networks.
Token Ring	A LAN incorporating logical ring and physical star topology. Ethernet is based on IEEE standard 802.5.

1.4 Protocol Structure

Protocols are the rules by which data communications devices such as the PROBEwatch client and DECpacketprobe agent carry out their communication process. The generalized model for protocol understanding is the Open Systems Interconnect (OSI) model.

1.4.1 OSI Model

The OSI model has seven layers. Each layer represents a particular subset of the communications process. The seven-layer model, shown in Figure 1–1, is often described as a “stack” or “suite.” You can identify network malfunctions by examining the detailed contents of these protocol stacks.

Figure 1–1 OSI Seven-Layer Model

```
--------------------------------------
             APPLICATION
--------------------------------------
             PRESENTATION
--------------------------------------
               SESSION
--------------------------------------
              TRANSPORT
--------------------------------------
               NETWORK
--------------------------------------
              DATA LINK
--------------------------------------
               PHYSICAL
--------------------------------------
```

Table 1–1 describes the functions for each layer in the OSI model.

Table 1–1 OSI Seven-Layer Functions

Layer	Function
Physical	The physical layer is responsible for the transmission of bit streams across a particular physical transmission medium. It involves a connection between two machines that exchange electrical signals.
Data Link	The data link layer performs the following: • Provides reliable data transmission from one node to another. • Shields higher layers from concerns about the physical transmission medium. It is concerned with the error-free transmission of frames of data.
Network	The network layer does the following: • Routes data from one network node to another. • Establishes, maintains, and terminates the network connection between two users. • Transfers data along the network connection. There can be only one network connection between two given users. However, there can be many possible routes to choose from when the particular connection is established.
Transport	The transport layer performs the following: • Provides data transfer between two given users. • Selects a particular class of service for monitoring transmissions once the connection is established. These transmissions maintain service quality. They also notify users if service quality is not maintained.
Session	The session layer provides the following: • Organizes and synchronizes the dialog between users. • Manages the data exchange between users. • Controls the sending and the receiving of data based on whether data can be sent and received concurrently or alternately.

(continued on next page)

Table 1–1 (Cont.) OSI Seven-Layer Functions

Layer	Function
Presentation	The presentation layer is responsible for the presentation of meaningful information to the network users. This may include any of the following: • Character code translation • Data conversion • Data compression and expansion
Application	The application layer allows application processes access to the system interconnection facilities. Once inside the interconnection facilities, the application processes can do the following: • Exchange information about services used to establish and terminate the connections between users. • Monitor and manage the systems being interconnected and the various resources they employ.

1.5 Frame Structure

Data transfer between the DECpacketprobe agent and the PROBEwatch client is implemented through data packets. The data packets are successively encapsulated by the information necessary to fulfill the requirements of each protocol layer. These encapsulated packets are referred to as *frames*. The format for an Ethernet frame is shown in Figure 1–2. Other transmission techniques are composed of similar frame segments with the specific protocols determining the detail.

Figure 1–2 Data Frame

```
+----------+-----------+------------+------------+-----------+-------+
| Preamble | Dest Addr | Source Addr | Length/Type | Data Field | Check |
+----------+-----------+------------+------------+-----------+-------+
```

Table 1–2 describes the frame structure.

Table 1–2 Frame Structure Description

Frame Segment	Description
Preamble	This segment provides synchronization and indicates the start of the frame. It is part of the physical transmission and is not logically part of the frame. The receiving device strips the preamble. The frame begins with the first byte of the destination address.
Destination Address	The six-byte address of the node that is receiving the frame.
Source Address	The six-byte address of the node that is transmitting the frame.
Length	The length of the packet presented as a byte count (ISO 8802.3 formatted packets).
Type	A value that is meaningful to higher network layers and is not defined as part of the Ethernet specification (Ethernet formatted packets).
Data Field	The data portion of the frame is passed to the data link layer by the client layer. It must be a multiple of eight bits. Ethernet defines a minimum frame size of 72 bytes and a maximum frame size of 1526 bytes, including the preamble. If the data to be sent is smaller than these sizes, it is the responsibility of the higher layers to pad it to the minimum frame size. If the data to be sent is larger than these sizes, it is the responsibility of the higher layers to break it into individual frames.
Check	Ethernet uses a frame check sequence to provide error checking. The field contains a cyclic redundancy check (CRC) value that is calculated from the other fields in the frame.

1.6 Protocol Analysis

The DECpacketprobe agent performs the following tasks:

- Captures network traffic in the form of frames from any operational PROBEwatch client.
- Screens and analyzes individual captured packets.

All data is captured at the individual segment by the attached agent. Data may be captured in the following ways:

- In promiscuous mode — All data packets on the segment are captured and stored.

- On a selective basis — User-created filters determine if a given packet is included in or excluded from the desired set.

1.6.1 Protocols Supported

The following industry-standard protocols are supported by the PROBEwatch protocol decode software. These protocols may be included in a domain.

APPAEP
APPAFP
APPARP
APPASP
APPATP
APPNBP
APPLDDP
APPLAP
APPPAP
APPRTMP
APPZIP
APPDSP
APPSDDP
CLNS
DECCTERM
DECDAP
DECDRP
DECLAT
DECLDATA
DECMOPDL
DECMOPRC
DECNSP
DECNICE
DECFOUND
DECSCP
DECSMB
DODARP
DODDNS
DODFTP
DODGGP
DODICMP
DODIP
DODNTB
DODNTDAT
DODNTNAM
DODRARP
DODSMB
DODSMTP
DODTCP
DODTFTP
DODTLNT
DODUDP
Ethernet
ES-IS
FTAM
IBMNETB
IBMSMB
IEEE802.2
IEEE802.3
IEEE802.5
ISO-Session
ISO-Presentation
NCP
NOVECHO
NOVERRP
NOVIPX
NOVRIP
NOVSPX
SNAFM
SNAPS
SNARHREQ
SNARHRES
SNARU
SNATH
SNAXID
SNMP
SUNMOUNT
SUNNFS
SUNPMAP
SUNRPC
SUNYP
TP 0/2/4
VINEMAIL
VINESARP
VINESICP
VINESIP
VINESIPC
VINESRTP
VINESMM
VINESSPP
VINESST
X400
XNSECHO
XNSERRP
XNSIPX
XNSPEXP
XNSRIP
XNSSMB
XNSSPX

1.7 Topology

The differences between the PROBEwatch client and the DECpacketprobe agent are as follows:

Category	Definition
PROBEwatch Client	The user station where operational commands are issued and where all results and diagnostic information are displayed. In a PROBEwatch client topology, it is feasible to have multiple clients active simultaneously within a single network.
DECpacketprobe Agent	A hardware/software device that is attached to a specific network segment. It gathers statistical information for that segment and provides a window into that segment. This lets you observe and gather network traffic information for more detailed analysis.

A typical network has multiple segments with each segment having its own agent. Agents communicate with clients using the SNMP protocol. This protocol follows one of the following paths:

Path	Definition
Inband	Uses the same network facilities as all other network nodes. For example, Ethernet.
Out of band	Uses a communications medium separate and distinct from the user network. For example, EIA–232.

2
Installation

PROBEwatch for Windows can be installed as a standalone Windows application. Once loaded, it provides communications with remote DECpacketprobe agents that may be on segments throughout a distributed network.

2.1 Hardware Requirements

The following hardware is required to install PROBEwatch for Windows:

- A 386 processor running at a minimum of 33 megahertz, or a 486 processor running at a minimum of 25 megahertz.
- A minimum of 8 megabytes of random-access memory (RAM). Additional memory improves performance.
- A 3½-inch 1.44-megabyte diskette drive.
- A minimum of 12 megabytes of available disk space.
- A mouse that is compatible with Windows 3.1. It is recomended that you use a mouse with PROBEwatch. If you do not use a mouse, you will not have point-and-click control.
- A network interface card (NIC) for inband communications. You must have an NDIS driver for your card.
- A color VGA or SVGA monitor.
- An Ethernet port (16-bit adapter recommended).

The following hardware is optional:

- A printer supported by Windows. PROBEwatch supports all the devices listed in the Windows Printer Setup. If you use a driver that is not part of the Windows package, you may need to install it as an unlisted device.

PROBEwatch should be able to accommodate any configuration that meets the hardware requirements. For details on specific devices and software packages recommended for Microsoft Windows, refer to the Windows Version 3.1 Applications Reference List and Hardware Compatibility List.

2.2 Software Requirements

You need the following software to install PROBEwatch for Windows:

- MS–DOS Version 5.0 or higher
- Microsoft Windows Version 3.1 or higher
- An NDIS driver for the Ethernet adapter board

2.3 PROBEwatch Kit Contents

The PROBEwatch kit should contain the following items:

- PROBEwatch software on two 3½-inch, 1.44-megabyte diskettes.

  A README.TXT file provides information about product features, and may contain last-minute installation information. Please read this file before installing PROBEwatch.
- *PROBEwatch for Windows User Manual* (this book)

2.4 Installing PROBEwatch

To install PROBEwatch for Windows:

1. Turn on your personal computer (PC) and run Windows.
2. Put the PROBEwatch diskette, labeled *Disk 1* in drive A (or B as appropriate).
3. Choose the Run option from the Program Manager’s File menu.
4. Enter the following in the Command Line field of the Run dialog box:

   ```
   A:\install
   ```
5. Click on OK.

   An informational screen is displayed.
6. Click on OK

The PROBEwatch installation Main Menu is displayed. Table 2–1 shows the menu choices.

Table 2–1 PROBEwatch Installation Main Menu Choices

Choice	Result
Install PROBEwatch and network	Installs PROBEwatch; installs and configures the network. If you want, this option will update AUTOEXEC.BAT and install the PROBEwatch icon.
Install PROBEwatch only	Installs PROBEwatch and, if you want, will automatically update AUTOEXEC.BAT and install the PROBEwatch icon. If your PC does not have an IP network, you can install PROBEwatch, but you cannot run PROBEwatch without an IP network. Your network must provide WINSOCK.DLL
Install and configure the network	Installs and configures an IP network on your PC.
Install PROBEwatch Icon	Creates an icon for starting PROBEwatch and allows you to place it in an existing Windows icon group or in its own group. The alternative to starting PROBEwatch with an icon is to run NSMAN.EXE from the File Manager.
Set Network Configuration Parameters	Allows you to modify your network configuration parameters.
Exit	Exits from the installation menu.

The following steps assume you are installing both PROBEwatch and the network. The steps for installing only PROBEwatch or only the network are a subset of these steps.

Press Esc to cancel the installation procedure and return to the procedure's Main Menu at any time.

7. Choose Install PROBEwatch and the network and click on OK.
8. Choose the drive where you want the files to reside.

   A dialog box asks you to choose the drive you want the PROBEwatch files installed on. Click on OK.
9. Choose the directory where you want to install PROBEwatch.

   A dialog box asks you to choose the directory and displays the default directory C:\ PROBEW. If you choose a nonexistent directory, the procedure creates it for you. The procedure also creates subdirectories under the main directory.

The procedure copies the files to the directory. If you have previously installed the PROBEwatch IP network, a dialog box informs you that a file named PWTCP.INI already exists and asks if you want to replace it. That file contains the network configuration parameters. Do not replace it, if you intend to change only one or two of your network configuration parameters. You will have the opportunity to change them later in the installation procedure.

2.4.1 Install Icon

Once the PROBEwatch files are installed, or by choosing Install PROBEwatch Icon from the Main Menu, the Install Icon menu is displayed. This section of the install procedure also allows you to set the network configuration parameters, select the network you will be using with PROBEwatch, and select your network card. Table 2–2 shows the menu choices.

Table 2–2 Install Icon Menu Choices

Choice	Result
Install in PROBEwatch Windows group	Creates the PROBEwatch icon and the PROBEwatch application group. When you open Windows, the PROBEwatch group will be the top group.
Install Icon in an Existing Group	Displays a list of the existing Windows applications groups. When you select a group, the procedure creates the PROBEwatch icon and places it in the selected group.
Do Not Install Icon	Unless you already have an icon for PROBEwatch, you must start PROBEwatch by running NSMAN.EXE from the File Manager.

1. Choose your Install Icon option and click on OK.

   The Set Network Configuration Parameters dialog box appears. The tab key will move the cursor between fields. Supply the following information, which you can obtain from your system or network administrator:

   a. The name of your PC

   b. The IP address of your PC

   c. The IP address of the default gateway (a router or brouter)

   d. Your local IP domain name

   e. The IP address of the network name server

   f. The network subnet mask

   g. Your user name

2. Enter the information and click on OK.

   A confirmation screen lists your choices and gives you a chance to make corrections if necessary. If everything is correct, click on Yes.

   A dialog box asks you to specify the type of network you will be using. Table 2–3 shows the choices available.

Table 2–3 Types of Networks Available for PROBEwatch

Choice	Description
NDIS network and SLIP	Sets up NDIS and SLIP services.
SLIP network only	Sets up SLIP service only.

3. Choose the type of network you will be using and click on OK.

   Generally, you will want to install both NDIS and SLIP. If you selected an NDIS network, a dialog box asks you to specify the type of network card you will be using. Table 2–4 shows the choices available for the network card.

Table 2–4 Network Card Options

Choice	Description
EtherWORKS 3 network card	Places the driver EWRK3.DOS and the data file EWRK3.PRO in the \IPSTACK subdirectory of your PROBEwatch directory.
Ethernet (DEPCA) network card	Places the driver DEPCA.DOS and the data file DEPCA.PRO in the \IPSTACK subdirectory of your PROBEwatch directory.
Other	Choose this option if you plan to use a non-Digital network card. When you choose this option, a dialog box asks you to supply the path to and the name of the driver for your network interface card. If you choose Other, you may need to merge the PROTOCOL.INI that PROBEwatch creates with the PROTOCOL.INI file supplied with your NDIS driver.

4. Choose the type of network card you will be using and click on OK.

   If you chose Other, a dialog box asks you to supply the path and filename for the network interface card driver. Enter the information and click on OK.

A dialog box appears informing you that to use PROBEwatch you must first start your new network by running the STRTNDIS.BAT file, if you installed an NDIS network or STRTSLIP.BAT, if you installed a SLIP network only. The dialog box asks whether you want the command to run the file added to AUTOEXEC.BAT. If you do not put the network startup command in AUTOEXEC.BAT, you will have to remember to execute the command before running PROBEwatch.

Although choosing to install an NDIS network also enables you to run a SLIP network, you cannot automatically add the STRTSLIP startup command to AUTOEXEC.BAT or AUTOEXEC.EXM, unless you choose to install a SLIP network only.

5. Choose whether to put the network startup command in AUTOEXEC.BAT or AUTOEXEC.EXM.

   A dialog box informs you that changes may be necessary in your AUTOEXEC.BAT and CONFIG.SYS files. Table 2–5 shows the choices available for modifying AUTOEXEC.BAT and CONFIG.SYS.

Table 2–5 Choices for Modifying AUTOEXEC.BAT and CONFIG.SYS

Choice	Result
Go Ahead and Modify	The procedure creates a backup of the file with the extension *0x*, where *x* is an interger. Then it asks you for the information it needs and edits the file.
Create Example Files	The procedure allows you to modify the file, but assists you by first creating a sample file with the extension AUTOEXEC.EXM and CONFIG.EXM. If you select this option, you must remember to make the modifications yourself, when you exit from the installation procedure.
Bypass these changes	The procedure does not modify or create any files. Select this option *only* if you have previously installed PROBEwatch, and you chose the same drive and directory this time.

6. Choose your option for modifying the system files and click on OK.

   A dialog box asks you to indicate the drive from which the systems boots. This is the drive whose root directory contains the AUTOEXEC.BAT and CONFIG.SYS files.

7. Enter the boot drive and click on OK.

   Dialog boxes display the paths to the AUTOEXEC.BAT and CONFIG.SYS (or AUTOEXEC.EXM and CONFIG.EXM) file and allows you to modify the paths, if necessary.

8. Indicate the correct paths and click on OK.

   A list of the files modified by the installation procedure appears, including files created by the procedure.

9. Click on OK to dismiss the list of files.

   The Main Menu is displayed.

10. Choose Exit and click on OK.

    If you installed a network, a message informs you to run the network startup file (STRTNDIS.BAT or STRTSLIP.BAT, depending on the type of network you choose) to connect your PC to the network.

11. Click on OK to dismiss the message.

    If you choose to modify AUTOEXEC.BAT yourself, a message reminds you to do it before starting PROBEwatch.

    If you modified AUTOEXEC.BAT, a message reminds you to reboot your computer. The modifications do not take effect until you reboot.

2.5 Checking the PROBEwatch Directory Structure

The PROBEwatch installation procedure creates a default directory structure. Unless you specified otherwise, you should have the directories shown in Table 2–6.

Table 2–6 Default PROBEwatch Directory Structure

Directory	Contents
C:\ PROBEW	NSMAN.EXE and other files used by PROBEwatch, with the following directories.
C:\ PROBEW\ IPSTACK	The network service files, if you installed the PROBEwatch network.

3
Getting Started

This chapter describes how to start PROBEwatch for Windows and provides an overview of the operations you can perform.

3.1 Starting PROBEwatch for Windows

Your network must be running before you can start PROBEwatch for Windows. If you installed PROBEwatch and network, and allowed the install procedure to modify your AUTOEXEC.BAT and CONFIG.SYS files, the network will start automatically. If you installed your network using the PROBEwatch installation procedure, start your network using one of the following methods:

- If you are using an NDIS network, start the network with the following command:

  ```
  PROBEwatch_drive:\PROBEwatch_path\IPSTACK\STRTNDIS
  ```

  For example:

  ```
  C:\PROBEW\IPSTACK\strtndis
  ```

- If you are using a SLIP network, start your network using the procedure described in Appendix A.
- If you are using a PATHWORKS network, you may need to start your network using the procedure described in Appendix C.

3.1.1 Editing the HOSTS. File

To start PROBEwatch, you must supply information about the probes that PROBEwatch will use to monitor the network. If you do not have an active IP Name Server, then the information must be put in the HOSTS. file. The HOSTS. file resides in the \PROBEW\IPSTACK directory. The format of the HOSTS. file is as follows:

```
IP Address  Host Name  Alias  Comments
```

The components of the HOST. file are separated by tabs or spaces.

Table 3–1 HOST. File contents

Field	Description
IP Address	IP Address of the probe.
Host Name	Name of the probe. The name must match the name given when adding agents in the top level PROBEwatch screen.
Alias	One or more Alias names may be associated with a probe. This field is optional.
Comments	Comments about the probe. The # character is a comment field delimiter. Any data on the same line, after this character, will be ignored. This field is optional.

In order to run PROBEwatch, you must at least supply the IP address and Host name of one DECpacketprobe.

3.1.2 Invoking PROBEwatch

To start a PROBEwatch session, do the following:

1. Start MS Windows
2. From the Program Manager window, double click on the PROBEwatch group icon.
3. From the PROBEwatch window, double click on the PROBEwatch icon.

Double clicking on the PROBEwatch icon causes the PROBEwatch top screen to display. Using the Add function of this screen, the user then must enter the names of the DECpacketprobe agents which are to be managed and must enter the appropriate parameters for colors and description. Section 3.2.1 contains the necessary steps to add an agent.

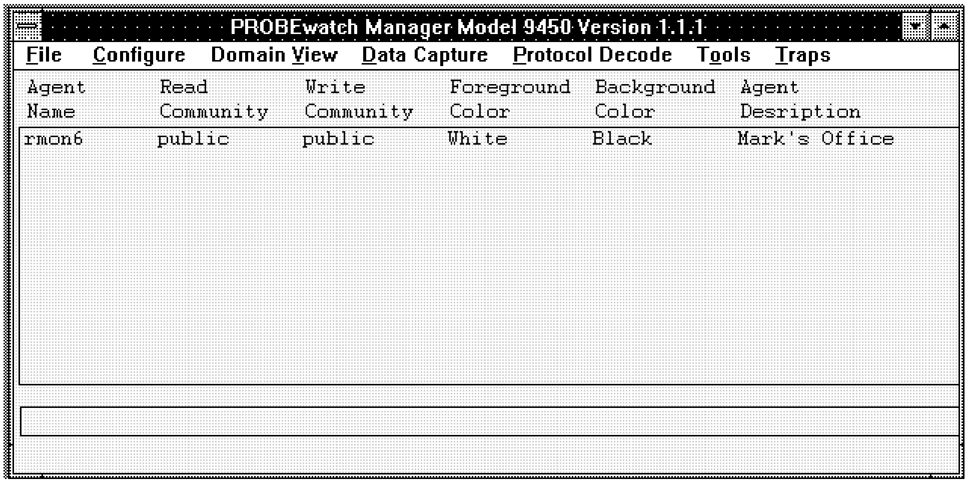
Once the top screen has been brought up using the above procedure and an agent has been added, you may perform virtually all PROBEwatch functions as described in the manual.

3.2 Top-Level Operations

The PROBEwatch Management System top-level menu is the beginning point for all PROBEwatch operations. Figure 3–1 displays the PROBEwatch Management Screen. The menu choices are as follows:

File
Configure
Domain View
Data Capture
Protocol Decode
Tools
Traps

Figure 3–1 PROBEwatch Management Screen



Agent Name	Read Community	Write Community	Foreground Color	Background Color	Agent Desription
rmon6	public	public	White	Black	Mark's Office

LJ-03565-SIX

In addition, the screen contains a summary listing of all currently defined agents. The bottom section of the window, at various times, will contain messages. You may also, under the Configure pull-down menu, select Add Agent, Change Agent, and Delete Agent to modify agent definitions.

3.2.1 Add Agent

To add a new agent entry:

1. Pull down the Configure menu and click on Add Agent.

   The Add Agent screen is displayed.

2. Enter the required information into all fields. The name of the agent must match a name that is configured on your IP Name Server or one that is in the HOSTS. file.

3. Select any color combination with good contrast.

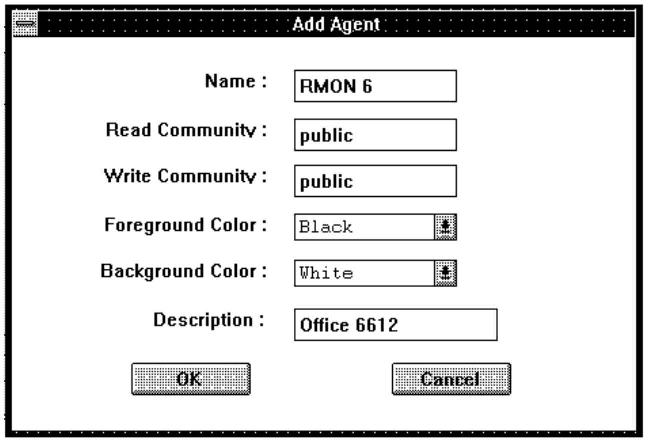
4. Click on OK.

Note

You can click on Cancel at this point to discontinue the operation, make no change, and exit the screen.

Figure 3–2 shows the Add Agent screen.

Figure 3–2 Add Agent



Add Agent

Name : RMON 6

Read Community : public

Write Community : public

Foreground Color : Black

Background Color : White

Description : Office 6612

LJ-03566-SIX

Table 3–2 describes the Add Agent screen selections.

Table 3–2 Add Agent Screen Selections

Entry	Definition
Agent Name	The name from the /PROBEW/HOSTS. file or IP Name Server.
Read Community	A basic term to SNMP. It defines a collection of devices that are authorized to communicate with one another. For purposes of PROBEwatch, the community defaults to "public." This entry displays the community for the Client.
Write Community	A basic term to SNMP. It defines a collection of devices that are authorized to communicate with one another. For purposes of PROBEwatch, the community defaults to "public." This entry displays the community for the Agent.
Foreground Color	The name of the foreground color selected for this agent.
Background Color	The name of the background color selected for this agent. Each agent should have a different background color for easy identification when multiple sessions are under way.
Agent Description	A character string that logically identifies the selected agent. It would typically have some reference to the segment the agent is connected to.

3.2.2 Change Agent

Selecting Change Agent lets you change any of the agent parameters. The Change Agent screen is the same as the Add Agent screen.

3.2.3 Delete Agent

Selecting Delete Agent removes that agent entry after you click on Yes on a confirmation screen.

3.3 Domain View

A domain is a collection of one or more manageable entities (protocols). These entities include many industry-standard protocols. The Domain View application subdivides the network into a series of "domains" that are logical subsets of the entire segment accessed by a DECpacketprobe agent. For example, a domain may be "all," "TCP only," "DECnet only," "SNA only," or any other logically defined subset of the segment. The Domain View application includes the full functions necessary to define the domain under study. In a typical network application, multiple domains may be operating simultaneously, gathering statistical information and data pertinent to that subset of the network.

The Domain View function provides an English-language interface. It allows access and display of all the statistical information available from the RMON–MIB agents. Knowledge of the RMON–MIB standard definitions is not required. The Domain View application also provides access to a highly flexible graphing mechanism called Quick Graph. This allows you to graphically display a wide variety of network statistics in multiple formats.

See Chapter 5 for more details.

3.4 Data Capture

The Data Capture function allows you to do the following without reference to specific RMON–MIB groups:

- Select a logical filter definition
- Capture data
- Perform full seven-level protocol decode on the captured data in a quick and easy manner

Data Capture emulates the operation of widely available portable LAN analyzers. It performs the capture function on remote network segments but displays the results locally.

Data is captured at the individual segment level by the attached agent. Data may be captured in one of two ways:

- In promiscuous mode—All data packets on the segment are captured and stored.
- On a selective basis—User-selected filters determine if a given packet is to be included in or excluded from the desired set.

Table 3–3 describes the functions available through Data Capture.

Table 3–3 Data Capture Functions

Function	Description
Packet Capture	Acting under the control of selected filters, matched packets are captured and stored. This function allows you to define the means and extent of the data to be captured for a selected agent. Multiple inclusive or exclusive filters may be applied to any given capture sequence. Packet sizes may be controlled to conserve memory space and to limit decoding displays to the initial portion of the packet that contains most of the pertinent information. Buffer sizes may be user-selected and may wrap or stop when full.
Protocol Decode	When data has been captured by an agent and transmitted to the client, this function allows you to select individual packets for display and decode. Display may be in raw or HEX mode, or in decoded ASCII characters for each of the seven layers. The resulting display may be color-coded under your control for each layer.

See Chapter 6 for more details.

3.5 Protocol Decode

The Protocol Decode function is accessed from the top screen without any relation to a specific agent. Use this function when you have collected data files from previous data capture sessions and stored the data in files at the client. You can directly access these files and perform complete protocol decode as required. Under certain circumstances, data files may be imported from other devices by way of ftp transfer and then be subjected to protocol decode as if they came from a network agent. See Chapter 7 for more information.

3.6 Management Tool: Discovery

The Tools pull-down menu contains one option, Discovery.

Statistics in the RMON–MIB standard are based on the following unique identifier for the hosts in the network: the interface MAC address. Unfortunately for most users, the MAC address is not a logically useful identifier because data is not presented in a usable format. Therefore, cumbersome translations must be made.

The Discovery application is a background program that learns both the IP address and the logical name of the hosts on a segment. It allows data to be presented on the basis of the logical name or the IP address, both of which are more meaningful. See Chapter 8 for more details.

3.7 Traps

Trap messages caused by alarm and event conditions may be generated by any agent in the network and reported to a centralized management station. The Traps screen allows you to access a listing of the trap messages sent by any SNMP agent in the network to your PROBEwatch station. The trap messages are composed of all messages sent since the last time the client function was initiated. Trap messages are also logged at the local agent. They may be accessed by an inquiry to the specific agent. See Chapter 9 for more details.

4

Fundamentals of Operation

To make use of agents with PROBEwatch for Windows, you should understand how they operate. This chapter addresses the fundamentals of manipulating RMON–MIB agent activities and relates how PROBEwatch establishes control.

4.1 Control Entries

A DECpacketprobe agent can perform several tasks simultaneously, collecting data on a segment while collecting statistics for underlying EtherStats counters, for instance. At the same time, an agent may also be under the direction of multiple clients or users for which it is performing different tasks.

Note

To avoid conflicts, only one client application should make the settings on an agent.

Since multiple agent activities may be occurring simultaneously, you need a way to create, start, and stop any specific activity. Within the context of the RMON–MIB, this is done by establishing a *control entry.* The collection of specific statistics is enabled by creating and applying a control entry in the appropriate group and is disabled by deleting the corresponding control entry. An RMON–MIB agent collects real-time statistics on behalf of each control entry.

Once a control entry has been created and applied, the agent associated with that entry continues to collect the data specified until the control entry is deleted or some other limitation such as memory availability is reached. Counters wrap upon reaching their maximum count and data buffers stop when full or wrap, depending on user-entered parameters for that entry.

In PROBEwatch Domain View functions, control entries are automatically established based on the activity initiated by you. You can see the control entries associated with Domain View operations in the View Control screens for each group. See Chapter 5 for details.

4.2 Common Terms

The following common terms, related to control entries, are used by the RMON–MIB standard:

- Index
- Data source
- Status
- Owner

These widely used terms are defined in the following sections. There are other terms used only in a few selected groups. A detailed definition of these other terms is included in the context of the screens.

4.2.1 Index

The index is the number that uniquely identifies a control entry. When adding a new entry, you must insert a number that identifies it. A common convention is to use the next unused number in an ascending sequence. However, you can use any number not already in use. Numbers may range from 1 to 65535. Entries are listed in numerical order on the summary screen. A duplicate index number causes a fault message to display on the Add screen and requires a new selection.

As a convention, PROBEwatch control entries are in the range of 1 to 16383. When you access the Create screen for a control entry, an index number is automatically entered on the screen. This index number is the next highest number associated with the existing control entries. You may choose to use this number or overwrite it with your own number. For reference, Domain View index numbers start at 49152 and extend to 65535.

4.2.2 Data Source

A data source is a MIB object identifier that identifies the particular interface on the agent from which the control entry is set up to collect data. The data source for a particular agent is interface 1, which is designated as:

```
ifIndex1
```

Note

The DECpacketprobe agent supports one interface only.

4.2.3 Status

This function indicates that a control entry is one of the following:

Entry	Description
Valid (1)[1]	The entry is active.
Invalid (4)[1]	The entry is inactive.
Create Request (2)[1]	The entry is in the process of creation.

[1] The corresponding integer value from the RMON–MIB standard is shown in parentheses.

4.2.4 Owner

The owner is a user-inserted logical identifier. This is an alphanumeric combination that identifies the person responsible for the control entry. This is used for administrative purposes only.

5
Domain View

PROBEwatch Domain View is a DECpacketprobe client application that provides all the power of the RMON–MIB standard but which masks the details of the RMON–MIB from the user. Most users will find the Domain View mode of operation both easier to work with and sufficiently powerful and varied to perform almost all network diagnostic functions.

You can select one or more domains for which network traffic is to be concurrently collected. Domains can be defined using any combination of filters supported by the RMON–MIB.

Internally, a domain consists of a channel and the supporting filters that together define some subset of network traffic. Agent control tables for statistics, history, host, matrix, and packet capture are automatically attached, as required, to a specific domain using the underlying channel as the data source.

Domain View takes advantage of the ability of DECpacketprobe agents to support the use of a channel as a data source for the host, matrix, statistics, and history groups. This capability allows a wide range of statistics to be gathered for a user-defined subset (domain) of network traffic.

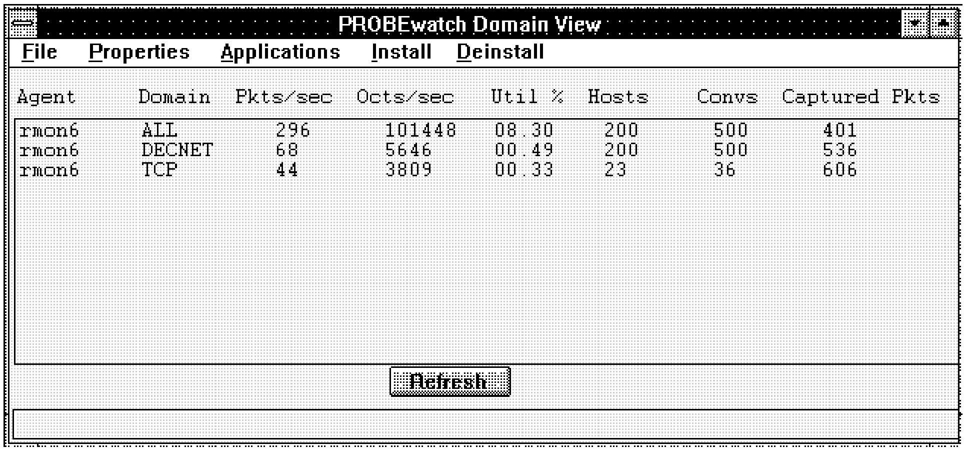
5.1 Operation

Starting from the top screen of PROBEwatch, highlight the agent of interest by clicking on the entry in the agent list and then on Domain View. The selection screen for Domain View functions is displayed showing a variety of menu items. The choices are:

File
Properties
Applications
Install
Deinstall

In addition, the screen contains a field showing a list of currently defined domains with summarized statistical information. This field is called the Agent Summary. Figure 5–1 shows the Domain View screen.

Figure 5–1 Domain View Screen



```
Agent     Domain   Pkts/sec  Octs/sec  Util %  Hosts  Convs  Captured Pkts
rmon6     ALL        296     101448    08.30    200    500     401
rmon6     DECNET     68      5646      00.49    200    500     536
rmon6     TCP        44      3809      00.33    23     36      606
```

LJ-03567-SIX

The Agent Summary provides a display of statistics for domains associated with the selected agent in tabular form, with one line per domain. The display is updated every update period as established in the Domain View Properties screen. A pushbutton, Refresh, allows you to update the display after entering the screen to ensure all changes made after entering the Agent Summary screen are included in the current display.

Table 5–1 describes the information included for each agent/domain on the Domain View screen.

Table 5–1 Domain View Screen Fields

Field	Description
Pkts/Sec	Calculated over the update period from etherStatsPkts, that is: $\frac{\text{etherStatsPkts(end) - etherStatsPkts(start)}}{\text{<properties.update\_period>}}$ If the Statistics option is not enabled for the agent/domain, "—" is displayed in place of a value.
Octets/Sec	Calculated over the update period from etherStatsOctets (tokenPStatsOctets). If the Statistics option is not enabled for the agent/domain, "—" is displayed in place of a value.
Utilization %	The average percentage network utilization during the period. For 10 Mbit/sec Ethernet, utilization is calculated as: $\frac{\text{octets} + (8 * \text{pkts})}{\text{seconds} * 12500}$ For 4 Mbit/sec Token Ring, utilization is calculated as: $\frac{\text{octets} + (6 * \text{pkts})}{\text{seconds} * 5000}$ For 16 Mbit/sec Token Ring, utilization is calculated as: $\frac{\text{octets} + (6 * \text{pkts})}{\text{seconds} * 20000}$ The calculations include the overhead per frame. For Ethernet, this is the 8-octet preamble. For Token Ring, this includes 3 octets of delimiter (SD, ED, and FS) per packet, plus one 3-octet token between each packet. If the Statistics option is not enabled for the agent/domain, "—" is displayed in place of a value.
Hosts	The number of hosts in the host table. "(Full)" is displayed after this count if the host table is full. If the Host/Conversation option is not enabled for this agent/domain, "—" is displayed in place of a count.
Conversations	The number of matrices in the matrix table. "(Full)" is displayed after this count if the matrix table is full. If the Host/Conversation option is not enabled for this agent/domain, "—" is displayed in place of a count.

(continued on next page)

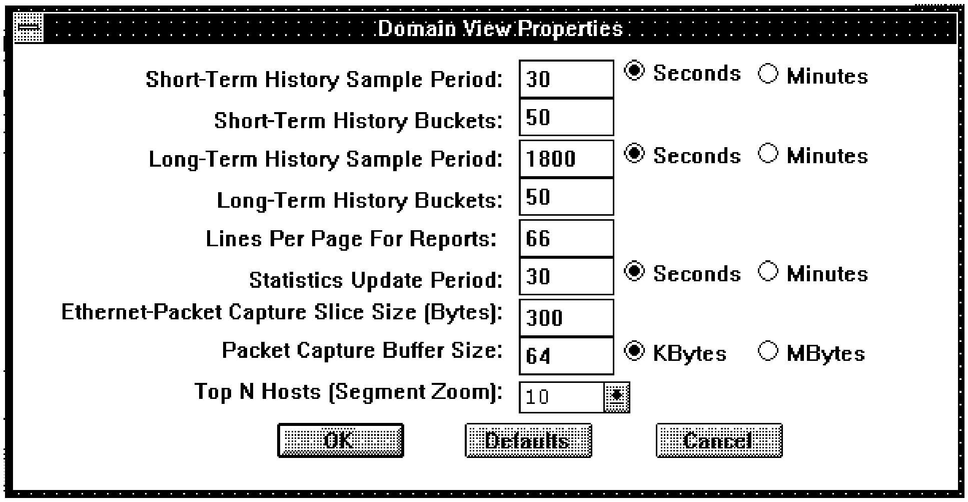
Table 5–1 (Cont.) Domain View Screen Fields

Field	Description
Captured Packets	The number of captured packets available in the capture buffer. "(Full)" is displayed after this count if the capture buffer is full. If the Packet Capture option is not enabled for this agent/domain, "—" is displayed in place of a count.

5.2 Properties

Properties lets you adjust a number of Domain View parameters to your own taste. Factory default settings can be restored at any time. Current values are stored in a disk file named "PROPERTY.DV," and any changes you make are saved to this file when you click on the OK button, after verification against acceptable ranges. Figure 5–2 screen shows a Domain View Properties screen.

Figure 5–2 Domain View Properties Screen



Short-Term History Sample Period: 30 ● Seconds ○ Minutes

Short-Term History Buckets: 50

Long-Term History Sample Period: 1800 ● Seconds ○ Minutes

Long-Term History Buckets: 50

Lines Per Page For Reports: 66

Statistics Update Period: 30 ● Seconds ○ Minutes

Ethernet-Packet Capture Slice Size (Bytes): 300

Packet Capture Buffer Size: 64 ● KBytes ○ MBytes

Top N Hosts (Segment Zoom): 10

LJ-03568-SIX

5.2.1 Operation

From the Domain View screen, click on Properties. The setup screen for entering Properties is displayed.

The Properties screen includes three action modes: OK, Defaults, and Cancel. In addition, entry fields are presented which allows you to set up the background properties. Fields that may be changed are shown on the screen within boxes. You enter the desired information in each field and then click on OK. This initiates an SNMP session, which instructs the selected agent to set values in accordance with the properties definition. The fields that may be changed are described below. Several of the fields include time selection options in seconds or minutes and one, Packet Capture Buffer, includes a size option in Kbytes or Mbytes. Standard default conditions are preselected.

Table 5–2 contains a description of each entry on the Domain View Properties screen.

Table 5–2 Domain View Properties

Field	Description
Short-Term History Sample Period	The time interval between successive samples. The default is 30 seconds and the acceptable range is 5 to 1800.
Short-Term History Buckets	The number of samples that will be stored at any given time by the agent for retrieval and display. The default is 50 and the acceptable range is 5 to 1800.
Long-Term History Sample Period	The time interval between successive samples. The default is 1800 seconds (30 minutes) and the acceptable range is 5 to 1800.
Long-Term History Buckets	The number of samples that will be stored at any given time by the agent for retrieval and display. The default is 50 and the acceptable range is 5 to 1800.
Lines per Page for Reports	The number of line entries shown when the data is displayed. The default is 66 and the acceptable range is 10 to 999999.
Statistics Update Period	The refresh rate of the selected data screen in seconds. The default is 30 and the acceptable range is 10 to 1800.
Ethernet Packet Capture Slice Size (Bytes)	The maximum number of bytes to be captured and stored for each Ethernet packet. The default is 1518 bytes and the acceptable range is 14 to 1600.

(continued on next page)

Table 5–2 (Cont.) Domain View Properties

Field	Description
Packet Capture Buffer Size	The maximum number of bytes to be stored in the capture buffer for a packet capture sequence. The default is 65536 bytes and the acceptable range is 16 Kbytes to 2 Mbytes.
Top N Hosts (Segment Zoom)	The number of line entries shown when the data for top N hosts is displayed. The default is 10 and the acceptable values are 5, 10, 15, 20, and 25.

After entering the changes in the Domain View Properties screen, click on OK to establish the new parameters. The Cancel button restores the parameter settings that were current when you opened the window and effectively cancels any changes made. The Defaults button re-establishes the default values that are factory pre-established.

5.3 Applications

You can access the majority of Domain View functions through the Applications menu on the Domain View screen. The selections from the Applications menu are:

- Segment Zoom
- Host List
- Conversation
- View Packets
- WatchDog

The following sections describe them in detail.

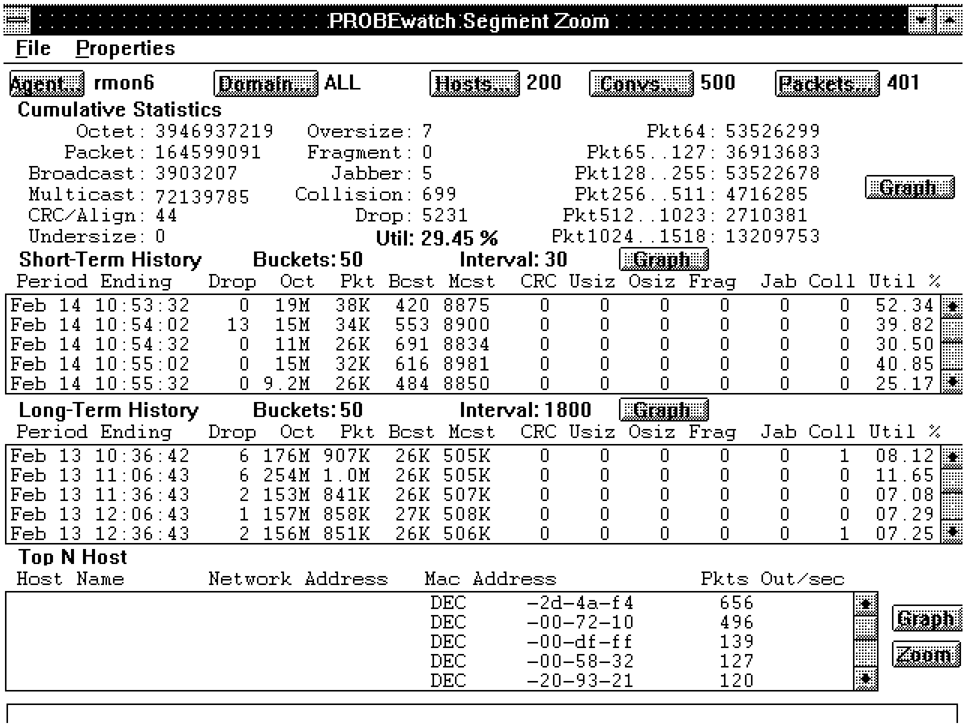
5.3.1 Segment Zoom

Segment Zoom is intended to display much of the statistical information available from a particular agent regarding a single domain. You select the agent and domain from the Agent Summary listing by clicking on the entry in the summary field. Most of the fields are refreshed every update period.

5.3.1.1 Operation

From the Domain View screen, highlight the agent/domain to be displayed by clicking on that entry in the Agent Summary. Click on Applications and click on Segment Zoom. The screen showing a full complement of summary statistical information for the selected agent/domain is displayed. Figure 5–3 shows a Segment Zoom screen.

Figure 5–3 Segment Zoom Screen



Agent... rmon6 Domain... ALL Hosts... 200 Convs... 500 Packets... 401

Cumulative Statistics

```
     Octet: 3946937219   Oversize: 7              Pkt64: 53526299
    Packet: 164599091    Fragment: 0         Pkt65..127: 36913683
 Broadcast: 3903207        Jabber: 5        Pkt128..255: 53522678
 Multicast: 72139785    Collision: 699      Pkt256..511: 4716285
 CRC/Align: 44               Drop: 5231    Pkt512..1023: 2710381
 Undersize: 0          Util: 29.45 %      Pkt1024..1518: 13209753
```

Short-Term History Buckets: 50 Interval: 30

Period Ending	Drop	Oct	Pkt	Bcst	Mcst	CRC	Usiz	Osiz	Frag	Jab	Coll	Util %
Feb 14 10:53:32	0	19M	38K	420	8875	0	0	0	0	0	0	52.34
Feb 14 10:54:02	13	15M	34K	553	8900	0	0	0	0	0	0	39.82
Feb 14 10:54:32	0	11M	26K	691	8834	0	0	0	0	0	0	30.50
Feb 14 10:55:02	0	15M	32K	616	8981	0	0	0	0	0	0	40.85
Feb 14 10:55:32	0	9.2M	26K	484	8850	0	0	0	0	0	0	25.17

Long-Term History Buckets: 50 Interval: 1800

Period Ending	Drop	Oct	Pkt	Bcst	Mcst	CRC	Usiz	Osiz	Frag	Jab	Coll	Util %
Feb 13 10:36:42	6	176M	907K	26K	505K	0	0	0	0	0	1	08.12
Feb 13 11:06:43	6	254M	1.0M	26K	505K	0	0	0	0	0	0	11.65
Feb 13 11:36:43	2	153M	841K	26K	507K	0	0	0	0	0	0	07.08
Feb 13 12:06:43	1	157M	858K	27K	508K	0	0	0	0	0	0	07.29
Feb 13 12:36:43	2	156M	851K	26K	506K	0	0	0	0	0	1	07.25

Top N Host

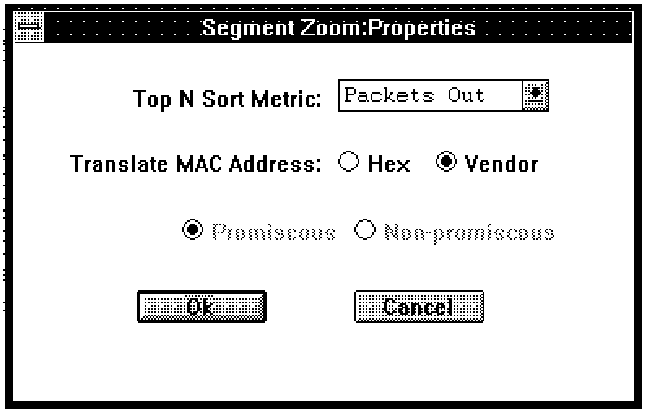
Host Name	Network Address	Mac Address	Pkts Out/sec
		DEC -2d-4a-f4	656
		DEC -00-72-10	496
		DEC -00-df-ff	139
		DEC -00-58-32	127
		DEC -20-93-21	120

LJ-03569-SIX

5.3.1.2 Segment Zoom Properties

Click on Properties and a screen is displayed, which details the current display parameters and allows changes to selected items. Figure 5–4 shows a Segment Zoom:Properties screen.

Figure 5–4 Segment Zoom:Properties Screen



Segment Zoom:Properties

Top N Sort Metric: Packets Out

Translate MAC Address: ○ Hex ● Vendor

● Promiscous ○ Non-promiscous

LJ-03570-SIX

Table 5–3 contains a description of each entry on the Segment Zoom:Properties screen.

Table 5–3 Segment Zoom:Properties Screen Fields

Field	Description
Top N Sort Metric	Specifies the sort criterion for the Top N Host portion of the Segment Zoom screen using a choice list (Packets In, Packets Out, and so on). The default criterion is outPkts. You can change this selection at any time. The change becomes effective after the Top N report currently being gathered has been displayed. The number (N) of hosts displayed is taken from Domain View Properties screen. For a Token Ring agent, you can specify the display of either Promiscuous or Non-promiscuous statistics and history by pushing an exclusive-choice button. You can change the selection at any time. The default at startup is Promiscuous. The buttons are protected (fainted) in the case of an Ethernet interface.
Translate MAC Address	Allows you to display MAC addresses in hexadecimal form only or with the identification of the manufacturer.

5.3.1.3 Agent Pushbutton

The Agent pushbutton on the Segment Zoom screen identifies the agent for which the information is presented. Clicking on the Agent pushbutton causes the display of the System and Interface Information for the selected agent. Table 5–4 describes the Agent System Information. This information is obtained from the MIB2 system group. It is not refreshed.

Table 5–4 Agent System Information

Field	MIB Object
Description	From sysDescr
Location	From sysLocation
Contact	From sysContact
Name	From sysName
Up since	Absolute time, derived from sysUpTime

Table 5–5 describes the Agent Interface Information. This information is obtained from the MIB2 interfaces group. Only Operational Status and “Since” are refreshed.

Table 5–5 Agent Interface Information

Field	MIB Object
Description	From ifDescr0
Type	From ifType
Speed	From ifSpeed (displayed in Mbits/sec)
Physical Addr	From ifPhysAddr
Since	Absolute time of last Op Status change

5.3.1.4 Domain Pushbutton

The Domain pushbutton on the Segment Zoom screen identifies the domain for which the information is presented. Clicking on the Domain pushbutton displays the Domain Information. The information includes:

- Domain Name
- Description
- Accept Type
- Filters attached

5.3.1.5 Hosts Pushbutton (Segment Zoom)

The Hosts pushbutton on the Segment Zoom screen identifies the number of hosts in the host table. If the Host option is not enabled for this agent/domain, “N/A” is displayed in place of a count. Clicking on the Hosts pushbutton displays the Host List screen. This screen is the same screen that displays when you select Host List from the Applications pull-down menu on the Domain View screen. Host List is discussed in Section 5.3.3.

5.3.1.6 Convs Pushbutton (Segment Zoom)

The Convs pushbutton on the Segment Zoom screen identifies the number of matrices in the matrix table. If the Host/Conversation option is not enabled for this agent/domain, “N/A” is displayed in place of a count. Clicking on the Convs pushbutton displays the Conversation List screen. This screen is the same screen that displays if you select Conversation from the Applications pull-down menu on the Domain screen. Conversation List is discussed in Section 5.3.4.

5.3.1.7 Packets Pushbutton

The Packets pushbutton on the Segment Zoom screen identifies the number of captured packets available in the capture buffer. If the Packet Capture option is not enabled for this agent/domain, “N/A” is displayed in place of a count.

5.3.1.8 Segment Zoom Fields

Table 5–6 contains a description of each field in the Segment Zoom screen.

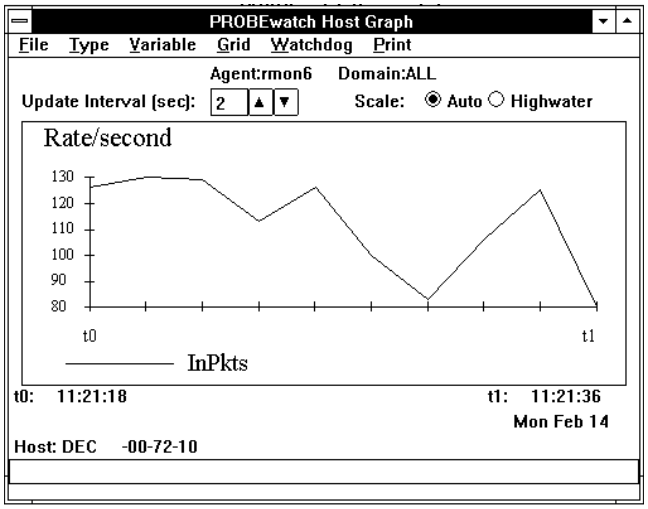
Table 5–6 Segment Zoom Screen Fields

Field	Description
Cumulative Statistics	This information is obtained from the etherStatsTable for an Ethernet interface, or from the user-chosen Promiscuous /Non-promiscuous tokenRingStatsTable for a Token Ring interface. Values are refreshed. This information is omitted if the Statistics option is not enabled for the agent/domain.
Long-Term History and Short-Term History	This information is obtained from the long-term and short-term history tables associated with the domain. Only the most recent *n* buckets are displayed. In the case of a Token Ring interface, either the Promiscuous or Non-promiscuous history information is displayed, depending on your selected option. History information is not displayed if the Statistics option is not enabled for the agent/domain.
Top N Host	Top N Host statistics displayed by Segment Zoom are obtained from a Host TopN table created by Segment Zoom itself. The Top N display is omitted if Hosts/Conversations are not enabled for the agent/domain. The Top N display shows the top N hosts over the last update period for the currently selected RateBase. Nothing is displayed until the first period has elapsed. At the beginning of each update period, the client normally sets the parameter that effectively enables the TopN collection. If the top N sort criterion has been changed by the user during the update period, the client must delete and recreate the HostTopNControlTable to establish the new TopNRateBase.

5.3.2 Graph for Domain View

Graph is a set of relatively simple grapher programs intended to provide a graph zoom function for many of the Domain View windows. For example, from the Segment Zoom window, you can select (highlight) a particular host from the Top Hosts list, and click on the Graph pushbutton to obtain a graphical display of traffic to and from that host. Figure 5–5 shows a Graph screen.

Figure 5–5 Graph Screen



Agent:rmon6 Domain:ALL

Update Interval (sec): 2 ▲ ▼ Scale: ◉ Auto ○ Highwater

t0: 11:21:18 t1: 11:21:36

Mon Feb 14

Host: DEC -00-72-10

LJ-03576-SIX

Variants of Graph are supported as follows:

- Statistics Graph including Utilization
- Short Term/Long Term History
- Host Graph
- Conversation Graph

Each of the variants operates by periodically sampling the values of the MIB variables of the appropriate RMON table associated with a specified agent and domain. Except as noted, variable values are graphed as per-second rates against the sample time. The graph is updated at the end of each sample period. Sixty samples are shown on each graph sample period from one to sixty seconds, so that the graph window shows activity for a period ranging from one minute to one hour.

5.3.2.1 Operation

Starting from the top screen of PROBEwatch, click on Domain View and release. The selection screen for Domain View functions will be displayed showing a variety of pushbutton items. The choices are: File, Properties, Applications, Install, and Deinstall. In addition, the screen contains a summary listing field showing a list of currently defined agents and domains, together with summary statistical information. This field is designated, Agent Summary.

Highlight the agent/domain to be displayed by clicking on that entry in the Agent Summary. Click on Applications, drag to Segment Zoom and release. The screen showing a full complement of summary statistical information for the selected agent/domain is displayed. Click on one of the Graph pushbuttons on the right side of the Segment Zoom screen.

Each of the variants starts immediately using default settings. Using the control panel, you can adjust several of the graph characteristics at any time. Any of the characteristics can be changed without losing previous samples.

Table 5–7 contains a description of each Graph screen entry.

Table 5–7 Graph Screen Entries

Entry	Description
Update Interval	You can adjust the sample period from one to ninety nine seconds using the up/down arrows. The default at startup is two seconds.
Scale	For all variants, you can choose one of the following: • Auto — Adjusts the maximum Y-axis value automatically to the largest value currently shown on the graph. • Highwater — Adjusts the maximum Y-axis value to the largest value seen since the graph was started.

(continued on next page)

Table 5–7 (Cont.) Graph Screen Entries

Entry	Description
Type	For all variants, you can choose one of the following: Plot Scatter Area 2-D Bar 3-D Bar 2-D Stack 3-D Stack
Variable	For the Statistics variant, you can select one of the Statistics table variables, such as Packets (etherStatsPkts). A pseudo-variable, Utilization % (calculated from Octets and Packets) can also be selected. The value of the selected variable and its cumulative average value (since the graph was started) are plotted simultaneously. You may plot multiple variables from the Statistics variant by clicking on multiple parameters while pressing the Control. You must also press the Control key when clicking on OK. For the Host variant, you can select Packets In/Out or Octets In/Out. The traffic rates to and from the selected host are plotted simultaneously. For the Conversation variant, you can select Packets, Octets, or Errors. The traffic between the selected hosts (A to B and B to A is plotted simultaneously.)
Grid	The Grid pushbutton allows you to apply X or Y grid lines to the graph for easier viewing.
Packet Distribution (Statistics only)	A pie chart representation of current and average packet distribution.
Watchdog	The WatchDog pushbutton invokes the WatchDog utility. For further information, refer to Section 5.3.6

(continued on next page)

Table 5–7 (Cont.) Graph Screen Entries

Entry	Description
Print	The Print pushbutton produces an encapsulated, device-independent PostScript (EPSF-2.0) representation of the graph that can be dumped to a PostScript compatible printer. You may store and print graphs using a user defined file name. In the Graph screen, click on Print. This results in the display of a screen which requires the entry of a file name. You may enter the file name and click on OK which causes the graph image to be stored in the file as a Post Script file. Printing of the file can then be accomplished and the contents of that file will be retained until it is deleted or overwritten.

Typical examples of Graph displays are shown. Presentation characteristics may be altered to fit individual preferences and size may be adjusted for convenience.

5.3.3 Host List

Host List provides a complete list of hosts detected by the selected agent /domain. If the Host/Conversation option is not enabled for the selected agent/domain, the error message “Host/Conversation not enabled for this agent/domain!” is displayed after the selection of Hosts. The Host list can be presented according to Discovery Order or MAC Order or by one of the statistical values contained in the table: Packets In, Packets Out, Octets In, Octets Out, Errors Out, Broadcasts Out, or Multicasts Out.

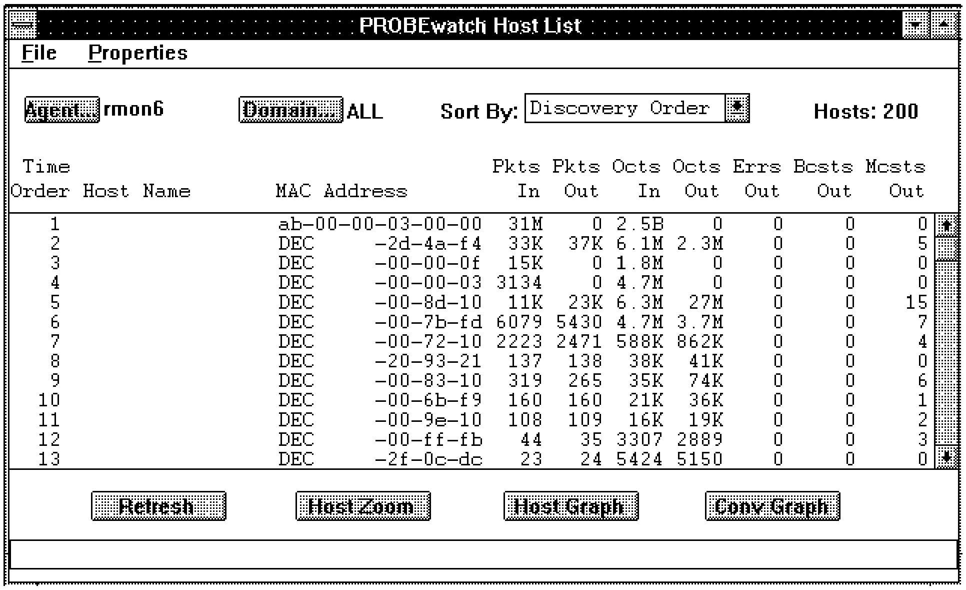
5.3.3.1 Operation

Starting from the top screen of PROBEwatch, click on Domain View and release. The selection screen for Domain View functions is displayed showing a variety of pushbutton items. The choices are: File, Properties, Applications, Install, and Deinstall. In addition, the screen contains a summary listing field showing a list of currently defined agents and domains, together with summary statistical information. This field is designated, Agent Summary.

From the Domain screen highlight the agent/domain to be displayed by clicking on that entry in the Agent Summary. Click on Applications and display the selection list. Click on Host List. The Host List screen displays showing a full complement of summary statistical information for the selected agent/domain. Figure 5–6 shows a Host List screen The Hosts screen may be displayed by clicking on the Host List pushbutton in the Segment Zoom display screen.

Statistics are displayed using one line per host. You are able to scroll through the list using the scroll bar.

Figure 5–6 Host List Screen



Agent... rmon6   Domain... ALL   Sort By: Discovery Order   Hosts: 200

```
 Time                                    Pkts Pkts Octs Octs Errs Bcsts Mcsts
Order Host Name       MAC Address          In  Out   In  Out  Out   Out   Out
   1                  ab-00-00-03-00-00  31M    0 2.5B    0    0     0     0
   2                  DEC     -2d-4a-f4  33K  37K 6.1M 2.3M    0     0     5
   3                  DEC     -00-00-0f  15K    0 1.8M    0    0     0     0
   4                  DEC     -00-00-03 3134    0 4.7M    0    0     0     0
   5                  DEC     -00-8d-10  11K  23K 6.3M  27M    0     0    15
   6                  DEC     -00-7b-fd 6079 5430 4.7M 3.7M    0     0     7
   7                  DEC     -00-72-10 2223 2471 588K 862K    0     0     4
   8                  DEC     -20-93-21  137  138  38K  41K    0     0     0
   9                  DEC     -00-83-10  319  265  35K  74K    0     0     6
  10                  DEC     -00-6b-f9  160  160  21K  36K    0     0     1
  11                  DEC     -00-9e-10  108  109  16K  19K    0     0     2
  12                  DEC     -00-ff-fb   44   35 3307 2889    0     0     3
  13                  DEC     -2f-0c-dc   23   24 5424 5150    0     0     0
```

LJ-03571-SIX

5.3.3.2 Host List Properties

Clicking on Properties allows you to establish the format of the MAC address displayed. Selecting Translate MAC Address causes the MAC address to show vendor name or full Hex representation.

5.3.3.3 Agent Pushbuton

The Agent pushbutton identifies the agent for which the information is presented. Clicking on the Agent pushbutton causes the display of the System and Interface Information for selected the agent. Table 5–8 describes the Agent System Information. This information is obtained from the MIB2 system group. It is not refreshed.

Table 5–8 Agent System Information

Field	MIB Object
Description	From sysDescr
Contact	From sysContact
Name	From sysName
Location	From sysLocation
Up since	Absolute time, derived from sysUpTime

Table 5–9 describes the Agent Interface Information. This information is obtained from the MIB2 interfaces group. Only Operational Status and “Since” are refreshed.

Table 5–9 Agent Interface Information

Field	MIB Object
Description	From ifDescr0
Type	From ifType
Speed	From ifSpeed (displayed as 10 Mbits/sec)
Physical Addr	From ifPhysAddr
Since	Absolute time of last Op Status change

5.3.3.4 Domain Pushbutton

The Domain pushbutton identifies the domain for which the information is presented. Clicking on the Domain pushbutton causes the display of the Domain Information. The information includes:

- Domain Name
- Description
- Accept Type
- Filters attached

5.3.3.5 Sort By

Sort By allows you to select the way the Host List is displayed. The options are as follows:

- Discovery order
- MAC order
- Packets in
- Packets out
- Octets in
- Octets out
- Errors out
- Broadcasts out
- Multicasts out

5.3.3.6 Refresh

Refresh updates the entries on the Host List screen.

5.3.3.7 Host Zoom

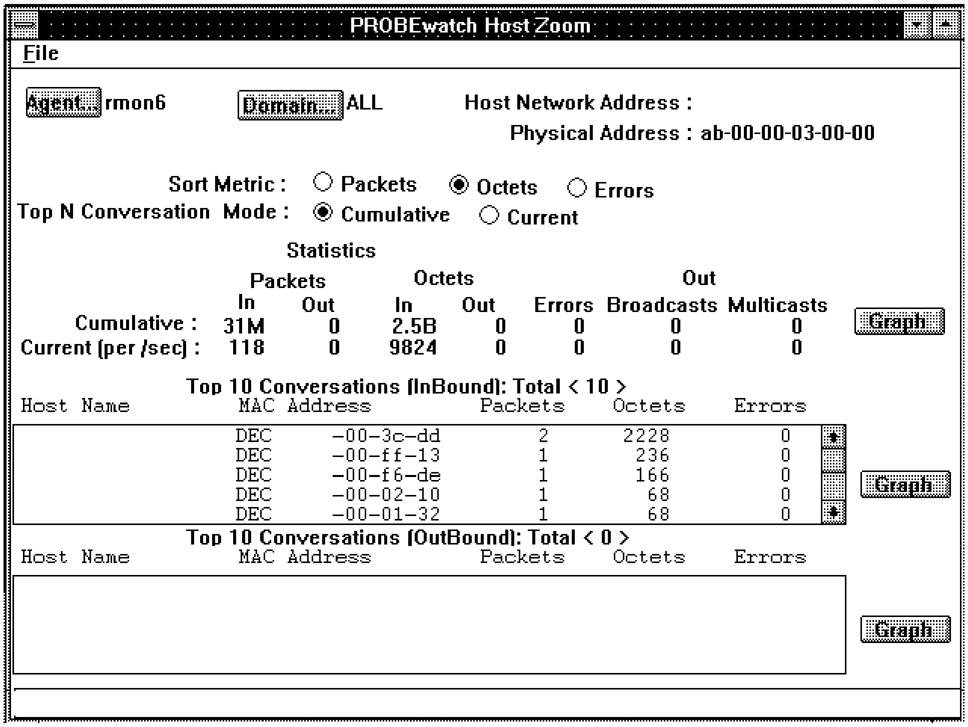
Host Zoom displays detailed statistical information about traffic to and from a user-specified host from the point of view of a particular agent/domain. Host Zoom can not be selected unless the agent/domain has the Hosts/Conversations option enabled.

5.3.3.8 Host Zoom Operation

From the Domain screen, highlight the agent/domain to be displayed by clicking on that entry in the Agent Summary. Click on Applications and display the selection list. Click on Host List. The Host List screen displays showing a full complement of summary statistical information for the selected agent/domain. Highlight the host to be zoomed on by clicking on the host line in the Top 10 host display. Click on the Zoom pushbutton. The Host Zoom screen is displayed. Zoom may also be initiated by clicking on the pushbutton in the Host List display screen. Figure 5–7 shows a Host Zoom Screen.

Table 5–10 contains a description of each Host Zoom screen field.

Figure 5–7 Host Zoom Screen



Agent... rmon6 Domain... ALL Host Network Address :

Physical Address : ab-00-00-03-00-00

Sort Metric : ○ Packets ● Octets ○ Errors

Top N Conversation Mode : ● Cumulative ○ Current

Statistics

	Packets		Octets			Out	
	In	Out	In	Out	Errors	Broadcasts	Multicasts
Cumulative :	31M	0	2.5B	0	0	0	0
Current (per /sec) :	118	0	9824	0	0	0	0

Top 10 Conversations (InBound): Total < 10 >

```
Host Name          MAC Address          Packets    Octets    Errors
                   DEC     -00-3c-dd       2        2228        0
                   DEC     -00-ff-13       1         236        0
                   DEC     -00-f6-de       1         166        0
                   DEC     -00-02-10       1          68        0
                   DEC     -00-01-32       1          68        0
```

Top 10 Conversations (OutBound): Total < 0 >

```
Host Name          MAC Address          Packets    Octets    Errors
```

LJ-03572-SIX

Table 5–10 Host Zoom Screen Fields

Field	Description
Sort Metric	You select the sort variable for the top N conversation displays by selecting Packets, Octets, or Errors.
Host Network Address	Shows the DECnet or IP address, if applicable, for the selected host.
Physical Address	Shows the full hex representation of the host MAC address. Also shows the applicable vendor in parenthesis after the Hex address.
Top N Conversation Mode	You can specify if the Top N Conversations information is to be based on cumulative packet counts or on delta values for the current display period, by pressing either the Current or Cumulative button.
Statistics	The statistics information is updated once every update period. Statistics displayed are In Pkts, Out Pkts, In Octets, Out Octets, Out Errors, Out Broadcasts, and Out Multicasts. Two lines of statistics are displayed: the first line contains cumulative values; the second line contains calculated per-second values over the previous sample period. The second line is not displayed until the first update period is completed. For current per-second values, values greater than 0 but less than one are displayed as "< 1". **Note** The target host may not appear in the agent/domain's host table. It may also disappear and reappear due to the aging of the table.

(continued on next page)

Table 5–10 (Cont.) Host Zoom Screen Fields

Field	Description
Top N Conversations (Inbound and Outbound)	This information is calculated from the agent/domain's matrix tables. For the "inbound" display, all entries with destination address equal to target host address are uploaded and sorted. For the "outbound" display, all entries with source address equal to target host address are uploaded and sorted. The number (N) of conversations is taken from the properties screen. Both inbound and outbound displays are updated every update period. If the Cumulative option is chosen, values displayed are absolute (since table creation). If the Current option is chosen, values displayed are per-second rates for the previous sample period. "Current" values are not displayed until the end of the first sample period. Note that the target host may not appear in the agent /domain's matrix tables, and may disappear and reappear.
Graph pushbuttons	Graph pushbuttons are implemented for Statistics, Top N Conversations (Inbound), and Top N Conversations (Outbound). Clicking on these pushbuttons results in graphical display of the selected data.

5.3.3.9 Host Graph

This pushbutton invokes the Graph utility. The Graph utility is discussed in Section 5.3.2.

5.3.3.10 Conv Graph

This pushbutton invokes the Graph utility. This graph will display the conversation between two addresses. Select the first address by clicking on the entry in the Host Zoom screen. Select the second address by holding the Ctrl key down and clicking on the second address. The Graph utility is discussed in Section 5.3.2.

5.3.3.11 Host List Summary

The Host List Summary contains a summary of each host that has been discovered. This information includes:

- Host Name
- MAC Address
- Packets In/Out
- Octets In/Out

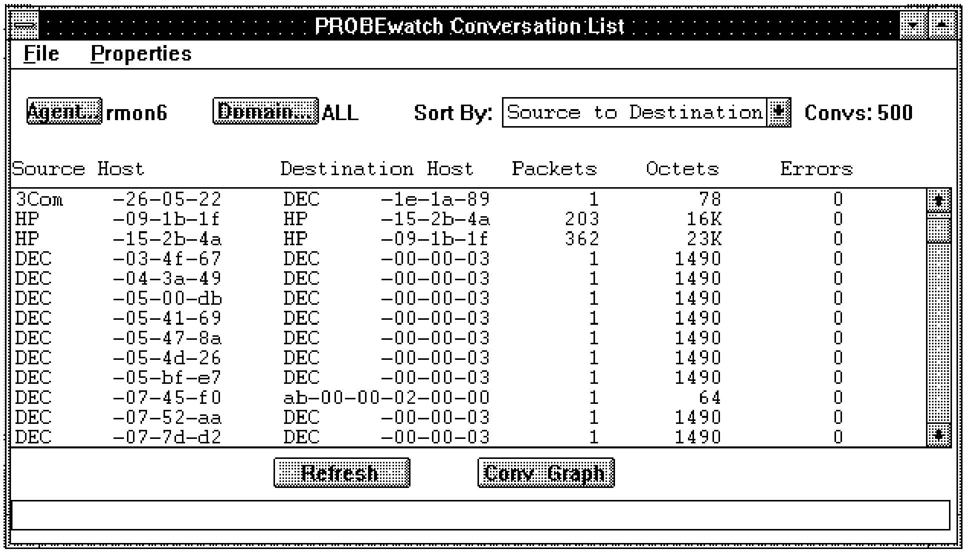
- Errors Out
- Broadcasts Out
- Multicasts Out

5.3.4 Conversation List

A Conversation List that provides a complete list of conversations detected by the selected agent/domain may be displayed by clicking on the Conversations List pushbutton in the Segment Zoom display screen. You can select the sort order using exclusive-choice pushbuttons. You can specify Destination-Source order, Source-Destination order, or that the list be sorted according to one of the statistical values contained in the table: Packets, Octets, or Errors.

If the Host/Conversation option is not enabled for the selected agent/domain, the error message "Host/Conversation not enabled for this agent/domain!" is displayed after the pushbutton is pushed. Figure 5–8 shows a Conversation List screen.

Figure 5–8 Conversation List Screen



Agent... rmon6 Domain... ALL Sort By: Source to Destination Convs: 500

```
Source Host            Destination Host     Packets    Octets     Errors
3Com     -26-05-22     DEC      -1e-1a-89         1        78          0
HP       -09-1b-1f     HP       -15-2b-4a       203       16K          0
HP       -15-2b-4a     HP       -09-1b-1f       362       23K          0
DEC      -03-4f-67     DEC      -00-00-03         1      1490          0
DEC      -04-3a-49     DEC      -00-00-03         1      1490          0
DEC      -05-00-db     DEC      -00-00-03         1      1490          0
DEC      -05-41-69     DEC      -00-00-03         1      1490          0
DEC      -05-47-8a     DEC      -00-00-03         1      1490          0
DEC      -05-4d-26     DEC      -00-00-03         1      1490          0
DEC      -05-bf-e7     DEC      -00-00-03         1      1490          0
DEC      -07-45-f0     ab-00-00-02-00-00          1        64          0
DEC      -07-52-aa     DEC      -00-00-03         1      1490          0
DEC      -07-7d-d2     DEC      -00-00-03         1      1490          0
```

LJ-03573-SIX

5.3.4.1 Operation

Starting from the top screen of PROBEwatch, click on Domain View and release. The selection screen for Domain View functions is displayed showing a variety of pushbutton items. The choices are: File, Properties, Applications, Install, and Deinstall. In addition, the screen contains a summary listing field showing a list of currently defined agents and domains, together with summary statistical information. This field is designated Agent Summary.

Highlight the agent/domain to be displayed by clicking on that entry in the Agent Summary. Click on Applications and display the selection list: Segment Zoom, Host List, Conversation, WatchDog, and View Packets. Click on Conversation. A list of all the conversations detected by the agent/domain is displayed.

Statistics are displayed using one line per conversation showing Packets, Octets, and Errors. You may scroll through the list using the scroll bar. Table 5–11 contains a description of the Conversations List screen fields.

Table 5–11 Conversations List Screen Fields

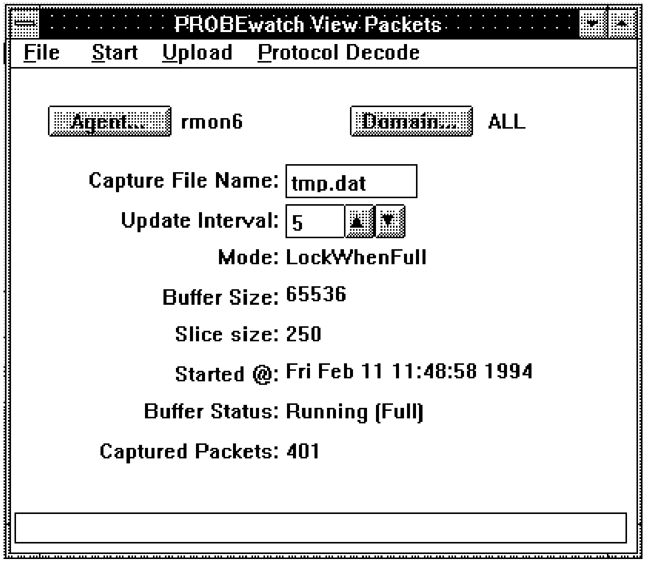
Field	Description
Total Conversations	Shows a count of the total number of conversations which have been detected by the agent for the domain selected.
Translate MAC Address	Allows you to select the address presented as Hex, Hex with vendor name, or IP. Default is IP.
Graph	Graph is implemented for Conversation. An entry in the conversation list must be highlighted first. Variables are Utilization, Packets, Octets, and Errors.

5.3.5 View Packets

The View Packets function allows you to enter the Packet Capture/Protocol Decode function directly from the Domain View screen. Using this method of launching the Packet Capture/Protocol decode function, you may immediately upload packets thathave been previously captured in the agent capture buffer because the Packet Capture group has been enabled as part of the selected agent/domain startup.

If the Packet Capture group has not been enabled, the Packet Capture screen may not be launched from the Domain View top screen. Figure 5–9 shows a View Packets screen.

Figure 5–9 View Packets Screen



Agent... rmon6

Domain... ALL

Capture File Name: tmp.dat

Update Interval: 5

Mode: LockWhenFull

Buffer Size: 65536

Slice size: 250

Started @: Fri Feb 11 11:48:58 1994

Buffer Status: Running (Full)

Captured Packets: 401

LJ-03574-SIX

5.3.5.1 Operation

Starting from the top screen of PROBEwatch, highlight the agent of interest by clicking on the entry in the agent list and then click on Domain View. The selection screen for Domain View functions is displayed showing a variety of pushbutton items. The choices are:

- File
- Properties
- Applications
- Install
- Deinstall

In addition, the screen contains a summary listing field showing a list of currently defined agents and domains, together with summary statistical information. This field is designated, Agent Summary.

Highlight the agent/domain to be displayed by clicking on that entry in the Agent Summary. Click on Applications and display the selection list:

- Segment Zoom

- Host List
- Conversation
- WatchDog
- View Packets

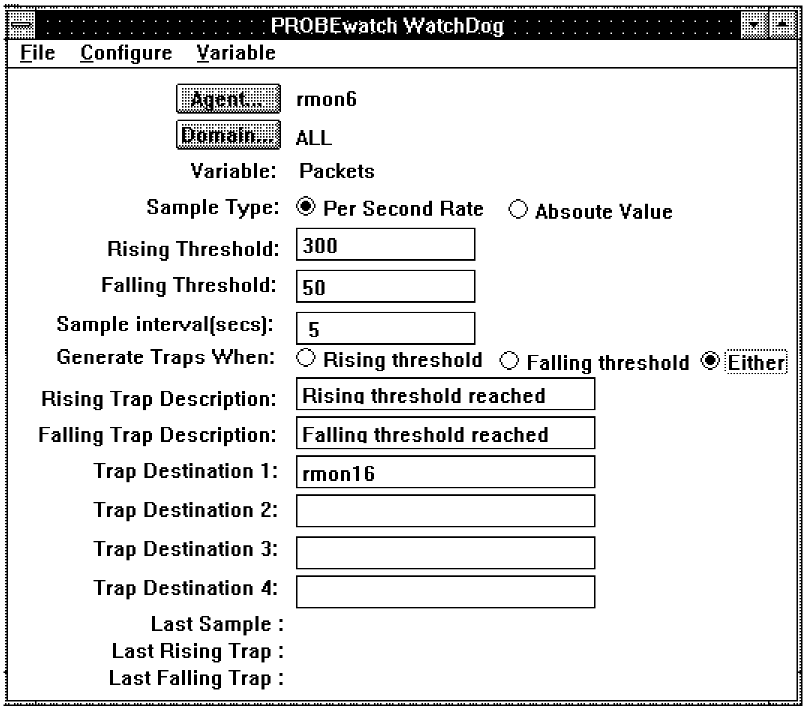
Click on View Packets. The Data Capture screen is displayed. The choices are Start, Upload, and Protocol Decode. You may upload packets already captured in the buffer or start a new packet capture sequence and then initiate protocol decode. Refer to Chapter 6 for additional information on capturing and uploading packets. Refer to Chapter 7 for additional information on Protocol Decode.

5.3.6 WatchDog

Domain View provides a high-level interface, called WatchDog, to the RMON–MIB Alarm and Event groups. WatchDog notifies you (through a trap message) when a statistic value exceeds or falls below a user-defined threshold.

WatchDog is a simplified and straightforward means of establishing and activating alarms and traps. This process relates to the Alarm and Event groups of RMON as Segment Zoom relates to the Statistics, History, HostTopN, Matrix, and Host groups. This feature allows alarms to be set for protocol-specific parameters such as the number of IP packets for a time period as opposed to the total number of packets. Figure 5–10 shows a WatchDog screen.

Figure 5–10 WatchDog Screen



Agent... rmon6

Domain... ALL

Variable: Packets

Sample Type: ● Per Second Rate ○ Absoute Value

Rising Threshold: 300

Falling Threshold: 50

Sample interval(secs): 5

Generate Traps When: ○ Rising threshold ○ Falling threshold ● Either

Rising Trap Description: Risinq threshold reached

Falling Trap Description: Fallinq threshold reached

Trap Destination 1: rmon16

Trap Destination 2:

Trap Destination 3:

Trap Destination 4:

Last Sample :

Last Rising Trap :

Last Falling Trap :

LJ-03575-SIX

5.3.6.1 Operation

Starting from the top screen of PROBEwatch, highlight the agent of interest by clicking on the entry in the agent list and then click on Domain View. The selection screen for Domain View functions is displayed showing a variety of pushbutton items. The choices are: File, Properties, Applications, Install, and Deinstall. In addition, the screen contains a summary listing field showing a list of currently defined agents and domains, together with summary statistical information. This field is designated, Agent Summary.

Highlight the agent/domain to be displayed by clicking on that entry in the Agent Summary. Click on Applications and display the selection list: Segment Zoom, Host List, Conversation, WatchDog, and View Packets. Click on WatchDog. The WatchDog screen which allows you to establish an alarm function is displayed. The screen displays fields, in boxes, which information may be entered by clicking on the desired field.

WatchDog may also be launced from the Host and the Conversation Graph screens. Depending upon where the function is launched, you will have a different set of alarm variables available.

Table 5–12 contains a description of each WatchDog screen field.

Table 5–12 WatchDog Screen Fields

Field	Description
Configure	Allows you to alter alarms as follows: • Create — Causes an alarm condition to be established based on the infromation entered. • Modify — Allows modification of an existing alarm condition. • Delete — Deletes an existing alarm condition.
Variable	The name of the parameter which is to be monitored. This parameter is selected from a menu of 6 available selections, each of which in turn has several possibilities reached by dragging through the selection to the selected variable. For Ethernet agents, the available variables are Ethernet Statistics and Miscellaneous. Other choices are faded. For Token Ring agents, the available variables are Token Ring Promiscuous, Token Ring Non-promiscuous, and Miscellaneous. Other choices are faded. When launched from the Host Quick Graph, the available variable is Host Statistics. Other choices are faded. When launched from the Conversation Quick Graph, the available variable is Conversation Statistics. Other choices are faded.
Agent	The name of the agent selected in the Agent Summary field before initiating the WatchDog session.
Domain	The domain of the agent selected in the Agent Summary field before initiating the WatchDog session.
Sample Type	Selects Absolute or Delta values by highlighting the required entry.

(continued on next page)

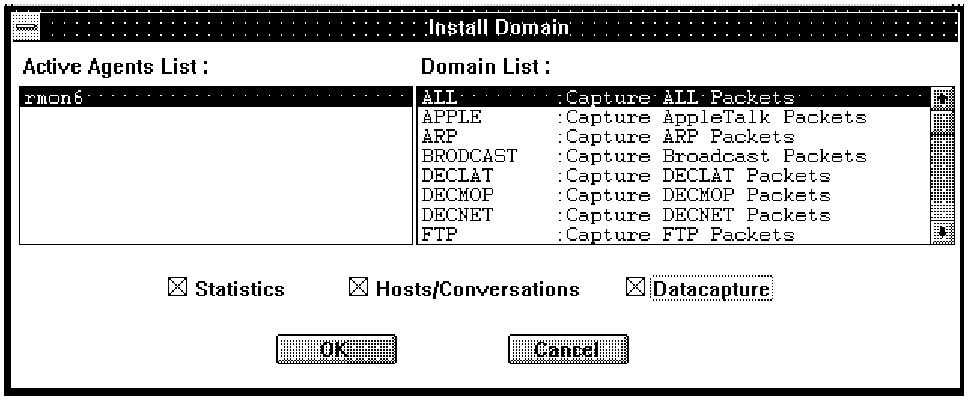
Table 5–12 (Cont.) WatchDog Screen Fields

Field	Description
Rising Threshold	A threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event will be generated. Another such event will not be generated until the sampled value falls below this threshold and reaches the Falling Threshold.
Falling Threshold	A threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event will be generated. Another such event will not be generated until the sampled value rises above this threshold and reaches the Rising Threshold.
Sample Interval (secs)	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds.
Generate Trap When	Selects Rising, Falling or both Rising and Falling conditions relative to the threshold values established by highlighting the required entry.
Rising Trap Description-	When an rising alarm condition is reached, the text message entered in this field is transmitted as part of the trap message to the reporting station.
FallingTrap Description	When an falling alarm condition is reached, the text message entered in this field is transmitted as part of the trap message to the reporting station.
Last Sample	Value of the parameter selected for the last sample period.
Last Rising/Falling Trap	Date and time of last trap condition due to exceeding the rising/falling threshold.

5.4 Install

Domain Install lets you add, delete, or modify a domain at a selected agent. Agent and domain can be selected by choice list. All active agents are displayed in the agent choice list. All available domains are available in the domain choice list.

Figure 5–11 Install Domain Screen



```
rmon6
```

```
ALL         :Capture ALL Packets
APPLE       :Capture AppleTalk Packets
ARP         :Capture ARP Packets
BRODCAST    :Capture Broadcast Packets
DECLAT      :Capture DECLAT Packets
DECMOP      :Capture DECMOP Packets
DECNET      :Capture DECNET Packets
FTP         :Capture FTP Packets
```

☒ Statistics ☒ Hosts/Conversations ☒ Datacapture

LJ-03577-SIX

5.4.1 Operation

Starting from the top screen of PROBEwatch, click on Domain View. The selection screen for Domain View functions is displayed. The choices are: File, Properties, Applications, Install, and Deinstall. Click on Install. The screen showing two scrollable lists of currently defined agents and domains will be displayed. Figure 5–11 shows an Install Domain screen. You may scroll through the list to select a particular agent name and then scroll through the second list to select a particular domain.

Following selection of agent and domain, you click on one or more of the check boxes for Enable/Disable Groups, Statistics, Host/Conversation, or Datacapture.

Note

At least one of the check boxes must be checked if the domain is to be configured.

You can enable or disable each of these functions by clicking on the appropriate box. Changes are made effective when the OK button is pushed. Clicking on cancel aborts the operation and results in no change.

When the OK button is pushed, the client (re)configures the agent to install the domain as selected by you. If none of the functions are enabled, the domain is completely deleted at the agent.

Note that you are given the option to enable some (rather than all) of these functions so that agent resources are not unnecessarily consumed. The functions correspond to control entries as follows:

Function	Channel Table and Filter Table(s)
Statistics	Statistics table and two history tables.
Host/Conversation	Host table and matrix table
Packetcapture	Capture buffer table

The channel table can be considered the “parent” of the other control tables for a given domain. Additional control tables are mapped back to the parent channel table.

5.5 Deinstall

Domain Deinstall causes the deletion of a currently defined domain. From the PROBEwatch screen, click on an entry in the Agent Summary listing. Clicking on Deinstall causes the display of a confirmation screen which poses the question, “Are You Sure” and offers a Yes or No choice. Clicking on Yes deletes the selected domain. Clicking on No aborts the deinstall command and results in no action.

6 Data Capture

Data Capture is the utility used to capture packets selectively from the DECpacketprobe agent. The ability to "hide" most of the RMON–MIB based information from the user and instead use standard English language instructions makes this utility simple to use.

With this utility, you can capture the traffic for either standard prototcols or user-defined protocols.

6.1 Operation

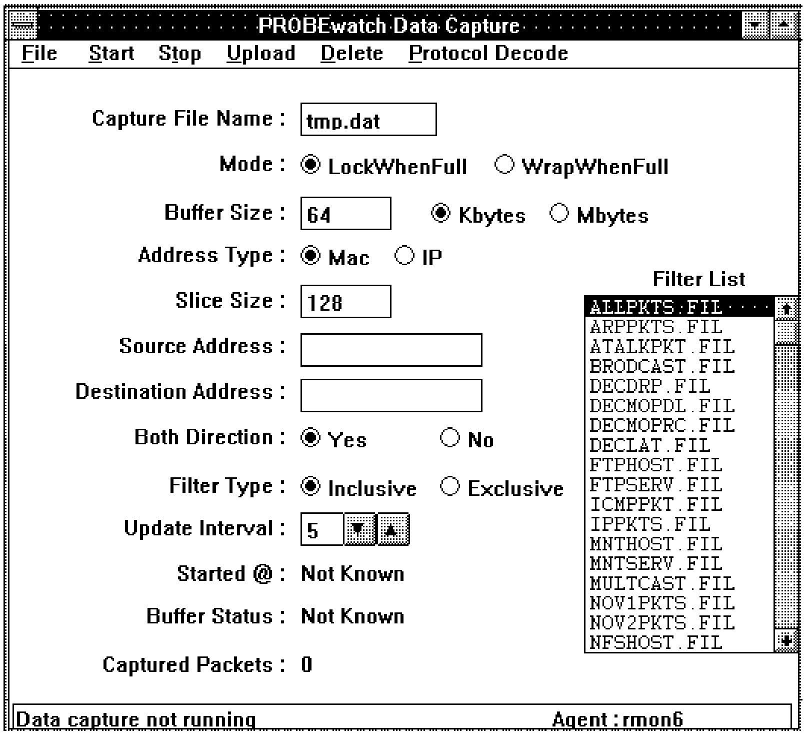
Starting from the top screen of PROBEwatch, highlight the agent of interest by clicking on the entry in the agent list. Then click on Data Capture. The setup screen for performing a quick data capture and protocol decode session is displayed.

The background and foreground colors of the window are taken from user-defined colors for that agent. Figure 6–1 shows a Data Capture screen.

The Data Capture screen includes five action modes:

- Start
- Stop
- Upload
- Delete
- Protocol Decode

Figure 6–1 Data Capture Screen



Capture File Name : tmp.dat

Mode : ● LockWhenFull ○ WrapWhenFull

Buffer Size : 64 ● Kbytes ○ Mbytes

Address Type : ● Mac ○ IP

Slice Size : 128

Source Address :

Destination Address :

Both Direction : ● Yes ○ No

Filter Type : ● Inclusive ○ Exclusive

Update Interval : 5

Started @ : Not Known

Buffer Status : Not Known

Captured Packets : 0

Filter List

ALLPKTS.FIL
ARPPKTS.FIL
ATALKPKT.FIL
BRODCAST.FIL
DECDRP.FIL
DECMOPDL.FIL
DECMOPRC.FIL
DECLAT.FIL
FTPHOST.FIL
FTPSERV.FIL
ICMPPKT.FIL
IPPKTS.FIL
MNTHOST.FIL
MNTSERV.FIL
MULTCAST.FIL
NOV1PKTS.FIL
NOV2PKTS.FIL
NFSHOST.FIL

Data capture not running Agent : rmon6

LJ-03578-SIX

Entry fields allow you to set up the conditions for a capture session. You must enter the requested information before initiating a capture session. The entry fields to be completed are:

- Capture File Name
- Buffer Size
- Slice Size
- Source Address
- Destination Address
- Update Interval

In addition, four fields require the selection of parameters from a selection list:

- Mode
- Address Type
- Both Directions
- Filter Type

Standard default conditions are preselected. Table 6–1 contains a description of each field on the Data Capture screen.

Table 6–1 Data Capture Screen Fields

Field	Description
Start	Initializes the data capture session for the selected agent.
Stop	Ends a data capture session for the selected agent.
Upload	At the completion of a data capture session, the captured data is stored in a buffer in the agent. This function allows you to transfer packets captured at the agent to the client. The file specified stores the uploaded packets for examination and protocol decode. Clicking on Upload Pkts initiates the upload process to the file specified in the Capture File Name. Once the upload process begins, a status report is shown in the lower margin of the screen which shows the count of packets uploaded. When the upload process is complete, click on Protocol Decode to begin the protocol decode process.
Delete	Deletes the current entry inside the agent.
Protocol Decode	Displays the Protocol Decode Utility screen.
Capture File Name	Specifies the name of the file in which the packets from the agent are uploaded.
Mode	Determines if the session will halt (LockWhenFull) when the capture buffer is full or continue (WrapWhenFull) with the most recent packets, overwriting the earliest until a specific stop command is initiated.
Buffer Size	Specifies the maximum number of octets to be saved in this capture buffer, including any implementation-specific overhead in Kbytes or Mbytes.

(continued on next page)

Table 6–1 (Cont.) Data Capture Screen Fields

Field	Description
Address Type	Specifies the address type as either MAC, IP, or interpeted DECnet. Depending on this, the address or symbol entered at Source and Destination Address are interpreted. (Valid symbols are defined in file nsnames.def).
Slice Size	Specifies the maximum number of octets of each packet that will be saved in the capture buffer. For example, if a 1500 octet packet is received and this field is set to 500, then only 500 octets of the packet will be stored in the associated capture buffer. If this variable is set to 0, the capture buffer will save as many octets as is possible.
Source/Destination Address	Can be a valid MAC address, valid IP address, or valid name. These addresses are used to create more specific filters related to the source/destination of the data to be captured.
Filter List	Can be Standard or Custom. If you select Standard, you can specify up to 4 protocols from the given choice list of protocols by clicking on the selected entries. If you select Custom, you can choose up to 4 filters from the list of 44 predefined filters, or from the additional user-defined filter definitions.
Update Interval	Specifies the time, in seconds, for which the status fields described below are updated. The minimum and also the default value is 5 seconds. You can increase or decrease the time by clicking on the Up or Down arrows. Once capturing is started, three fields are activated at the bottom of the window. These values are updated at the update interval specified.
Started @	Displays the date and time at which the packet capture function was initiated.
Buffer Status	Displays “Running” and the time at which the capture process began, if capture is already on. Displays “Stopped” if the capture process is stopped. If a capture entry does not exist, this field displays “Not Known”. It also displays the buffer status in brackets: “Full” or “Available”.
Captured Packets	Displays the number of packets captured in the agent with the matched condition, if capture is on. This field is periodically updated during the capture process.

6.1.1 Performing Data Capture

To perform a data capture session:

1. Enter information into each field on the Data Capture screen as necessary.
2. Click on Start.

   The Started @ field displays the time and date the capture session started. The Buffer Status field indicates that the process is running (available or full). The Captured Packets field indicates the number of captured packets.
3. Click on Stop.

   When the required sample of packets has been captured, click on stop. This step halts the capture process. The captured packets are stored in the agent.
4. Click on Upload.

   Click on Upload Packets to transmit the captured packets to the client. As a default, the packets will be placed in a buffer designated tmp.dat and each subsequent upload will cause a confirmation screen to be displayed so that you can verfy that you want to overwrite what is currently in the buffer. If you want to save the uploaded information for further detailed examination, you should specify a unique buffer name to store the uploaded packets.
5. Click on Protocol Decode.

   Once you have uploaded the packets, you can use the Protocol Decode utility to examine the packets. Click on Protocol Decode. The Protocol Decode Summary screen is displayed, including the contents of the uploaded packets.

   For details on the Protocol Decode function, see Chapter 7.

7

Protocol Decode

A data communications network, whether a local network or a distributed internetwork, is subject to a wide variety of fault conditions. Hardware may fail, errors may occur as data is transmitted on the respective physical links, software may create convoluted and bandwith-consuming sessions, and network response time may mysteriously lengthen. The typical user sees only the result of these problems: the inability to complete network-dependent tasks in a reasonable timeframe or, in some cases, a complete network failure when there is no response to user activity.

In situations such as these, PROBEwatch for Windows provides a means for the network administrator to examine detailed network operation. A starting point might be to examine cumulative statistics of network activity. This process often provides clues about the nature of the fault condition but does not uniquely determine where the problem exists. The next logical step is to examine the specific data messages that are being sent from the troubled segment. Through this process, an experienced user can often quickly identify a fault condition and take corrective action. The means to perform this function is through the Protocol Decode Utility.

The protocol decode process begins with a data capture session performed by the DECpacketprobe agent on the network segment under observation. Next, the collected data is transmitted from the agent to the client, where it is stored. You accomplish these steps through the Data Capture functions (see Chapter 6). Finally, you can then examine the individual frames with full seven-layer decode using the Protocol Decode Utility screen for access to and display of the data.

7.1 Operation

Once captured data is uploaded to the client from any agent, it is stored in a specified capture file in the client. The protocol decode function is then initiated. You can access this function in multiple ways:

- Directly from the topmost screen of PROBEwatch
- From the Data Capture function as described in Chapter 6
- From the Domain View top screen through the Applications pull-down menu

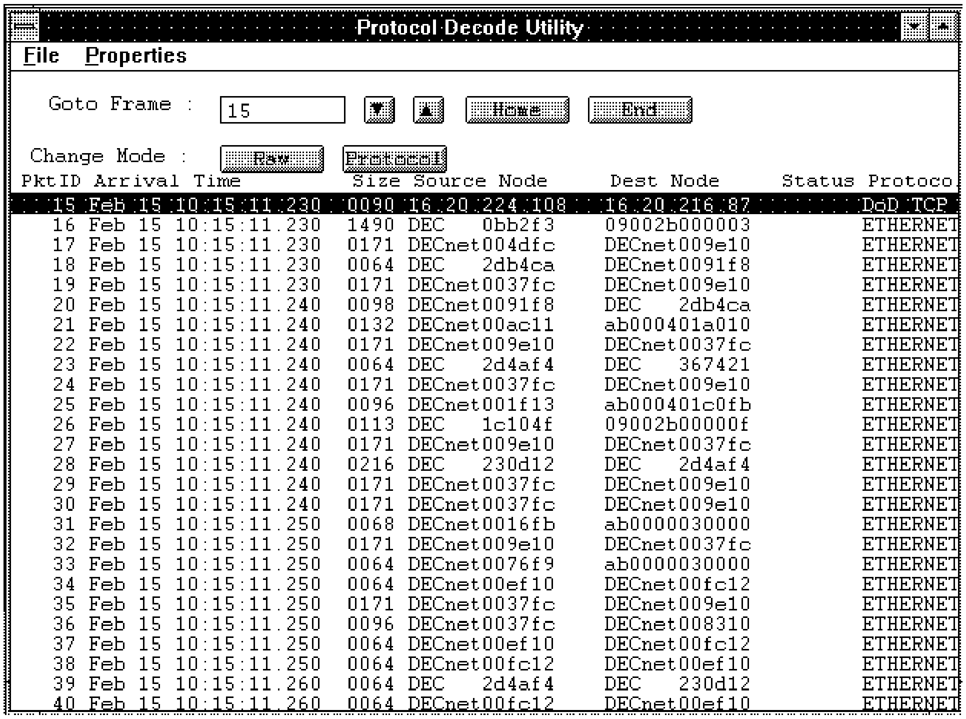
The following provides a general overview of the Protocol Decode operation when accessed from the PROBEwatch top screen. Accessing in this way requires you to enter the name of a prestored data file to perform protocol decode on that data. Details of accessing the Protocol Decode utility from the other functions are described in their respective chapters.

Starting from the top screen of PROBEwatch, highlight the agent of interest by clicking on the entry in the agent list. Then click on Protocol Decode. The Protocol Decode Utility screen is displayed. Figure 7–1 shows a Protocol Decode Utility screen. Operational choices include:

- File
- Properties
- Goto Frame (with an entry field)
- Change Mode

In addition, the screen contains a display field where the contents of the data file will be displayed in summary format.

Figure 7–1 Protocol Decode Utility Screen



```
PktID Arrival Time          Size Source Node      Dest Node      Status Protoco
   15 Feb 15 10:15:11.230  0090 16.20.224.108    16.20.216.87          DoD TCP
   16 Feb 15 10:15:11.230  1490 DEC    0bb2f3     09002b000003          ETHERNET
   17 Feb 15 10:15:11.230  0171 DECnet004dfc     DECnet009e10          ETHERNET
   18 Feb 15 10:15:11.230  0064 DEC    2db4ca     DECnet0091f8          ETHERNET
   19 Feb 15 10:15:11.230  0171 DECnet0037fc     DECnet009e10          ETHERNET
   20 Feb 15 10:15:11.240  0098 DECnet0091f8     DEC    2db4ca         ETHERNET
   21 Feb 15 10:15:11.240  0132 DECnet00ac11     ab000401a010          ETHERNET
   22 Feb 15 10:15:11.240  0171 DECnet009e10     DECnet0037fc          ETHERNET
   23 Feb 15 10:15:11.240  0064 DEC    2d4af4     DEC    367421         ETHERNET
   24 Feb 15 10:15:11.240  0171 DECnet0037fc     DECnet009e10          ETHERNET
   25 Feb 15 10:15:11.240  0096 DECnet001f13     ab000401c0fb          ETHERNET
   26 Feb 15 10:15:11.240  0113 DEC    1c104f     09002b00000f          ETHERNET
   27 Feb 15 10:15:11.240  0171 DECnet009e10     DECnet0037fc          ETHERNET
   28 Feb 15 10:15:11.240  0216 DEC    230d12     DEC    2d4af4         ETHERNET
   29 Feb 15 10:15:11.240  0171 DECnet0037fc     DECnet009e10          ETHERNET
   30 Feb 15 10:15:11.240  0171 DECnet0037fc     DECnet009e10          ETHERNET
   31 Feb 15 10:15:11.250  0068 DECnet0016fb     ab0000030000          ETHERNET
   32 Feb 15 10:15:11.250  0171 DECnet009e10     DECnet0037fc          ETHERNET
   33 Feb 15 10:15:11.250  0064 DECnet0076f9     ab0000030000          ETHERNET
   34 Feb 15 10:15:11.250  0064 DECnet00ef10     DECnet00fc12          ETHERNET
   35 Feb 15 10:15:11.250  0171 DECnet0037fc     DECnet009e10          ETHERNET
   36 Feb 15 10:15:11.250  0096 DECnet0037fc     DECnet008310          ETHERNET
   37 Feb 15 10:15:11.250  0064 DECnet00ef10     DECnet00fc12          ETHERNET
   38 Feb 15 10:15:11.250  0064 DECnet00fc12     DECnet00ef10          ETHERNET
   39 Feb 15 10:15:11.260  0064 DEC    2d4af4     DEC    230d12         ETHERNET
   40 Feb 15 10:15:11.260  0064 DECnet00fc12     DECnet00ef10          ETHERNET
```

LJ-03579-SIX

7.1.1 Properties

Clicking on Properties causes display of an entry screen with four fields. Table 7–1 contains a description of each entry on the Protocol Decode Properties screen.

Table 7–1 Protocol Decode Properties

Entry	Description
Raw Mode	Determines whether the decoded bytes will be displayed as ASCII or EBCDIC characters.
Time Mode	Determines if the time displayed is Absolute (Month Day Time) or Delta (time difference between the arrival of the first frame and the one shown, in *hh:min:sec:ttt*).
Address Mode	Sets the Source/Destinatination address display as Network (IP), Vendor (Vendor specific MAC), or Hex.
Zoom Mode	Causes the zoom function to be enabled or disabled.

To make your selection, click on the required value and click on OK.

7.1.2 Decode

To run the Protocol Decode process from the Protocol Decode Utility screen:

1. Access a stored data file by clicking on File, and then clicking on Open. This causes the display of a selection screen where the names of stored data files are available in the client directory.
2. Select a *.dat file from the file list and then load that file by clicking on OK.

When you access the Protocol Decode Utility from Data Capture or from Packet Capture, the data file is automatically loaded.

7.2 Summary Mode

After completing the above steps, the file is displayed in summary mode in which each frame is represented by a single line numbered from 1 to *n*, where *n* is the total count of frames in the capture buffer.

The summary display field includes information regarding each frame. Table 7–2 contains a description of each entry in the Protocol Decode summary.

Table 7–2 Protocol Decode Utility Screen Entries

Entry	Description
Pkt ID	The index number of the frame, starting with 1. You can scroll through the list of frames by using the cursor. The frame currently selected is highlighted.
Arrival Time	The time stamp indicating the date and time at which this frame was captured. The format of the time stamp is *Month Day hh:mm:ss:ttt* (Absolute Mode) or *hh:mm:ss:ttt* (Delta Mode), where the last three digits indicate milliseconds (thousandths of seconds).
Size	The number of bytes in the frame.
Source Node	The HEX address of the node that sent that frame. If Vendor Name has been selected as the default, the address will be decoded showing the name of the vendor of the interface device.
Destination Node	The HEX address of the destination node specified in the frame. If vendor name has been selected as the default, the address will be decoded showing the name of the vendor of the interface device.
Status	If a frame is faulty, the type of fault (Runt, Jabber, CRC, or Align) is shown. More than one may apply.
Protocol	Identifies the highest level protocol included in that frame.

In the summary mode presentation, use of Goto Frame causes the display to show the first frame on the first line (Home) or the last frame on the last line (End). Clicking on either selection initiates the action. Clicking on the up and down arrows increments or decrements the frame by one.

In addition, inserting a frame number in the Frame Number field and pressing Enter causes that frame to be shown on the first line. Likewise, dragging the pointer on the scroll knob shown to the right of the packet field causes the summary frame display to scroll up or down respectively. The number of the last frame of the loaded frame file is automatically inserted at the end of the scroll bar.

7.2.1 Raw Mode

Clicking on Raw in the Change Mode field creates a display of the individual frame highlighted by the cursor, in Raw mode. Each row in the display area contains frame byte number, 32 HEX digits for 16 frame bytes, and 16 ASCII (EBCDIC) equivalents of the frame bytes. The display field heading includes Frame Number, Size, Arrival Time, and display mode (ASCII or EBCDIC).

In the Raw mode presentation, use of Goto Frame causes the display to show the raw decode of the the first frame in the file (Home) or the raw decode of the last frame in the file (End). Clicking on either selection initiates the action.

In addition, inserting a frame number in the Frame Number field causes the raw decode of that frame to be shown. Likewise, clicking on the Up or Down arrows in the Goto Frame field causes the raw mode frame display to scroll up or down. The number of the last frame of the loaded frame file is automatically inserted at the end of the scroll bar. Clicking on Summary returns you the the Summary screen.

7.2.2 Protocol Mode

Clicking on Protocol in the Change Mode field of either the Summary screen or the Raw screen results in the display of the frame highlighted by the cursor, in seven-level, decoded format. The decoding is fully automatic and causes the frame to be displayed in up to seven windows, each of which corresponds to successive layers of the protocol. You can scroll through each window and examine in detail the contents of each layer expressed in a readable format. If the frame contains no identifiable protocol after a certain layer, the rest of the frame is displayed as a raw dump in the last window, labelled User Data.

7.2.3 Zoom Mode

Clicking on Zoom in the Change Mode field of the Protocol screen results in the full screen display of the first layer decode. This screen in turn allows you to scroll forward or backward through the protocol layers by clicking on next layer or prev layer. You can examine new frames by using any of the techniques described earlier to scroll through the frames displayed in the Summary Mode screen.

8
Tools

Note

Only the Discovery option is currently active on the Tools pull-down menu.

Discovery is a background application that runs on DECpacketprobe agents for a user-specified time. It learns the physical (MAC) address of all active hosts on the network segment and maps them to IP addresses and host names while also identifying the node type (router, bridge, and so on). The resulting cross-reference table is stored in a file on your PROBEwatch station. This cross-reference file is named *XXXXXXXX*.dat, where *XXXXXXXX* represents the IP address of the agent where Discovery was started.

Since the file name and the file format created by Discovery is known to all the applications running under PROBEwatch for Windows, these applications can display the network IP address or host name instead of the physical address. This information is usually more meaningful to the network administrator in diagnosing network problems.

To eliminate unnecessary processing in the agent and limit network overhead, the Discovery process times out and makes no further updates to the cross-reference file until you rerun Discovery. For networks with rapid changes, you can run Discovery at routine intervals to update the cross-reference file. For hosts that come on the network after a Discovery process is complete, the application displays show the MAC address. Whenever you identify a host that has not been “discovered,” you may run Discovery to update the cross-reference file.

Discovery learns the:

- Network address of nodes that are on the agent’s segment.

Note

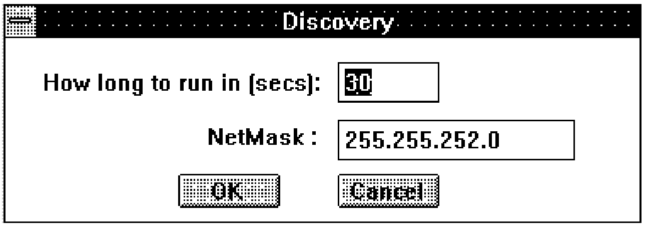
Only IP address discovery is implemented in Version 1.0 of PROBEwatch for Windows.

- Bridges on the network.
- Routers on the network.
- IP addresses of outside nodes that are conversing with nodes on the agent’s segment.

8.1 Operation

Starting from the top screen of PROBEwatch, click on Tools, drag to Discovery, and release. The setup screen for running a Discovery session is displayed. Figure 8–1 shows the screen.

Figure 8–1 Discovery Screen



How long to run in (secs): 30

NetMask : 255.255.252.0

LJ-03580-SIX

Fields that must be completed are shown on the screen with underlines:

- How long to run — Specifies the time, in seconds, that Discovery will run. For small networks, 60 seconds is usually adequate to identify all active hosts. For larger networks, times up to 10 minutes (600 seconds) is reasonable.
- Netmask — Specifies the subnet mask used to determine if a host is directly connected to a specific segment or if it must be reached through a router.

Enter the requested information in each underlined field. Click on Apply to initiate an SNMP session that instructs the selected agent to learn the IP address and logical names of the hosts on the segment. The process continues for the duration specified by you and exits the program when complete.

When the session is complete, all PROBEwatch for Windows applications have access to the cross-reference file and can display addresses in IP and logical name formats. If no name is present, the IP address is shown in *XXX.XXX.XXX.XXX* format if the host was discovered. The default representation is the interface MAC address.

9
Traps

Traps set through the WatchDog function are a simplified and direct method of establishing alarm and event conditions for trap messages. Trap messages, caused by the alarm and event conditions, may be generated by any agent in the network and reported to a centralized management station.

The Traps screen allows you to access a listing of the trap messages sent by any agent in the network to the client whose IP address is that of the station. The trap messages displayed are composed of all messages sent since the last time the Client function was initiated.

Trap messages are also logged at the local agent and may be accessed by an inquiry to the specific agent.

9.1 Operation

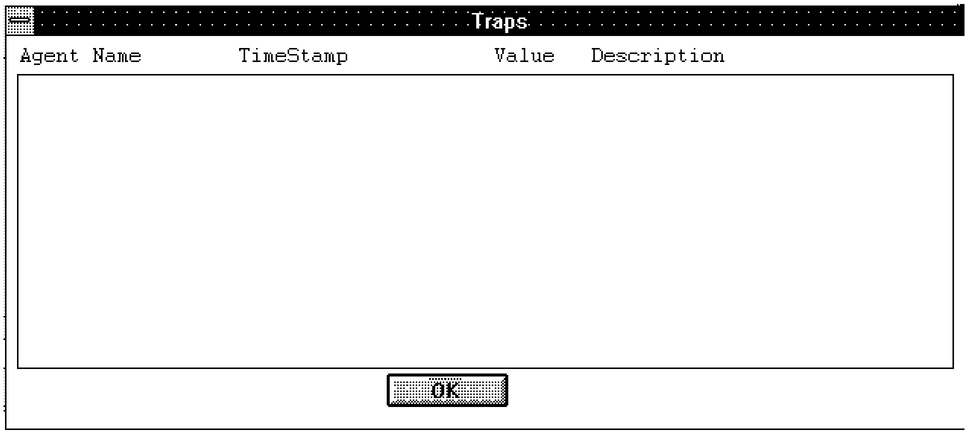
Starting from the top screen of PROBEwatch, click on Traps, drag to View Traps, and release. The Traps screen is displayed containing the following information:

Field	Description
Agent Name	The name of the agent that generated the trap.
Time Stamp	The time the trap was generated.
Value	The value that caused the trap to be generated.
Description	The threshold that was exceeded.

Figure 9–1 shows a Traps screen.

Also included on the Traps pull-down menu are Beep On and Beep Off. This feature allows you to be alerted when a trap is received.

Figure 9–1 Traps Screen



LJ-03581-SIX

A

Running PROBEwatch for Windows with the SLIP Protocol

This appendix describes how to run PROBEwatch with the SLIP protocol connected to a DECpacketprobe agent and how to exit from a SLIP session.

A.1 Making a SLIP Connection

To make a SLIP connection between your PC and a DECpacketprobe agent:

1. Connect your PC to a DECpacketprobe, a DEChub 900MS, or a terminal server that supports SLIP through a serial port on your PC, or connect to a terminal server through a modem.
2. Exit Windows, if you are currently running Windows.
3. Use the **CD** command to make your \ PROBEW\ IPSTACK directory the default directory. For example:

   ```
   c: cd \probew\ipstack
   ```

4. Ensure that the **[TCP/IP]** section of the PWTCP.INI file includes the following line:

   ```
   NetworkType =2
   ```

5. Enter the SETHOST terminal emulator command as follows:

   ```
   c: sethost
   ```

A.2 Running a SLIP Session

To run PROBEwatch with a SLIP connection to a DECpacketprobe:

1. From the **SETHOST** main menu, press F3 to access the Setup menu.
2. From the Setup menu, select communication.

3. From the Communications menu, select the speed.

Note

The speed you select will be the baud rate for the SLIP connection. Be sure that the speed you select matches the baud rate in the **[SLIP]** section of TCP.INI file in your \PROBEW\IPSTACK directory.

4. From the **SETHOST** main menu, press Return to access the DECpacketprobe menu.
5. From the DECpacketprobe menu, select Start SLIP Connection.
6. Press Ctrl+F10 to exit from the **SETHOST** program.
7. Enter the following command at the DOS prompt to start your network:

```
c: strtslip
```

8. Enter the following command at the DOS prompt to start Windows:

```
c: win
```

9. Start PROBEwatch, following the instructions in Chapter 3.

   PROBEwatch should perform as it does under IP networks, except that it will be somewhat slower.

A.3 Exiting the SLIP Session

To exit from the SLIP session:

1. Exit from PROBEwatch by selecting **Exit** from the File menu on the ???
2. Exit from Windows by, for example, selecting **Exit Windows** from the Program Manager's File menu.
3. Enter the following command at the DOS prompt to stop your network:

```
c: stopnet
```

4. Reset the DECpacketprobe agent.

B

MIB Groups and Communities

This appendix provides information about the management information base (MIB) groups that are supported by DECpacketprobe. It also provides information about the slot table and communities.

B.1 MIB Groups

A MIB is a collection of manageable objects for a given entity. The following standard MIBs are supported by DECpacketprobe:

- MIBII
- System and interface groups (RFC 1213)
- Remote LAN Monitoring MIB (RFC 1271)

B.1.1 MIBII

MIBII, like its predecessor, the Internet-standard MIB, contains only essential elements. There is no need for individual objects to be optional. Rather, the objects are arranged into the following groups:

- System
- Interfaces
- Address translation (deprecated)
- IP
- ICMP
- TCP (not supported by DECpacketprobe)
- UDP
- EGP (not supported by DECpacketprobe)
- Transmission (not supported by DECpacketprobe)

- SNMP

Note

Only System and Interfaces are supported by Version 1.0 of DECpacketprobe.

These groups are the basic unit of conformance. This method is as follows:

If the semantics of a group is applicable to an implementation, then it must implement all objects in that group. For example, an implementation must implement the EGP (Exterior Gateway Protocol) group if, and only if, it implements the EGP.

B.2 Communities

A community, in the SNMP sense, is a set of manageable attributes that are managed as a group. Normally, there is a one-community-to-one-agent relationship. The manageable attributes are usually contained within a single hardware device, or within a single enclosure, when referenced with hubs. The single hardware device, or the collection of devices within a hub, is treated as one community. A particular manageable entity is uniquely identified on the network by the combination of an IP address and a community string.

A community string is a sequence of ASCII characters that is checked by the SNMP agent for access control to the manageable entity. The community string can be thought of as a password. Two strings are associated with a given community: the read-only string and the read/write string. For a Get or a Get Next operation, the agent accepts either the read-only or the read/write string. However, for a Set operation, the agent accepts only the read/write string.

C

Running PROBEwatch for Windows with a PATHWORKS Network

This appendix contains instructions for those who will be using PROBEwatch with a PATHWORKS TCP/IP network.

C.1 Setting Up Your Network Prior to Using PROBEwatch

If you are running a TCP/IP network with PATHWORKS Version 5.0, no special instructions are needed to run PROBEwatch.

If you are running a DECnet network with PATHWORKS Version 5.0, perform the following steps to run PROBEwatch:

1. Use the PROBEwatch installation procedure to install an IP (NDIS) network.
2. Enter the following command at the MS–DOS prompt:

```
PROBEwatch_drive:PROBEwatch_path\ipstack\strtndis
```

You are now ready to start PROBEwatch.

If you are running a network with PATHWORKS Version 4.1, perform the following steps to use PROBEwatch:

1. Use the PROBEwatch installation procedure to install an IP (NDIS) network.
2. Enter the following command at the MS–DOS prompt:

```
pathworks_drive:pathworks_path\stopnet
PROBEwatch_drive:PROBEwatch_path\ipstack\strtndis
```

You are now ready to start PROBEwatch.

D

Default Names

Table D–1 contains the protocol default names and protocol IDs.

Table D–1 Default Table

Protocol	Protocol ID	Protocol	Protocol ID
	Ethernet Type		
DODIP	0x0800	XNSIDP_1	0x0600
XNSIDP_2	0x0807	DODIP	0x0800
DODARP	0x0806	DODRARP	0x8035
VINESIP	0x0BAD	DECMOPDL	0x6001
DECMOPRC	0x6002	DECDRP	0x6003
DECLAT	0x6004	DECCLUSTER	0x6007
NOVELL_1	0x8137	NOVELL_2	0x8138
APPLETALK	0x809B	APPLEARP	0x80F3
SNATH	0x04	SNAXID	0x05
NETBIOS	0xF0		
	SAPS		
IP_SAP	0xaa	OSI_SAP	0xfe
NOVELL1_SAP	0xe0	NOVELL2_SAP	0xff
	IP Ports		
DODICMP	1	DODGGP	3
DODTCP	6	DODUDP	17

(continued on next page)

Table D–1 (Cont.) Default Table

Protocol	Protocol ID	Protocol	Protocol ID
	TCP Ports		
FTP	21	TELNET	23
SMTP	25	TFTP	69
DNS	53	SUNRPC	111
NTB_NAME	137	NTB_SESSION	139
EXEC	512	RLOGIN	513
SHELL	514	UNIX_SPOOLER	515
EFS	520	TEMPO	526
COURIER	530	CONFERENCE	531
NETNEWS	532	UUCP	540
REMOTEFS	556	INGRESLOCK	1524
	UDP Ports		
NAMESERVER	42	DODDNS	53
DODTFTP	69	NTBNAME	137
NTBDATA	138	SNMP	161
SNMPTRAP	162	BIFF	512
WHO	513	SYSLOG	514
TALK	517	NTALK	518
ROUTE	520	TIMED	525
NETWALL	533	APPLE_TALK	770

(continued on next page)

Table D–1 (Cont.) Default Table

Protocol	Protocol ID	Protocol	Protocol ID
MAC Addresses For Various Vendors			
Broadcast	0xffffffffffff	Multicast	0x01
FrnSoft	0x00808c	Cisco	0x00000c
Fibron	0x00000d	NeXT	0x00000f
DIAB	0x000020	VisTec	0x000022
TRW	0x00002a	S&Koch	0x00005a

(continued on next page)

Table D–1 (Cont.) Default Table

Protocol	Protocol ID	Protocol	Protocol ID
	MAC Addresses For Various Vendors		
NetGen	0x000065	Concor	0x000069
MIPS	0x00006b	Ardent	0x00007a
SynOpt	0x000081	Cayman	0x000089
Proteo	0x000093	Ameris	0x00009f
NetSys	0x0000a9	Xerox	0x0000aa
Wang	0x0000d3	CIMLin	0x0000b3
AllenB	0x0000bc	WesDig	0x0000c0
Eon-HP	0x0000c6	3ComPS	0x0000d8
Gould	0x0000dd	Acer	0x0000e2
BBN	0x000102	Kabel	0x001700
FrnSof	0x00808c	Intel	0x00aa00
Wang	0x00d300	UBas1	0x00dd00
UBas2	0x00dd01	Wang	0x0100d3
MICInt	0x020701	BBNInt	0x020406
3Com	0x02608c	CMC	0x02cf1f
SunOLD	0x080001	Bridge	0x080002
ACC	0x080003	Symbol	0x080005
BBN	0x080008	HP	0x080009
Nestar	0x08000a	UniSys	0x08000b
AT&T	0x080010	Tektro	0x080011
Exceln	0x080014	NSC	0x080017
DG-A	0x08001a	DG-B	0x08001b
Apollo	0x08001e	Sun	0x080020

(continued on next page)

Table D–1 (Cont.) Default Table

Protocol	Protocol ID	Protocol	Protocol ID
MAC Addresses For Various Vendors			
NBI	0x080022	CDC	0x080025
PCSSys	0x080027	TI	0x080028
DEC	0x08002b	Prime	0x08002f
InterG	0x080036	FujXer	0x080037
Spider	0x080039	DCA	0x080041
Xylogi	0x080045	Sony	0x080046
Sequen	0x080047	Univat	0x080049
Encore	0x08004c	BICC	0x08004e
IBM	0x08005a	ComDes	0x080067
Ridge	0x080068	SilicG	0x080069
Exceln	0x08006e	DDE	0x080075
Vitali	0x08007c	XIOS	0x080080
Imagen	0x080086	Xyplex	0x080087
Kinet	0x080089	Pyrami	0x08008b
XyVis	0x08008d	IBM	0x10005a
DEC	0xaa0003	DEC	0xaa0004
Novell Ports			
NOVRIP	1	NOVECHO	2
NOVERROR	3	NOVPEP	4
NOVSPX	5	Netware	17
NTB_DATA	137	NTB_NAME	138
NTB_SESSION	139	SNA_TH	1
ISO_TP	0x90	ISO_PRE	0x96
ISO_SESS	0x95		

E

PROBEwatch for Windows Troubleshooting

This appendix describes steps to take if PROBEwatch for Windows will not start when you use the methods described in Section 1.8, or in Appendix B for running PROBEwatch with SLIP.

If PROBEwatch does not start, first check that your network is up and the DECpacketprobe you are trying to connect to is in working order. If PROBEwatch still does not start, check the PROBEwatch installation. This appendix includes the following topics:

- Checking the network connection to the DECpacketprobe
- Checking the PROBEwatch installation
- Checking the NDIS network installation
- Checking the SLIP network installation
- Checking the setup for a non-Digital network interface card

E.1 Checking the Network Connection to the DECpacketprobe

If PROBEwatch does not start, perform the following steps:

1. Ensure that you have the correct IP address and community name of a DECpacketprobe on the network. Check with your network administrator.
2. Attempt to start PROBEwatch again, using a correct IP address and community name.

   If PROBEwatch still does not start, use the PING command to test whether your network is up and the object you are trying to connect to is in working order. First PING an object that you know should respond.

3. Use the CD command to make your \ PROBEW\ IPSTACK directory the default directory. For example:

   ```
   c: cd \probew\ipstack
   ```

4. Enter the following command at the DOS prompt:

   ```
   c: ping ip_address
   ```

   where an ip_address is of the form d.d.d.d, d being an integer from 0 to 255. For example:

   ```
   c: ping 00.20.30.40
   ```

If the PING command is successful, try it again using the IP name of the DECpacketprobe as defined in the HOSTS. file or on the IP Name Server.

If the network is not up, you will receive a message that you were unable to connect to the object. If the network was installed by the PROBEwatch installation procedure, check that the network was installed properly.

- Refer to Section E.3, if you installed an NDIS network.
- Refer to Section E.4, if you installed SLIP.
- Refer to Section E.5, if you are using a non-Digital network interface card.

If the network is up but the DECpacketprobe you specified in the PING command is not operating properly, you will receive a message that the object did not respond. In that case, refer to the hardware manual for the DECpacketprobe.

E.2 Checking the PROBEwatch Installation

To check the PROBEwatch installation, do the following:

1. Ensure that the following .EXE files are among those in your top-level PROBEwatch installation directory (the installation procedure places these in C:\ PROBEW by default):
   - NSMAN.EXE
   - DVMAIN.EXE
2. Ensure that the PROBEwatch Agent file XXXXX.AGE, is in the directory you selected for your user data file. The .AGE files should be under your top-level PROBEwatch directory, by default.

3. If you used the PROBEwatch installation procedure to install your network, ensure that you have the directory \ IPSTACK under your top-level PROBEwatch directory. Enter the following command at the DOS prompt:

   ```
   c: dir \path_to_probewatch_directory\IPSTACK
   ```

4. Ensure that your AUTOEXEC.BAT file is edited as follows:

   If you added a network startup command to AUTOEXEC.BAT, after using the PROBEwatch installation procedure to install the network, the following line must appear before the command, if any, that starts WINDOWS:

   ```
   call probewatch_drive:path-to-probewatch_directory\IPSTACK\STRTNDIS
   ```

E.3 Checking the NDIS Network Installation

If you used the PROBEwatch installation procedure to install an NDIS network, do the following to check whether the network is properly installed:

1. Ensure that subdirectory \ IPSTACK in your PROBEwatch directory contains the following files:
   - PWTCP.INI
   - STRTNDIS.BAT
   - PROTOCOL.INI.
   - WINSOCK.DLL
2. Ensure that the contents of PWTCP.INI include the following lines, in the indicated sections. The parameter names are case sensitive.

   ```
   [TCPGLOBAL]
     UserName = user_name
     HostName = pc_name
     NetFiles = drive:\path\IPSTACK

   [TCPIP]
     IPAddress = pc_ip_address
     SubnetMask = subnet_mask
     DefaultGW0 = default_gateway_ip_address
     NetworkType = network_type_identifier

   [DNR]
     NameServer0 = first_name_server_to_query_ip_address
     Domain = local_domain_ip_name
   ```

where:

an ip_address or a subnet_mask is of the form d.d.d.d, d being an integer from 0 to 255.

network_type_identifier is 0, for Ethernet, 2, for SLIP.

For example:

```
[TCPGLOBAL]
UserName = d_dinant
HostName = daves_pc
NetFiles = c:\probew\ipstack
[TCPIP]
IPAddress = 00.00.00.00
SubnetMask = 00.00.00.00
DefaultGW0 = 00.00.00.00
NetworkType = 0
[DNR]
NameServer0 = 00.00.00.00
Domain = dod.xxx.com
```

If your subnet mask or DefaultGWO has xxx.xxx.xxx.xxx, then you need to edit this file and put in valid IP format numbers.

3. Ensure that the contents of STRTNDIS.BAT include the following lines:

Note

The REM lines below are not included in STRTNDIS.BAT. They appear here only, for explanatory purposes.

```
probewatch_drive:
CD \path_to_probewatch_directory\IPSTACK
SET PCSA = probewatch_drive:path_to_probewatch_directory\IPSTACK
LD PROTMAN.DOS /i:probewatch_drive:path_to_probewatch_directory\IPSTACK
REM the next commands save the current path in IPSTACK\OLDPATH.BAT
IF %PATH% == "" GOTO no_path
 PATH > probewatch_drive:\path_to_ipstack\OLDPATH.BAT
 GO TO path_done
:no_path
ECHO SET PATH => probewatch_drive\path_to_ipstack\OLDPATH.BAT
:path_done
SET PATH = %PCSA%,%PATH%
REM end of commands for saving the current path
LD ndis_network_card_driver
```

For example:

```
c:
cd \probew\ipstack
set PCSA = c:\probew\ipstack
ld protman.dos /i:c:\hubstack\ipstack
if %path% == "" goto no_path
 path >c:\probew\ipstack\oldpath.bat
 goto path_done
:no_path
echo set path =>c:\probew\ipstack\oldpath.bat
:path_done
SET PATH=%PCSA%;%PATH%
ld ewrk3.dos
```

Note

If you change the network card and use the installation program to modify your network parameters, check the STRTNDIS.BAT file to be sure that the line that loaded the previous driver begins with REM, as follows:

```
rem ld previous_network_card_driver
```

4. Ensure that the protocol file appropriate to your network card was copied into file PROTOCOL.INI. Depending on the network option you selected at installation, the installation procedure copies the contents of file IPSTACK\ EWRK3.PRO or IPSTACK\ DEPCA.PRO to PROTOCOL.INI.
5. Ensure that the file SYSTEM.INI in your WINDOWS directory is edited as follows:
   - In the [Boot] section, the NETWORK.DRV = command is as follows:

     ```
     network.drv = pcsa.drv
     ```

   - In the [386Enh] section, the NETWORK = command is as follows:

     ```
     network = *dosnet,*vnetbios,decpw.386
     ```

6. Ensure that your AUTOEXEC.BAT file is edited as follows:

   If you added a network startup command to AUTOEXEC.BAT, after using the PROBEwatch installation procedure to install the network, the following line must appear before the command, if any, that starts WINDOWS:

   ```
   call probewatch_drive:path-to-probewatch_directory\IPSTACK\STRTNDIS
   ```

7. Ensure that you are not trying to run DECnet and PROBEwatch at the same time, unless you are running PATHWORKS Version 5.0. If you are running PATHWORKS Version 4.0, enter the following commands at the DOS prompt, before starting PROBEwatch:

   ```
   c: pathworks_path\stopnet
   c: probewatch_path\strtndis
   ```

E.4 Checking the SLIP Network Installation

If you used the PROBEwatch installation procedure to install your SLIP network, do the following to check whether your Digital IP network is properly installed:

1. Ensure that subdirectory \IPSTACK in your PROBEwatch directory contains the following files:
   - PWTCP.INI
   - STRTSLIP.BAT
   - WINSOCK.DLL
2. Ensure that the contents of file STRTSLIP.BAT include the following lines:

   ```
   probewatch_drive:
   CD \path_to_probewatch_directory\IPSTACK
   SET PCSA = probewatch_drive:path_to_probewatch_directory\IPSTACK
   SAVE
   SCHK.EXE /NDIS
   DLLASYNC.EXE
   TCPIP.EXE
   DNR.EXE
   INETNAME.EXE
   TN.EXE
   BAPI.EXE
   ```

   For example:

   ```
   c:
   cd \nets\probew\ipstack
   set pcsa =c:\nets\probew\ipstack
   save
   schk /ndis
   dllasync
   tcpip
   dnr
   inetname
   tn
   bapi
   ```

3. Ensure that the [TCPIP] section of file PWTCP.INI includes the following line:

   ```
   NetworkType = 2
   ```

4. Ensure that the [SLIP] section of file PWTCP.INI includes the following lines:

   ```
   CommPort = COMn
   Speed = speed
   ModemControl = no
   ```

   where:

   n is the number of the COM port you are using for you SLIP connection. The default is COM1.

   speed is the baud rate your SLIP connection is using. The default is 9600.

E.5 Checking a Non-Digital Network Interface Card Setup

If you used the PROBEwatch installation procedure to install your network and chose Other as network interface card type, ensure that your PC is properly set up for your card.

1. Ensure that the file probewatch_path\IPSTACK\STRTNDIS.BAT includes the following line:

   ```
   LD your_ndis_network_card_driver
   ```

   The name of the driver should be the name you supplied during the installation procedure, when you selected Other as the card type.

   Note

   If you change the network card and use the installation program to modify your network parameters, check the STRTNDIS.BAT file to be sure that the line that loaded the previous driver begins with REM, as follows:

   ```
   rem ld previous_network_card_driver
   ```

2. Ensure that the protocol file appropriate to your network card was copied into file probewatch_path\IPSTACK\PROTOCOL.INI.

3. Before starting PROBEwatch, start your network with the following command:

```
cd path-to-probewatch_directory\IPSTACK\STRTNDIS
```

Index