

# PROBEwatch for ULTRIX

---

## User Manual

Order Number: AA-Q0GAA-TE

**Revision Update Information:** This is a new manual.

---

**First Edition, August 1993**

The information in this document is subject to change without notice and should not be construed as a commitment by Digital Equipment Corporation. Digital Equipment Corporation assumes no responsibility for any errors that may appear in this document.

The software described in this document is furnished under a license and may be used or copied only in accordance with the terms of such license.

No responsibility is assumed for the use or reliability of software on equipment that is not supplied by Digital Equipment Corporation or its affiliated companies.

Restricted Rights: Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of DFARS 252.227-7013, or in FAR 52.227-19 or FAR 52.227-14, Alt. III, as applicable.

Digital conducts its business in a manner that conserves the environment and protects the safety and health of its employees, customers, suppliers, partners, and the community.

© Digital Equipment Corporation and Frontier Software Development, Inc. 1993.

All Rights Reserved.  
Printed in the U.S.A.

The following are trademarks of Digital Equipment Corporation: DEC, DECbridge, DECconnect, DEChub, DECmcc, DECnet, DECrepeater, DECserver, DECpacketprobe, Digital, HUBwatch, LAT, MicroVAX, ThinWire, UNIBUS, VMS, VAX, and the Digital logo.

The following are third-party trademarks:

OSF, and OSF/Motif are trademarks of the Open Software Foundation, Inc. Windows is a trademark of Microsoft Corporation. PostScript is a trademark of Adobe Systems, Inc. and may be registered in certain jurisdictions.

All other trademarks and registered trademarks are the property of their respective holders.

This document was prepared using VAX DOCUMENT, Version 2.1.

---

# Contents

<b>Preface</b> .....	ix
<b>1 Introduction</b>	
1.1 Function .....	1-1
1.2 Standards .....	1-1
1.3 Basic Terms .....	1-2
1.4 Protocol Structure .....	1-3
1.4.1 OSI Model .....	1-3
1.5 Frame Structure .....	1-5
1.6 Protocol Analysis .....	1-7
1.6.1 Protocols Supported .....	1-7
1.7 Topology .....	1-8
1.8 PROBEwatch Operation .....	1-8
1.8.1 Operation of PROBEwatch with Polycenter Network Manager .....	1-9
1.8.2 Operation of PROBEwatch Without Polycenter Network Manager .....	1-9
<b>2 Installation and Overview</b>	
2.1 Mouse Operation .....	2-1
2.2 Getting Started .....	2-2
2.2.1 Installing Standalone .....	2-4
2.2.2 Installing PROBEwatch With Polycenter Network Manager .....	2-4
2.2.3 Accessing the DECpacketprobe Agent .....	2-6
2.2.3.1 Configure .....	2-7
2.2.3.2 Statistics .....	2-9
2.2.3.3 Filters .....	2-11
2.2.4 Accessing PROBEwatch .....	2-11
2.3 Top Level Operations .....	2-11
2.4 Domain View .....	2-14

2.5	Data Capture .....	2-15
2.6	Protocol Decode .....	2-16
2.7	Management Tools .....	2-16
2.7.1	Discovery .....	2-16
2.7.2	Names Editor .....	2-17
2.8	Traps .....	2-17

### 3 Fundamentals of Operation

3.1	Control Entries .....	3-1
3.1.1	Add .....	3-3
3.1.2	Change .....	3-3
3.1.3	Delete .....	3-3
3.2	Common Terms .....	3-4
3.2.1	Index .....	3-4
3.2.2	Data Source .....	3-4
3.2.3	Status .....	3-5
3.2.4	Owner .....	3-5
3.3	Symbolic Names .....	3-5
3.3.1	Default Names .....	3-9

### 4 Domain View

4.1	Description .....	4-1
4.2	Operation .....	4-2
4.2.1	Segment .....	4-5
4.2.2	Editor .....	4-5
4.2.3	Properties .....	4-5
4.2.4	Watchdog .....	4-5
4.2.5	Scope .....	4-5
4.2.6	View Packets .....	4-5
4.3	Segment .....	4-5
4.3.1	Operation .....	4-7
4.3.2	Segment Zoom Push Buttons .....	4-10
4.3.2.1	Host List .....	4-10
4.3.2.2	Host Zoom .....	4-11
4.3.2.3	Conversation List .....	4-13
4.3.2.4	Quick Graph for Domain View .....	4-14
4.3.2.5	Command Line Operation .....	4-15
4.4	Domain .....	4-19
4.4.1	Install .....	4-19
4.4.2	Deinstall .....	4-19
4.5	Editor .....	4-20

4.5.1	Operation .....	4-21
4.6	Properties .....	4-24
4.6.1	Operation .....	4-24
4.6.1.1	Properties Push Buttons .....	4-26
4.6.2	Watchdog .....	4-28
4.6.2.1	Operation .....	4-28
4.6.3	Scope .....	4-30
4.6.3.1	Operation .....	4-30
4.6.4	View Packets .....	4-32
4.6.4.1	View Packets Push Buttons .....	4-34
<b>5</b>	<b>Data Capture</b>	
5.1	General .....	5-1
5.1.1	Operation .....	5-1
<b>6</b>	<b>Protocol Decode</b>	
6.1	Framework .....	6-1
6.1.1	Sequence .....	6-2
6.1.2	Protocol Decode Operation .....	6-2
6.2	Viewing Packets .....	6-5
6.3	Change Mode .....	6-6
6.3.1	Raw Mode .....	6-6
6.3.2	Protocol Mode .....	6-8
6.4	Zoom Mode .....	6-10
6.5	Post-Capture Filters .....	6-10
<b>7</b>	<b>Management Tools</b>	
7.1	Discovery .....	7-1
7.2	Names Editor .....	7-4
<b>8</b>	<b>Traps</b>	
8.1	Description .....	8-1

## A MIB Groups and Communities

A.1	Introduction . . . . .	A-1
A.2	MIB Groups . . . . .	A-1
A.2.1	MIBII . . . . .	A-2
A.3	Communities . . . . .	A-2

## B Documentation and Ordering Information

B.1	Introduction . . . . .	B-1
B.2	Related Documentation . . . . .	B-1
B.3	Ordering Information . . . . .	B-1

## Index

## Figures

2-1	Management System Window . . . . .	2-5
2-2	Four Alternatives . . . . .	2-6
2-3	View Options . . . . .	2-8
2-4	PROBEwatch Management Screen . . . . .	2-12
2-5	Add Agent . . . . .	2-14
4-1	Domain View . . . . .	4-3
4-2	Segment Zoom . . . . .	4-8
4-3	Quick Graph: Network Statistics 3-D Bar . . . . .	4-17
4-4	Quick Graph: Host . . . . .	4-18
4-5	Domain Install Screen . . . . .	4-19
4-6	Domain Editor . . . . .	4-20
4-7	Create: Domain . . . . .	4-22
4-8	Domain View Properties . . . . .	4-25
4-9	Watchdog Screen . . . . .	4-29
4-10	Scope Screen . . . . .	4-31
4-11	View Packets Screen . . . . .	4-33
5-1	Data Capture . . . . .	5-2
6-1	PROBEwatch Protocol Decode . . . . .	6-3
6-2	Raw Decode . . . . .	6-7
6-3	Protocol Decode . . . . .	6-9
6-4	Post-Capture Filtering . . . . .	6-11
7-1	Popup Discovery . . . . .	7-3

7-2	Names Editor Screen .....	7-5
8-1	Trap Window .....	8-2

## Tables

1-1	OSI Seven-Layer Functions .....	1-4
1-2	Frame Structure Description .....	1-6
2-1	Configure Selection Functions .....	2-7
2-2	Statistics Selection Functions .....	2-9
2-3	Filters Selection Functions .....	2-11
2-4	Agent Selections .....	2-13
2-5	Data Capture Functions .....	2-16
3-1	Data Collection Parameters .....	3-2
3-2	Default Table .....	3-9
4-1	Segment Zoom Screen Fields .....	4-6
4-2	Segment Zoom Field Descriptions .....	4-9
4-3	Graph Characteristics .....	4-15
4-4	Domain editor Fields .....	4-21
4-5	Domain View Properties Field Descriptions .....	4-26
4-6	Watchdog Field Descriptions .....	4-30
4-7	Scope Field Descriptions .....	4-32
4-8	View Packets Field Descriptions .....	4-32
4-9	View Packets Push Buttons .....	4-34
5-1	Data Capture Screen Push Buttons .....	5-3
5-2	Data Capture Screen Fields .....	5-4





---

## Preface

This document describes the installation and operation of the PROBEwatch Remote Monitoring Management Information Base compatible client. This product is designed for use on a centralized network management console in a distributed heterogeneous network.

The client function commands and interoperates with DECpacketprobe 90. The agents collect and store statistical and message data for the network segment to which they are attached.

### Document Organization

This manual is comprised of the following chapters:

- 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. Also provides information on getting started and using the top-level screen menu options.
- Chapter 3—Addresses control entries, common terms, and symbolic names used with PROBEwatch.
- Chapter 4—Explains how Domain View is a PROBEwatch function that provides all the power of the RMON standard while hiding the details of the RMON-MIB from the user.
- Chapter 5—Describes how this utility captures packets from the DECpacketprobe 90 agent in a selective manner.
- Chapter 6—Defines protocol decode and shows you how to use it.
- Chapter 7—Describes the following PROBEwatch tools: Discovery, and Names Editor.
- Chapter 8—Defines traps and their uses.
- Appendix A—Contains descriptions for each object within the RMON MIB.

- Appendix B—Contains information on how to order related documentation.

## Conventions

The following table lists the conventions used in this manual.

Convention	Meaning								
<b>Note</b>	Contains important information.								
<span style="border: 1px solid black; padding: 2px;">Return</span>	A key name enclosed in a box indicates that you press that key. In this example, you would press the Return key only.								
<i>Italic type</i>	Emphasizes important information, indicates variables, and indicates complete titles of documents.								
<b>Boldface type</b>	Indicates user input.								
Monospaced type	Indicates text that the system displays on the screen.								
Click on	To press and release a mouse button when the pointer is positioned on an active object.								
Drag	To press and hold a mouse button, move the mouse, and then release the button.								
MB	Indicates a mouse button.								
	<table border="1"> <thead> <tr> <th>Mouse Button</th> <th>Position</th> </tr> </thead> <tbody> <tr> <td>MB1</td> <td>Left mouse button</td> </tr> <tr> <td>MB2</td> <td>Middle mouse button (right button on a two button mouse)</td> </tr> <tr> <td>MB3</td> <td>Right mouse button</td> </tr> </tbody> </table>	Mouse Button	Position	MB1	Left mouse button	MB2	Middle mouse button (right button on a two button mouse)	MB3	Right mouse button
Mouse Button	Position								
MB1	Left mouse button								
MB2	Middle mouse button (right button on a two button mouse)								
MB3	Right mouse button								
Underline	Indicates the underlined letter on the screen menu item, option or button. 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 border="1"> <thead> <tr> <th>To . . .</th> <th>Press . . .</th> </tr> </thead> <tbody> <tr> <td>Access menu items</td> <td><span style="border: 1px solid black; padding: 2px;">Alt</span> and the underlined letter</td> </tr> <tr> <td>Access options</td> <td><span style="border: 1px solid black; padding: 2px;">Shift</span> and the underlined letter</td> </tr> <tr> <td>Activate buttons</td> <td><span style="border: 1px solid black; padding: 2px;">Alt</span> and the underlined letter</td> </tr> </tbody> </table>	To . . .	Press . . .	Access menu items	<span style="border: 1px solid black; padding: 2px;">Alt</span> and the underlined letter	Access options	<span style="border: 1px solid black; padding: 2px;">Shift</span> and the underlined letter	Activate buttons	<span style="border: 1px solid black; padding: 2px;">Alt</span> and the underlined letter
To . . .	Press . . .								
Access menu items	<span style="border: 1px solid black; padding: 2px;">Alt</span> and the underlined letter								
Access options	<span style="border: 1px solid black; padding: 2px;">Shift</span> and the underlined letter								
Activate buttons	<span style="border: 1px solid black; padding: 2px;">Alt</span> and the underlined letter								

# 1

---

## Introduction

The PROBEwatch client is a network diagnostic application providing network users with the capability to identify and to isolate fault conditions in data communications networks.

### 1.1 Function

As a distributed system, PROBEwatch (in conjunction with a DECpacketprobe) is capable of the following:

- Collecting a wide range of statistical data
- Displaying captured and fully decoded network traffic
- Setting user-defined alarm conditions
- Obtaining realtime updates from all segments of a widely dispersed internetwork from a centralized SNMP-compatible network management console

### 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 90.
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.

## Introduction

### 1.2 Standards

Also, 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 in order to use PROBEwatch.

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 present 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.
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 utilize the same network addressing scheme. Multiple networks may be interconnected together 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.

## Introduction

### 1.3 Basic Terms

Term	Definition
Node	A node is an individually addressable location on a data communications network. In RMON-MIB terminology, a <i>host</i> and a <i>node</i> are the same. A node may be any number of physical devices including personal computers, a larger scale server computer, a printer, etc. 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.

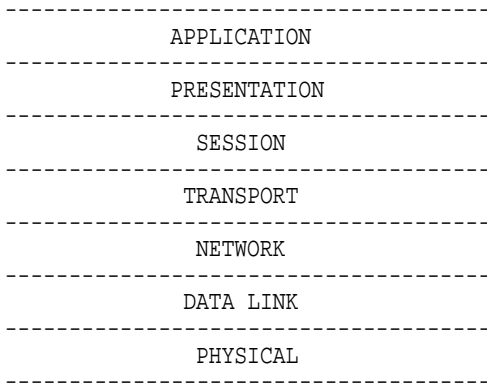
## 1.4 Protocol Structure

Protocols are the rules by which data communications devices 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, displayed in the following illustration is often described as a “stack” or “suite.” You can identify network malfunctions by examining the detailed contents of these protocol stacks.

**Introduction**  
**1.4 Protocol Structure**



**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: <ul style="list-style-type: none"> <li>• Provides reliable data transmission from one node to another</li> <li>• Shields higher layers from concerns about the physical transmission medium</li> </ul> It is concerned with the error-free transmission of frames of data.
Network	The network layer does the following: <ul style="list-style-type: none"> <li>• Routes data from one network node to another</li> <li>• Establishes, maintains, and terminates the network connection between two users</li> <li>• Transfers data along the network connection</li> </ul> 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.

(continued on next page)

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

Layer	Function
Transport	<p>The transport layer performs the following:</p> <ul style="list-style-type: none"><li>• Provides data transfer between two given users</li><li>• 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.</li></ul>
Session	<p>The session layer provides the following:</p> <ul style="list-style-type: none"><li>• Organizes and synchronizes the dialog between users</li><li>• Manages the data exchange between users</li><li>• Controls the sending and the receiving of data based on whether data can be sent and received concurrently or alternately</li></ul>
Presentation	<p>The presentation layer is responsible for the presentation of meaningful information to the network users. This may include any of the following:</p> <ul style="list-style-type: none"><li>• Character code translation</li><li>• Data conversion</li><li>• Data compression and expansion</li></ul>
Application	<p>The application layer allows application processes access to the system interconnection facilities. Once inside the interconnection facilities, the application processes can do the following:</p> <ul style="list-style-type: none"><li>• Exchange information about services used to establish and terminate the connections between users</li><li>• Monitor and manage the systems being interconnected and the various resources they employ</li></ul>

## 1.5 Frame Structure

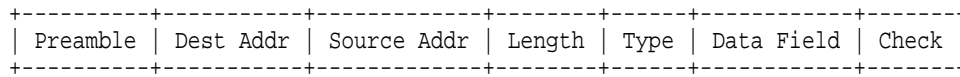
Data transfer is implemented through data packets. They are successively encapsulated by the information necessary to fulfill the requirements of each protocol layer. These encapsulated packets are referred to as frames. The format for an Ethernet frame is shown in Figure 2. Other transmission

## Introduction

### 1.5 Frame Structure

techniques are composed of similar frame segments with the specific protocols determining the detail.

**Figure 2: Frame**



**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 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 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

DECpacketprobe 90 performs the following tasks:

- Captures network traffic in the form of frames from any operational PROBEwatch.
- 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 given packet is included in or excluded from the desired set.

### 1.6.1 Protocols Supported

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

Ethernet	IEEE8023	IEEE8025	IEEE8022
DODIP	DODARP	DODRARP	DODICMP
DODGGP	DODTCP	DODUDP	DODSMTP
DODFTP	DODTFTP	DODDNS	DODTLNT
DODNTB	DODNTDAT	DODNTNAM	DODSMB
NOVIPX	NOVSPX	NOVRIP	NOVECHO
NOVERRP	NCP	XNSIPX	XNSSPX
XNSRIP	XNSECHO	XNSERRP	XNSPEXP
XNSSMB	DECGRP	DECMOPDL	DECMOPRC
DECLAT	DECLDATA	DECNSP	DECSCP
DECDAF	DECNICE	DECFOUND	DECCTERM
DECSMB	APPLAP	APPARP	APPSDDP
APPLDDP	APPNBP	APPATP	APPZIP
APPRTMP	APPAEP	APPPAP	APPASP
APPDSP	APPAFP	VINESIP	VINESRTP
VINESARP	VINESICP	VINESIPC	VINESSPP
VINESMM	VINESST	VINEMAIL	SNMP

## Introduction

### 1.6 Protocol Analysis

SUNNFS	SUNRPC	SUNMOUNT	SUNPMAP
SUNYP	SNAXID	SNATH	IBMNETB
SNARHREQ	SNARHRES	SNARU	SNAFM
SNAPS	IBMSMB	CLNS	ES-IS
TP 0/2/4	ISO-Session	ISO-Presentation	FTAM
X400			

### 1.7 Topology

The differences between PROBEwatch and DECpacketprobe 90 are as follows:

Category	Definition
Client	The user console 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.
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 is one of the following:

Protocol	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.

### 1.8 PROBEwatch Operation

PROBEwatch can be installed to operate either in conjunction with Digital's Polycenter products or as a standalone application on an ULTRIX workstation.

### 1.8.1 Operation of PROBEwatch with Polycenter Network Manager

PROBEwatch is a software package that operates in conjunction with the Polycenter Network Manager on the Polycenter SNMP Manager, including:

- Complete statistics gathering
- Event and alarm generation
- Packet capture and decode

Polycenter Network Manager and Polycenter SNMP Manager provide the following:

- Background operational tools for client operation while the PROBEwatch software provides application-specific functions related to RMON-MIB support.
- Other network device management besides RMON-MIB devices.
- Implementation of a network map file. This file includes a topographical display of the entire network. You use this display to select network elements to perform operations.

Each DECpacketprobe is graphically represented on the network map. When you select a DECpacketprobe from the map, it becomes the target of commands issued by the client; thus, starting a diagnostic process.

### 1.8.2 Operation of PROBEwatch Without Polycenter Network Manager

You can operate PROBEwatch, from the ULTRIX shell, without Polycenter Network Manager. However, the following features will not be available:

- Network map
- Flashing alarm icons
- Customizeable reports of statistics



# 2

---

## Installation and Overview

In conjunction with DECpacketprobe 90 software, PROBEwatch provides support for the following:

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

The software comes on a TK50 tape. Once loaded, it provides communications with remote DECpacketprobe RMON-MIB agents that may be located on segments throughout a distributed network.

Refer to the Software Product Description (SPD 46.01) which is included in the software kit, for hardware and software requirements necessary to run PROBEwatch.

### 2.1 Mouse Operation

Most operations relating to PROBEwatch are accomplished through the use of a mouse. The mouse has three buttons defined as follows:

Button Location	Button Number	Action	Definition
Left	MB1	Select	Used to select an element or manipulate control.
Center	MB2	Adjust	Used to extend or reduce the number of selected elements.
Right	MB3	Menu	Used to display a menu and select an operation.

## Installation and Overview

### 2.1 Mouse Operation

Working with a mouse involves three types of actions:

Action	Definition
Click	Press the mouse button and quickly release it. This initiates the selected action.
Press	Press and hold down the button. Releasing the button initiates an action.
Drag	Press and hold down the button and move the pointer to a new location. Releasing the button terminates the movement.

## 2.2 Getting Started

The following procedure gets you started.

1. Log on as superuser to the system where you are installing PROBEwatch.
2. Ensure you are at the root (/) directory by entering the following command:  
`cd /`
3. Install PROBEwatch.

#### **From the TK50 tape:**

- a. Mount the TK50 onto its tape drive.
- b. Load the software.

Enter the `setld` command for the load function, followed by the device special file name for the tape drive where the media is mounted.

#### **Example:**

If you load the TK50 on tape unit 0, enter the following command:

```
setld -l /dev/rmt0h
```

The following information appears on the screen.

```
Please make sure your installation tape is mounted and on line.
```

- c. When the tape rewind and wind operations are complete and the tape drive indicates online status, enter `y` at the following prompt.

```
Are you ready (y/n)? y
```

#### **From a remote system:**

Load the software by entering the `setld` command for the load function.

## Installation and Overview 2.2 Getting Started

If you are loading PROBEwatch subsets that reside in a /var/adm/ris distribution area on a remote system, include the name of the RIS server system on which the PROBEwatch subsets are located.

### **Example:**

```
setld -l bigsys:
```

A menu listing all the available software subsets appears on the screen. The numbers corresponding to the PROBEwatch subsets vary from system to system, depending on what products are available in the RIS area and how many subsets each product has.

4. Enter the number of each subset you want to load.

---

### **Note**

---

This example shows the subset selections for the local installation from tape. For an installation from a RIS server, the numbers corresponding to the PROBEwatch subsets vary from server to server, depending on what products are available in the RIS area and how many subsets each product has.

---

```
*** Enter Subset Selections ***  
The subsets listed below are optional:  
1) 216PWULT100 BASE KIT  
2) All of the Above  
3) None of the Above  
4) Exit without installing subsets  
Enter your choice(s): 1
```

In this example, subset 1 was chosen.

5. Verify your choice.

If you entered 1 in response to the prompt, the following information appears:

```
You are installing the following subsets:  
216PWULT100 BASE KIT  
Is this correct? (y/n): y
```

The system displays copying information.

## Installation and Overview

### 2.2 Getting Started

6. Respond y or n to the next prompt:

```
Do you want to install the configuration
to run PROBEwatch on this system [y/n]? y
```

#### 2.2.1 Installing Standalone

The following instructions show how to install PROBEwatch on a standalone system.

1. Enter the PROBEwatch client directory.  

```
% cd /usr/trafficatch/client
```
2. Copy the rmon schema file to the agent directory.  

```
% cp rmon.schema /usr/agents
```
3. Copy the hub schema file to the struct directory.  

```
% cp hub.schema /usr/struct
```
4. Copy the icon file to the icon directory.  

```
% cp hub.icon /usr/icons
```
5. Update the /var/adm/snmp.hosts file.  

```
hub public public 10/usr/agents/rmon.schema
```
6. Start the PROBEwatch program.  

```
% pwmanager &
```

---

**Note**

---

If you are using the PROBEwatch in a standalone configuration go to Section 2.3.

---

#### 2.2.2 Installing PROBEwatch With Polycenter Network Manager

Operation of the PROBEwatch functions begins when you display the network map. Follow these steps to display the map.

1. Move the pointer to Edit and press MB3.
2. Drag MB3 through Create and through Component to display a popup window that includes the list of available elements.
3. Select the DECpacketprobe agent in the list and release MB3.



## Installation and Overview 2.2 Getting Started

A Properties window for the selected element appears as shown in Figure 2-1.

4. Enter the agent name and the agent's IP address.
5. Click MB1 on the Ping.  
RMON and SNMP check boxes.
6. Click MB1 on Apply.

**Figure 2-1 Management System Window**

The above sequence identifies the DECpacketprobe agent and creates an icon on the network map.

7. You should position the DECpacketprobe icon at an appropriate position on the network map and graphically connect the icon to the segment to which it is physically connected.

## Installation and Overview

### 2.2 Getting Started

#### 2.2.3 Accessing the DECpacketprobe Agent

When the network map displays, do the following:

1. Move the pointer to the icon that represents the DECpacketprobe agent and press MB3.
2. Click MB3 on User Commands.
3. Drag MB3 to RMONManager and release.

The DECpacketprobe manager menu displays. It shows the top level selections for each operation. As shown in Figure 2-2, you can make selections through the following alternatives:

- Configure
- Statistics
- Filters
- Data Capture

**Figure 2-2 Four Alternatives**

four alternatives

### 2.2.3.1 Configure

Table 2–1 describes the functions available in the Configure selection.

**Table 2–1 Configure Selection Functions**

Function	Description
Defaults	<p>This function lets you insert default values for the following parameters:</p> <ul style="list-style-type: none"><li>Owner</li><li>Data Source</li><li>Translate MAC address</li><li>Time Reference</li></ul> <p>After being set, the default values appear in any screen requiring these entries, until changed.</p>
System	<p>This function is the System group of MIBII. It contains administrative information regarding the specified agent. A portion of the information is read from the agent and a portion is inserted by the network manager.</p>
Admin	<p>This function sets up reporting conditions and report destinations for alarms that are generated by agents.</p>

**Installation and Overview**  
**2.2 Getting Started**

**Figure 2-3 View Options**

view options

2.2.3.2 Statistics

Table 2–2 describes the functions available through the Statistics selection.

Table 2–2 Statistics Selection Functions

Function	Description
Interface	This function is the Interface group of MIBII. It contains detailed information regarding the agent interface.

(continued on next page)

**Installation and Overview**  
**2.2 Getting Started**

**Table 2–2 (Cont.) Statistics Selection Functions**

Function	Description
<b>RMON Groups</b>	
EtherStats	An array of operational statistics including the following: Packets Octets Broadcasts Collisions Dropped packets Fragments CRCalignment errors Undersize/oversize
History	An historical representation of all statistics based on user-defined sample intervals and bucket counters for customized trend analysis.
Host	A table for each active node that includes a variety of node statistics. This includes the order in which the nodes were discovered. The host table provides the means of gathering MIB data for all nodes, retrievable under SNMP for non-SNMP devices.
HostTopN	A user-defined study of sorted host statistics providing detailed information of the top "n" occurrences. Performed locally by the agent, this function substantially reduces network traffic.
Matrix	A visual representation that shows the amount of traffic and number of errors between each pair of nodes. Retrieved by either source or destination address.
Event	This provides the ability to create entries in the monitor log and/or generate SNMP trap messages from the agent to the client. Events can be initiated by a crossed threshold on any counter or from a specific packet match count. Events may, in turn, trigger other functions such as a data capture session. The log includes the time of day for each event and a description of the event.
Alarm	You may set a wide variety of thresholds and sampling intervals on any statistic to create an alarm condition. Threshold values may be set as an absolute value, a rising or a falling value, or a delta value so that each node or segment may be fully customized.

### 2.2.3.3 Filters

Table 2–3 describes the functions available through the Filters selection.

**Table 2–3 Filters Selection Functions**

Function	Description
Channel	When a data capture session is in operation, data is collected after it is subjected to one or more filter conditions. To uniquely identify the results of a filter process, the data stream that passes through the filter is defined as being a specific “channel.” Thus, a Channel Control Entry is defined for each packet capture operation and contains all the required parameters for that operation. Multiple channels capturing wholly different data from the same segment may operate simultaneously.
Filter	A filter screens out packet information. You can define specific packet match filters that serve as a stop/start mechanism for all packet capture activity. Filters may be combined with “and,” “not,” or “or” functions to capture either broad or unique network events. This selection allows you to create and save a variety of predefined filters that may be applied as desired for selective data capture.

### 2.2.4 Accessing PROBEwatch

When the network map displays, do the following:

- Click on the icon representing the segment agent.
- Click on Monitor.  
The selection screen displays.
- Click on MIB Values.  
Another selection screen displays. (What is the name of this screen?)
- Click on RMON-MIB PROBEwatch Manager.  
The PROBEwatch Management System top-level menu displays.

## 2.3 Top Level Operations

The PROBEwatch Management System top level menu is the beginning point for all PROBEwatch operations. The menu choices are as follows:

Domain View  
Data Capture  
Protocol Decode  
Management Tools

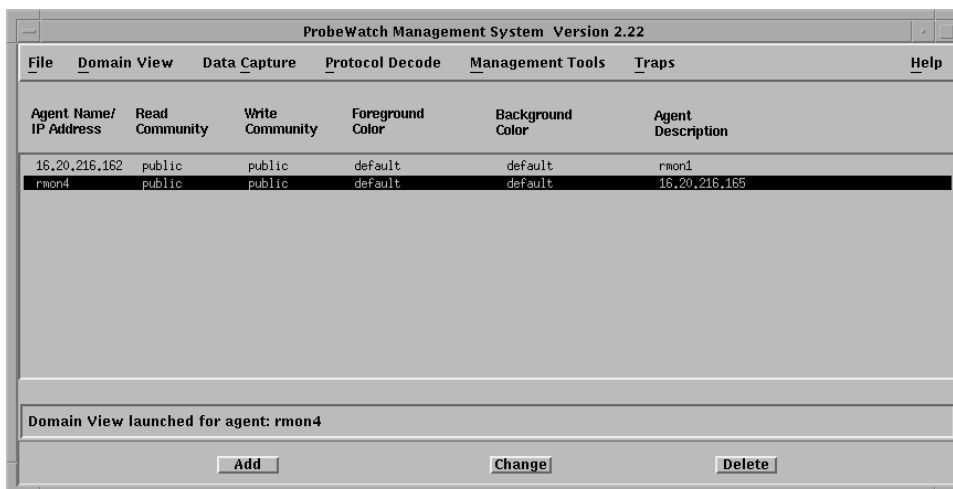
## Installation and Overview

### 2.3 Top Level Operations

#### Traps

In addition, the screen contains a summary listing of all currently defined agents. You may also select Add, Change, and Delete to modify agent definitions.

Figure 2–4 PROBEwatch Management Screen



LJ-003352-SIX

---

#### Note

See Chapter 4 through Chapter 8 for functional operation of PROBEwatch.

---

Table 2–4 includes information regarding each entry.



## Installation and Overview

### 2.3 Top Level Operations

**Table 2–4 Agent Selections**

Agent	Definition
Agent Name/IP Address	The name from the /etc/hosts file or the IP address of the agent.
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 will be “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 will be “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.

#### Add

To add a new agent entry, do the following:

- Click on Add.  
The Add Agent screen displays.
- Enter the required information into all fields with underlines.
- Select any color.
- Click on Apply.

---

#### Note

---

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

---

#### Change

Selection of Change lets you change any of the agent parameters.

## Installation and Overview

### 2.3 Top Level Operations

Figure 2-5 Add Agent

Field	Value
Name	^
Read Community	public
Write Community	public
Foreground Color	default
Background Color	default
Description	

LJ-003353-SIX

#### Delete

Selection of Delete removes that agent entry after clicking “yes” on a confirmation screen.

## 2.4 Domain View

The Domain View function provides an English language interface. It allows access and display of all the statistical information available from the RMON agents. Knowledge of the cryptic RMON 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.

## Installation and Overview

### 2.4 Domain View

A domain is a collection of one or more manageable entities (protocols). These entities include the industry standard protocols as well as any user definable protocols. The Domain View application subdivides the network into a series of “domains” that are logical subsets of the entire network accessed by an RMON 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/or data pertinent to that subset of the network.

## 2.5 Data Capture

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

- To select a logical filter definition
- To capture data
- To 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-created filters determine if a given packet is to be included in or excluded from the desired set.

Table 2-5 describes the functions available through Data Capture.

## Installation and Overview

### 2.5 Data Capture

**Table 2–5 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 a remote 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.

## 2.6 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 6 for more information.

## 2.7 Management Tools

The following management tools are discussed in this section.

### 2.7.1 Discovery

Statistics in the RMON 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.

### **2.7.2 Names Editor**

## **2.8 Traps**

Trap messages caused by alarm/event conditions may be generated by any agent in the network and reported to a centralized management console. The Trap screen allows you to access a listing of the trap messages sent by any agent in the network to your console. The trap messages will be 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.



---

## Fundamentals of Operation

DECpacketprobe 90 agents have the capability to perform several tasks simultaneously. They can collect data on a segment while collecting statistics. For example, the collection of statistics may be underway for the underlying EtherStats counters while performing a variety of other tasks. Furthermore, an agent may simultaneously be under the direction of multiple clients or multiple users for which it is performing different tasks.

---

**Note**

---

Only one client application should make the settings on an agent.

---

### 3.1 Control Entries

Since multiple activities may be occurring simultaneously, there must be a method to create, start, and stop any specific function. Within the context of the RMON-MIB, this is performed by the establishment of 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 agent collects realtime statistics on behalf of each of the Control Entries.

## Fundamentals of Operation

### 3.1 Control Entries

---

#### Note

---

It is essential that you understand the concept of, and the manipulation of, Control Entries to make use of an RMON-MIB agent.

In Domain View functions, control entries are automatically established based on the activity initiated by you. The control entries associated with Domain View operations are seen in the View Control screens for each group.

---

The use of Control Entries is a common element throughout the utilization of the RMON-MIB client. The general format and process of this entry is repeated for every instance in which statistical data or network traffic is collected. Data collection begins only after a control entry is created for a specific parameter.

**Table 3–1 Data Collection Parameters**

Configure	Statistics	Filters	Data Capture
Admin	EtherStats	Channels	Packet Capture
	History	Filters	
	Host		
	HostTopN		
	Matrix		
	Event		
	Alarm		

---

The top level screen for any of the parameters listed in Table 3–1 displays when you select that parameter from the RMON Manager's top level menu. The following choices are available when you want to affect the control entries for a particular parameter.

- Add
- Change
- Delete

A few control entry screens include other selections. In addition, the screen contains a summary field where all of the currently valid Control Entries are listed.



## Fundamentals of Operation

### 3.1 Control Entries

#### 3.1.1 Add

To create a new Control Entry, do the following:

1. Click MB1 on Add.
2. Enter the appropriate information.
3. Click MB1 on Apply.

The client sends SNMP messages to the selected agent. The agent allocates the required memory space to store the collected data. It also starts the data collection process. You may then request data from the agent for display on the client console for that entry.

---

**Note**

---

Other than the defaults, you cannot use the data collection options until a control entry is active on the screen. It is important to recognize that other than the default counters, no data collection occurs until a control entry is activated through the Domain View operation.

---

#### 3.1.2 Change

The Change screen allows you to modify certain information for the selected control entry. Changes to the diagnostic process would require changes to the selected control entry.

#### 3.1.3 Delete

To remove the selected control entry from the Control Entry list, do the following:

1. Click MB1 on Delete.

A confirmation question displays asking if you really want to delete the entry.

2. Click on Yes or No.

A Yes answer deactivates the collection of data associated with that entry.

## Fundamentals of Operation

### 3.2 Common Terms

## 3.2 Common Terms

The following common terms 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.

### 3.2.1 Index

The index is the number that uniquely identifies that particular 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 a normal ascending sequence. However, any number not in use can be used. 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 requiring 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.

### 3.2.2 Data Source

A data source is a MIB object identifier that identifies the particular interface on the agent from which the control entry is setup to collect data. For current purposes, the Data Source for a particular agent is interface 1 which is designated as:

ifIndex1

---

**Note**

---

The DECpacketprobe 90 agent supports one interface only.

---

### 3.2.3 Status

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

Entry	Description
Valid (1) <sup>1</sup>	The entry is active.
Invalid (4) <sup>1</sup>	The entry is inactive.
Create Request (2) <sup>1</sup>	The entry is in the process of creation.

<sup>1</sup>The RMON standard corresponding integer value is shown in parentheses.

### 3.2.4 Owner

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

## 3.3 Symbolic Names

Throughout PROBEwatch, and more specifically in the Filter Editing Utility, there are requirements to enter item identifiers. Some examples of these identifiers are as follows:

- IP addresses
- MAC addresses
- Protocol types
- Other information that is normally in numerical format

It is often difficult to remember these identifiers without immediate access to reference files. PROBEwatch provides a mechanism (what mechanism??) and a storage file allowing you to establish and to store logical or symbolic names for these items. It also allows the entry of these equivalent names in the entry fields.

#### Example

The user has to specify a filter format to edit any filter. This format is used to find information about fields of each protocol layer. Fields are displayed as follows:

## Fundamentals of Operation

### 3.3 Symbolic Names

```
-----  
Filter Format Name:   dodudp.frf  
Description:        _____  
HEX DUMP enable:    (y/n)  
LAN type:           (Ethernet/Token Ring)  
  
    (prompt)          (text area)          (hex area)  
ETHERNET (protocol layer 1)  
  DEST ADDR:        FrnSof001_____  00808c000001  
  SRC ADDR:         0x0123456789AB_____  0123456789AB  
  Ether Type:       DODIP_____  0800  
  
(protocol layer 2)  
field 1:            _____  
field 2:            _____  
field 3:            _____  
field 4:            _____  
  
(protocol layer 3)  
field 1:            _____  
field 2:            _____  
field 3:            _____  
field 4:            _____  
-----
```

## Fundamentals of Operation

### 3.3 Symbolic Names

Each field has three areas:

- Prompt area.
- Text area where you enter values up to 20 characters long.
- Optional Hex area where Hex values corresponding to entered values by you are displayed.

You can enter the values in the text area in the following formats:

- Hex
- Decimal
- IP address
- Name

Don't care characters are the following:

- 'x' or 'X'
- Allowed only in Hex format
- Allowed only in filter editing, not in NSCLI/NT

Hex format:

- Valid characters are '0' - '9', 'a' - 'f', 'A' - 'F', 'x', 'X'
- First two characters have to be '0x'
- For example:

```
0x1abcdXXX
```

Decimal format:

- Valid characters are '0' - '9'
- For example:

```
012343
```

IP Address format:

- Valid characters are '0' - '9', and '.'
- For example:

```
128.20.20.1
```

Name format:

- Valid characters are '0' - '9', 'a' - 'z', 'A' - 'Z', and '\_'

## Fundamentals of Operation

### 3.3 Symbolic Names

- First character has to be alphabetic.
- For example,

```
FrnSof001
```

If you enter a text string that is mapped to some number string, you have to make a corresponding entry for that string in a file named NSNAMES.DEF. NSNAMES.DEF resides under directory /usr/trafficcatch/client. NSNAMES.DEF is an ASCII text file with the following format:

- '#' is used for comments as a very first character in line.
- String1<delimiter>string2<CR/LF>
- String1 is in name format as defined above.
- String2 is in Hex, decimal, or IP format, as defined above.
- Delimiter can be spaces or Tab characters.
- Blank lines are allowed.
- Maximum length of any line in this file is 80 characters.

#### Examples

```
# This is list of hosts in main building.
host_nce      128.20.20.1
MIPS          0x000060XXXXXX
DODIP         0x0800

SNMP_PORT     161
TRAP_PORT     162

FrnSof        0x00808cXXXXXX
FrnSof001     0x00808c000001
```

If ...	And ...	Then ...
Hex_dump is enabled		each time you press <b>Enter</b> on the field, the corresponding HEX equivalent is updated on the right side.
Hex_dump is enabled	filter is loaded from file or saved to file,	The corresponding Hex equivalent is updated on the right side.

## Fundamentals of Operation

### 3.3 Symbolic Names

If ...	And ...	Then ...
"string1" is not mapped to any string,		an Error message displays each time you press <input type="button" value="Enter"/> on the field, or the filter is saved to a file.
"string1" is mapped to a string whose corresponding length is not matched with the length of the field,		an Error message displays each time you press <input type="button" value="Enter"/> on the field, or the filter is saved to a file.

**Note**

It is your responsibility to create all valid entries in NSNAMES.DEF.

#### 3.3.1 Default Names

PROBEwatch has a preestablished list of items that comprise a default list for the NSNAMES.DEF file. These include the following:

- Identification of a variety of commonly used protocols
- A list of vendor-specific MAC addresses
- A collection of other commonly utilized name/numeric equivalents

The contents of the default table are as follows:

**Table 3–2 Default Table**

Protocol	Protocol ID	Protocol	Protocol ID
<b>Ethernet Type</b>			
DODIP	0x0800	XNSIDP_1	0x0600
XNSIDP_2	0x0807	DODIP	0x0800
DODARP	0x0806	DODRARP	0x8035
VINESIP	0x0BAD	DECMOPDL	0x6001
DECMOPRC	0x6002	DECDRP	0x6003

(continued on next page)

**Fundamentals of Operation**  
**3.3 Symbolic Names**

**Table 3–2 (Cont.) Default Table**

<b>Protocol</b>	<b>Protocol ID</b>	<b>Protocol</b>	<b>Protocol ID</b>
<b>Ethernet Type</b>			
DECLAT	0x6004	DECCLUSTER	0x6007
NOVELL_1	0x8137	NOVELL_2	0x8138
APPLETALK	0x809B	APPLEARP	0x80F3
SNATH	0x04	SNAXID	0x05
NETBIOS	0xF0		
<b>SAPS</b>			
IP_SAP	0xaa	OSI_SAP	0xfe
NOVELL1_SAP	0xe0	NOVELL2_SAP	0xff
<b>IP Ports</b>			
DODICMP	1	DODGGP	3
DODTCP	6	DODUDP	17
<b>TCP Ports</b>			
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_	515
		SPOOLER	
EFS	520	TEMPO	526
COURIER	530	CONFERENCE	531
NETNEWS	532	UUCP	540
REMOTEFs	556	INGRESLOCK	1524

(continued on next page)



**Fundamentals of Operation**  
**3.3 Symbolic Names**

**Table 3–2 (Cont.) Default Table**

<b>Protocol</b>	<b>Protocol ID</b>	<b>Protocol</b>	<b>Protocol ID</b>
<b>UDP Ports</b>			
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
<b>Novell Ports</b>			
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		

(continued on next page)

**Fundamentals of Operation**  
**3.3 Symbolic Names**

**Table 3–2 (Cont.) Default Table**

<b>Protocol</b>	<b>Protocol ID</b>	<b>Protocol</b>	<b>Protocol ID</b>
<b>MAC Addresses For Various Vendors</b>			
Broadcast	0xffffffff	Multicast	0x01
FrnSoft	0x00808c	Cisco	0x00000c
Fibron	0x00000d	NeXT	0x00000f
DIAB	0x000020	VisTec	0x000022
TRW	0x00002a	S&Koch	0x00005a
NetGen	0x000065	Concor	0x000069
MIPS	0x00006b	Ardent	0x00007a
SynOpt	0x000081	Cayman	0x000089

(continued on next page)

**Fundamentals of Operation**  
**3.3 Symbolic Names**

**Table 3–2 (Cont.) Default Table**

<b>Protocol</b>	<b>Protocol ID</b>	<b>Protocol</b>	<b>Protocol ID</b>
<b>MAC Addresses For Various Vendors</b>			
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)

## Fundamentals of Operation

### 3.3 Symbolic Names

**Table 3–2 (Cont.) Default Table**

Protocol	Protocol ID	Protocol	Protocol ID
<b>MAC Addresses For Various Vendors</b>			
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

---

## Domain View

### 4.1 Description

PROBEwatch Domain View is an RMON client application that provides all the power of the RMON standard while *hiding* the details of the RMON-MIB from the user. It operates using both the Protocol Decode utility and the Filter Editor utility. In most cases, you will find the Domain View mode of operation both easier to operate and sufficiently powerful and varied to perform almost all network diagnostic functions.

A domain is a collection of one or more manageable entities (protocols). These entities include the industry-standard protocols or any user definable protocols. You can select one or more domain entities for which network traffic is to be collected concurrently. Domain entities can be user defined using any combination of filters supported by RMON.

Internally, a domain consists of a channel and the supporting filters that together define some subset of network traffic. Agent control tables for the following groups are automatically created for each selected domain.

---

**Note**

---

The agent should be set up by one client application, but may be accessed by many.

---

Host TopN tables are attached to the domain implicitly through their corresponding host tables.

---

**Note**

---

Events, alarms, and admin tables are not attached to particular domains.

---

## Domain View

### 4.1 Description

Domain View takes advantage of the ability of DECpacketprobe agents to support the use of a channel as a data source for the following groups:

- Host
- Matrix
- Statistics
- History
- Packet capture

This capability allows a wide range of statistics to be gathered for a user-defined subset (domain) of network traffic.

Domain View provides a high-level interface to the RMON alarm and event groups called a Watchdog. A watchdog notifies you (by way of a trap message) when a statistic value exceeds or falls below a user-defined threshold.

In general, Domain View provides a full interface to RMON MIB agents. Some capabilities of RMON MIB are not supported by the initial version of Domain View. These capabilities include:

- Turning a channel on or off by way of an event.
- Triggering an event when a packet passes into a channel.
- Generating a trap by an event without logging, and with logging.
- Setting an alarm on an arbitrary MIB variable. Only a limited selection of MIB variables can be observed by a Watchdog.

### 4.2 Operation

To begin operation of Domain View, do the following:

1. Start from the top screen of the PROBEwatch Management System.
2. Highlight the agent you want by clicking on the entry in the agent list or on the icon on the Polycenter map.
3. Click on Domain View and drag to Launch.

The selection screen displays the following pushbutton items:

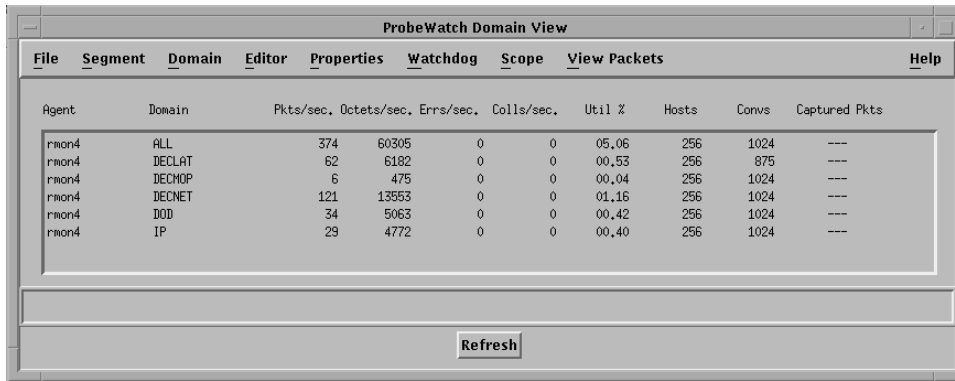
Segment  
Domain  
Editor  
Properties  
Watchdog

## Domain View 4.2 Operation

Scope  
View Packets

Also, the Agent Summary field contains a summary listing of currently defined domains, with their summary statistical information.

Figure 4-1 Domain View



The screenshot shows a window titled "ProbeWatch Domain View" with a menu bar containing "File", "Segment", "Domain", "Editor", "Properties", "Watchdog", "Scope", "View Packets", and "Help". The main area contains a table with the following data:

Agent	Domain	Pkts/sec.	Octets/sec.	Errs/sec.	Colls/sec.	Util %	Hosts	Convs	Captured Pkts
rmon4	ALL	374	60305	0	0	05,06	256	1024	---
rmon4	DECLAT	62	6182	0	0	00,53	256	875	---
rmon4	DECMOP	6	475	0	0	00,04	256	1024	---
rmon4	DECNET	121	13553	0	0	01,15	256	1024	---
rmon4	DOD	34	5063	0	0	00,42	256	1024	---
rmon4	IP	29	4772	0	0	00,40	256	1024	---

Below the table is a "Refresh" button.

LJ-003354-SIX

Agent Summary information displays in tabular form, with one line per domain. The display is updated every update period as established by you in the Properties screen.

## Domain View

### 4.2 Operation

The following information is included for each agent/domain:

Item	Description
Pkts/Sec	<p>Calculated over the update period from etherStatsPkts. For example,</p> $\frac{\text{etherStatsPkts}(\text{end}) - \text{etherStatsPkts}(\text{start})}{\langle \text{properties.update\_period} \rangle}$ <p>If the Statistics option is not enabled for the agent/domain, N/A displays in place of a value.</p>
Octets/Sec	<p>Calculated over the update period from etherStatsOctets (tokenPStatsOctets). If the Statistics option is not enabled for the agent/domain, N/A displays in place of a value.</p>
Errors/Sec	<p>Calculated over the update period. For Ethernet, this is based on etherStatsCRCAlignErrors. If the Statistics option is not enabled for the agent/domain, N/A displays in place of a value.</p>
Collisions/Sec	<p>Calculated over the update period from the etherStats collision counter. If the Statistics option is not enabled for the agent/domain, N/A displays in place of a value.</p>
Utilization %	<p>The average percentage network utilization during the period.</p> <ul style="list-style-type: none"> <li>– For 10 Mbit/sec Ethernet, utilization is calculated as:           <math display="block">\frac{\text{octets} + (8 * \text{pkts})}{\text{seconds} * 12500}</math> </li> </ul> <p>The calculations include the overhead per frame. For Ethernet, this is the eight-octet preamble.</p> <p>If the utilization is non-zero, but less than 1%, *** displays. If the Statistics option is not enabled for the agent/domain, N/A displays in place of a value.</p>
Hosts	<p>The number of hosts in the host table. (Full) displays if the host table is full. If the Host/Conversation option is not enabled for this agent/domain, N/A displays in place of a count.</p>
Conversations	<p>The number of matrices in the matrix table. (Full) displays if the matrix table is full. If the Host/Conversation option is not enabled for this agent/domain, N/A displays in place of a count.</p>
Captured Packets	<p>The number of captured packets available in the capture buffer. (Full) displays if the capture buffer is full. If the Packet Capture option is not enabled for this agent/domain, N/A displays in place of a count.</p>



#### **4.2.1 Segment**

Segment displays the statistical information available from a particular agent about a single domain. The agent and the domain are selected from the Agent Summary listing by clicking on the entry in the summary field. Most of the fields are refreshed every update period.

#### **4.2.2 Editor**

Domain Editor is used to create, change, or delete the definition of a domain. Domain definitions are stored in a single file. Each domain file contains summary information that provides a basic description of the domain.

#### **4.2.3 Properties**

Properties lets you adjust a number of Domain View parameters as you choose. Factory default settings can be restored at any time. Current values are stored in a file. Any changes made by you are saved to this file when you click on Apply after verification.

#### **4.2.4 Watchdog**

Watchdog is a simplified alarm/event function that provides you with notification of alarm conditions.

#### **4.2.5 Scope**

Scope lets you add other agents and their domains to the Domain View screen.

#### **4.2.6 View Packets**

### **4.3 Segment**

Segment displays the statistical information available from a particular agent for a single domain. The agent and the domain are selected from the Agent Summary. Once an agent and domain have been selected a Segment Zoom screen can be opened. From the Segment Zoom display screen, the statistical and graphic functions are shown in Table 4-1.

## Domain View

### 4.3 Segment

**Table 4–1 Segment Zoom Screen Fields**

Field	Description
Host List	<p>Provides a complete list of hosts detected by the selected agent /domain. Use the exclusive-choice push buttons to select the following sort orders:</p> <ul style="list-style-type: none"><li>• Discovery</li><li>• MAC address</li></ul> <p>You can also specify that the list be sorted according to one of the following statistical values contained in the table:</p> <ul style="list-style-type: none"><li>• Packets In</li><li>• Packets Out</li><li>• Octets In</li><li>• Octets Out</li><li>• Errors Out</li><li>• Broadcasts Out</li><li>• Multicasts Out</li></ul>
Host Zoom	<p>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 cannot be selected unless the agent/domain has the Hosts/Conversations option enabled.</p>
Conversation List	<p>Provides a complete list of conversations detected by the selected agent/domain. Use the exclusive-choice push buttons to select the following source orders:</p> <ul style="list-style-type: none"><li>• Destination to Source</li><li>• Source to Destination</li></ul> <p>You can also specify that the list be sorted according to one of the following statistical values:</p> <ul style="list-style-type: none"><li>• Packets</li><li>• Octets</li><li>• Errors</li></ul>

### **4.3.1 Operation**

To begin operation of Segment Zoom, do the following:

1. From the Domain View screen, click on the Agent/Domain entry you want to display.
2. Click on Segment and drag to Zoom.

The screen displays the following:

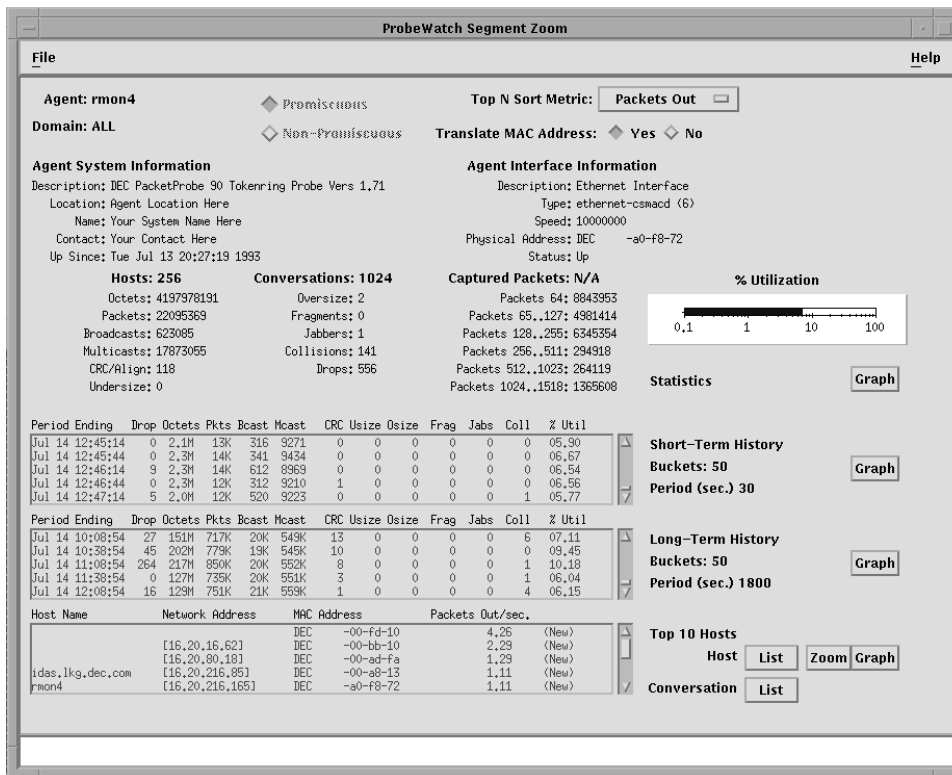
- A full complement of system information
- Interface information
- Summary statistical information

Figure 4-2 displays the Segment Zoom screen.

## Domain View

### 4.3 Segment

Figure 4-2 Segment Zoom



LJ-003355-SIX

**Table 4–2 Segment Zoom Field Descriptions**

Field	Description
Top N Sort Metric	<p>You can specify the sort criterion used for the Top N hosts portion of the display using a choice list with the following choice examples: Packets In, Packets Out. The default criterion is Packets Out. This selection can be changed at any time. The change becomes effective after the Top N report currently being gathered displays.</p> <p>The number (N) of hosts displayed is taken from the Properties screen.</p> <p>The buttons are protected (faded) in an Ethernet agent.</p>
Agent System Information	<p>This information is obtained from the MIBII system group. It is <b>not</b> refreshed.</p> <p>Description      From sysDescr            Location        From sysLocation            Name            From sysName            Contact         From sysContact            Up since        Absolute time, derived from sysUpTime</p>
Agent Interface Information	<p>This information is obtained from the MIBII interfaces group. Only Operational Status and Since are refreshed.</p> <p>Description:      From ifDescr            Type:            From ifType            Speed:           From ifSpeed (displayed as 10 Mbits/sec)</p> <p>Physical Addr:    From ifPhysAddr            Status:           From ifOperStatus, Up or Down</p>
Hosts	<p>The number of hosts in the host table. (Table full) displays if the host table is full. If the Host/Conversation option is not enabled for this agent/domain, N/A displays in place of a count.</p>
Conversations	<p>The number of matrices in the matrix table. (Table full) displays if the matrix table is full. If the Host/Conversation option is not enabled for this agent/domain, N/A displays in place of a count.</p>
Captured Pkts	<p>The number of captured packets available in the capture buffer. (Buffer full) displays if the capture buffer is full. If the Packet Capture option is not enabled for this agent /domain, N/A displays in place of a count.</p>

(continued on next page)

## Domain View

### 4.3 Segment

**Table 4–2 (Cont.) Segment Zoom Field Descriptions**

Field	Description
Cumulative Statistics	This information is obtained from the etherStatsTable for an Ethernet interface. Values are refreshed. This information is omitted if the Statistics option is not enabled for the agent/domain.
Short-term History and Long-term History	This information is obtained from the short-term and long-term history tables associated with the domain. Only the most recent N buckets display.  History information is not displayed if the Statistics option is not enabled for the agent/domain.
Top N Hosts	Top N Host statistics are obtained from a Host TopN table created by Segment Zoom. 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 displays 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 you during the update period, the client must delete and recreate the HostTopNControlTable in order to establish the new TopNRateBase.

#### 4.3.2 Segment Zoom Push Buttons

This section defines how to use the following segment zoom push buttons:

- Host list
- Host zoom
- Conversation list

##### 4.3.2.1 Host List

Click on Host List to display a complete list of hosts detected by the selected agent/domain. You can select the sort order of these hosts in the following ways:

- Use the exclusive-choice push buttons
- Sort according to discovery order or by one of the following statistical values:
  - MAC Order
  - Packets In
  - Packets Out

## Domain View 4.3 Segment

Octets In  
Octets Out  
Errors Out  
Broadcast Out  
Multicast Out

If the Host/Conversation option is not enabled for the selected agent/domain, the following error message displays:

```
Host/Conversation not enabled for this agent/domain!
```

### Operation

To begin operation of Host List click on the Host List push button in the lower right hand corner of the Segment Zoom screen.

A list of all the hosts detected by the agent/domain displays.

The retrieval of the host table from the agent is relatively slow. To show progress, the completion percentage displays periodically. Percentage is calculated using hostControlTableSize.

Statistics display using one line per host. Use the scroll bar to scroll through the list.

### 4.3.2.2 Host Zoom

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

### Operation

To begin operation of Host Zoom, do the following:

1. Select a host from the Host List.
2. Click on the Host Zoom push button in the lower right hand corner of the Segment Zoom screen.

A list of all the hosts detected by the agent/domain displays.

Host	Description
Current/Cumulative Option	Press either the Current or Cumulative buttons to specify if the Top N Conversations information is to be based on delta values for the current display period or on cumulative packet counts.

## Domain View

### 4.3 Segment

Host	Description
Host System Information	<p>Host System Information displays only if you select the host by name or by IP address.</p> <p><b>Condition:</b> The selected host must support SNMP and be able to respond to a request for MIBII system group and interface group information.</p> <p>The physical address of the host is obtained from MIBII and displays under the host name.</p> <p>System information includes the following:</p> <ul style="list-style-type: none"> <li>description (sysDescr)</li> <li>contact (sysContact)</li> <li>name (sysName)</li> <li>location (sysLocation)</li> <li>“Up since” (derived from sysUpTime)</li> </ul> <p>Host system information does not have to be updated.</p>
Statistics	<p>The statistics information is updated once every update period. The following statistics display:</p> <ul style="list-style-type: none"> <li>inPkts</li> <li>outPkts</li> <li>inOctets</li> <li>outOctets</li> <li>outErrors</li> <li>outBroadcastPkts</li> <li>outMulticastPkts</li> </ul> <p>The following lines of statistics display:</p> <ul style="list-style-type: none"> <li>First line — Cumulative values</li> <li>Second line — Current per-second values over the previous sample period</li> </ul> <p>The second line does not display until the first update period is completed. Current per-second values greater than 0 but less than one display as: &lt; 1.</p> <p>The selected host may not appear in the agent/domain's host table. It may also disappear and reappear due to the aging of the table.</p>



## Domain View 4.3 Segment

Host	Description
Top N Conversations (Inbound and Outbound)	<p>This information is calculated from the agent/domain's matrix tables.</p> <ul style="list-style-type: none"><li>• For the <i>inbound</i> display — All entries with a destination address equal to the selected host address are uploaded and sorted.</li><li>• For the <i>outbound</i> display — All entries with a source address equal to the selected host address are uploaded and sorted.</li></ul> <p>The number (N) of conversations is taken from the Properties screen.</p> <p>Both inbound and outbound displays are updated every update period. If the Cumulative option is chosen, values displayed are absolute (since the table creation date). If the Current option is chosen, values displayed are per-second rates for the previous sample period. "Current" values do not display until the end of the first sample period.</p> <p>The target host may not appear in the agent/domain's matrix tables. It may also disappear and reappear.</p>

### 4.3.2.3 Conversation List

A Conversation List provides a complete list of conversations detected by the selected agent/domain.

You can sort the conversations by using one of the following:

The exclusive-choice push buttons

The Destination-Source order

The Source-Destination order

The following statistical values:

- Packets
- Octets
- Errors

If the Host/Conversation option is not enabled for the selected agent/domain, the following error message displays:

```
Host/Conversation not enabled for this agent/domain!
```

## Domain View

### 4.3 Segment

#### Operation

To begin operation of Conversation List click on the Conversation List push button in the lower right hand corner of the Segment Zoom screen.

A list of all the conversations detected by the agent/domain displays.

The retrieval of the conversation (matrix) table from the agent is relatively slow. To show progress, the completion percentage displays periodically. Percentage is calculated using `matrixControlTableSize`.

Statistics display using one line per conversation. Use the scroll bar to scroll through the list.

#### 4.3.2.4 Quick Graph for Domain View

Quick Graph is a set of relatively simple graphic programs intended to provide a “graph zoom” function for many of the Domain View windows. For example, from the Segment Zoom window, select a particular host from the Top Hosts list, and press the graph pushbutton to obtain a graphical display of traffic to and from that host.

Quick Graph supports the following variants:

- Statistics Quick Graph (Network Utilization for selected domain)
- Short-term History Quick Graph
- Long-term History Quick Graph
- Host Quick 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 show on each graph. The sample period can be adjusted by you from one to 60 seconds, so that the graph window shows activity for a period ranging from one minute to one hour.

#### Operation

To begin operation click on one of the Graph push buttons on the right hand side of the Segment Zoom screen.

Each of the variants starts with default settings. You can adjust several of the graph characteristics at any time by using the control panel. Any of the characteristics can be changed without losing previous samples. The only exception to this is the sample period.

**Table 4–3 Graph Characteristics**

Characteristics	Description
Type	For all variants, you can select one of the following: <ul style="list-style-type: none"> <li>Plot</li> <li>Area</li> <li>A 2-D bar</li> <li>A 3-D bar</li> </ul>
Scaling Option	For all variants, you can choose one of the following: <ul style="list-style-type: none"> <li>• Auto — Adjusts the maximum Y-axis value automatically to the largest value currently shown on the graph.</li> <li>• High-water — Adjusts the maximum Y-axis value to the largest value seen since the graph was started.</li> </ul>
Variable Selection	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. 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.)
View	TBD
Hard Copy	Hard copy produces an encapsulated, device-independent PostScript (EPSF-2.0) representation of the graph that can be dumped to a PostScript compatible printer. The output filename is currently fixed as QGRAPH.PS.
Sample Period	You can adjust the sample period from one to 60 seconds using a slider. The default at startup is two seconds.

#### 4.3.2.5 Command Line Operation

Each of the Quick Graph variants is an independent executable that can be started either from the command line or from another executable using the “system” function. Command arguments and examples are shown below for those who may be interested in initiating a Quick Graph directly as opposed to activating the push button from the Segment Zoom screen.

## Domain View

### 4.3 Segment

#### Statistics variant:

```
qgraph_stat agent domain instance type
```

#### Examples:

```
qgraph_stat penguin SNMP 49152 ET  
qgraph_stat 128.20.20.7 "" 1 TRNP
```

#### Host variant:

```
qgraph_host agent domain instance host hostmac
```

#### Examples:

```
qgraph_host penguin UDP 49153 loon 08-01-23-ef-fd-04  
qgraph_host 128.20.20.7 All "" 08-01-23-ef-fd-04
```

#### Conversation variant:

```
qgraph_conv agent domain instance \  
hostA hostmacA hostB hostmacB
```

#### Examples:

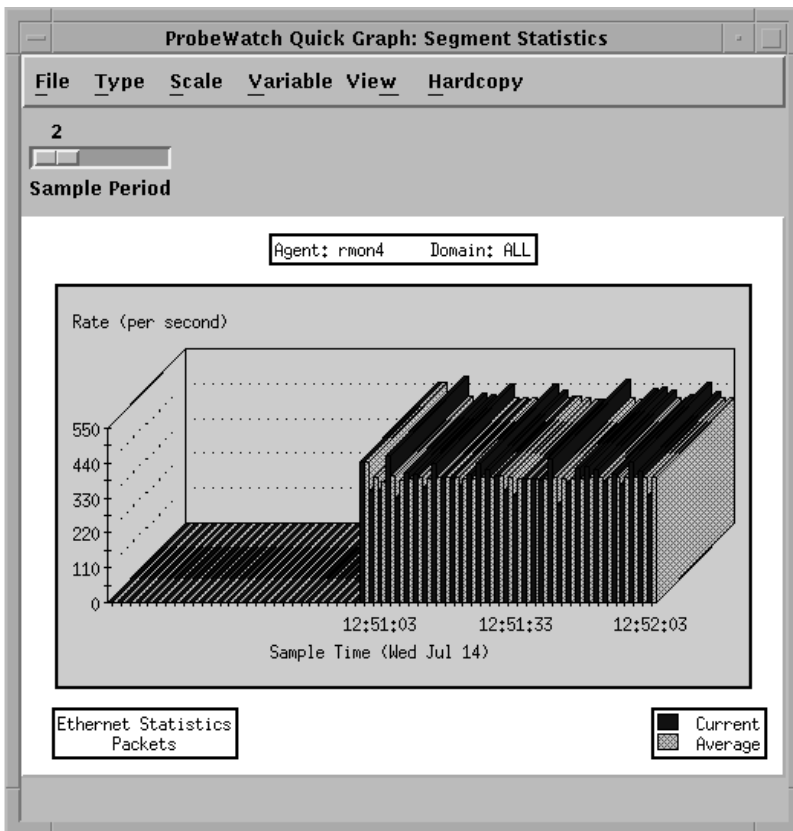
```
qgraph_conv penguin snmp 49155 loon 08-01-23-ef-fd-04 \  
waxwing 08-01-23-5d-00-f0  
qgraph_conv penguin All 49154 waxwing 08-01-23-5d-00-f0 \  
broadcast ff-ff-ff-ff-ff-ff
```

Arguments	Description
Agent	The name or the IP address of the agent.
Domain	The domain name. Can be null (""). Used for display purposes only.
Instance	The index of the table from which statistics are to be sampled. Values are 1 . . . 65535.
Type	Statistics type: "ET" for etherStats .
Host[AB]	The name or the IP address of the host. Can be null (""). Used for display purposes only.
Hostmac[AB]	The MAC address of the host in dashed hex notation (xx-xx-xx-xx-xx-xx).

Figure 4–3 and Figure 4–4 are typical examples of Quick Graph displays. Presentation characteristics may be altered to fit individual preferences. Size may be adjusted for convenience.

Domain View  
4.3 Segment

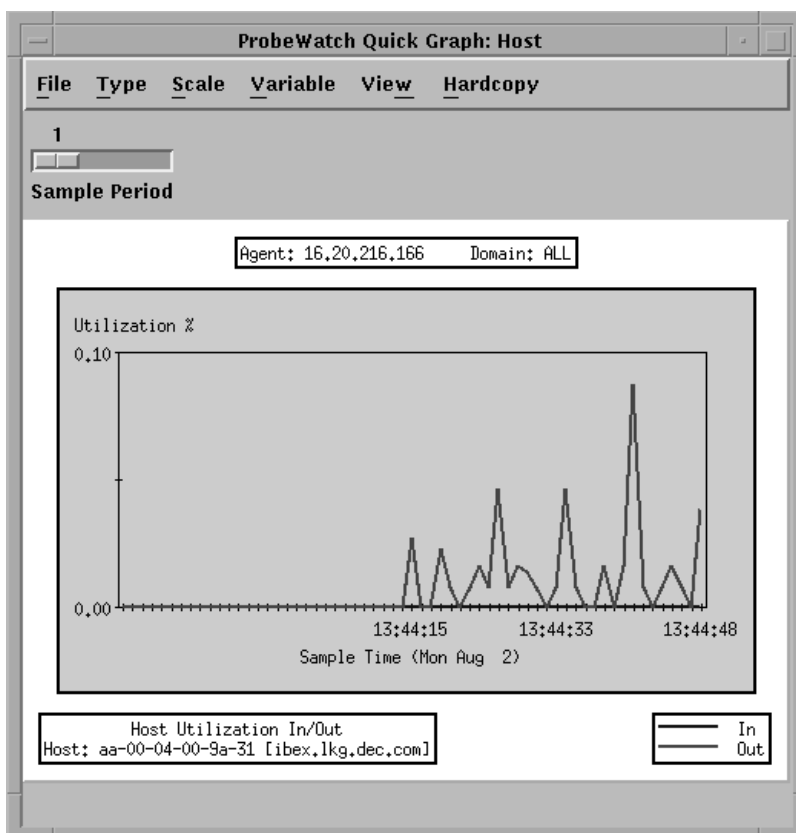
Figure 4-3 Quick Graph: Network Statistics 3-D Bar



LJ-003356-SIX

## Domain View 4.3 Segment

Figure 4-4 Quick Graph: Host



LJ-003357-SIX

## 4.4 Domain

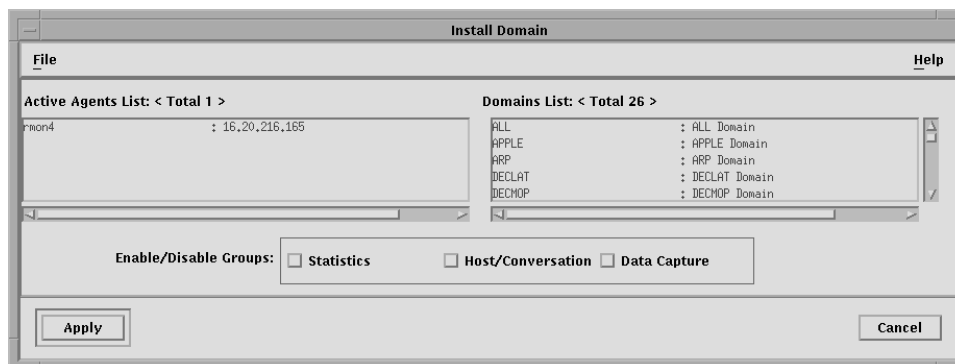
### 4.4.1 Install

Install allows you to add domains to active agents. The Domain Install Screen contains an active agents list and a domain list. Also, you can enable or disable the following groups:

- Statistics
- Host/Conversation
- Data Capture

Figure 4–5 contains the Domain Install Screen.

Figure 4–5 Domain Install Screen



LJ-003358-SIX

### 4.4.2 Deinstall

Deinstall allows you to remove a domain from an active agent. To deinstall a domain, do the following:

1. Select a domain from the Domali View Screen.
2. Click on Domain and drag to Deinstall.

## Domain View

### 4.5 Editor

## 4.5 Editor

Domain Editor is used to create, change, or delete the definition of a domain. Domain definitions are stored in a single file. For each domain, the file contains summary information that provides a basic description of the domain.

---

### Note

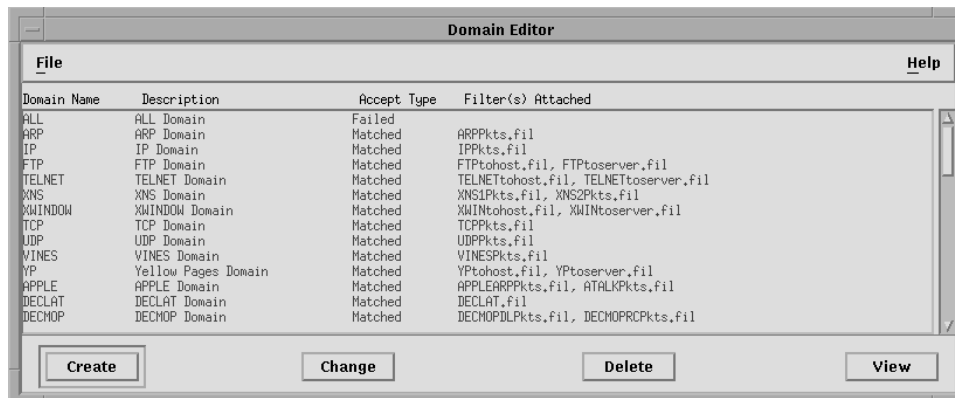
---

The Domain Editor does not install a domain for a particular agent. It is strictly an offline utility.

---

The Domain Editor displays a scrollable list of currently defined domains. This list also includes descriptions, accept types, and filter lists associated with the domains. You may scroll through the list to select a particular domain. Figure 4–6 contains a Domain Editor screen.

Figure 4–6 Domain Editor



LJ-003359-SIX



### 4.5.1 Operation

To begin operation, do the following:

1. Click on Editor on the Domain View screen and drag to Modify.  
The scrollable list displays.
2. Select the domain you want.
3. Click on one of the following:
  - Create
  - Change
  - Delete
  - View

**Table 4–4 Domain editor Fields**

Item	Description
Domain name	The user-defined name for the selected domain.
Description	A word description of the domain.
Accept type	Specifies whether the filter passes packets that match or that fail to match the selected filters.
Filter(s) Attached	Up to 16 filters may be associated with a domain. Up to four individual filter names may be displayed in the summary. If more are used, you can determine the associated filters through the View selection that shows the complete list.

#### **Create**

To enter the information necessary to create a new domain definition, do the following:

1. Click on Create.  
Figure 4–7 displays.

The Domain Editor screen requires the following fields to be completed:

- Name
- Description
- Accept Type
  - Matched
  - Failed

## Domain View 4.5 Editor

Figure 4–7 Create: Domain

The screenshot shows a dialog box titled "Create : Domain". It has a menu bar with "File" and "Help". The main area contains the following fields and controls:

- Name:** A text input field.
- Description:** A text input field.
- Accept Type:** Two radio buttons, "Matched" (which is selected) and "Failed".
- Filters:** Eight rows, each with a label "Filter 1" through "Filter 8" and a corresponding text input field.
- Buttons:** "Apply" and "Cancel" buttons at the bottom.

LJ-003360-SIX

2. Click on Filter 1 and select a filter.
3. Create as many filters as needed.
4. Click on Apply.

---

### Note

---

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

---

## Domain View 4.5 Editor

Each domain definition may have up to 16 filters applied to it. The screen has 16 entry positions for these filters.

5. Click MB1 on Filter 1.

The filter file list displays.

6. Click on any entry in that list.

7. Click on Apply.

The selected filter name appears as Filter 1 on the Create: Domain screen. Repeat the above sequence as many times as necessary (up to 16).

---

### Short Cut

---

Follow this sequence for adding multiple filter file selections to the Create: Domain screen at the same time, starting with Filter 1.

1. Click MB1 on Filter 1.
2. Click on up to 16 selections.
3. Click on Apply.

---

When all of the required filters have been entered into the table,

8. Click on Apply.

The new Domain definition is established.

Both the Create and Change options provide a checklist of available filter files (\*.fil).

---

### Note

---

You must exercise caution when changing or deleting a domain. The domain may currently be installed at an agent and the associated control tables could be left “dangling.” You should examine all agents before initiating a Change or Delete. You must deinstall the domain from an agent before deleting or changing the domain definition.

---

## Domain View

### 4.5 Editor

#### Change

Change allows you to change information or filters contained within a domain. To change a domain, do the following:

1. Select a domain with MB1.
2. Click on Change.

The Change Domain screen appears. This screen is identical to the Create Domain screen, Figure 4-7, but with information on the selected domain entered in the fields.

#### Delete

Delete allows you to delete a domain. To delete a domain, do the following:

1. Select a domain with MB1.
2. Click on Delete.

You will be asked to verify that you want to delete the domain.

#### View

View allows you to view information or filters contained within a domain. View is the same as Change, except you cant modify any informatino. To view a domain, do the following:

1. Select a domain with MB1.
2. Click on View.

The View Domain screen appears. This screen is identical to the Create Domain screen, Figure 4-7, but with information on the selected domain entered in the fields.

## 4.6 Properties

Properties lets you adjust a number of Domain View parameters. Factory default settings can be restored at any time. Current values are stored in a disk file named DV.PROPERTIES. Any changes made by you are saved to this file when you click on Apply after verification.

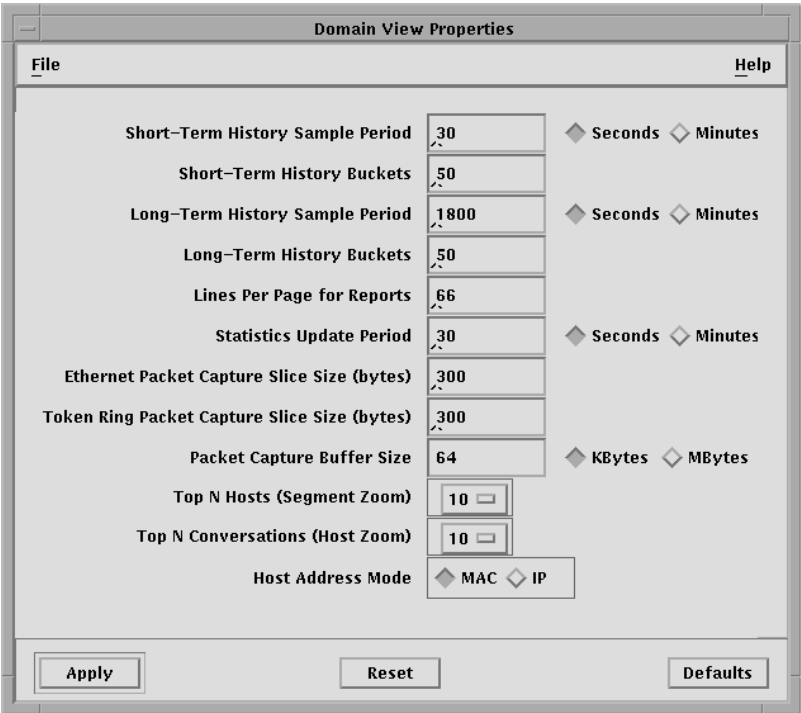
### 4.6.1 Operation

To begin operation, click on Properties on the Domain View screen and drag to Modify.

Figure 4-8 contains the setup screen for entering Properties displays.

# Domain View 4.6 Properties

Figure 4-8 Domain View Properties



LJ-003361-SIX

## Domain View

### 4.6 Properties

#### 4.6.1.1 Properties Push Buttons

The Properties screen has the following push buttons:

- Apply
- Reset
- Defaults

Entry fields allow you to set up background properties for the domain.

After entering all the desired information onto the screen, click on Apply. This initiates an SNMP session that instructs the selected agent to set values in accordance with the just-entered properties definitions.

The Reset button restores the parameter settings that were current when the window was opened and effectively cancels any changes made.

The Default button reestablishes the default values that are factory preestablished.

Standard default conditions are preselected.

Table 4–5 describes each field in the Domain View Properties screen.

**Table 4–5 Domain View Properties Field Descriptions**

Field Name	Description
Short-term History Sample Period	The time interval between successive samples. The default is 30 seconds and the acceptable range is 5-1800.
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 5-1800.
Long-term History Sample Period	The time interval between successive samples. The default is 1800 seconds (30 minutes) and the acceptable range is 5-1800.
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 5-1800.
Lines per Page for Reports	The number of line entries shown when the data displays. The default is 66 and the acceptable range is 10-999999.

(continued on next page)

## Domain View 4.6 Properties

**Table 4–5 (Cont.) Domain View Properties Field Descriptions**

Field Name	Description
Statistics Update Period	The refresh rate (in seconds) of the selected data screen. The default is 30 and the acceptable range is 10-1800.
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 14-1600.
Token Ring Packet Capture Slice Size (Bytes)	The maximum number of bytes to be captured and stored for each Token Ring packet. The default is 4096 bytes and the acceptable range is 14-10000.
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-2 Mbytes.
Top N Hosts (Segment Zoom)	The number of line entries shown when the data for Top N hosts displays. The default is 10 and the acceptable values are 5, 10, 15, 20, and 25.
Top N Conversations (Host Zoom)	The number of line entries shown when the data for Top N conversations displays. The default is 10 and the acceptable values are 5, 10, 15, 20, and 25.
Host Address Mode	The type of address MAC or IP.

## **Domain View**

### **4.6 Properties**

#### **4.6.2 Watchdog**

The Watchdog screen allows you to create a process, running in the background, to monitor user defined thresholds. When these thresholds are exceeded a trap will be generated.

##### **4.6.2.1 Operation**

To begin operation, do the following:

1. From the Domain View screen click on Watchdog and drag to Launch.
2. Edit fields as necessary.



Figure 4-9 Watchdog Screen

ProbeWatch Domain View Watchdog

File Help

Agent: 16.20.216.166  
Domain: ALL  
Variable:   
Sample Type:  Per-Second Rate  Absolute Value  
Rising Threshold:   
Falling Threshold:   
Sample Interval (secs):   
Generate Trap When:  Rising Threshold Reached  
 Falling Threshold Reached  
 Either  
Rising Trap Description:   
Falling Trap Description:   
Trap Destination 1:   
Trap Destination 2:   
Trap Destination 3:   
Trap Destination 4:   
Last Sample: 324.00 per second  
Last Rising Trap: Mon Aug 2 14:37:48 1993  
Last Falling Trap: (None)

LJ-003362-SIX

## Domain View

### 4.6 Properties

Table 4–6 describes each field of the Watchdog screen.

**Table 4–6 Watchdog Field Descriptions**

Field Name	Description
Agent	The agent selected in the Domain View screen.
Domain	Selected domains.
Variable	Allows you to select variables from the RMON Statistics Group as well as a few miscellaneous variables.
Sample Type	Allows you to select between per second sample or an absolute value
Rising Threshold	A user defineable upper limit. When this limit is exceeded a trap will be generated
Falling Threshold	A user defineable lower limit. When this limit is exceeded a trap will be generated
Sample Interval	The frequency of comparison between the variable and the threshold
Generate Trap When	Allows you to choose either the upper limit, lower limit or both, for trap generation.
Rising Trap discription	
Trap Destination 1 through 4	The address of the client to which the trap will be sent

#### 4.6.3 Scope

Scope allows you to select other agents and domains. These agents and domains will appear in the Domain View screen.

##### 4.6.3.1 Operation

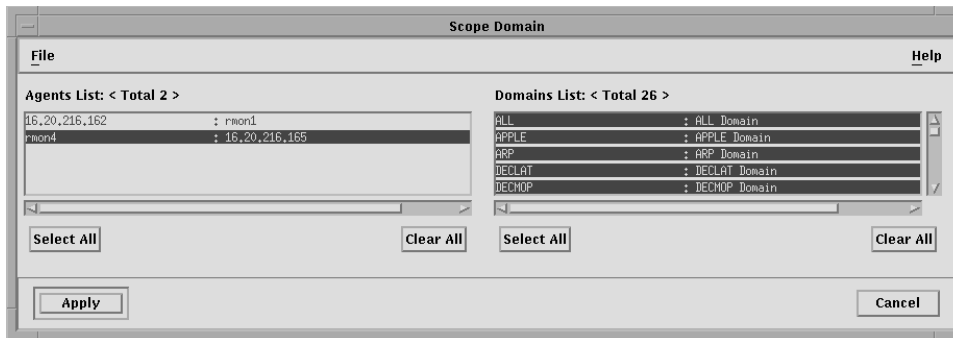
To begin operation, do the following:

1. From the Domain View screen click on Scope and drag to Modify
2. Select an agent from the Agent List
3. Select one or more domains from the Domain List

Figure 4–10 contains a Scope screen.

## Domain View 4.6 Properties

Figure 4-10 Scope Screen



LJ-003363-SIX

## Domain View

### 4.6 Properties

**Table 4–7 Scope Field Descriptions**

Field Name	Description
Agent List	Lists each agent
Domains List	Lists each protocol

#### Push Buttons

**Select All**—Allows you to select all agents or protocols.

**Clear All**—Allows you to clear all agents or protocols.

#### 4.6.4 View Packets

View Packets allows you to start a data capture and protocol decode for selected domains.

To begin operation, click on View Packets and drag to Launch.

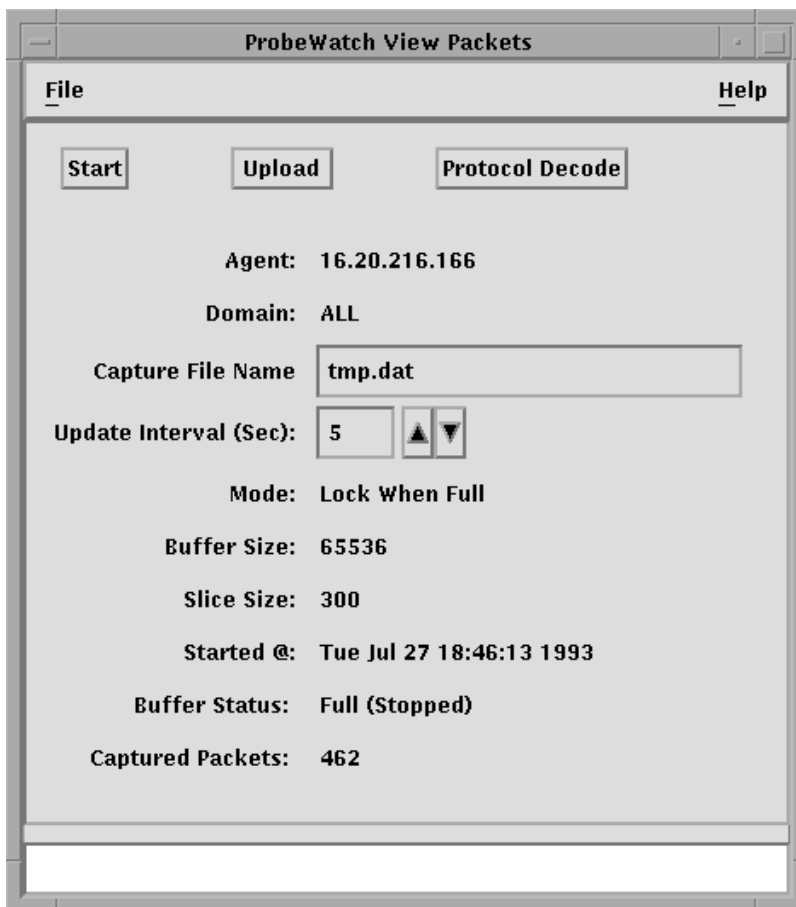
**Table 4–8 View Packets Field Descriptions**

Field Name	Description
Domain	Name or IP address of the selected agent.
Domain	List of selected domains.
Capture file name	Name of the file where the captured data is to be stored.
Update interval (sec)	Time interval of when Buffer Status and Captured Packets is updated.
Mode	Current mode of operation
Buffer size	Size of capture buffer
Slice size	Maximum number of octets of each packet that will be saved in the capture buffer.
Started @	Time capture process was started.
Buffer status	Status of the buffer.
Captured packets	Number of captured packets

## Domain View 4.6 Properties

Figure 4-11 contains a View Packets screen.

Figure 4-11 View Packets Screen



LJ-003364-SIX

## Domain View

### 4.6 Properties

#### 4.6.4.1 View Packets Push Buttons

Table 4–9 describes the View Packets push buttons.

**Table 4–9 View Packets Push Buttons**

Button	Description
Start	Starts the capture process
Upload	Uploads the data from the probe to a selected file in the client
Protocol Decode	Decodes the packets for viewing

### 5.1 General

The Data Capture utility captures packets from the DECpacketprobe 90 agent in a selective manner. It is simple to use because it hides most of the RMON-based information from you and uses English language instructions.

You can capture the traffic for either standard protocols or user-defined protocols.

The background and the foreground colors of the window are taken from the user-defined colors for the particular agent for which you are capturing data.

#### 5.1.1 Operation

Follow these instructions to open the Data Capture utility.

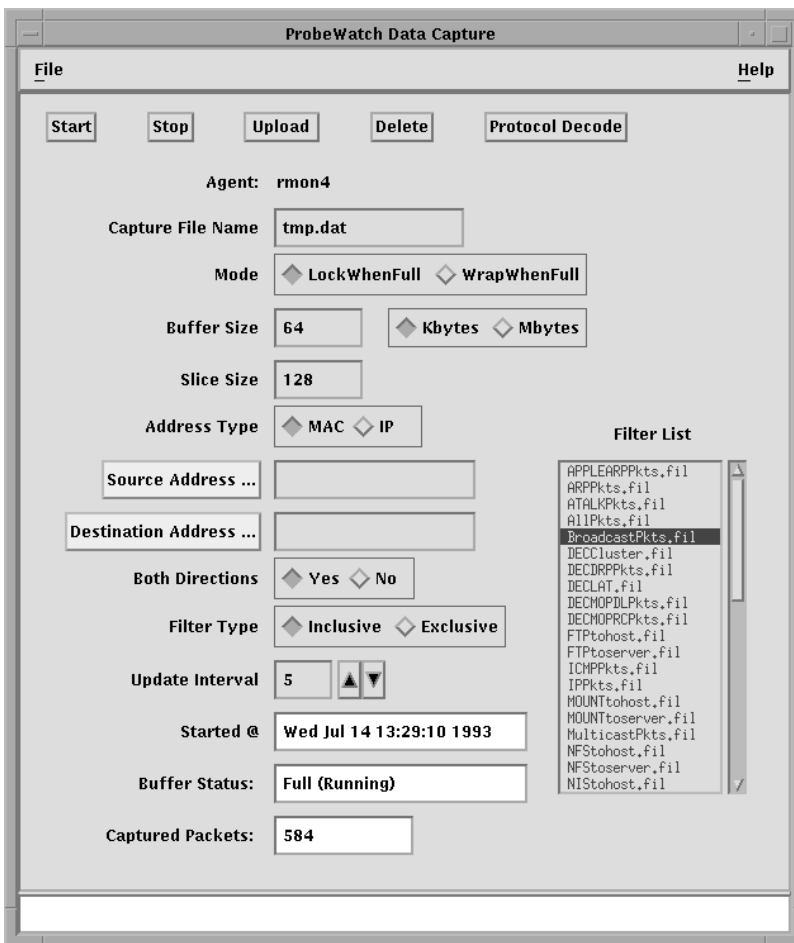
1. Start from the top screen of PROBEwatch application.
2. Click on Data Capture and drag to Launch.

The setup screen for performing a data capture/protocol decode session displays.

Entry fields allow you to set up the conditions for a capture session. Figure 5-1 contains a Data Captuer screen.

## Data Capture 5.1 General

Figure 5–1 Data Capture



LJ-003365-SIX

3. Enter information into the following fields, as applies:

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



## Data Capture 5.1 General

The following fields require the selection of parameters from a selection list.

- Mode
- Address Type
- Both Directions
- Filter Type

5. Click on Start.

This initiates an SNMP session that instructs the selected agent to begin collecting packets in accordance with the filter definition. Standard default conditions are preselected.

When the required sample of packets has been captured, do the following:

6. Click on Stop.

7. Click on Upload to transmit the captured packets to the client.

As a default, the packets will be placed in a buffer designated TMP.DAT. Each subsequent upload causes a confirmation screen to display verifying that you want to overwrite what is currently in the buffer. If the uploaded information is to be saved for further examination, you should specify a unique buffer name to store the uploaded packets.

8. Once uploaded, click on Protocol Decode.

The Protocol Decode Summary screen displays including the contents of the uploaded packets.

Table 5–1 and Table 5–2 contain a more detailed description of each part of the Data Capture Screen.

**Table 5–1 Data Capture Screen Push Buttons**

Mode	Definition
Start	Initializes a data capture session for the selected agent.
Stop	Ends a data capture session for the selected agent.

(continued on next page)

## Data Capture

### 5.1 General

**Table 5–1 (Cont.) Data Capture Screen Push Buttons**

Mode	Definition
Upload	<p>Allows you to transfer packets captured at the agent to the client. At the completion of a data capture sequence, the captured data is stored in a buffer in the agent.</p> <ol style="list-style-type: none"> <li>Click on Upload. The upload process is initiated to the file specified in the Capture File Name. The specified file stores the uploaded packets for examination and protocol decode. A status report displays in the lower margin. It shows the number of packets uploaded.</li> <li>Once complete, click on Protocol Decode. The protocol decode process begins.</li> </ol>
Delete	Used to delete the current entry inside the agent. This includes channel(s?), filters, and bufferControl entries.
Protocol Decode	This displays the protocol decode utility screen.

**Table 5–2 Data Capture Screen Fields**

Mode	Definition
Capture File Name	The name of the file where the agent packets are uploaded. It is created in the /usr/probewatch/client directory.
Mode	<p>Determines if the session will do one of the following:</p> <ul style="list-style-type: none"> <li>LockWhenFull will halt when the capture buffer is full.</li> <li>WrapWhenFull will allow the most recent packets to overwrite the earliest until a specific stop command is initiated.</li> </ul>
Buffer Size	The requested maximum number of octets to be saved in this captureBuffer. This includes any implementation-specific overhead.
Slice Size	<p>The maximum number of octets of each packet that will be saved in the capture buffer.</p> <p>For example, if a 1500 octet packet is received and Slice Size is set to 500, then only 500 octets of the packet will be stored in the capture buffer. If this variable is set to 0, the capture buffer saves as many octets as is possible.</p>

(continued on next page)

**Table 5–2 (Cont.) Data Capture Screen Fields**

Mode	Definition
Address Type	You can specify the address type as either MAC or IP. Depending on this, the address or symbol entered at Source and Destination Address is interpreted. (Valid symbols are defined in the file NSNAMES.DEF).
Source /Destination Address	The following choices are allowed: <ul style="list-style-type: none"> <li>• Valid MAC address</li> <li>• Valid IP address</li> <li>• Valid Name</li> </ul> <p>These addresses are used to create more specific filters related to the source/destination of the data to be captured.</p>
Both Directions	Determines whether to capture traffic from source-to-destination only or in both directions (source-to-destination or destination-to-source).
Filter Type	This can be one of the following: <ul style="list-style-type: none"> <li>• Inclusive — Captures all traffic if the specified condition is matched.</li> <li>• Exclusive — Captures all traffic if the specified condition is not matched.</li> </ul>
Update Interval	The time interval that screen will be updated.
Started @	Indicates the time when the data capture was initiated.
Buffer Status	If capture is already on, it shows “Running.” If capture is stopped, it shows “Stopped.” If a capture entry does not exist, it shows “Not Known”. It also shows the following buffer status in brackets: [Full] or [Available].
Captured Packets	If capture is on, it shows the number of packets captured in the agent with the matched condition.

For further details of the Protocol Decode function, see Chapter 6.



### 6.1 Framework

A data communications network, whether totally local or a distributed internetwork, is subject to a variety of fault conditions. Some examples of these fault conditions are as follows:

- Hardware may fail.
- Errors may occur as data is transmitted on the respective physical links.
- Software may create convoluted and bandwidth consuming sessions.
- Network response time may mysteriously lengthen.

You see only the result of these problems:

- The inability to complete network dependent tasks in a reasonable amount of time
- A complete network failure when there is no response to user activity

In situations such as these, PROBEwatch's protocol decode function provides a way for the network administrator to examine detailed network operations.

The following are just a couple of ways the protocol decode function helps the administrator analyze network problems.

- Examine cumulative statistics of network activity.  
This process often provides clues as to the nature of the fault condition but does not uniquely determine where the problem exists.
- Examine the specific data messages that are being sent on the troubled segment.

Through this process, the administrator can quickly identify a fault condition enabling corrective action to be taken.

## Protocol Decode

### 6.1 Framework

#### 6.1.1 Sequence

The protocol decode process begins with a data capture session performed by the DECPacketProbe agent on the segment under observation.

Then, the collected data is transmitted from the agent to the client. The data is stored in the client in a specified capture file.

The function that performs this task is Data Capture.

You can use the Protocol Decode screen to examine the individual frames. The Protocol Decode screen gives you full seven-layer decode access to and display of the data.

#### 6.1.2 Protocol Decode Operation

To open the Protocol Decode function do the following.

1. Start from the top screen of the PROBEwatch application.
2. Click on Protocol Decode and drag to Launch.

The Protocol Decode Utility screen displays. The following operational choices display:

- Properties
- Colors
- Post Capture Filters
- Learn Addresses
- Change Mode
- Goto Frame
- Frame Number (an entry field)

Also, the screen contains a display field where the contents of the data file are displayed in summary format. Figure 6–1 contains a Protocol Decode screen.

##### Properties

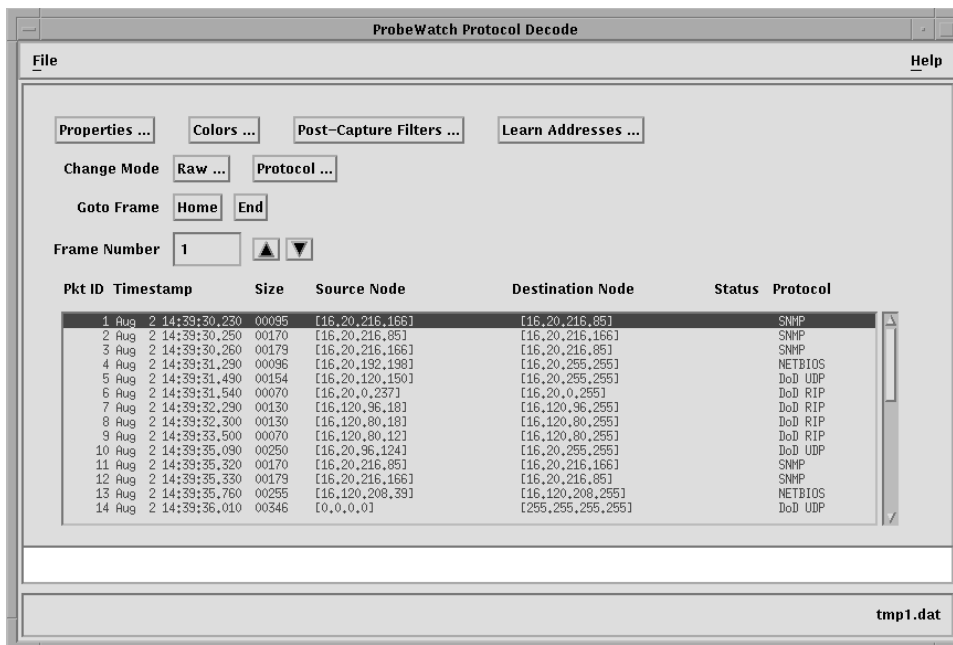
The following describes the contents of the Properties screen.

1. Click on Properties.

An entry screen displays with the following fields:

## Protocol Decode 6.1 Framework

Figure 6–1 PROBEwatch Protocol Decode



LJ-003366-SIX

## Protocol Decode

### 6.1 Framework

Field	Description
Raw Mode	Displays the decoded bytes in either ASCII or EBCDIC characters.
Time Mode	Displays the time as either Absolute (Month Day Time) or Delta (time difference between the arrival of the first frame and the one shown. The format is hh:mm:ss:ttt). Where: ttt indicates milliseconds (thousandths of seconds.)
Address Mode	Allows the selection of the different address types.
Zoom Mode	Enables or disables the zoom function.

2. After making your choices, click on Apply.

#### Colors

This operational choice lets you select the color format of the seven layers of the protocol decode display. Selections are made for the Raw display and the seven-layer display for both Foreground and Background.

1. Click on Colors.
2. Click on each selection.  
A color chart displays.
3. Scroll through the 70 (69?) choices, selecting one for each layer.  
After you have selected the colors, click on any of the following:

Field	Description
Load	Enters the default values for color selection.
Save	Saves the color selection created. Replaces the default values with this new set of values.
Apply	Allows customized colors for this session only. Once the session is complete, the previous default values are reestablished.
Reset	Reestablishes the original values. This applies only after you make changes in the color entries but before you save them.



## 6.2 Viewing Packets

To view the captured packets click on File and drag to load. Select the file that contains the captured packets and click on OK. The file displays in summary mode. 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 following information is included for each frame.

Field	Description
Pkt ID	The index number of the packet. It begins with 1. Use the cursor to scroll through the list. The selected packet is highlighted.
Timestamp	The date and the time this packet was captured. The format is as follows: Month Day hh:mm:ss:ttt Where: ttt indicates milliseconds (thousandths of seconds).
Size	The number of bytes in the frame.
Source Node	The Hex address of the node sending this frame. If Vendor Name is the default, the address shows the name of the vendor of the interface device.
Destination Node	The Hex address of the destination node. If Vendor Name is the default, the address shows the name of the vendor of the interface device.
Status	The type of fault if a packet is faulty. The possibilities are as follows: <ul style="list-style-type: none"><li>• Runt</li><li>• Jabber</li><li>• CRC</li><li>• Align</li></ul> More than one may apply.
Protocol	This identifies the highest level protocol included in that packet.

The Goto Frame displays one of the following:

- The first frame on the first line (Home)
- The last frame on the last line (End)

## Protocol Decode

### 6.2 Viewing Packets

Click on either selection.

Inserting a frame number in the Frame Number field causes that frame to display on the first line.

In the same way, clicking on ↑ or ↓ in the Frame Number field causes the summary frame display to scroll up or down.

### 6.3 Change Mode

There are two modes available for viewing packets:

- Raw Mode—Displays the hex and ASCII format of the packet.
- Protocol Mode—Displays the packet along with protocol layer information.

#### 6.3.1 Raw Mode

To create a display of the individual frame in Raw mode, do the following:

1. Select the frame.
2. Click on Raw in the Change Mode field.

The display field heading includes the following:

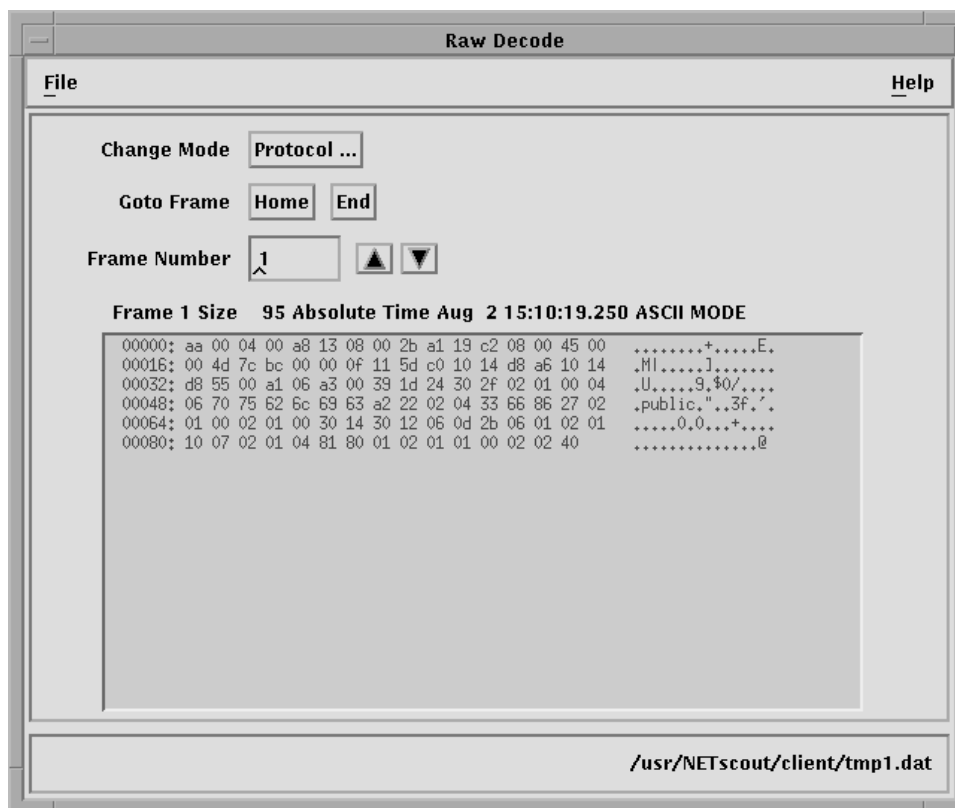
Frame Number  
Size  
Absolute Time  
Display mode (ASCII or EBCDIC)

Each row in the display contains the following:

Frame byte number  
32 HEX digits for 16 frame bytes  
16 ASCII (EBCDIC) equivalents of the frame bytes

## Protocol Decode 6.3 Change Mode

Figure 6–2 Raw Decode





LJ-003367-SIX

The Goto Frame displays the raw decode of one of the following:

- The first frame in the file (Home)
- The last frame in the file (End)

Click on either selection.

Inserting a frame number in the Frame Number field causes the raw decode of that frame to display.

In the same way, clicking on  or  in the Frame Number field causes the raw mode frame display to scroll up or down.

## **Protocol Decode**

### **6.3 Change Mode**

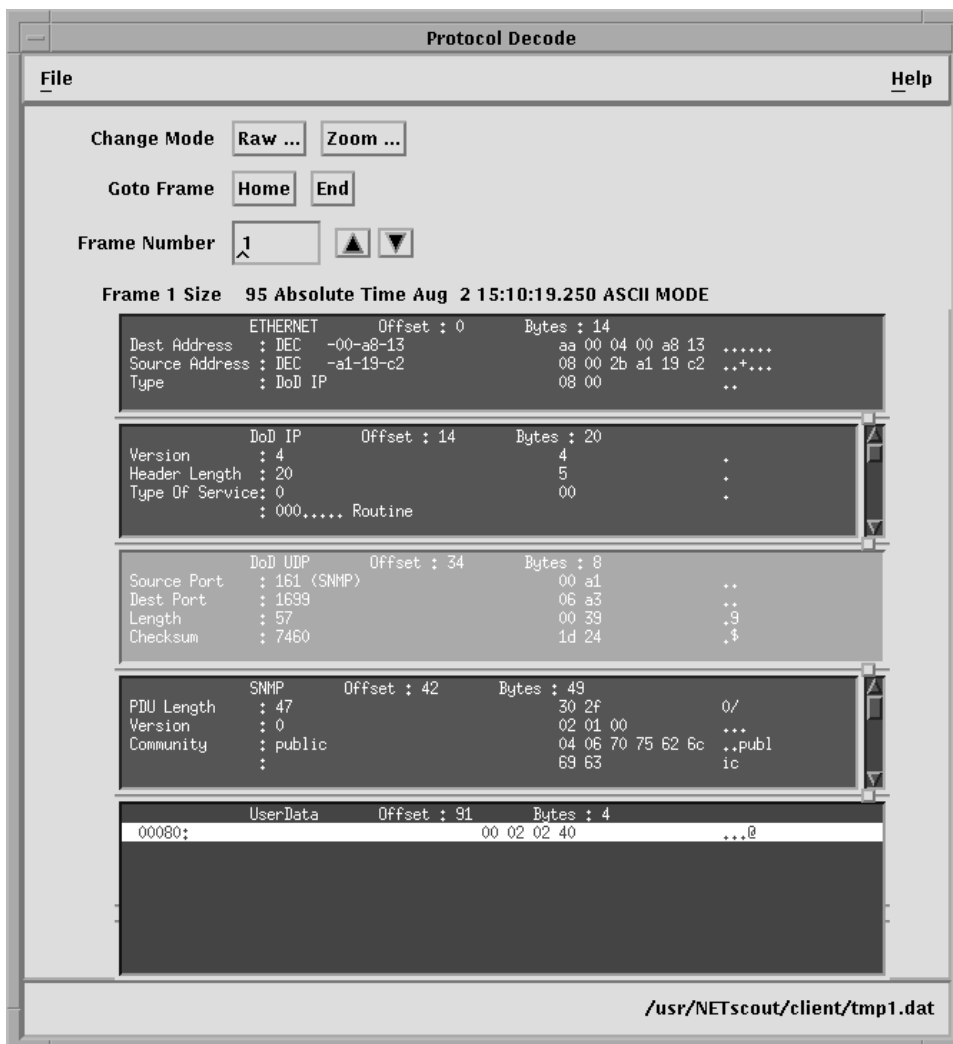
#### **6.3.2 Protocol Mode**

To display the selected frame in seven-level, decoded format, click on Protocol in the Change Mode field of either the Summary screen or the Raw screen.

The decoding is automatic. The frame displays in up to seven windows. Each window corresponds to successive layers of the protocol. The contents of each layer is expressed in a readable format. You can scroll through each window and examine the contents in detail. If the frame contains no identifiable protocol after a certain layer, the rest of the frame displays as a raw dump in the last window labeled User Data.

## Protocol Decode 6.3 Change Mode

Figure 6-3 Protocol Decode



LJ-003368-SIX

## Protocol Decode

### 6.4 Zoom Mode

## 6.4 Zoom Mode

Zoom mode displays an enlarged version of the Protocol Decode screen one layer at a time.

1. To display a full screen of the first layer decode, click on Zoom in the Change Mode field of the Protocol screen.
2. To view the protocol layers, do the following:
  - Click on next layer to scroll forward.
  - Click on previous layer to scroll backward.

## 6.5 Post-Capture Filters

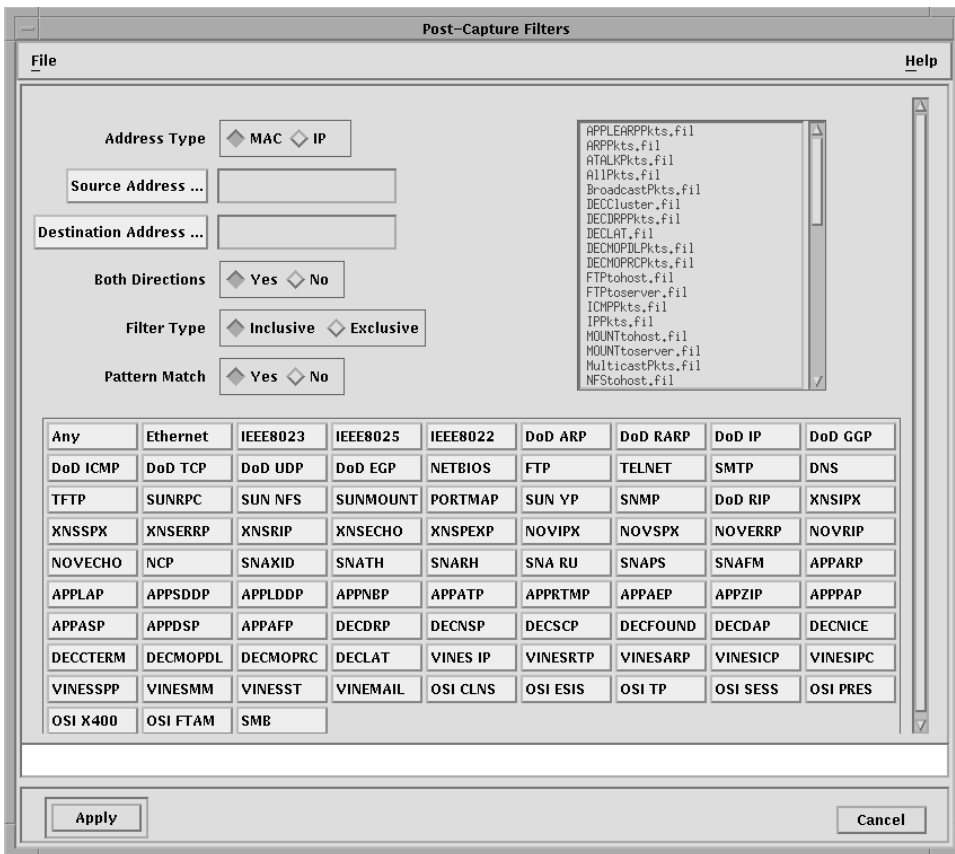
Data that has been previously captured may be filtered further through the use of the Post-Capture Filter function.

Once a file has been loaded, do the following:

1. Click on Post-Capture Filters.  
A filter selection screen displays.
2. Select the filter definition to be used.  
Once the filter definition has been established, do the following:
3. Click on Apply.  
The Summary Mode screen displays containing only those packets that have passed the Post-Capture Filter definition. Detailed protocol decode may then continue.

## Protocol Decode 6.5 Post-Capture Filters

Figure 6-4 Post-Capture Filtering



LJ-003370-SIX

## Protocol Decode

### 6.5 Post-Capture Filters

Field	Description
Address Type	You can specify the address type as either MAC or IP. Depending on this, the address or symbol entered at Source and Destination Address are interpreted. Valid symbols are defined in file NSNAMES.DEF.
Source/Destination Address	The following entries are allowed:  Valid MAC address Valid IP address Valid Name  These addresses are used to create more specific filters related to the source/destination of the data to be captured.
Both Directions	This field determines whether to capture traffic from source-to-destination only or from source-to-destination or destination-to-source.
Filter Type	This can be either of the following: <ul style="list-style-type: none"><li>• Inclusive — Captures all traffic if the specified condition is matched.</li><li>• Exclusive — Captures all traffic if the specified condition is not matched.</li></ul>
Protocol Mode	This can be either of the following: <ul style="list-style-type: none"><li>• Standard — You can specify up to four protocols from the given choice list of 84 protocols by clicking on the selected entries.</li><li>• Custom — You can choose up to four filters from the list of 44 predefined filters, or from the additional filter definitions you entered.</li></ul>



---

## Management Tools

### 7.1 Discovery

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 segment. It then maps the hosts to IP addresses and host names while also identifying the node type (router, bridge, server) for each host. It stores the resulting cross reference table in an XXXXXXXX.DAT file in the client, where XXXXXXXX represents the IP address of the agent where Discovery was started.

The file name and the file format created by Discovery are known to all the applications running under PROBEwatch. These applications now display the network IP address or host name instead of the physical address. This is usually more meaningful in diagnosing network problems.

To eliminate unnecessary processing in the agent and to limit network overhead, the Discovery process times out. No further updates are made until Discovery is rerun.

For networks with rapid changes, the Discovery process could be run at routine intervals so the cross reference file may be updated.

For those hosts that come on the network after a Discovery routine has completed, the data displays show the MAC address. You can run a Discovery routine and update the file any time you identify a host that has not been “discovered.”

## Management Tools

### 7.1 Discovery

Discovery learns the following items:

- The network address of the nodes that are on the agent's segment

---

**Note**

---

Only IP address discovery is implemented in Version 1.0.

---

- The bridges on the network
- The routers on the network
- The IP addresses of outside nodes that are conversing with nodes on the agent's segment

#### **Operation**

To run a Discovery session, do the following:

1. Start from the top screen for the PROBEwatch application.
2. Click on Management Tools.
3. Drag down to Discovery and release.

The setup screen displays.

**Management Tools  
7.1 Discovery**

**Figure 7-1 Popup Discovery**



LJ-003371-SIX

## Management Tools

### 7.1 Discovery

4. Complete the following fields:

Field	Description
How long to run	This field specifies the time, in seconds, that the learn program will run. For small networks, 60 seconds would normally be adequate to identify all active hosts. For larger networks, times up to 10 minutes (600 seconds) are reasonable.
Netmask	The subnet mask that is used to determine if a host is directly connected to a specific segment or if it must be reached through a router.

5. Click on Apply.

This initiates an SNMP session that instructs the selected agent to learn the IP and logical names of the hosts on the segment. The learning process continues for the duration specified by you and, when complete, exits the program.

Upon completion, all display screens have access to the learned file and are able to display addresses in MAC, IP, or logical name formats.

The selection of the format is made in the Defaults screen where Hex, Vendor Name, or IP formats are the choices.

If IP is selected as a default, the host addresses display by Logical Name if that name has been discovered.

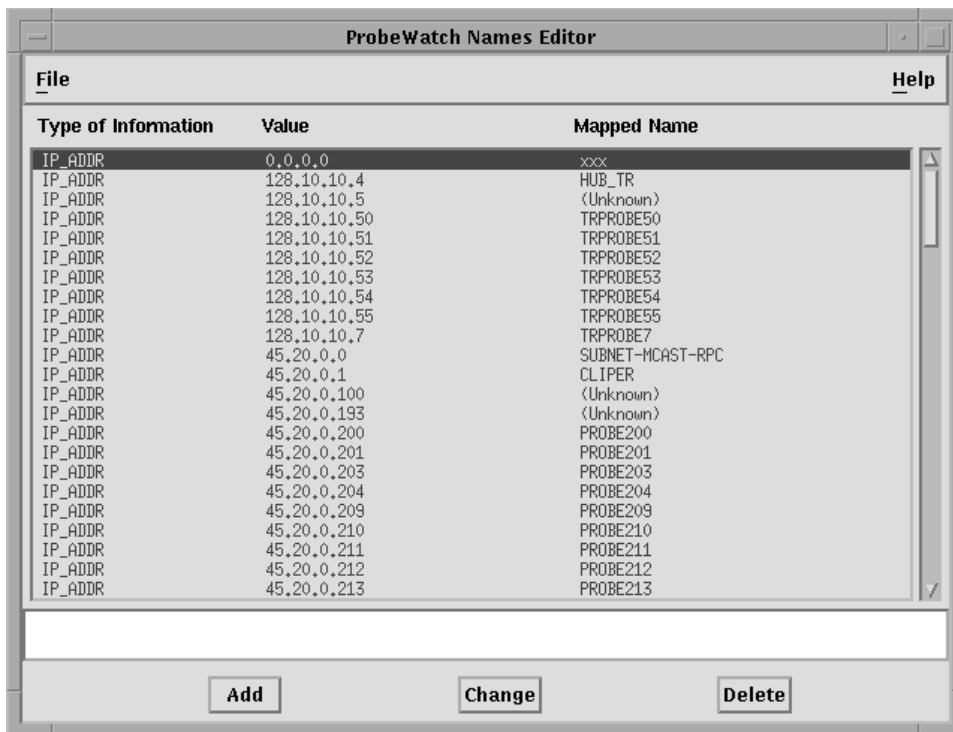
If no name is present, the IP address is shown in XXX.XXX.XXX.XXX format if the host was discovered.

The default representation is the interface MAC address.

### 7.2 Names Editor

## Management Tools 7.2 Names Editor

Figure 7-2 Names Editor Screen



LJ-003372-SIX



## 8.1 Description

Trap messages caused by alarm/event conditions may be generated by any agent in the network and reported to a centralized management console. The Trap screen allows you to access a listing of the trap messages sent by any agent in the network to your console. The trap messages will be 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.

The Watchdog function, implements the method of establishing alarm/event conditions. The Trap log (Figure 8–1) is accessed by clicking on Traps in the PROBEwatch Management System screen.

To access editing utilities for traps, do the following:

1. Click MB1 when the pointer is in the body of the Trap screen.

The following options display:

- File
- View
- Edit
- Find
- Extras

File is the only usable choice for normal user purposes.

2. Click on File.

The following choices display:

- Load File
- Save Current File
- Store as New File
- Include File
- Empty Document

3. Click on Save Current File.

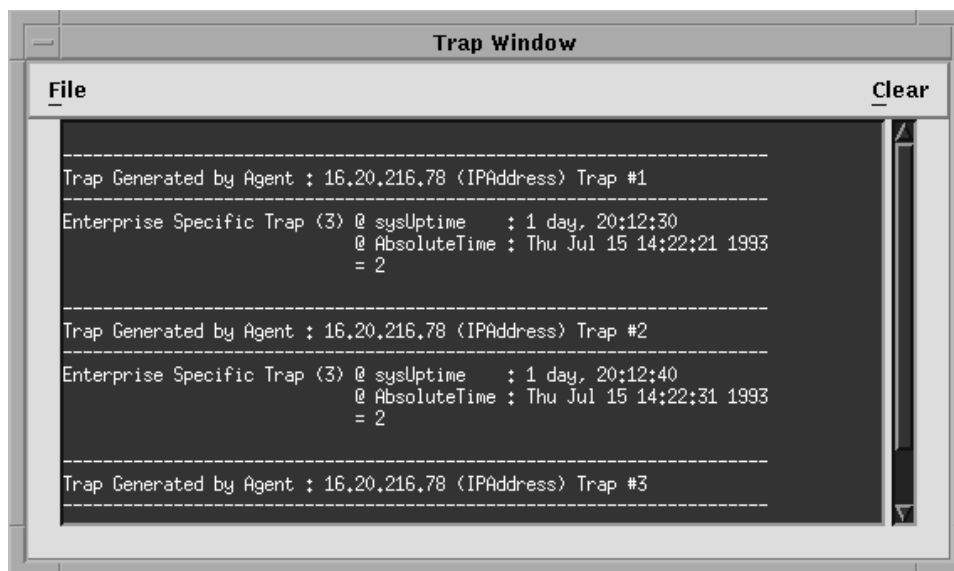
## Traps

### 8.1 Description

An entry screen displays.

4. Enter a file name.
5. Click on Store As New File.  
The trap log is stored for future use.  
To delete the current log file:
6. Click on Empty Document.

Figure 8–1 Trap Window



LJ-003373-SIX



# A

---

## MIB Groups and Communities

### A.1 Introduction

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.

### A.2 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)
- Ethernet remote monitoring MIB (RFC 1271)

### A.2.1 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 90.

---

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.

### A.3 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. There are two strings 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.



# B

---

## Documentation and Ordering Information

### B.1 Introduction

This appendix lists documentation that is related to PROBEwatch. It also provides ordering information.

### B.2 Related Documentation

You can order the following documents from Digital:

Document Title	Order Number
Open DECconnect Building Wiring Components and Application Catalog	EB-K2407-42
DECconnect System Planning and Configuration Guide	EK-DECSY-CG
DEChub 90 Owner's Manual	EK-DEHUB-OM
DECpacketprobe for Ethernet User's Guide	EK-PROBE-UM. A01
Polycenter Network Manager 200	QA-VM9AA-GZ
Polycenter SNMP Manager 300	QA-YUGAB-GZ

### B.3 Ordering Information

You can order options and documentation by mail, phone, or electronically.

#### Need Help?

If you need help deciding which documentation best meets your needs, please call 1-800-DIGITAL (1-800-344-4825) and press 2 for technical assistance.

### Electronic Orders

To place an order through your account at the Electronic Store, dial 1-800-234-1998, using a modem set to 2400 or 9600 baud. You must use a VT terminal or terminal emulator set at 8 bits, no parity. If you need help, call 1-800-DIGITAL (1-800-344-4825) and ask for an Electronic Store specialist.

### Telephone or Direct Mail Orders

---

<b>If You Are From . . .</b>	<b>Call . . .</b>	<b>Or Write . . .</b>
U.S.A.	DECdirect Phone: 800-DIGITAL (800-344-4825) FAX: (603) 884-5597	Digital Equipment Corporation P.O. Box CS2008 Nashua, NH 03061
Puerto Rico	Phone: (809) 781-0505 FAX: (809) 749-8377	Digital Equipment Caribbean, Inc. 3 Digital Plaza, 1st Street Suite 200 Metro Office Park San Juan, Puerto Rico 00920
Canada	Phone: 800-267-6215 FAX: (613) 592-1946	Digital Equipment of Canada Ltd. 100 Herzberg Road Kanata, Ontario, Canada K2K 2A6 Attn: DECdirect Sales
International	—	Local Digital subsidiary or approved distributor

---

### **Digital Personnel**

You can order documentation by electronic mail. Contact the following organizations for instructions:

---

<b>If You Need . . .</b>	<b>Call . . .</b>	<b>Contact . . .</b>
Software documentation <sup>1</sup>	DTN: 241-3023 (508) 874-3023	Software Supply Business Digital Equipment Corporation 1 Digital Drive Westminster, MA 01473
Hardware documentation	DTN: 234-4325 (508) 351-4325 FAX: (508) 351-4467	Publishing & Circulation Services Digital Equipment Corporation NRO2-2/I5 444 Whitney Street Northboro, MA 01532

---

<sup>1</sup>Call to request an Internal Software Order Form (EN-01740-07).

---





---

# Index

## A

---

- Agent
  - definition, 1-8
  - summary, 4-3
- Agent/domain information
  - captured pkts, 4-4
  - collisions/sec, 4-4
  - conversations, 4-4
  - errors/sec, 4-4
  - hosts, 4-4
  - octets/sec, 4-4
  - pkts/sec, 4-4
  - utilization, 4-4
- Agent selections
  - agent, 2-12
  - background color, 2-12
  - description, 2-12
  - foreground color, 2-12
  - read (community), 2-12
  - write (community), 2-12
- Analyze network problems, 6-1
- Auto scaling, 4-15

## B

---

- Basic terms
  - DECpacketprobe agent, 1-2
  - definition, 1-2
  - IP address, 1-2
  - network, 1-2
  - node, 1-2
  - PROBEwatch client, 1-2

## C

---

- Change a domain, 4-24
- Client Definition, 1-8
- Colors, 6-4
- Colors values
  - apply, 6-4
  - load, 6-4
  - reset, 6-4
  - save, 6-4
- Command line operation, 4-15
- Common terms, 3-4
  - data source, 3-4
  - index, 3-4
  - owner, 3-5
  - status, 3-5
- Communities, A-2
- Configure
  - admin, 2-7
  - defaults, 2-7
  - system, 2-7
- Control entries, 3-1
- Control entry actions
  - add, 3-3
  - change, 3-3
  - delete, 3-3
- Conversation list, 4-13
  - destination to source, 4-6
  - operation, 4-14
  - source to destination, 4-6
- Conversation quick graph, 4-14
- Conversation variant, 4-16

Create a domain, 4-21  
Current/cumulative option, 4-11

## D

---

Data Capture, 2-15, 5-1, 6-2  
  operation, 5-1  
Data Capture functions  
  packet Capture, 2-15  
  protocol decode, 2-15  
Data Capture screen fields, 5-4  
  address type, 5-4  
  both directions, 5-5  
  buffer size, 5-4  
  buffer status, 5-5  
  captured packets, 5-5  
  file name, 5-4  
  filter type, 5-5  
  LockWhenFull, 5-4  
  mode, 5-4  
  slice size, 5-4  
  source/destination address, 5-5  
  started @, 5-5  
  update interval, 5-5  
  WrapWhenFull, 5-4  
Data Capture screen push buttons  
  decode, 5-4  
  delete, 5-4  
  start, 5-3  
  stop, 5-3  
  upload, 5-3  
Data collection parameters, 3-2  
Decimal format, 3-7  
DECpacketprobe agent, 2-6  
DECpacketprobe menus  
  configure, 2-7  
  filters, 2-11  
  statistics, 2-9  
Default names, 3-9  
  ethernet type, 3-9  
  IP ports, 3-10  
  MAC addresses, 3-11  
  Novell ports, 3-11  
  SAPS, 3-10  
  TCP ports, 3-10  
Default names (cont'd)  
  UDP ports, 3-10  
Delete a domain, 4-24  
Destination-source, 4-13  
Destination to source, 4-6  
Discovery, 4-6  
  operation, 7-2  
Documentation  
  ordering, B-1  
  related, B-1  
Document organization, ix  
Domain  
  change, 4-24  
  delete, 4-24  
  view, 4-24  
Domain editor, 4-5, 4-20  
  operation, 4-21  
Domain editor fields  
  accept type, 4-21  
  attached filters, 4-21  
  domain description, 4-21  
  domain name, 4-21  
Domain Editor fields, 4-21  
Domain pulldown, 4-19  
Domain view, 4-1  
Domain view properties field descriptions,  
  4-26  
  ethernet packet capture slice size,  
    4-27  
  lines per page for reports, 4-26  
  long-term history buckets, 4-26  
  long-term history sample period, 4-26  
  packet capture buffer size, 4-27  
  short-term history buckets, 4-26  
  short-term history sample period, 4-26  
  statistics update period, 4-26  
  token ring packet capture slice size,  
    4-27  
  top N conversations (host zoom), 4-27  
  top N hosts (segment zoom), 4-27  
Domain views, 2-14  
  definition, 4-1  
  operation, 4-2  
  properties, 4-24  
  quick graph, 4-14

## **E**

---

### Editor

- names, 2-17

## **F**

---

Fault conditions, 6-1

### Filters

- channel, 2-11
- filter, 2-11

### Filter types

- exclusive, 5-5, 6-12
- inclusive, 5-5, 6-12

Frame structures, 1-5

- check, 1-6
- data field, 1-6
- destination address, 1-6
- length, 1-6
- preamble, 1-6
- source address, 1-6
- type, 1-6

Fundamentals of operation, 3-1

## **G**

---

GoTo frame, 6-5

## **H**

---

HEX format, 3-7

High-water scaling, 4-15

### Host

- quick graph, 4-14
- system information, 4-11
- variant, 4-16
- zoom, 4-11
- zoom operation, 4-11

Host list, 4-10

- discovery, 4-6
- MAC address, 4-6
- operation, 4-11

HostTopN, 4-1

How long to run, 7-4

## **I**

---

### Inband

- definition, 1-8

Installation, 2-1

Introduction, 1-1

IP Address format, 3-7

### Item identifiers

- IP addresses, 3-5
- MAC addresses, 3-5
- protocol types, 3-5

## **M**

---

MAC address, 4-6

Management tools, 7-1

- definition, 2-16
- discovery, 2-16, 7-1

### MIB

- groups and communities, A-1
- ITEF, A-2

### Mouse

- actions, 2-2
- operations, 2-1

## **N**

---

Name format, 3-7

Netmask, 7-4

## **O**

---

### Options

- ordering, B-1

### OSI functions

- application, 1-4
- data link, 1-4
- network, 1-4
- physical, 1-4
- presentation, 1-4
- session, 1-4
- transport, 1-4

OSI model, 1-3  
OSI seven-layer functions, 1-4  
Out of band Definition, 1-8  
Overview, 2-1

## **P**

---

Packets  
  view, 6-5  
Polycenter Network Manager, 1-9  
  installing PROBEwatch, 2-4  
Popup discovery, 7-2  
Popup fields  
  how long to run, 7-4  
  netmask, 7-4  
Post Capture Filter values  
  address type, 6-12  
  both directions, 6-12  
  filter type, 6-12  
  protocol mode, 6-12  
  source/destination address, 6-12  
PROBEwatch  
  function, 1-1  
  getting started, 2-2  
  installation with Polycenter Network  
  Manager, 2-4  
  protocol decode, 6-2  
  standalone installation, 2-4  
  standards, 1-1  
  top menu, 2-11  
  without Polycenter Network Manager,  
  1-9  
  with Polycenter Network Manager,  
  1-9  
PROBEwatch support  
  nine RMON-MIB groups, 2-1  
  seven-layer protocol analysis, 2-1  
Problems, 6-1  
  results of, 6-1  
Properties, 4-5, 4-24, 6-2  
  operation, 4-24  
  push buttons, 4-26  
Properties values  
  address mode, 6-4  
  raw mode, 6-4

Properties values (cont'd)  
  time mode, 6-4  
  zoom mode, 6-4  
Protocol analysis, 1-7  
Protocol decode, 6-1  
  framework, 6-1  
Protocol Decode, 2-16  
  change mode, 6-6  
  operation, 6-2  
  protocol mode, 6-8  
  raw mode, 6-6  
  sequence, 6-1  
  zoom mode, 6-10  
Protocol modes  
  custom, 6-12  
  standard, 6-12  
Protocol Structure, 1-3  
Push buttons  
  segment zoom, 4-5

## **Q**

---

Quick graph  
  command line operation, 4-15  
  domain view, 4-14  
  host, 4-14, 4-18  
  long term history, 4-14  
  network statistics, 4-16  
  operation, 4-14  
  short term history, 4-14  
  statistics, 4-14  
Quick graph arguments, 4-16  
  agent, 4-16  
  domain, 4-16  
  hostMAC[AB], 4-16  
  host[AB], 4-16  
  instance, 4-16  
  type, 4-16  
Quick graph characteristics, 4-15  
  hard copy, 4-15  
  sample period, 4-15  
  scaling, 4-15  
  type, 4-15  
  variable selection, 4-15  
  view, 4-15

## R

---

- RMON groups
  - alarm, 2-9
  - etherStats, 2-9
  - event, 2-9
  - history, 2-9
  - host, 2-9
  - hostTopN, 2-9
  - matrix, 2-9
- RMON-MIB, 1-1

## S

---

- Scaling options
  - auto, 4-15
  - high-water, 4-15
- Scope, 4-5, 4-30
- Segment, 4-5
  - operation, 4-7
- Segment Zoom
  - conversation list, 4-6
  - host list, 4-6
  - host zoom, 4-6
- Segment Zoom field descriptions, 4-7
  - agent interface information, 4-9
  - agent system information, 4-9
  - captured pkts, 4-9
  - conversations, 4-9
  - cumulative statistics, 4-9
  - hosts, 4-9
  - long-term history, 4-10
  - short-term history, 4-10
  - top N hosts, 4-10
  - top N sort metric, 4-9
- Segment Zoom push buttons, 4-10
  - conversation list, 4-13
  - host list, 4-10
  - host zoom, 4-11
- Simple Network Management Protocol, 1-1
- SNMP, 1-1

- Source-destination, 4-13
- Source-destination addresses
  - valid IP address, 5-5
  - valid MAC address, 5-5
  - valid name, 5-5
- Source to destination, 4-6
- Standalone operation, 1-8
- Statistics, 4-12
  - quick graph, 4-14
  - variant, 4-15
- Statistics selections
  - interface, 2-9
  - RMON groups, 2-9
- Summary mode values
  - destination node, 6-5
  - pkt ID, 6-5
  - protocol, 6-5
  - size, 6-5
  - source node, 6-5
  - status, 6-5
  - timestamp, 6-5
- Symbolic names, 3-5

## T

---

- Top menu selections
  - data capture, 2-11, 2-15
  - domain view, 2-11, 2-14
  - filter editing, 2-11
  - management tools, 2-11, 2-16
  - names editor, 2-17
  - protocol decode, 2-11, 2-16
  - traps, 2-11
- Top N conversations, 4-12
  - inbound, 4-12
  - outbound, 4-12
- Topology, 1-8
- Traps, 2-17, 7-4
  - descriptions, 8-1
  - editing, 8-1
  - editing options, 8-1

## **U**

---

Using DECpacketprobe agent, 2-6  
Using PROBEwatch, 2-11

## **V**

---

View  
    domain, 4-24  
    packets, 6-5  
View Packets, 4-5, 4-32

## **W**

---

Watchdog, 4-2, 4-5, 4-28