Nways Manager Remote Monitor

User’s Guide

SA33-0367-04

Nways Manager Remote Monitor

User’s Guide

SA33-0367-04

Note

Before using this information and the product it supports, be sure to read the general information under "Appendix A. Notices" on page 135.

Fourth Edition (May 1999)

This edition applies to Version 2 of the Nways Manager Remote Monitor.

Order publications through your IBM representative or the IBM branch office serving your locality. Publications are not stocked at the address given below.

A form for readers' comments appears at the back of this publication. If the form has been removed, address your comments to:

Department CGFA- Design & Information Development
IBM Corporation
PO Box 12195
RESEARCH TRIANGLE PARK, NC 27709-9990
USA.

You can also submit your comments about this publication online at:
`http://www.networking.ibm.com/support/feedback.nsf/docsoverall`

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Contents

Figures

Tables

About This Guide

This guide describes Nways Manager Remote Monitor and explains how you can use this application to gather real-time and historical information on your network.

For a description of the minimum system configuration requirements and supported operating systems, as well as minimum agent firmware and SmartAgent software versions, refer to the release notes shipped with this product. These also contain the very latest information on Nways Manager Remote Monitor.

This guide is intended for network administrators. It assumes a working knowledge of local area network (LAN) operations.

How to Use This Guide

Table 1 shows where to look for specific information.

Table 1. Where to Find Specific Information

If you are looking for...	Turn to...
An overview of the Nways Manager Remote Monitor applications and an introduction to the Remote Monitoring standard.	Chapter 1
Information on how to contact and view network devices, using Nways Manager Remote Monitor.	Chapter 2
Information on performing device configuration.	Chapter 3
Procedures for configuring the main window, opening multiple windows and reading main window graphs.	Chapter 4
Procedures for gathering current statistical data about the network.	Chapter 5
Procedures for monitoring for specific events on the network.	Chapter 6
Procedures for capturing data from the network and carrying out packet decode and analysis.	Chapter 7
Procedures for using the Address Mapping, Protocol Distribution, Data Export and Data Collector applications.	Chapter 8
IBM NetView, and Procedures for integrating Nways Manager Remote Monitor with HP OpenView.	Appendix B and Appendix C
List of supported decodes and relevant documentation for both RMON Views and ECAM applications.	Appendix D
Procedures for using the Roving Analysis Port (RAP), PACMIB.	Appendix E
List of the variables used in RMON Views and ECAM applications.	Appendix F
Procedures for viewing statistics by network layer (RMON2/ECAM).	Appendix G
List of Known Problems	Appendix H

User Guide Conventions

Table 2 and Table 3 list conventions that are used throughout this guide.

Table 2. Notice Icons

Type	Description
Note	Important features or instructions.
Attention	Risk of system damage or loss of data.

Table 3. Text Conventions

Convention	Description
″Enter″ versus ″Type″	The word ″enter″ means you must type something, then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says ″type.″
Text represented as `commands`	This typeface is used to represent commands that you enter, for example: `SETDefault !0 -IP NETaddr = 0.0.0.0`
Keys	When specific keys are referred to in the text, they are described by their labels, such as ″the Return key″ or ″the Escape key,″ or they may be shown as **Return** or **Esc**. If you need to press two or more keys simultaneously, the keys are linked with a plus sign (+), for example: Press **Ctrl**+**Alt**+**Del**.

User Interface Conventions

The following buttons are used in dialog boxes in the Nways Manager Remote Monitor user interface:

Table 4. Dialog Box Button Conventions

Click this button...	To do this...
Apply	Bring changes into effect.
Cancel	Abandon your changes and return to the previous level.
Close	Return to the previous level.
Help	Access online help.
OK	Bring changes into effect and return to previous level.

Terminology Used in This Guide

This section lists several terms and their definitions as used in this guide.

Device A generic term used to refer to any network management device, such as a probe or agent.

Ethernet This refers to Ethernet, 100BASE-FX Ethernet and 100BASE-TX Ethernet (also known as Fast Ethernet), unless otherwise stated in the guide.

Firmware This is the software running in a device.

Probe An RMON or RMON2-capable device.

Station A generic term used to refer to workstations or other equipment installed on your network, also referred to as a Host.

Related Web Sites

The following Web sites contain useful networking information.

Nways Management

http://www.networking.ibm.com/netmgt

SNMP

SNMPv2 Working Group information:

http://snmp.net.cmu.edu/bin/snmpv2

RMON

RMON Request for Comment:

http://ds.internic.net/rfc/rfc1757.txt

RMON2 Request for Comment:

http://ds.internic.net/rfc/rfc2021.txt

RMON2 Protocol Identifiers:

http://ds.internic.net/rfc/rfc2074.txt

Miscellaneous

Links to network management information:

http://snmp.cs.utwente.nl

Internet Engineering Task Force home page:

http://www.ietf.cnri.reston.va.us

Network Management Resource Database:

http://www.onramp.net/˜cwk/net-manage.cgi

Online Help

Online help is available for Nways Manager Remote Monitor to help you use dialog boxes and menus, perform procedures, interpret statistics and troubleshoot your network.

You can access help for Nways Manager Remote Monitor in three ways:

- From the Help button in dialog boxes
- From the Help menu (Help Contents command)
- Toolbar

From within the Help system, you can also search for the information you need using the Contents button. Click **Help On Help** for background information.

Chapter 1. Nways Manager Remote Monitor Overview

This chapter introduces you to Nways Manager Remote Monitor. It contains the following sections:

- What is Nways Manager Remote Monitor?
- How Nways Manager Remote Monitor Works
- Supported Interface Types

What is Nways Manager Remote Monitor

Nways Manager Remote Monitor consists of an integrated set of applications that you can use to display and explore the real-time and historical data captured by RMON, ECAM, and RMON2-compliant devices on the network.

Use Nways Manager Remote Monitor to:

- Monitor current performance of LAN and WAN segments.
- View trends over time (Nways Manager Remote Monitor's main window shows the short-term trends, while the History View shows medium- to long-term trends).
- Spot signs of current problems (such as irregular packet sizes, errors and collisions).
- Configure alarms to monitor for specific events on a segment.
- Capture and display packets using filtering and decode functions.

At specified intervals, Nways Manager Remote Monitor polls remote network devices to retrieve essential network data, which it processes and displays in the main window. From the main window you can monitor the health of a segment, its current performance, and recent trends. You can also open new windows to monitor different segments at the same time.

For in-depth investigation, you can launch Nways Manager Remote Monitor's RMON Views and Applications from the main window. Using these you can do the following:

- Look at statistical and historical data
- Set up alarm conditions
- Monitor conversations between stations on the network
- Capture and display specific packets
- Compare statistics from different segments in the same graph

You can access additional functionality by downloading SmartAgent software to compliant devices. For further information, refer to "Downloading SmartAgent Software" on page 179.

Using Nways Manager Remote Monitor for Network Monitoring

You can use the Nways Manager Remote Monitor main window and RMON Views to monitor your network, collecting statistics to identify and deal with imminent problems.

- Use the main window and the Statistics View periodically to check network performance and utilization, watching for emerging problems and short-term trends.
- For specific problems, combine the Alarms View and Capture Application to collect packets leading up to or following a specified event. Then use the Decode Application and Conversation Analysis function to expose the cause of the problem.
- Use the Host and Matrix Views to get information on the busiest stations on your network.
- Use the History View to look at the fluctuations and trends in network statistics over time. This information can give you time to plan for and implement new capacity before existing capacity is exhausted.

The History View can also help you to spot sporadic fluctuations in network usage that might be solved by a reconfiguration of existing network resources. You can then implement a combination of Alarms and Capture to watch for a recurrence of this specific problem.

How Nways Manager Remote Monitor Works

This section introduces some of the basic concepts of remote network monitoring with Nways Manager Remote Monitor. It is divided into two parts:

- An overview of the Remote Monitoring (RMON) and RMON2 standards and the concepts behind remote network monitoring.
- A short description of the network monitoring tools provided by Nways Manager Remote Monitor.

RMON Overview

Prior to the RMON standard, monitoring applications could learn about the amount of traffic into and out of each device on a LAN, but could not easily learn about the traffic on the LAN as a whole.

The RMON standard brings the following advantages to network monitoring:

- It provides an effective and efficient way to monitor the behavior of the entire LAN.
- It is a widely used standard.
- It distributes the load of network monitoring between both remote devices and management stations.

RMON devices collect information about network behavior and transfer it on request to an analysis site. A device can be deployed as a stand-alone device or as an agent within a hub, router or switch. RMON devices have the following benefits:

- They improve the efficiency of staff by allowing them to remain in a centralized site while collecting information from widely dispersed LAN segments.
- They can monitor and collect information continuously and deliver it before problems occur, allowing administrators to take a proactive approach to managing their networks.
- Each remote device can handle requests from multiple management applications.

A client sets RMON variables on the device to specify measurement intervals, monitored thresholds and other operational parameters. The remote device collects and stores information and delivers it to a client on request. Devices can send an SNMP trap to a group of management stations when specified conditions have been detected, alerting the network administrator to a situation that requires immediate attention.

RMON2 Standard

RMON2 is an extension of the RMON standard. It collects statistics at the network and application layers of the protocol stack. Nways Manager Remote Monitor uses RMON2 functionality to allow the user to view the distribution of protocols on the network. It also uses address mapping to allow the user to discover network addresses over the entire network.

Note: RMON2 (ECAM) is IBM's precursor to the RMON2 standard.

Nways Manager Remote Monitor Basics

Nways Manager Remote Monitor is made up of the following:

- Nways Manager Remote Monitor Main Window
- Configuration Functions
- Analysis Functions (RMON Views)
- Tools

Nways Manager Remote Monitor Main Window

From the main window you can monitor key parameters of network health. The main window menu bar gives access to all other Nways Manager Remote Monitor functionality, and the toolbar contains the most frequently used functions.

Configuration Functions

Device Configuration
Configure devices on the network.

Address Translation
Configure the way Nways Manager Remote Monitor displays network addresses.

Protocol Directory
Configure the protocol directory on an RMON2 device.

Roving Analysis Port configuration and status
Configure analyzer and monitor ports for CoreBuilder switches and view status information for the switch. For more information, see Appendix E.

Analysis Functions (RMON Views)

RMON Statistics View
The Statistics View displays a real-time report of activity on your chosen

network segment and is the first place you should look if you suspect there are problems on a particular segment. Use this View to display statistics on any combination of packets, bytes, errors, size distributions or multicasts.

RMON History View

The History View allows you to gather data on your network's normal trends. When you have determined your network's normal activity, you can set alarms to trigger when network activity deviates from the norm. Use the History View to specify a sample period and spot trends over hours, days or weeks.

RMON Host View

The Host View is useful when determining which nodes are on your network, the state of those nodes, and which nodes may be causing problems. Host TopN statistics list the top 50 stations by various criteria.

RMON Matrix View

The Matrix View shows the amount of traffic and number of errors between stations on the network. This allows you to single out stations that might be responsible for generating problems.

RMON Ring Station (Token Ring) View

Collect and view ring information exclusive to Token Ring, including station status and last entered and last exited times.

Alarms

Alarms are the key to proactive network management, and allow you to trace specific events as they happen. You can use alarms on their own, or in conjunction with Capture and Decode. You can also use them to send traps.

Capture & Decode Applications

Use Capture to filter out those packets you need and store them for analysis. Use Decode to decode captured packets and display all major protocols in easily readable format. You can use Conversation Trace Analysis to track the component packets, along with their transmission times.

Address Map

Allows you to view and export network layer addresses. If you are using a device with ECAM SmartAgent software downloaded, you can also view duplicate addresses.

Protocol Distribution

Allows you to view and export or print RMON2 and RMON2 (ECAM) SmartAgent software protocol distribution data.

PACMIB

Enable or disable Port Address Correlation MIB data. The Port Address Correlation MIB maps port to host data and gathers port statistics. You can view the relationships between addresses seen on the segment from the ports that make up that segment. See Appendix E for more information.

Data Export Functions

Allow you to view and export Statistics, Host, History and Matrix statistical groups.

Tools

Data Collector

Gathers RMON and RMON2 data from devices on the network at regular intervals and stores this data in Comma Separated Variable (CSV) format files. Use this data in conjunction with a reporting tool.

ECAM Application

(Only available if you are using a device with RMON2 (ECAM) SmartAgent software loaded.) Collect and view Protocol Statistics across multiple LAN segments. You can go beyond the original RMON standard to network and application layer, including segment, host and conversation statistics for major protocols and application types.

Supported Interface Types

The following interface types are currently supported by Nways Manager Remote Monitor:

- Ethernet
- 100BASE-TX Ethernet
- 100BASE-FX Ethernet
- FDDI
- LAN emulation on Ethernet (aflane_8023)
- LAN emulation on Token Ring (aflane_8025)
- IBM proprietary virtual LAN interfaces (propVirtual)

Note: 100BASE-TX Ethernet, 100BASE-FX Ethernet, aflane_8023 and propVirtual interfaces are interpreted as Ethernet interfaces. Unless otherwise specified, the use of ″Ethernet″ in this guide includes all of the above. aflane_8025 interfaces are interpreted as Token Ring interfaces. Unless otherwise specified, the use of ″Token Ring″ in this guide also includes aflane_8025 interfaces.

Chapter 2. Launching and Configuring Nways Manager Remote Monitor

This chapter tells you how to launch Nways Manager Remote Monitor and specify a list of the devices that are available to be monitored. It contains the following sections:

- Overview
- Launching Nways Manager Remote Monitor
- Launching the Device Administration Dialog Box
- Setting Up and Verifying Devices
- Viewing Basic Device Information
- Managing RMON and RMON2 Tables

Overview

To make Nways Manager Remote Monitor operational, you must specify a list of the devices that are monitoring your network. When this is complete, you can start to monitor the health of your network via the main window and Nways Manager Remote Monitor Views and Applications.

Additional configuration, such as creating virtual interfaces and adding user-defined protocols can be carried out at any time. For further information on these, refer to “Chapter 3. Configuring Devices from Nways Manager Remote Monitor” on page 17.

Launching Nways Manager Remote Monitor

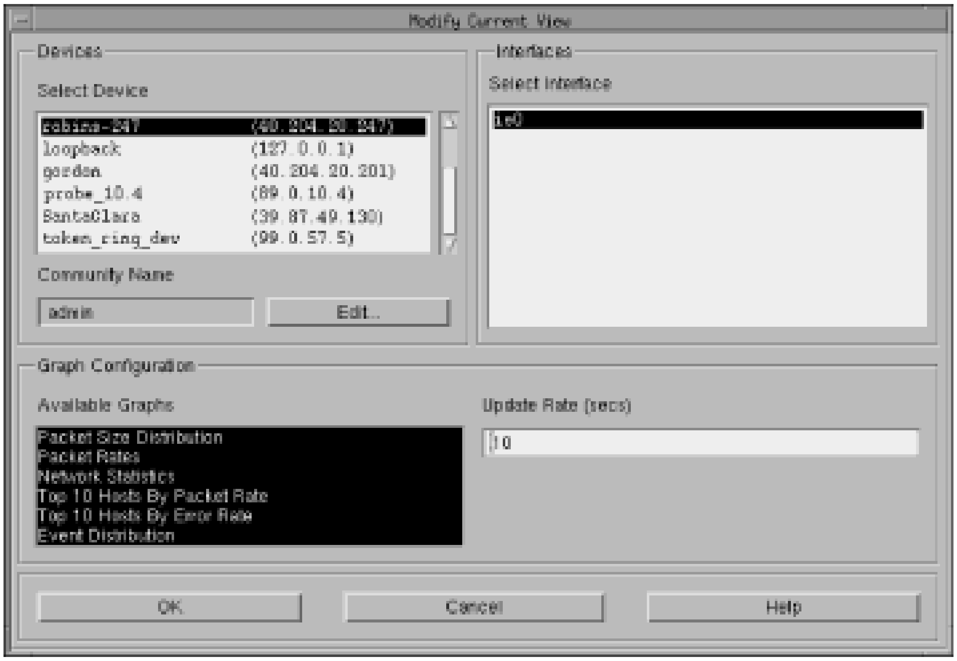
To launch Nways Manager Remote Monitor, run the following command:

```
rmon
```

This command assumes you have added the Nways Manager Remote Monitor directory to your path, as described in “Appendix H. Known Problems” on page 195.

Note: For information on launching Nways Manager Remote Monitor from HP-OpenView, and IBM NetView, refer to the relevant appendix.

A start-up screen is displayed, followed shortly by Nways Manager Remote Monitor’s main window. The Modify View dialog box (Figure 1 on page 8) appears, prompting you to choose which device you want to monitor:



Select Device

cabins-247	(40.204.20.247)
loopback	(127.0.0.1)
gordon	(40.204.20.201)
probe_10.4	(89.0.10.4)
SantaClara	(39.87.49.130)
token_ring_dev	(99.0.57.5)

Community Name: admin

Select Interface: le0

Available Graphs:
- Packet Size Distribution
- Packet Rates
- Network Statistics
- Top 10 Hosts By Packet Rate
- Top 10 Hosts By Error Rate
- Event Distribution

Update Rate (secs): 10

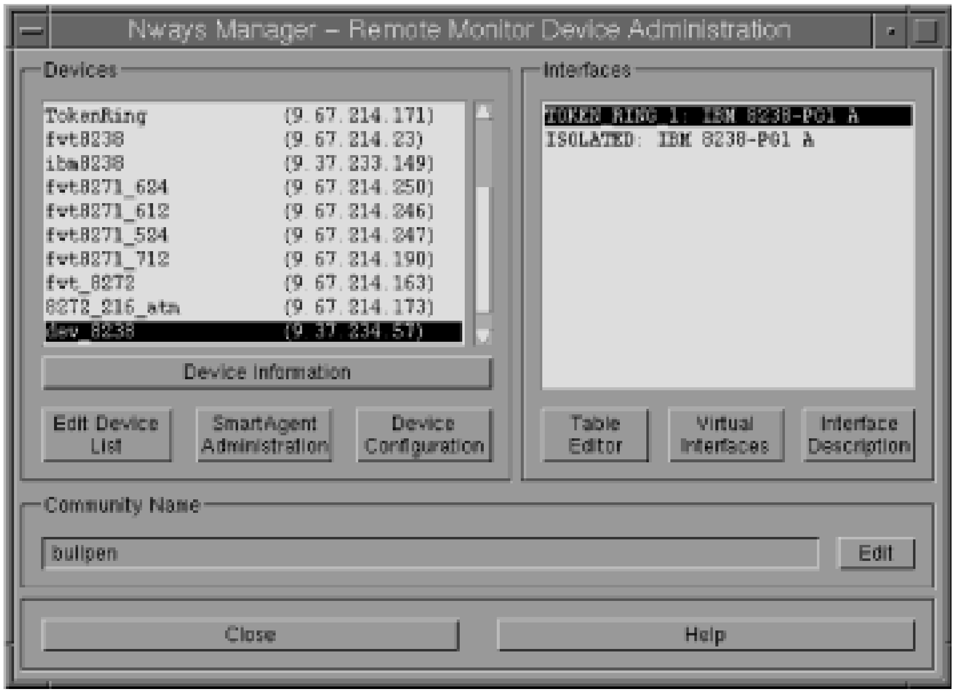
Figure 1. Modify Current View Dialog Box

Select the required device and interface in the Device and Interface areas, and click **OK** to display details of this device in Nways Manager Remote Monitor’s main window.

For further information on selecting devices, refer to “Customizing the Main Window” on page 54.

Launching the Device Administration Dialog Box

You carry out all configuration of devices from the Device Administration dialog box. To open this dialog box, select **Devices** from the Configure menu or click **Device Administration** in the toolbar.



```
TokenRing        (9.67.214.171)
fvt8238          (9.67.214.23)
ibm8238          (9.37.233.149)
fvt8271_624      (9.67.214.250)
fvt8271_612      (9.67.214.246)
fvt8271_524      (9.67.214.247)
fvt8271_712      (9.67.214.190)
fvt_8272         (9.67.214.163)
8272_216_atm     (9.67.214.173)
dev_8238         (9.37.234.57)
```

```
TOKEN_RING_1: IBM 8238-P01 A
ISOLATED: IBM 8238-P01 A
```

Community Name: bullpen

Figure 2. Device Administration Dialog Box

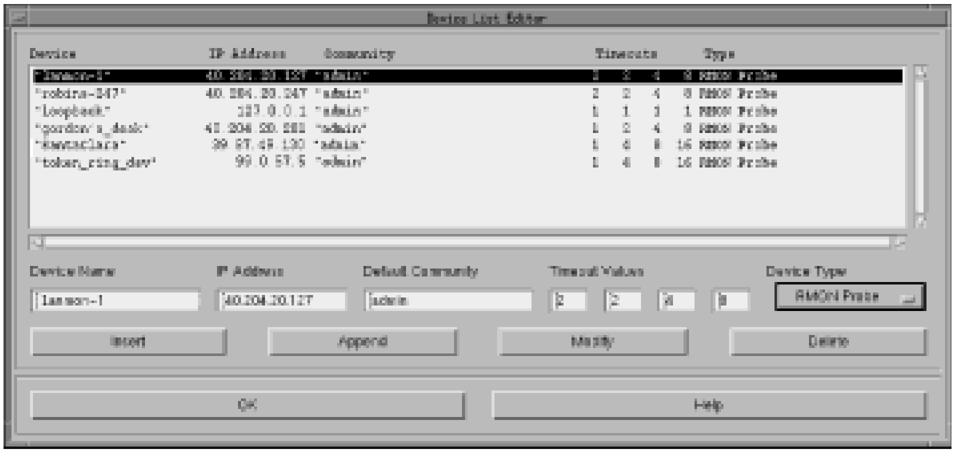
Setting Up and Verifying Devices

Specify which devices Nways Manager Remote Monitor can use to monitor the network by following these steps from the Device Administration dialog box.

Setting up a New Device

To set up a new device, follow these steps:

1. Click **Edit Device List** to open the Device List Editor, shown in Figure 3 on page 10.



Device	IP Address	Community	Timeouts				Type
"lanmon-1"	40.204.20.127	"admin"	2	2	4	8	RMON Probe
"robins-247"	40.204.20.247	"admin"	2	2	4	8	RMON Probe
"loopback"	127.0.0.1	"admin"	1	1	1	1	RMON Probe
"gordon's_desk"	40.204.20.201	"admin"	1	2	4	8	RMON Probe
"santaclara"	39.97.49.130	"admin"	1	4	8	16	RMON Probe
"token_ring_dev"	99.0.57.5	"admin"	1	4	8	16	RMON Probe

Device Name: lanmon-1
IP Address: 40.204.20.127
Default Community: admin
Timeout Values: 2 2 4 8
Device Type: RMON Probe

Figure 3. Device List Editor

By default, the device selected in the Device Administration dialog box is selected.

2. Enter a unique name in the Device Name field.
3. Enter the IP Address for the device.
4. In the Default Community field, Nways Manager Remote Monitor displays the default community name used to access the selected device. If appropriate, change this default name.
5. If appropriate, change the Timeout Values for the agent. The default values are all set to 1 second.

   The timeouts determine the intervals at which Nways Manager Remote Monitor polls a device before announcing that there is no response. The defaults are adequate for most installations. However if you are running over a slower connection, such as a serial cable, you may wish to increase the values, for example to 4, 6, 8, and 9 seconds.
6. Select the appropriate type for the device by clicking **Device Type** and selecting from the drop-down menu. See Appendix E for use of Roving Analysis Port features.
7. Click **Insert** or **Append** to add the new entry to the list. Insert places the new entry before the current selection, while Append adds it after the current selection.

The new device is shown in the Devices area of the Device Administration dialog box.

Modifying a Device Entry

To modify an existing device entry, follow these steps:

1. Select an entry in the Device List Editor dialog box. The details for the selected device appear in the fields beneath the list.
2. Change any of the entries as required.

Note: Changes made to community name or timeout values do not affect current Views.

3. Click **Modify** to apply the changes.
4. Click **OK** to return to the Device Administration dialog box.

Deleting a Device Entry

To delete a device entry from Nways Manager Remote Monitor, follow these steps:

1. Select an entry in the Device List Editor dialog box. The details for the selected device appear in the fields beneath the list.
2. Click **Delete** to delete the device entry. Checking a Device Entry

Checking a Device Entry

To verify that a device has been set up correctly and is contactable, select the device in the Select Device area of the Device Administration dialog box.

- If successful, a list of interfaces available on the device is displayed in the Interfaces area.
- If the device cannot be contacted, the message No response from device is displayed in the Select Interface area. This message may indicate that:
  - You have not set up the device details correctly.
  - The device is temporarily unavailable due to a network problem.
  - The specified time out values are not long enough for contact to be established.
  - The community name does not have the correct access rights.

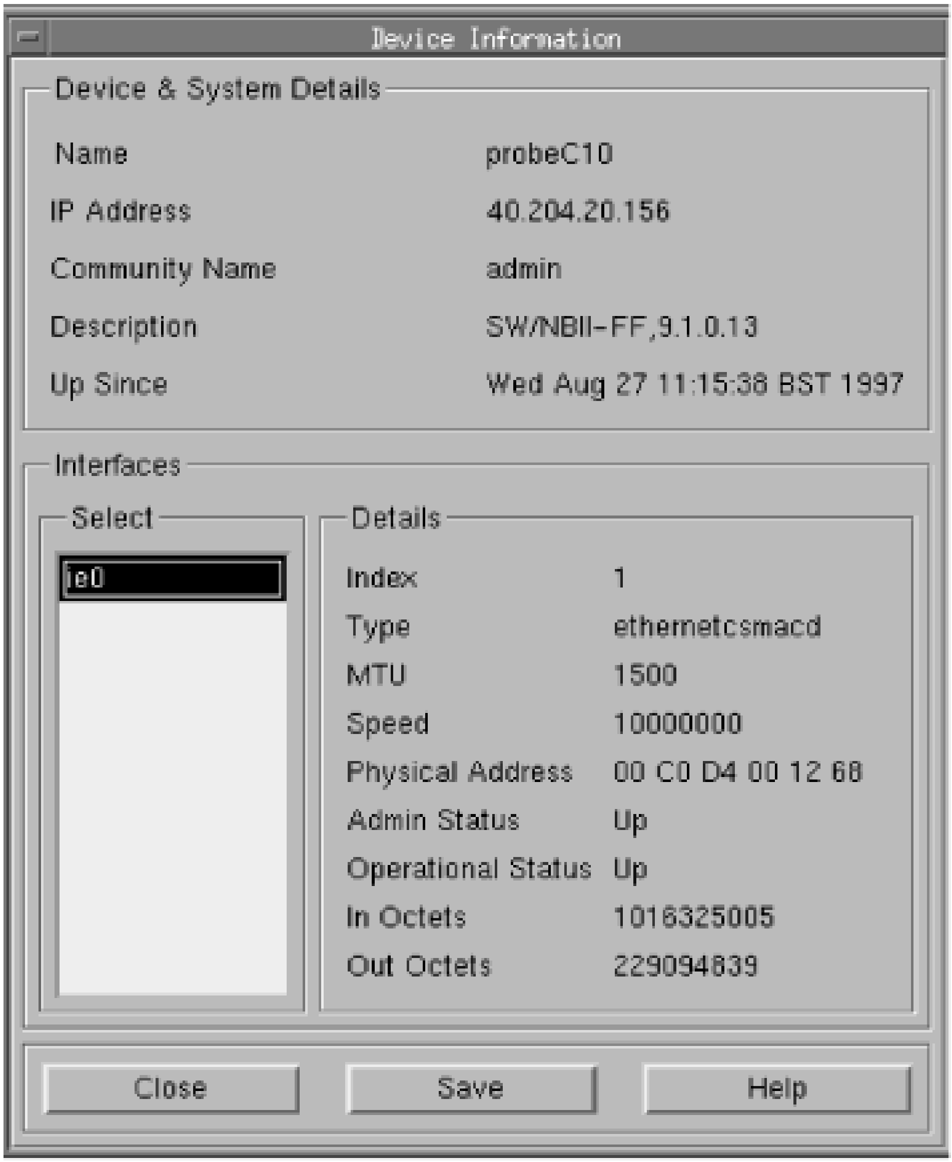
Check that the information entered in the Device List Editor dialog box is correct and try to contact the device again. You can check this information quickly using the Device Information dialog box, as described in Viewing Basic Device Information.

Once you have set up a device and have checked that it can be contacted by Nways Manager Remote Monitor, you must specify which RMON and/or RMON2 tables you want to create. For information on how to set up these tables, see “Managing RMON and RMON2 Tables” on page 13.

Viewing Basic Device Information

A summary of key information about the device currently being used for monitoring can be accessed from the Device Administration dialog box.

Click **Device Information** in the Device Administration dialog box. The Device Information dialog box appears, as shown in Figure 4.



Device & System Details

Name	probeC10
IP Address	40.204.20.156
Community Name	admin
Description	SW/NBII-FF,9.1.0.13
Up Since	Wed Aug 27 11:15:38 BST 1997

Interfaces

Select

ie0

Details

Index	1
Type	ethernetcsmacd
MTU	1500
Speed	10000000
Physical Address	00 C0 D4 00 12 68
Admin Status	Up
Operational Status	Up
In Octets	1016325005
Out Octets	229094839

Figure 4. Device Information Dialog Box

This dialog box is divided into two areas:

- Device and System Details
- Interfaces

Device and System Details

This area contains the device’s name, IP address, community name, system descriptor (a free-form field on RMON devices used by vendors to supply basic information about the device) and the time monitoring started.

Interfaces

In the Select list, click an interface to view interface details in the Details area.

Index The index for the selected interface, taken from the interface table on the device.

Type Physical interface type or virtual interface.

MTU The size (in bytes) of the largest packet that the interface can process.

Speed Theoretical capacity in bits per second.

Physical Address
The 12-digit MAC address.

Admin Status and Operational Status
The desired status of the interface and whether the interface is active.

In Octets and Out Octets
Total octets received and sent.

You can save the contents of the Device Administration dialog box to text file. Click **Save** to open the File dialog box and specify a filename and location. Click **OK** to save the information and return to the Device Information dialog box.

Managing RMON and RMON2 Tables

You can create and delete RMON and RMON2 tables for a device’s physical or virtual interfaces. You can also delete HostTopN tables.

1. Select a device in the Select Device list.
2. Click **Table Editor** to open the Table Editor dialog box, shown in Figure 5 on page 14.

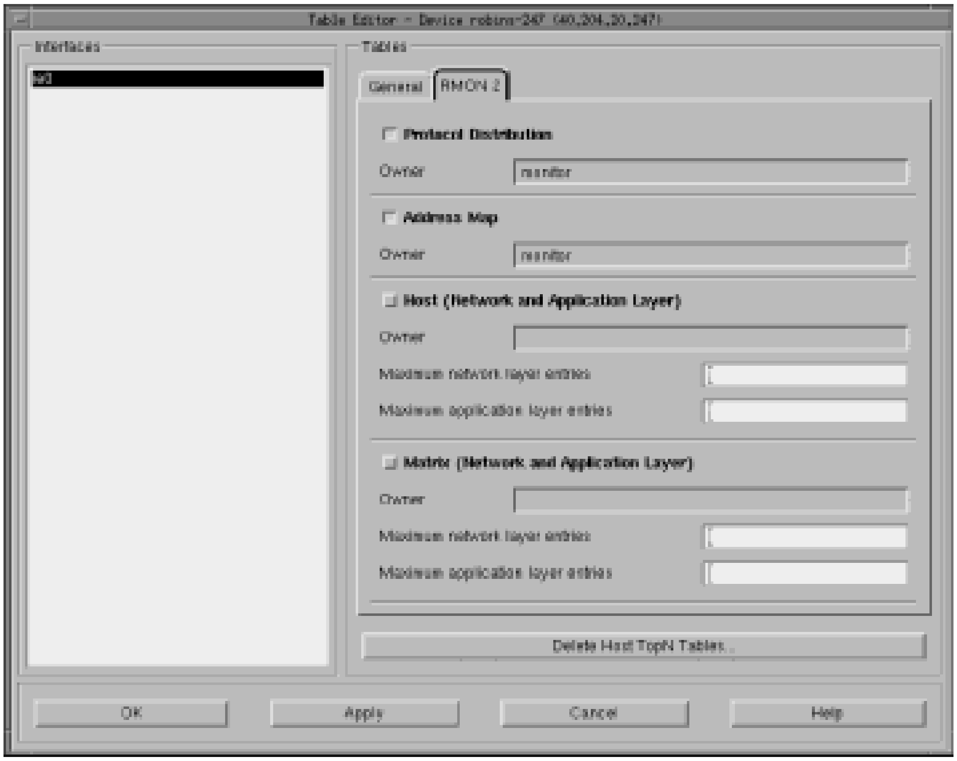


Table Editor - Device robins-247 (40.204.20.247)

Tables — RMON 2

□ Protocol Distribution

Owner: monitor

□ Address Map

Owner: monitor

□ Host (Network and Application Layer)

Owner:

Maximum network layer entries:

Maximum application layer entries:

□ Matrix (Network and Application Layer)

Owner:

Maximum network layer entries:

Maximum application layer entries:

Figure 5. Table Editor Dialog Box

3. Select an interface in the Interfaces area. This can be a physical or a virtual interface. For information on creating virtual interfaces, see “Configuring Virtual Interfaces” on page 37.

   Note: If table entries are greyed out, you do not have permission to create or delete them. This could be because you are using a community name which has no write permission to the tables, or because the device does not support certain tables.

4. Select the General or RMON2 tab to see the relevant tables.

   Note:

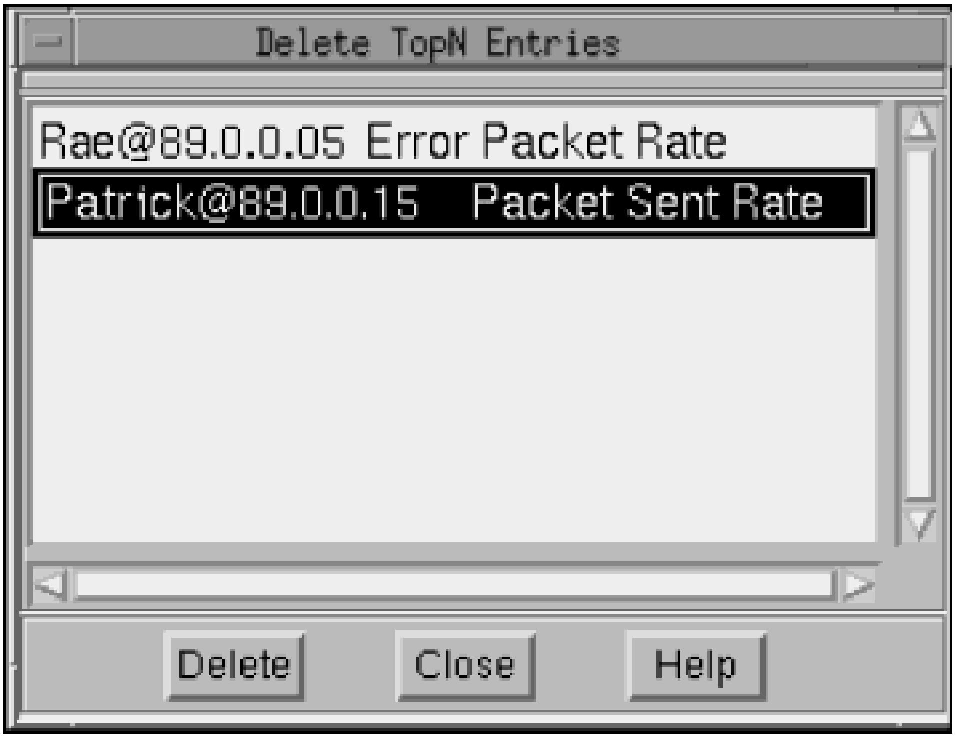
   If you are using RMON2 tables, it is assumed that the protocol directory already exists.

   When creating RMON2 Host and Matrix tables, you can specify the maximum number of network and application layer entries the device will create.

   To select the tables you want to use, do one of the following:

- To delete a table, deselect the table entry.
- To create a table, select the table entry.

5. Nways Manager Remote Monitor automatically creates HostTopN tables for certain graphs. To delete HostTopN table entries, click **Delete HostTopN Tables...** to open the Delete TopN Entries dialog box, shown in Figure 6.



Rae@89.0.0.05 Error Packet Rate
Patrick@89.0.0.15 Packet Sent Rate

Figure 6. Delete Table Entry Dialog Box

   a. Select an entry for deletion.
   b. Click **Delete** to permanently delete the entry from the list. The deletion takes effect immediately, and cannot be undone. Click **Close** to return to the Table Editor.

6. To activate any changes made in the Table Editor, click **Apply** or **OK**. To cancel the changes or select a different interface, click **Cancel**, returning you to the Device Administration dialog box.

Once you have created the tables you want to use, start monitoring your network using the main window, RMON Views, and Applications.

Chapter 3. Configuring Devices from Nways Manager Remote Monitor

This chapter tells you how to perform device configuration beyond that which is required to allow Nways Manager Remote Monitor to view network devices. It contains the following sections:

- Accessing Device Configuration
- Setting System Parameters
- Downloading Firmware
- Setting the IP Address, Subnet Mask, and Ring Number
- Setting Serial Link Connections
- Setting Static Routes, the Default Gateway, and Echo Interval
- Access Control Tables
- Setting Up Trap Communities
- Configuring Virtual Interfaces
- Setting the Address Translation Level
- Renaming Interfaces
- Managing User-Defined Protocols
- Specifying Vendor Prefixes

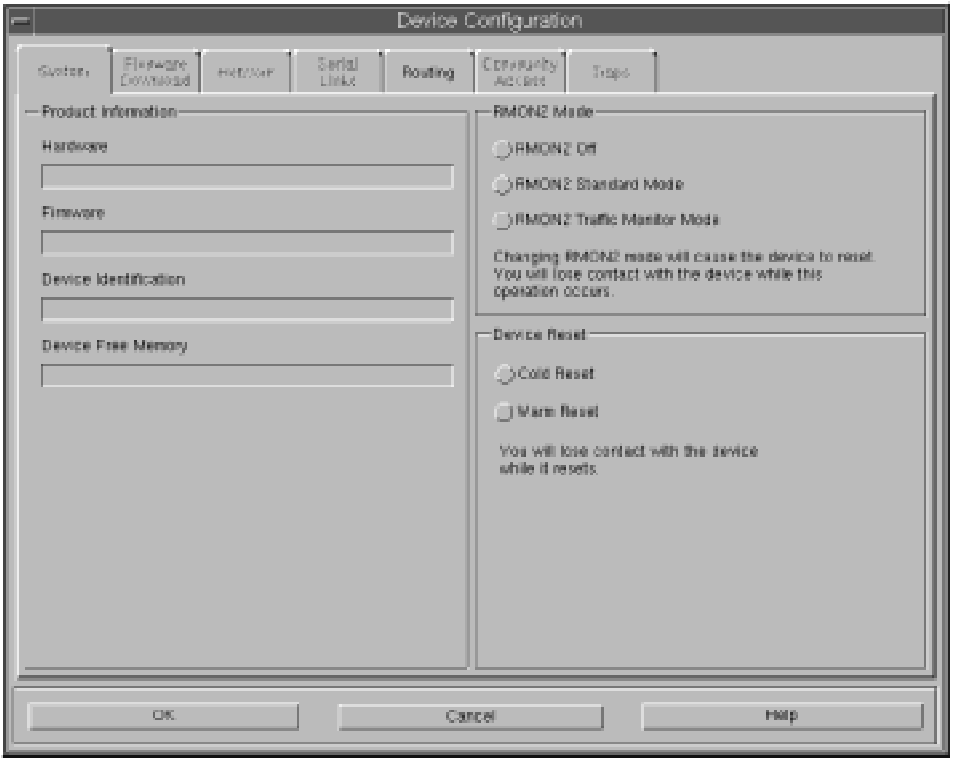
Accessing Device Configuration

You configure devices from the Device Configuration dialog box. To access this dialog box, follow these steps:

1. In the Device Administration dialog box, select the device you wish to configure.

   For devices that support multiple interfaces, such as IBM’s 8272, you can set the IP address on any of the listed physical interfaces.

   Note: If you set more than one IP address, ensure each is on a different subnet.
2. Click **Device Configuration** to display the Device Configuration dialog box, shown in Figure 7 on page 18.



Changing RMON2 mode will cause the device to reset. You will lose contact with the device while this operation occurs.

You will lose contact with the device while it resets.

Figure 7. Device Configuration Dialog Box

The Device Configuration dialog box contains the following tabs:

Table 5. Device Configuration Dialog Box Tabs

Tab	**Allows you to...**
System	• View hardware and firmware versions and device details • Reset a device using cold or warm starts • Set RMON2 mode to Standard or Nways Manager-Traffic Monitor • Enable/disable RMON2
Firmware Download	Download new firmware
Network	Set the IP address, subnet mask and ring number (Token Ring only) for each interface
Serial Links	Set up serial link connections. For more information, refer to “Setting Serial Link Connections” on page 26
Routing	Set up static routes, default gateway and echo interval
Community Access	Configure access control tables
Traps	Configure trap communities and trap destinations

Setting System Parameters

Use the System tab in the Device Configuration dialog box to carry out the following:

- View hardware and firmware information.
- Reset the device using a warm or cold reset.
- Set the RMON2 mode.

Viewing Hardware and Firmware Information

Table 6 details the contents of the Product Information area:

Table 6. Product Information

Field	Meaning
Hardware	Shows the board revision and memory of the device
Firmware	Shows the version of firmware on the device
Device Identification	Shows the class of device and that device's MAC address
Device Free Memory	The free memory of the device

Resetting a Device

To reset a device, select **Warm Reset**... or **Cold Reset**... in the Device Reset area. Both kinds of reset cause the device to reinitialize, but there are differences in the effect each has on the device. These differences are summarized for RMON and RMON2 variables in Table 7 and Table 8 on page 20. Refer to the keys provided with the tables.

Note: You can carry out configuration in other tabs before resetting the device, as the reset does not occur until you click **OK** in the Device Configuration dialog box.

Attention: Although you can use a cold reset to remove configuration information quickly and reset a device to factory defaults, note that a cold reset results in the loss of user-defined protocol information and community names.

Table 7. Configuration and RMON Data Preserved and Lost

Data Type	Warm Start	Cold Start
Configuration Data		
device configuration information (IP address, etc.)	P	P
autodiscovery echo interval	P	L
RMON2 mode	P	P
Standard/Traffix mode	P	P
tftp server address	P	P
download filename	P	P
date and time$_E$	P	P
serial port configuration information	P	P
community access table entries	P	L$_A$
configuration system telnet password	P	L
client table entries	P	L$_A$

Table 7. Configuration and RMON Data Preserved and Lost (continued)

Data Type	Warm Start	Cold Start
serial connection table	P	L
trap destination table	P	L
RMON Data:		
filter table	P	L
channel table	P	L
capture buffer control table	P	L
history control table	P	L[A]
host control table	P	L[A]
matrix control table	P	L[A]
host control table	P	L
matrix control table	P	L
host topN table	L	L
alarm table	P	L
event table	P	L[A]
captured packets	L	L
historical statistics	L	L
current statistics	L[C]	L[A]
host statistics tables	L	L
matrix statistics tables	L	L
host topN statistics tables	L	L
log tables	L	L
ring station tables[D]	L	L
source routing statistics[D]	L[C]	L[A]
ring station control table[D]	P	L[A]
encap control	P	L

Key

P=Data Preserved
L=Data Lost

A=Reverts to default
B=User defined protocols protocols
C=Control Information preserved
D=Token Ring only
E=Does not apply to 8271 RMON probes.

Table 8. RMON2 Data Preserved and Lost

Data Type	Warm Start	Cold Start
address map control tables	P	L[A]
address map table	L	L
protocol distribution control tables	P	L[A]
protocol distribution tables	L	L
higher-layer host control tables	P	L
network-layer host tables	L	L
application-layer host tables	L	L
higher-layer matrix control tables	P	L
network-layer matrix tables	L	L
application-layer matrix tables	L	L

Table 8. RMON2 Data Preserved and Lost (continued)

Data Type	Warm Start	Cold Start
network-layer matrix topN control tables	L	L
network-layer matrix topN tables	L	L
application-layer matrix topN control tables	L	L
application-layer matrix topN tables	L	L
user history control and objects	P	L
user history tables	L	L
protocol directory	L[A][B]	L[A]

Key

P=Data Preserved	[A]=Reverts to default
L=Data Lost	[B]=User-defined protocols preserved.

RMON2 Functionality

You can set the following RMON2 functionality in probes that provide DLM support:

- IBM’s HETMAC 8260 daughter card probes can be configured to use optimum table sizes for different management applications.
- RMON2 can be disabled so that the device can run SmartAgent software such as the RMON2 (ECAM) SmartAgent software.

  RMON2 (ECAM) is IBM’s precursor to the RMON2 standard, and is used by Nways Manager - Traffic Monitor application.

Note: For full RMON2 functionality, ensure you have the latest version of firmware installed.

Setting The Mode

The current mode of the device is displayed in the System Tab of the Device Configuration dialog box. The default is Standard Mode.

Note: If you change the mode, the device will automatically perform a cold reset so that the changes take effect.

There are three available modes:

Standard Mode
Sets appropriate table sizes on the device for use with Nways Manager Remote Monitoror a third party management application.

Nways Manager - Traffic Monitor Mode
Sets appropriate table sizes on the device for use with Nways Manager - Traffic Monitor. You should use this mode only if you have Nways Manager - Traffic Monitor V1.1 or above.

Off Disables RMON2. With RMON2 disabled you can download SmartAgent software to the device.

When you change the mode and click **OK**, the device will automatically cold reset, there is no need to click **Cold Reset**.

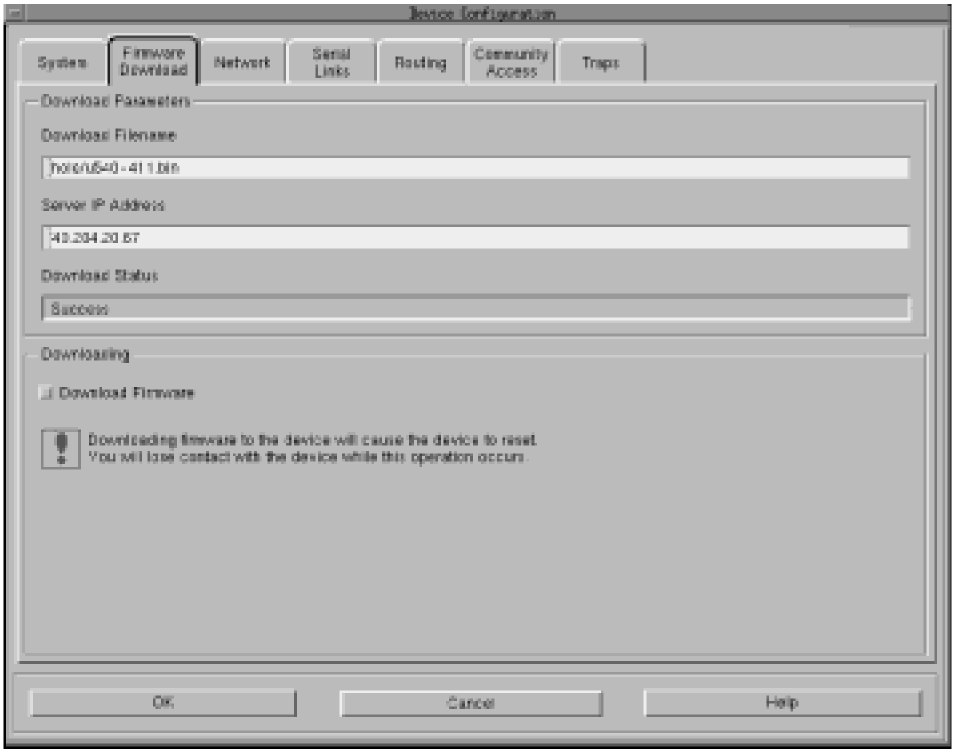
Downloading Firmware

Use the Firmware Download Tab (Figure 8) in the Device Configuration dialog box to download firmware.

To simplify device configuration, firmware files are stored on a TFTP server which can be accessed by the devices on the network. New versions of firmware can then be downloaded to the device from the server.

The Download Status field in the Device Configuration dialog box reflects the success of the last download made by the device.

Note: To download SmartAgent (ECAM) software, see “Downloading SmartAgent Software” on page 179.



Download Parameters

Download Filename: nois/u840-411.bin

Server IP Address: 40.204.20.67

Download Status: Success

Downloading

□ Download Firmware

Downloading firmware to the device will cause the device to reset.
You will lose contact with the device while this operation occurs.

Figure 8. Firmware Download Tab

Note: You must have TFTP configured on the server. Refer to the Installation and Release Notes for more information.

To download firmware, follow these steps:

1. In the Download Filename field, type the filename of the agent firmware. Nways Manager Remote Monitor uses the TFTP directory specified in the TFTP configuration as the location of this file. You have to specify a filename but do not need to specify a directory location in the Download Filename field.
2. In the Server IP Address field, type the IP address of the TFTP server.
3. Click **OK**.

   The device will automatically reset, during which time connection to the device is lost and you are returned to the Device Administration dialog box.

   Note: Firmware download will usually cause a warm reset, but may cold reset when downloading some firmware upgrades.
4. When the device has reset, return to the Device Configuration dialog box and check that the Status field has been set to Success.

   Note: If the download causes a cold restart, the correct status may not display in the Status field. If the firmware download is successful, the new firmware version is displayed in the Firmware field in the System tab.

   If the Status field is set to Failure, this may indicate one of the problems shown in Table 9. Check your TFTP server, and repeat steps 1-4 above.

Table 9. Possible Reasons for TFTP Failure

Problem	**Solution**
The file does not exist on the server.	Copy the file to the correct location.
The file has permissions such that the TFTP server cannot access it.	The file may need to be given global read/write/execute permissions before the TFTP server will allow a TFTP read of the file. This will depend upon the operating system of the TFTP server. Consult your local TFTP documentation for further information.
Despite sending several requests, the server failed to respond.	Check that the IP address entered for the TFTP server is correct.
The file transfer was aborted.	This may occur when the server becomes unavailable during the download process. Check that the TFTP server is available and repeat the download.
The device is unable to contact the network or could not find a route to the TFTP server.	Check that the device is correctly connected to the network. If the TFTP server is on a different subnet from the device, ensure that a default gateway address has been set up in the device’s Configuration System.

Table 9. Possible Reasons for TFTP Failure (continued)

Problem	Solution
The TFTP download failed.	Check you have the current firmware image for the hardware.
The TFTP server is misconfigured to run as a particular user when this user does not exist on the remote system.	Check the configuration of the TFTP server and the operating system on the machine hosting the server.

Setting the IP Address, Subnet Mask, and Ring Number

Use the Network Tab in the Device Configuration dialog box to set these parameters.

Setting the IP Address and Subnet Mask

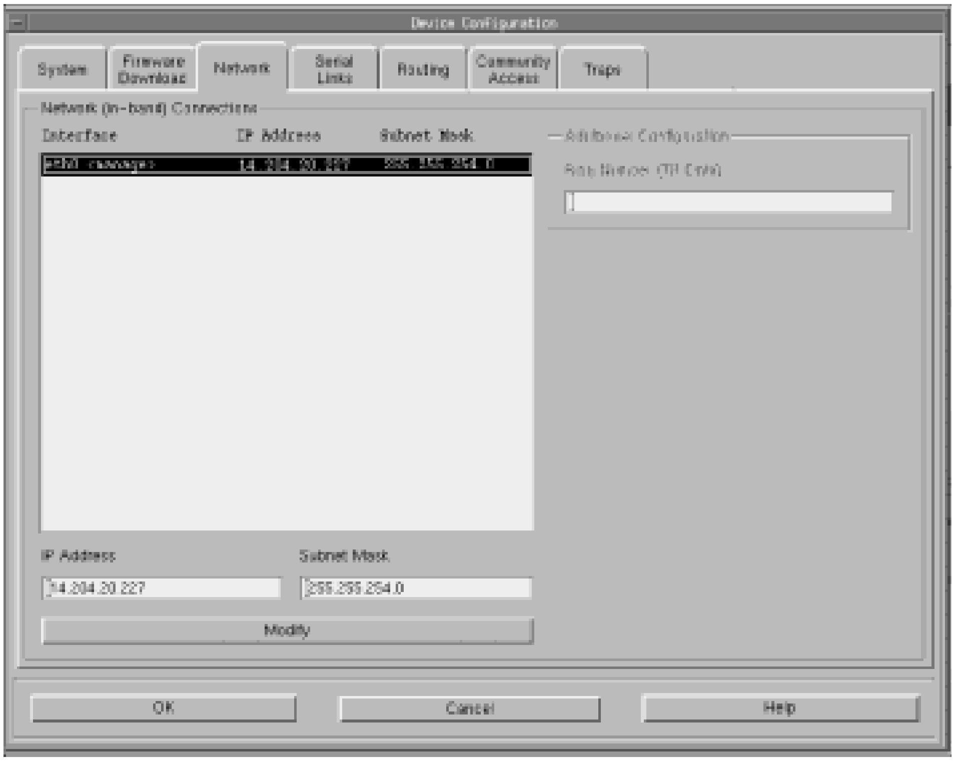
On multi-interface devices, you can set an IP address and subnet mask for most physical interfaces, including serial interfaces.

You cannot set the IP address of an interface on a 100BASE-TX Ethernet Module which is in In-line mode, because this Module cannot be managed over an In-line interface. You must use another interface on the device for management purposes.

You cannot set an IP address on a virtual interface (refer to “Configuring Virtual Interfaces” on page 37 for a description of virtual interfaces).

Setting IP addresses for different interfaces gives you greater flexibility for communicating with a device - if one interface is inaccessible, another interface could still be accessible. If you are unsure of the IP addresses allocated to you, contact your network administrator.

Attention: Where two or more interfaces on a device are monitoring the same subnet, only one interface can have an IP address. If you wish to assign more than one IP address, each interface must be connected to and configured for a different subnet.



Interface	IP Address	Subnet Mask
8270 <manager>	14.204.20.227	255.255.254.0

Ring Number (TR Only):

IP Address: 14.204.20.227

Subnet Mask: 255.255.254.0

Figure 9. Network Tab

To set the IP address and subnet mask, follow these steps:

1. Select the required interface.
2. In the IP Address field, enter the IP address for the device or for the selected interface on the device.
3. In the Subnet Mask field, enter the correct subnet mask for the class of IP address.
4. To apply the new values, click **Modify**.

The new settings will come into effect on the device the next time the device is reset.

Setting the Ring Number

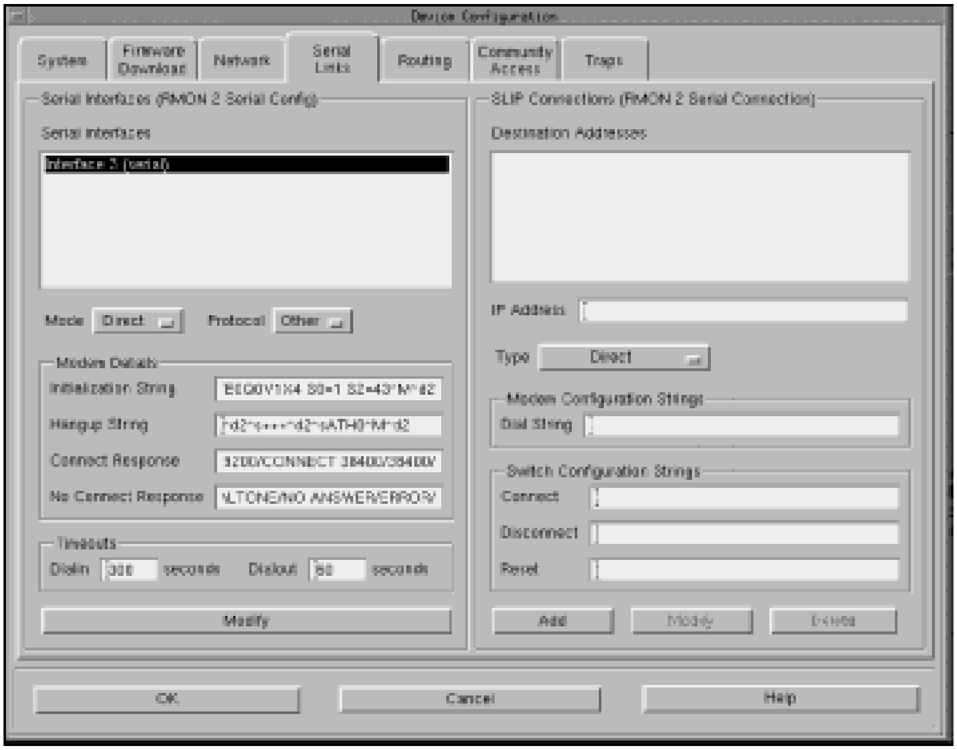
This is the ring number of your Token Ring segment where the device is located. It is used in source routing hop calculations.

Note: Some probes may not support this variable.

To set the ring number, enter the required value in the Ring Number field.

Setting Serial Link Connections

Use the Serial Links Tab (Figure 10) in the Device Configuration dialog box to set up serial link connections.


Serial Interfaces: Interface 3 (serial)

Mode: Direct

Protocol: Other

Initialization String: E0Q0V1X4 S0=1 S2=43^M^d2

Hangup String: ^d2^s+++^d2^sATH0^M^d2

Connect Response: 9200/CONNECT 38400/38400V

No Connect Response: \LTONE/NO ANSWER/ERROR/V

Dialin: 300 seconds

Dialout: 60 seconds

Type: Direct

Figure 10. Serial Links Tab

This tab consists of two separate areas:

Serial Interfaces
Allows you to configure serial interfaces on the device.

SLIP Connections
Allows you to set up SLIP connections to management stations.

Configuring Serial Interfaces

The device’s serial interface names appear in the Serial Interfaces area. This is set on the device, and cannot be modified from Nways Manager Remote Monitor.

To configure a device’s serial interfaces, follow these steps:

1. Select the mode of the serial connection. This can be set to one of the following:

Direct The device connects directly with the management station.

Modem The device requires a modem to connect to the management station.

2. Select the protocol to be used on the serial link. This may be default set to Other, or can be set to SLIP. It cannot be changed to the setting of Other.
3. Set the Modem Details. These are as follows:

Initialization String

This control string dictates how a modem attached to the serial interface should be initialized. If you have set the mode to Modem, the initialization is performed once during startup and again after each connection is terminated.

An initialization string that is appropriate for a wide variety of modems is: `ˆsˆMATE0Q0V1X4 S0=1 S2=43ˆM`

Hangup String

This control string specifies how to disconnect a modem connection on the serial interface. It is only used if the mode is set to Modem.

A hangup string that is appropriate for a wide variety of modems is: `ˆd2ˆs+++ˆd2ˆsATH0ˆMˆd2`

Connect Response

A text string containing substrings that describe the expected modem connection response code and associated bits per second ate. The substrings are delimited by the first character in the string.

A connect response string that is appropriate for a wide variety of modems is: `/CONNECT/300/CONNECT 1200/1200/CONNECT 2400/2400/CONNECT 4800/4800/CONNECT 9600/9600/CONNECT 14400/14400/CONNECT 19200/19200/CONNECT 38400/38400/`

No Connect Response

A text string containing response codes that may be generated by a modem to report the reason why a connection attempt has failed. The response codes are delimited by the first character in the string.

A no connect response string that is appropriate for a wide variety of modems is: `/NO CARRIER/BUSY/NO DIALTONE/NO ANSWER/ERROR/`

4. Set the Timeouts for the serial link connections.

Dialin Timeout
The dialin timeout is the length of time that incoming connections can be idle. After this time, the device will drop the connection.

Dialout Timeout
The dialout timeout is the length of time that outgoing connections can be idle. After this time, the device will drop the connection.

You may want to adjust the timeouts according to the type of link you are using. For example, if you are using a toll-free number, you may want to set high timeout values.

Configuring SLIP Connections

This area allows you to configure the device to set up SLIP connections to management stations.

Adding a SLIP Connection

To enable the device to make a SLIP connection to a management station, follow these steps:

1. Enter the IP address of the station to which the connection should be made.
2. Select the connection type you require from the following:

   Direct The connection does not require either a modem or a switch.

   Modem There is a modem between the device and the management station.

   Switch There is a switch between the device and the management station.

   Modem and Switch
   The connection requires both a modem and a switch.

   Depending on the connection type, certain fields are greyed out. You must fill in the appropriate information.
3. If you have chosen a Modem or Modem and Switch connection type you must set the dial string. This is a control string which specifies how to dial the phone number to establish a modem connection. The string should include the number's prefix and suffix.
4. If you have chosen a Switch or Modem and Switch connection type you must do the following:
   a. Set the connect string. This is a control string which specifies how to establish a data switch connection.
   b. Set the disconnect string. This is a control string which specifies how to terminate a data switch connection.
   c. Set the reset string. This is a control string which specifies how to reset a data switch in the event of a timeout.
5. Click **Add** to add the entry.

Modifying a SLIP Connection

To modify an existing SLIP connection, follow these steps:

1. Select a SLIP interface name from the list.
2. Make changes to the existing interface name as necessary.

3. Click **Modify**.

Deleting a SLIP Connection

To delete an existing SLIP connection, follow these steps:

1. Select the required SLIP destination IP address from the list.
2. Click **Delete**.

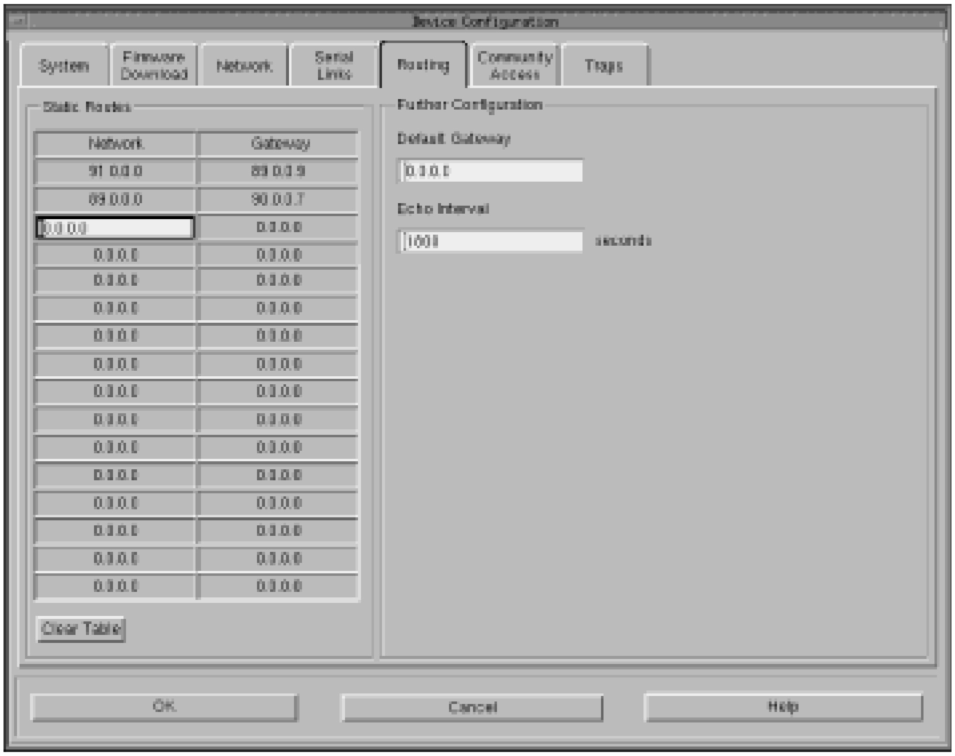
Setting Static Routes, the Default Gateway, and Echo Interval

Use the Routing Tab (Figure 11 on page 30) in the Device Configuration dialog box to set the default gateway and echo interval.

Setting Static Routes

Static routes are used to set up specific routes that the device should use to reach other networks, overriding the default gateway.

Use the Routing Tab (Figure 11 on page 30) in the Device Administration dialog box to set up static routes.



Static Routes

Network	Gateway
91.0.0.0	89.0.0.9
89.0.0.0	90.0.0.7
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0

Futher Configuration

Default Gateway: 0.0.0.0

Echo Interval: 1000 seconds

Figure 11. Routing Tab

The parameters are as follows:

Network The IP address of the destination network, for example 91.0.0.0.

Gateway The address of the router to which the packets should be sent, for example 89.0.0.9. This router must be on the same segment as the device.

1. To clear all static route entries in the table, click **Clear Table**. This will set all entries back to 0.0.0.0.
2. Click a field and edit the values as appropriate.
3. Your changes take effect once the device has been reset. Refer to “Setting System Parameters” on page 19 for details of how to reset a device from Nways Manager Remote Monitor.

Setting the Default Gateway

To set the default gateway, enter the IP address for the router or gateway in the Default Gateway field.

Setting the Echo Interval

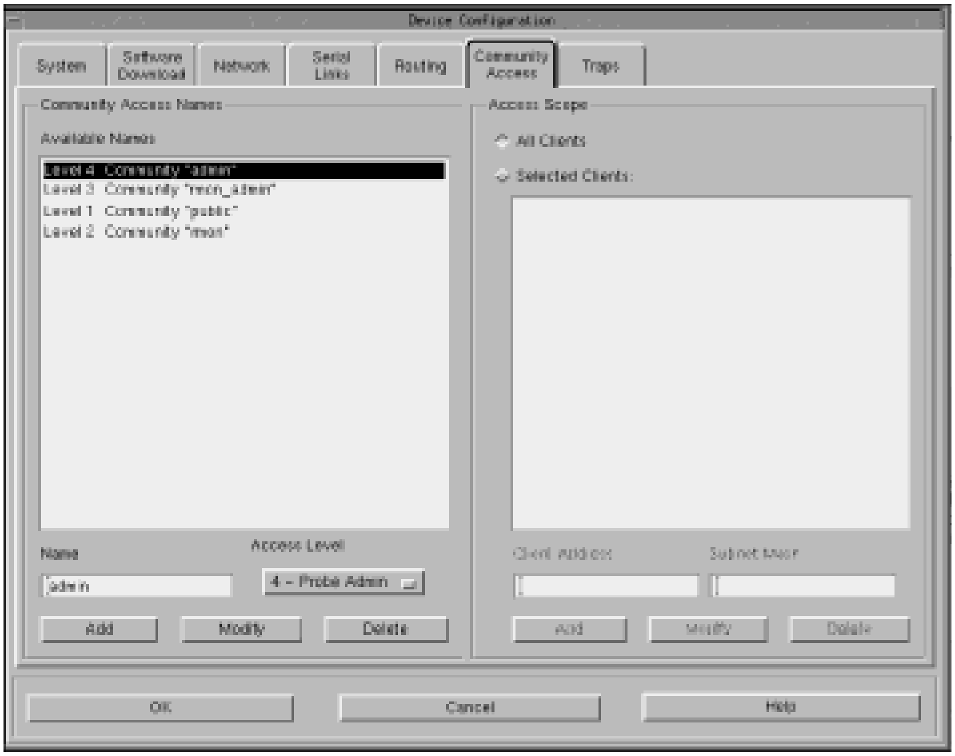
Devices can be set up to send a ping message to the default gateway periodically to maintain a route between your device and the management station. If your router requires a shorter interval between ping messages to keep the device in its routing tables, you may need to change the echo interval.

To set the echo interval, enter the ping interval in seconds in the Echo Interval field. The default value is 1800 seconds. The maximum value is 3600 seconds (1 hour).

Access Control Tables

The Community Access Tab (Figure 12 on page 32) lets you set community names with different security levels and then assign these names to specific end user workstations. This lets you limit access to a device's MIB to a selected set or ″community″ of management stations. By using more than one community, the device can provide different levels of access to different management stations.

Attention: A cold restart results in the loss of user-defined protocol information and community names.



Level 4 Community "admin"
Level 3 Community "mon_admin"
Level 1 Community "public"
Level 2 Community "mon"

Name: admin

Access Level: 4 – Probe Admin

Figure 12. Community Access Tab

Note: Any changes you make in the Community Access Tab will take effect immediately on the device being configured.

The tab is split into two sections:

- The Community Access Names area contains a list of the community names with their associated access levels (see Table 10 on page 33).
- The Access Scope area lists the stations that can use each community name in the Community Access Table.

Setting Up Community Names

To create a new community name with a specific security level, follow these steps:

1. Type a new entry in the Name field. The name must be unique.
2. Set the security level by clicking **Access Level** and selecting the appropriate level from the drop-down menu (see Table 10 on page 33).

Table 10. Security Access Levels

Level	Description
1	Read access to MIB-II objects (SNMP MIB)
2	Read access to MIB-II, RMON and RMON2 MIB and Configuration MIB objects, excluding the Access Control group and Capture Buffer table.
3	Read access to MIB-II, RMON and RMON2 MIB and Configuration MIB objects, excluding the Access Control group. Write access to RMON and RMON2 MIB and Configuration MIB objects, excluding Device Configuration, Interface and Access Control groups.
4	Read and write access to all MIB-II, RMON and RMON2 MIB and Configuration MIB objects.

3. Click **Add** to create the entry. By default, Nways Manager Remote Monitor allows all clients to use the new access name.

To change the settings for an existing community access entry, follow these steps:

1. Select an entry in the Community Access Table. The current settings are displayed in the Level and Community Name fields.
2. Change the name or security level as described above, then click **Modify** to apply the change.

To delete an existing community access entry, follow these steps:

1. Select the entry in the Table.
2. Click **Delete**.

Assigning Security Levels to Individual Workstations

The Access Scope area lists which clients can use each security level.

When you add a new access name in the Community Access Names area, All Clients in the Access Scope area is enabled by default.

To give individual workstations permission to use a particular access name, follow these steps:

1. Click **Selected Clients** in the Access Scope area. If your workstation is using the current level 4 access name, the address of your workstation will appear automatically in the list.
2. Enter the client IP address of the workstation and subnet mask in the Client Address and Subnet Mask fields.
3. Click **Add** to create the entry.

   Note: You can add groups of clients at the same time. For example if you add a Client Address of 89.56.45.0, and a Subnet Mask of 255.255.255.0, this means that all clients on the 89.56.45 network will be added to the Access Scope area.

Modifying a Client Entry

To modify a Client entry, follow these steps:

1. Select the entry in the list.
2. Change the IP Address and Subnet Mask values as required.
3. Click **Modify**.

Deleting a Client Entry

To delete an existing Client Table entry, follow these steps:

1. Select the entry in the list.
2. Click **Delete**.

Setting Up Trap Communities

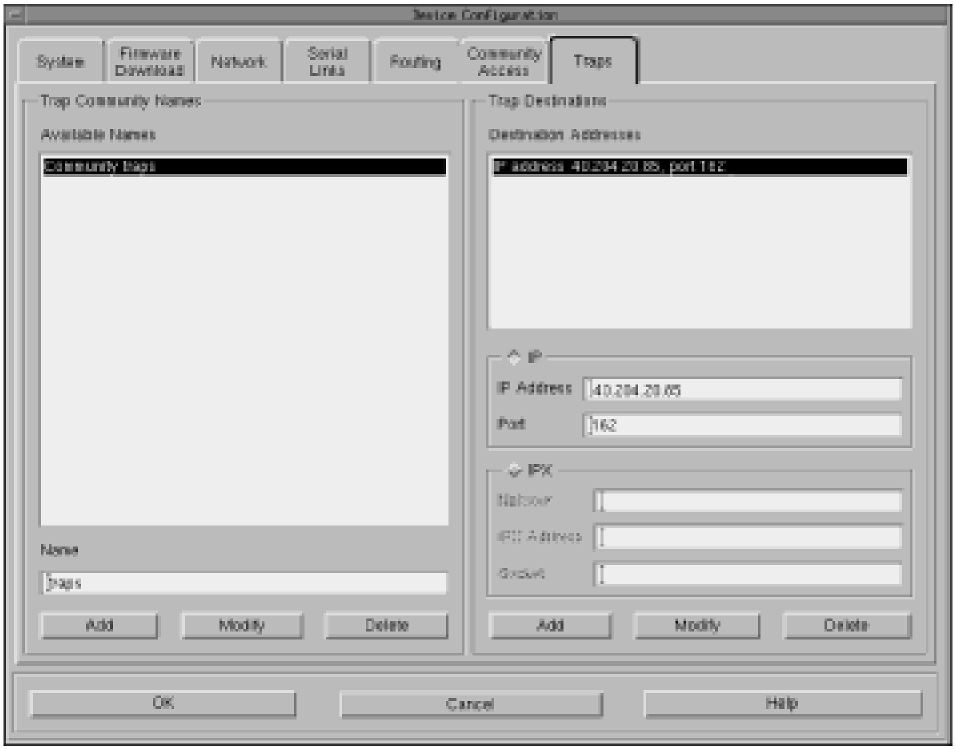
When an alarm on a device is triggered, the device can inform hosts on the network of this event by sending them an SNMP Trap packet. Not all the workstations on your network are informed of this event - only those that have previously requested to be informed. You control which workstations are informed by assigning a trap name to each alarm on a device and, for each trap name, assigning a list of workstations to be informed; the ″trap community″.

To set up trap communities, use the Traps Tab (see Figure 13 on page 35) in the Device Configuration dialog box.

There are two ways to assign trap communities:

- Nways Manager Remote Monitor will assign automatically the default traps community name to any new alarm you create. It checks that this community exists on any device it contacts and will also add the information for the workstation on which Nways Manager Remote Monitor is being run to the traps community.
- By typing a different community name in the Trap Destination Community Name field in the Alarm Entry Creation dialog box and editing the list of destination IP addresses, you can control precisely which workstations on your network receive alarm events from the device.

Note: Assigning trap communities to an alarm is described in “Configuring Alarms” on page 93.



Trap Community Names

Available Names: Community traps

Name: traps

Trap Destinations

Destination Addresses: IP address 40.204.20.65, port 162

◇ IP

IP Address: 40.204.20.65

Port: 162

◇ IPX

Network:

IPX Address:

Socket:

Figure 13. Traps Tab

Setting Up Trap Community Names

Adding Trap Community Names

To add a trap community name, follow these steps:

1. Type a unique name in the Name field.
2. Click **Add**. The name appears in the Available Names area.

Modifying Trap Community Names

To modify a community name, follow these steps:

1. Select the entry you wish to change. The name will appear in the Name field.
2. Edit this field as required.
3. Click **Modify** to apply the change.

Deleting Trap Community Names

To delete a community, follow these steps:

1. Select the entry to be deleted.
2. Click **Delete**.

Changing Trap Destinations

To change the list of destination workstations assigned to a trap community, select the community in the Available Names area. A list of destinations assigned to this community is displayed in the Destination Addresses list. The details shown for each destination depend on whether RMON2 is enabled on the device.

RMON2 Enabled

The destination address can be either an IP or an IPX address. The details displayed are as follows:

- For IP:
  - The IP address of the destination workstation.
  - The port number to connect to. This will usually be port 162 (SNMP Traps)
- For IPX:
  - The Network address of the destination workstation
  - The IPX address of the destination workstation
  - The socket number to connect to.

Note: Some devices may not support trap destinations with IPX addresses. For such devices, you should specify trap destinations with IP addresses only.

RMON2 Disabled

Note: You cannot configure trap destinations on some devices when RMON2 is disabled.

Each trap destination entry specifies a primary destination and an optional alternate destination in case the primary destination cannot be contacted. The details displayed are as follows:

- IP address of the primary destination

  Interface on the device through which the primary destination can be reached
- IP address of the alternate destination (optional)

  Interface on the device through which the alternate destination can be reached (optional)

Adding Trap Destinations

To add a destination workstation to the list, enter the address details and click **Add**.

Modifying and Deleting Trap Destinations

To modify the details for a destination workstation, select the entry in the Destination Addresses list, alter the values as required and click **Modify**.

To remove a destination workstation from the Destination Addresses list, select the entry in the list and click **Delete**.

Configuring Virtual Interfaces

Physical interfaces on a device collect data for network parameters, such as total packets, total errors, and so on. The Capture Application filters specific types of packet from the network for closer examination.

Virtual interfaces combine these functions to filter the data seen on the physical interface according to your filter specifications. For example, you could configure a virtual interface to filter statistics on WWW traffic only. Statistics gathered by a virtual interface are stored in standard RMON and RMON2 tables on the device.

Virtual interfaces cannot have the following RMON and RMON2 tables configured:

- Address map
- Protocol directory
- Token Ring station
- Token Ring source routing statistics

Note: Virtual interfaces are supported by devices in IBM’s 8238 and 8260 HETMAC. They may also be supported by other vendors’ devices (refer to the device vendor’s documentation for more information).

Creating Virtual Interfaces

To create a virtual interface, you must specify the device and the physical interface it should be attached to and the channel to be used.

1. In the Device Administration dialog box, select a device in the Devices list.
2. Click **Virtual Interfaces** to open the Add Virtual Interface Editor dialog box, shown in Figure 14 on page 38.

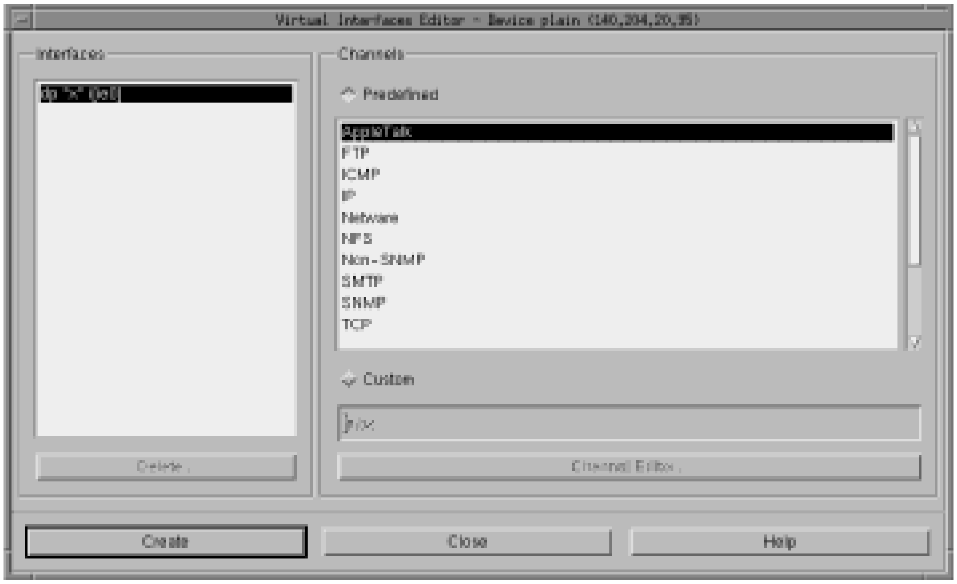


Figure 14. Virtual Interfaces Editor Dialog Box

This dialog box is divided into the following areas:

Interfaces
The physical interface to which the virtual interface should be attached.

Channels
A channel contains the specifications for filtering data. Use a predefined channel, according to the media type of the selected physical interface, or create your own custom channel.

3. Select a physical interface on the device from the Interfaces area.
4. Select a predefined channel, create your own custom channel or load a saved custom channel. For further information, refer to “Selecting a Predefined Channel” on page 38, and “Loading a Custom Channel” on page 41.
5. To create the virtual interface, click **OK**. You are returned to the Device Administration dialog box where the new virtual interface is displayed in the Interfaces area. The virtual interface appears as the name of the attached physical interface, followed by the channel description of the virtual interface in round brackets. For example:

```
ie0 (IP Source 89.0.0.2).
```

Note: For information on adding RMON and RMON2 tables to virtual interfaces, refer to Table 7 on page 19 and Table 8 on page 20.

Selecting a Predefined Channel

To select a predefined channel, activate Predefined, then select an entry in the list.

The list of predefined channels varies according to the media type of the selected physical interface.

Table 11. Predefined Channels

Channel	Description	Physical Interface Media Type		
		Ethernet	Token Ring	FDDI
AppleTalk	Pass AppleTalk packets only	■	■	■
FTP	Pass FTP packets only	■	■	■
ICMP	Pass ICMP packets only	■	■	■
IP	Pass IP packets only	■	■	■
LLC Frames	Pass LLC packets only		■	
MAC Frames	Pass MAC packets only		■	
Netware	Pass Netware packets only	■	■	■
NFS	Pass NFS packets only	■	■	■
Non-SNMP	Pass all packets except SNMP	■	■	■
SMTP	Pass SMTP packets only	■	■	■
SNMP	Pass SNMP packets only	■	■	■
TCP	Pass TCP packets	■	■	■
Telnet	Pass Telnet packets only	■	■	■
UDP	Pass UDP packets	■	■	■
WWW	Pass WWW packets only	■	■	■
XNS	Pass XNS packets only	■		
X-Windows	Pass X-Windows packets only	■	■	■

Creating your own Custom Channel

1. To create a custom channel, activate **Custom**.
2. Click **Channel Editor...** to open the Channel Editor dialog box, shown in Figure 15 on page 40.

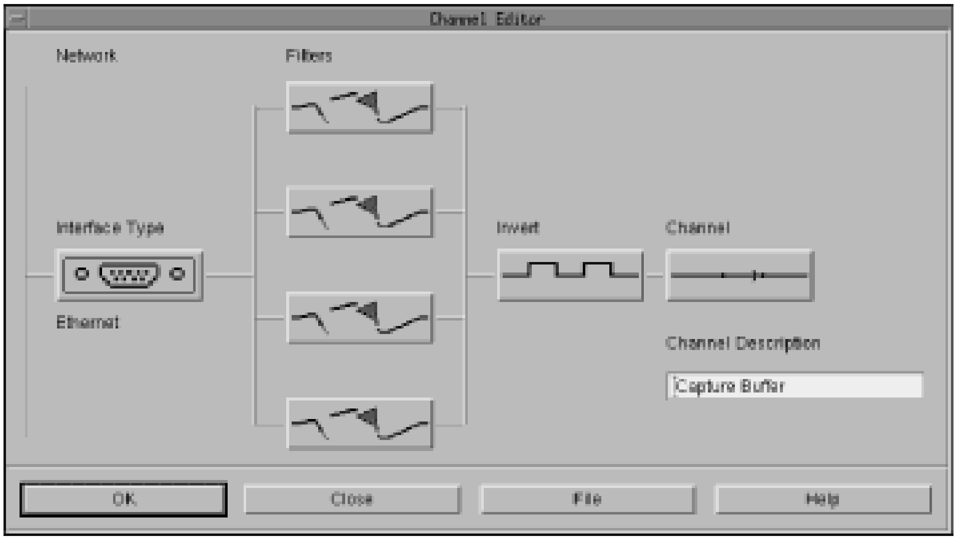
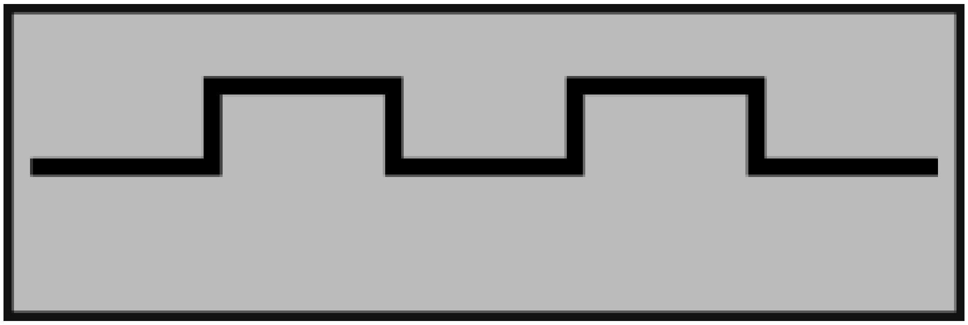


Figure 15. Channel Editor Dialog Box

Note: The Interface Type is set automatically to the media type of the original physical interface and cannot be modified.

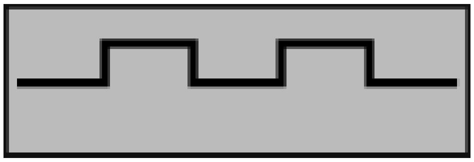
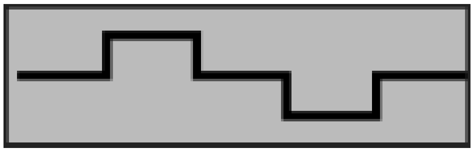
3. To set up a filter, click one of the Filter buttons to open the Filter Editor dialog box. You can set additional filters by clicking the other filter buttons in turn. Setting up a filter is described in “Using the Filter Editor” on page 111. Click **OK** to return to the Channel Editor.

4. The



Invert button lets you invert the logic of the filter:

Table 12. Invert Button

Invert Button	Description
	Pass the specified packets
	Pass Everything except the specified packets

5. Enter a unique name for the channel in the Channel Description field.

   You can save a channel to file so that it can be reloaded onto another interface at a later date. Click **File** to open the File Save/Load dialog box.

   a. Click **Save**.

   b. Enter a filename for this channel in the Selection field.

   c. Click **OK** to save the file and return to the Channel Editor dialog box.

6. To create this Channel, click **OK**. You are returned to the Virtual Interface Editor dialog box. The channel name is displayed in the Custom field.

Loading a Custom Channel

This lets you load a custom channel previously saved with the Channel Editor or extract the channel information from saved capture buffers created with the Capture Application. Using a saved Capture Application capture buffer lets you create a virtual interface with the same profile as your packet capture.

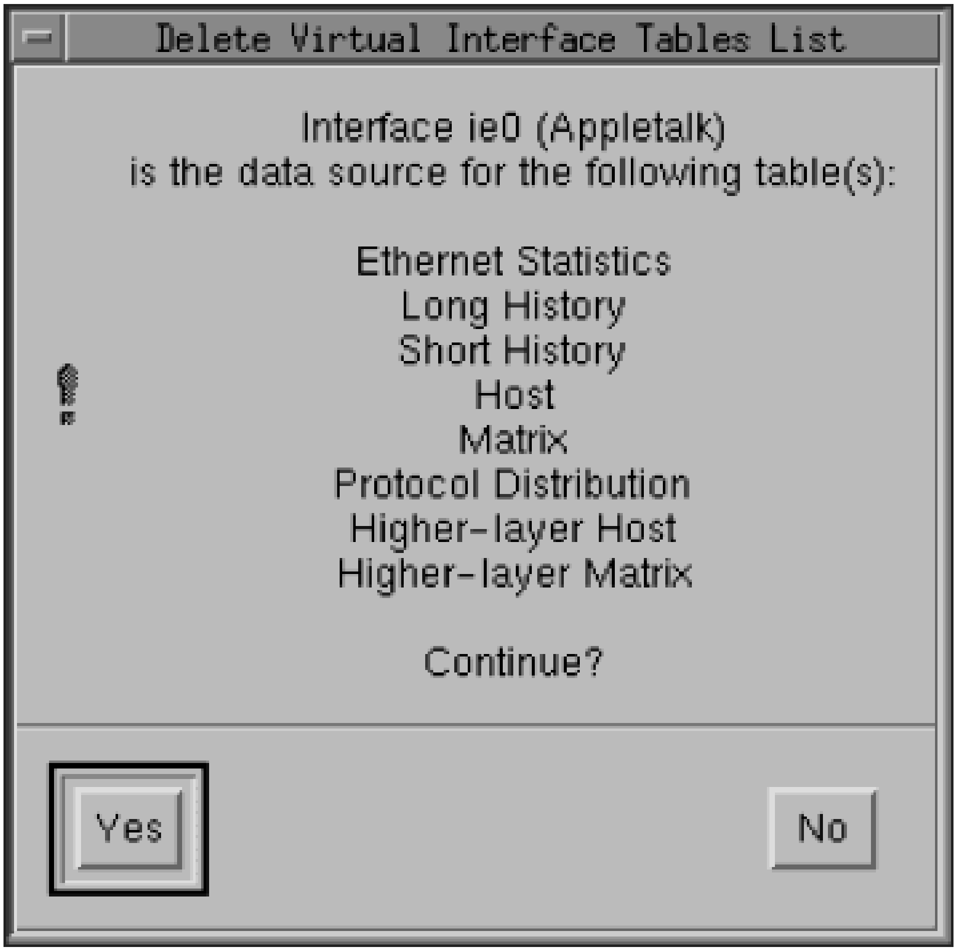
1. Click **Custom**.
2. Click **Channel Editor...** to open the Channel Editor.
3. Click **File** to open the File Save/Load dialog box.
4. Click **Load**.
5. Locate and select the channel file.
6. Click **OK** to load this file and return to the Channel Editor dialog box where the channel configuration details are displayed.
7. Click **OK** in the Channel Editor dialog box to create this custom channel and return to the Virtual Interface Editor dialog box.

Deleting Virtual Interfaces

Deletion of virtual interfaces is carried out from the Virtual Interfaces dialog box.

1. Select the virtual interface to be deleted in the Interfaces list.
2. Click **Delete**.

3. The Delete Virtual Interface Tables List dialog box appears, as shown in Figure 16. It asks you if you want to delete the virtual interface and its associated tables.



Delete Virtual Interface Tables List

Interface ie0 (Appletalk)
is the data source for the following table(s):

Ethernet Statistics
Long History
Short History
Host
Matrix
Protocol Distribution
Higher-layer Host
Higher-layer Matrix

Continue?

Figure 16. Delete Virtual Interface Tables List Dialog Box

Note: If the virtual interface is a shared resource, ensure that other users do not need access to it before you delete it.

4. Click **Yes** to confirm or **No** to return to the Virtual Interfaces dialog box.

Setting the Address Translation Level

The address translation level specifies the format Nways Manager Remote Monitor uses to name stations in the main window and in all its station-related views. If you change this setting, the changes will be made throughout all open Views and dialog boxes at the next update.

Nways Manager Remote Monitor always tries to display the highest level you have requested (see Table 13 on page 45). If this is not available, it uses the highest level name it can. As a result, you may see a mixture of different name levels in the graphs in the main window.

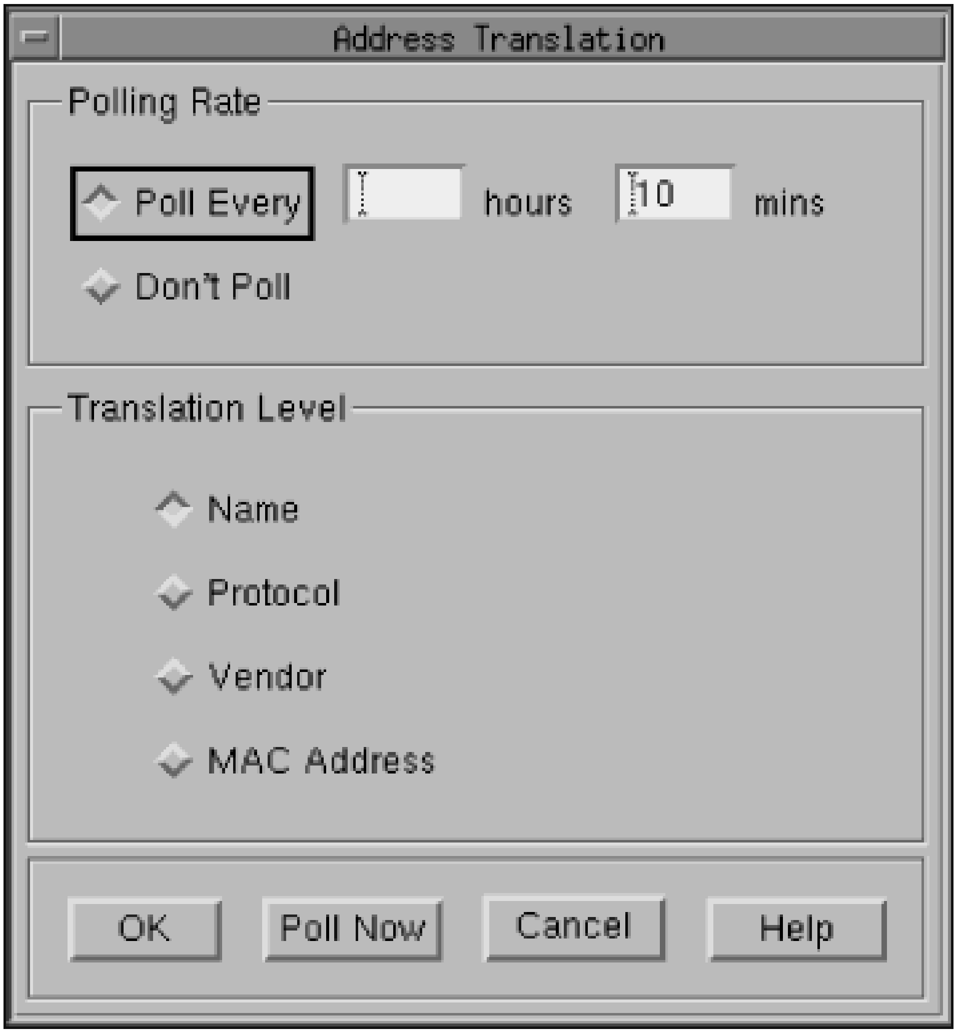
You can also set the frequency with which Nways Manager Remote Monitor uploads address translation information.

This feature also lets you control Nways Manager Remote Monitor's access to your system name service, such as NIS, /etc/hosts or DNS. The device can build a table of mappings from MAC address to network layer address for any packets seen. This table is then used by Nways Manager Remote Monitor to obtain any available name translations for the retrieved protocol address.

Note: Address translation information will be gathered from any devices currently being used for monitoring in the Nways Manager Remote Monitor main window.

To set the address translation level, follow these steps:

1. Select **Address Translation** from the Configure menu to open the Address Translation dialog box, shown in Figure 17 on page 44.



hours 10 mins

Figure 17. Address Translation Dialog Box

2. To set the frequency with which Nways Manager Remote Monitor should poll the network address translation information, activate one of the following:

Poll Every Activate and enter a polling frequency in hours and minutes. The default is every 10 minutes.

Don't Poll Activate to turn off polling.

You can also force Nways Manager Remote Monitor to start polling immediately by clicking **Poll Now** at the bottom of the dialog box.

Note: If Poll Now is greyed out, this means that a poll is in progress.

3. To set the level of address translation that Nways Manager Remote Monitor will attempt to display, click one of the Translation Levels.

   There are four levels available as shown in Table 13:

Table 13. Address Translation Levels

Level	Description
Name Translation	This is the name associated with the device. It may be the system name that has been found for the device or any user-defined name.
Protocol Address	The protocol address associated with the device; either IP, IPX or DECnet.
Vendor ID	The first six characters of this name are taken from the vendor ID contained in the vendor.map file, followed by the remaining six digits of the MAC address. Refer to “Specifying Vendor Prefixes” on page 49.
MAC Address	The 12-digit MAC address will be displayed.

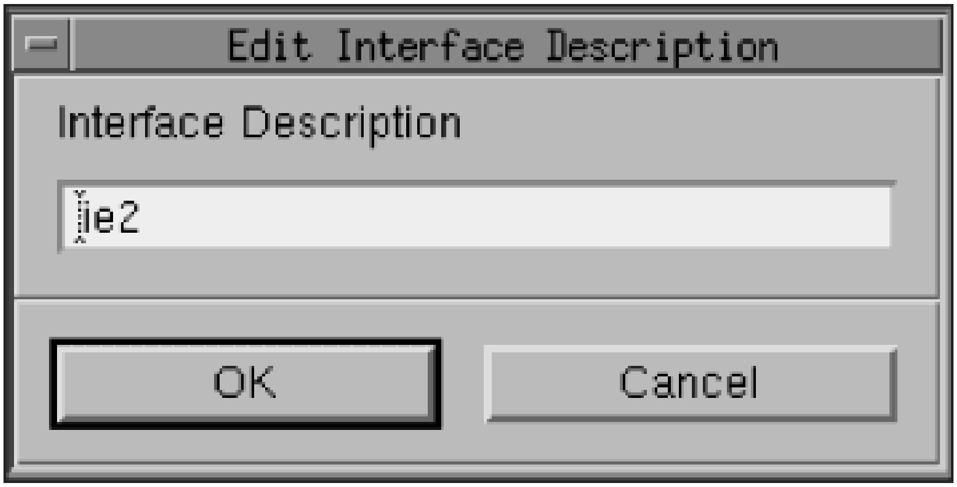
4. Click **OK** to save the settings and return to the main window.

Renaming Interfaces

If a device supports writable interface descriptions, you can change the name of the physical interfaces on that device from the Device Administration dialog box.

To change an interface description, follow these steps:

1. Select a device in the Devices list.
2. Select the physical interface whose name you want to change in the Interfaces list. If you select a virtual interface, Interface Description beneath the Interfaces list is greyed out.
3. Click **Interface Description** and the Edit Interface Description dialog box opens, as shown in Figure 18 on page 46.



ie2

Figure 18. Edit Interface Description Dialog Box

4. Edit the contents of the Interface Description field and click **OK**.
5. The new interface name is displayed in the Interfaces list. Any virtual interfaces attached to the changed physical interface are also updated, to show the new physical interface name followed by the virtual interface channel name.
6. To reset the interface name to its original description, click **Interface Description** to open the Edit Interface Description dialog box. Delete the contents of the Interface Description field and click **OK**.

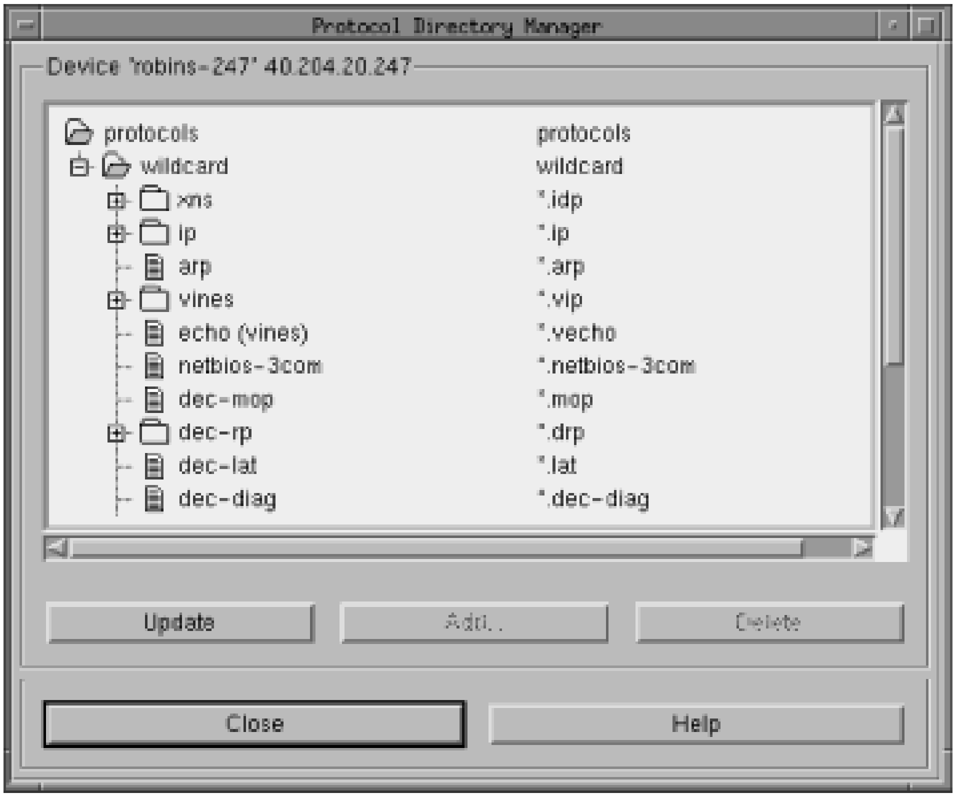
Managing User-Defined Protocols

The protocol directory forms part of the RMON2 standard, and lists all the protocols for which the device is gathering statistics. Nways Manager Remote Monitor allows you to view the protocol directory on an RMON2 device and to create or delete user-defined protocols.

If you are using customized protocols or protocol encapsulations on your network, Nways Manager Remote Monitor allows you to define these protocols and add them to your protocol directory. This enhances Nways Manager Remote Monitor’s Protocol Distribution View. For information on the protocols supported by RMON2-compliant devices, refer to Appendix D.

Viewing the Protocol Directory

Select Protocol Directory from the Configure menu in the main window to open the Protocol Directory Manager dialog box (Figure 19 on page 47).



Device 'robins-247' 40.204.20.247

protocols	protocols
wildcard	wildcard
xns	*.idp
ip	*.ip
arp	*.arp
vines	*.vip
echo (vines)	*.vecho
netbios-3com	*.netbios-3com
dec-mop	*.mop
dec-rp	*.drp
dec-lat	*.lat
dec-diag	*.dec-diag

Figure 19. Protocol Directory Manager Dialog Box

The dialog box displays all the protocols for which the device is gathering statistics.

This display consists of two columns - the first shows the protocol hierarchy, the second shows the full encapsulation path of each protocol.

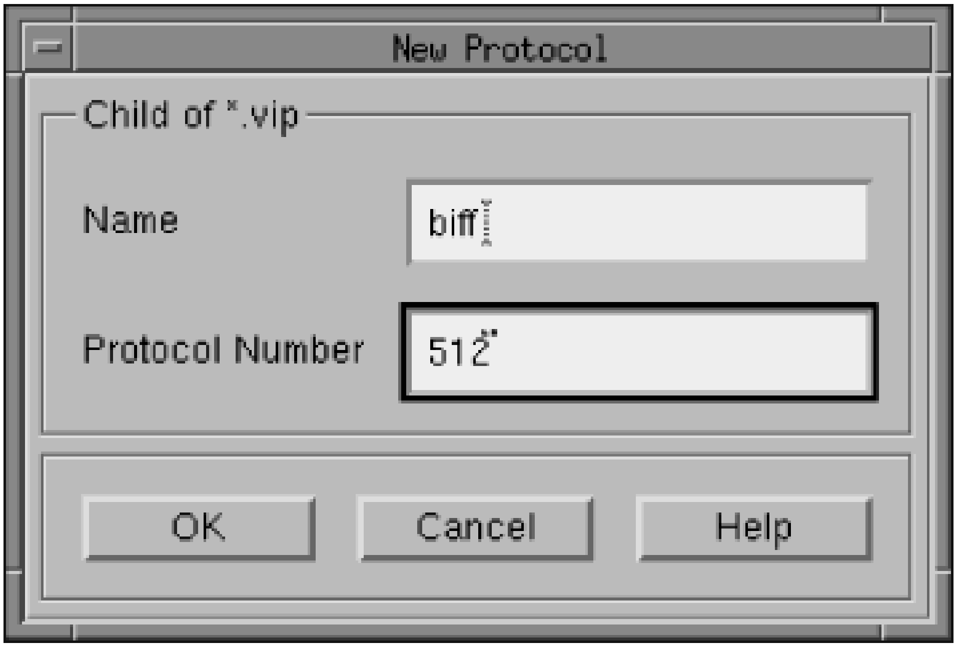
Note: If a protocol name is too long to fit in the display, it is displayed in an abbreviated form. To extend a column, click and drag the mouse at the right-hand edge of the column.

Adding a Protocol

To add a user-defined protocol, follow these steps:

1. Click **Add..** in the Protocol Directory dialog box to open the New Protocol dialog box, shown in Figure 20 on page 48.

   Note: If a protocol cannot be extended, **Add...** is disabled. Check that the device supports user-defined protocols.



Child of *.vip

Name: biff

Protocol Number: 512

Figure 20. New Protocol Dialog Box

2. Enter a name and protocol number for the protocol you want to add. If you are unable to add a protocol, this may be because:
   - The protocol you are trying to add already exists.
   - The device has run out of memory. You must delete a protocol and warm restart the device before adding another protocol.

     Note: If you cold restart the device, all user-defined protocol information is lost.
3. Click **OK** to return to the Protocol Directory Manager dialog box.

Deleting a Protocol

Nways Manager Remote Monitor allows you to delete protocols that you have added to a device. To delete a protocol, follow these steps:

1. Select the required protocol in the Protocol Directory Manager dialog box.
2. Click **Delete**. You are asked to confirm or cancel the deletion.

Specifying Vendor Prefixes

Every device has a unique MAC address. MAC addresses consist of two parts - the vendor prefix and the interface serial number. The vendor prefix consists of the first six digits of a MAC address. Each vendor is allocated a block of MAC addresses by the IEEE. The vendor then assigns a different interface serial number to each device it manufactures.

Nways Manager Remote Monitor comes with most common vendor prefixes defined. For example, it can automatically recognize a device with a MAC address 08005A000001 as an IBM device with an interface serial number 000001.

Note: The $ sign represents the interface serial number of the MAC address.

To display existing vendor prefixes, use a text editor to open the vendor.map file in the /usr/LANReMon/rmoncommon/maps directory. To add your own vendor prefix translations, edit the vendor.map file as follows:

1. Go to the end of the vendor.map file.
2. On a new line, type the vendor prefix you want to add, followed by the vendor ID. The vendor ID must be exactly six characters in length, followed by a $. If the vendor ID is shorter than six characters, use underscores to make it up to six characters. For example: 123456 myDev_$

   In this case, the number originally allocated is 123456. The vendor.map file entry means that all devices whose MAC address begins with 123456 will be displayed as myDev_ followed by the remaining six digits of the MAC address.

   Note: You must restart the application for changes to the vendor.map file to take effect.

Chapter 4. Nways Manager Remote Monitor Main Window

This chapter describes the information in Nways Manager Remote Monitor's main window. It contains the following sections:

- Overview
- Description of Nways Manager Remote Monitor Main Window
- Customizing the Main Window
- Accessing Multiple Windows
- Reading the Main Window
- Printing from Nways Manager Remote Monitor

Overview

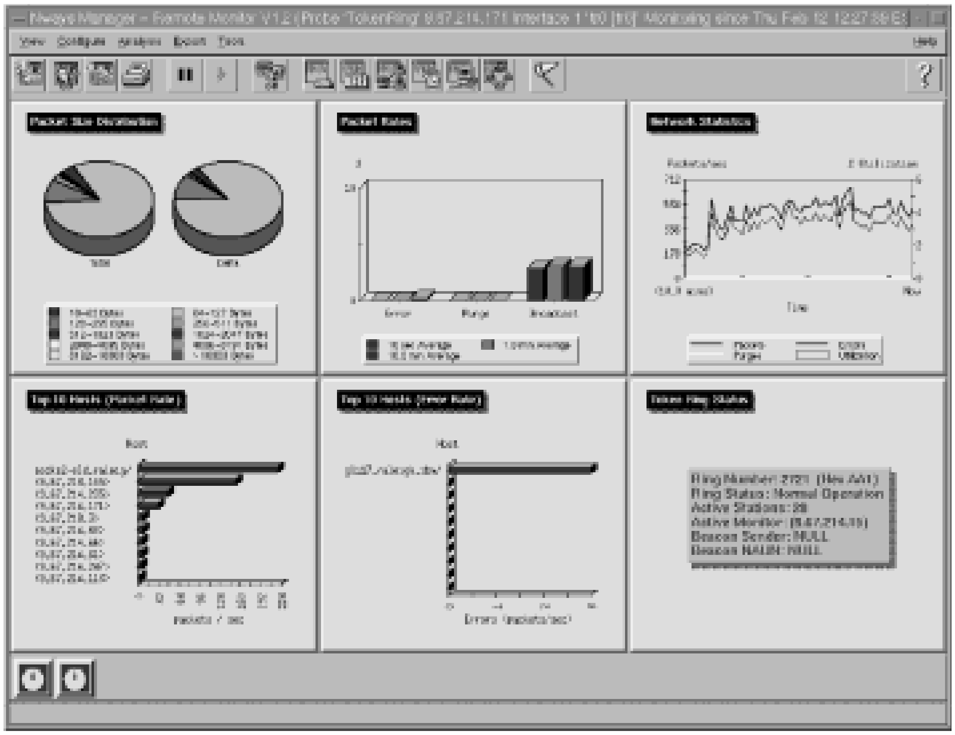
Nways Manager Remote Monitor's main window shows key error and usage information on a LAN segment. It also displays triggered alarms and status messages. By selecting a physical interface on a remote device, you can view the performance and condition of the entire monitored network segment. Selecting a virtual interface will let you view performance for a subset of network data. You can open other windows onto different segments to view multiple segments simultaneously. You can tailor the main window to your monitoring requirements by choosing to display all graphs or just a selection of them. You can also see parts of the displayed graphs in greater detail by clicking the part of the graph in which you are interested.

Description of Nways Manager Remote Monitor Main Window

Nways Manager Remote Monitor's main window allows you to monitor the performance of a network segment and also view triggered alarms, so that you can react to changing network conditions. You can open several main windows, which allows you to view several segments simultaneously.

The main window is divided into the following areas, as shown in Figure 21 on page 52:

- Menu Bar
- Toolbar
- Summary Area
- Alarm Bar
- Status Bar


Nways Manager - Remote Monitor V1.2 (Probe 'TokenRing' 9.67.214.171 Interface 1 'to0 [tr]' Monitoring since Thu Feb 12 12:27:59 E
View
Configure
Analysis
Export
Tools
Help
Packet Size Distribution
Packet Rates
Network Statistics
Top 10 Hosts (Packet Rate)
Top 10 Hosts (Error Rate)
Token Ring Status
Error
Purge
Broadcast
Time
Host
packets / sec

Ring Number: 2121 (Hex AA1)
Ring Status: Normal Operation
Active Stations: 38
Active Monitor: (9.67.214.15)
Beacon Sender: NULL
Beacon NAUN: NULL

Figure 21. Nways Manager Remote Monitor Main Window

Menu Bar

The menu bar located at the top of the window contains the following menu commands:

View This menu option deals mainly with main window parameters, and allows you to customize, pause, restart and print from the current main window.

Configure From this menu option you can access device administration, the protocol directory manager, address translation and Roving Analyzer Port functionality.

Analysis This menu option lets you access the RMON Views - Statistics, History, Host, Alarms, Matrix and Ring Station, as well as capture, address map, protocol distribution, and PACMIB functionality.

Export This menu option lets you select specific RMON statistical groups to view using the Data Export Application.

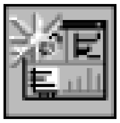
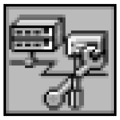
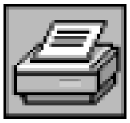
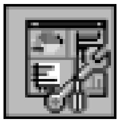
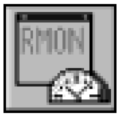
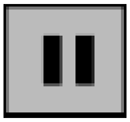
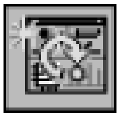
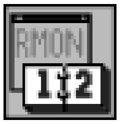
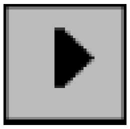
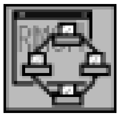
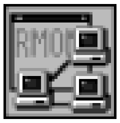
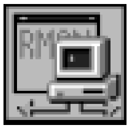
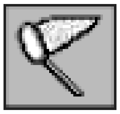
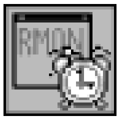
Tools This menu option allows you to access the Data Collection Application and ECAM functions.

Help This menu option provides help on Nways Manager Remote Monitor.

Tool Bar

The toolbar, located beneath the menu bar, displays a list of available Nways Manager Remote Monitor Applications and Views. Move the mouse over a button to see an on-screen description of the button. Click a button to launch the corresponding application dialog box. Table 14 explains these buttons:

Table 14. Main Window Toolbar Buttons

Button	Meaning	Button	Meaning	Button	Meaning
	New View		Device Administration		Print View
	Modify View		RMON Statistics		Pause main window
	Restart View		RMON History		Resume main window
	RMON Ring Station		RMON Host		RMON Matrix
	Capture Application		RMON Alarms		Online Help

Summary Area

The six panels of the summary area make up the largest area of the main window. These panels contain graphical displays of key network statistics and vary according to the media type of the monitored segment.

A guide to the different graphs is given in “Description of Available Graphs” on page 56.

Alarm Bar

The alarm bar is located beneath the summary area. If alarms have been configured on the monitored device, alarm icons will appear in this bar when the alarms trigger. (Alarms are described in Chapter 6.)

Status Bar

The status bar displays alarm status information and help information on toolbar and menu items. Move the mouse pointer over a toolbar button, menu item or alarm icon to view information about it in the status bar.

Customizing the Main Window

You customize the main window from the Modify Current View dialog box. From this dialog box you can select the:

1. LAN segment to be monitored.
2. Graphs to be displayed.
3. Refresh rate for displayed data.

To customize the main window, follow these steps:

1. Select **Modify** from the View menu, or click **Modify View** in the toolbar to open the Modify Current View dialog box.
2. Select the network segment to be monitored:
   a. Select a device in the Devices area. If the device is contactable, a list of available interfaces will be displayed in the Interfaces area.
   b. Select a physical or virtual interface in the Interfaces area. If you select a virtual interface, you will be monitoring the subset of data configured for that interface (refer to “Configuring Virtual Interfaces” on page 37).
3. The community name currently being used is displayed in the Community Name field. To change the community name:
   a. Click **Edit** to open the Edit Community Name dialog box, shown in Figure 22 on page 55.

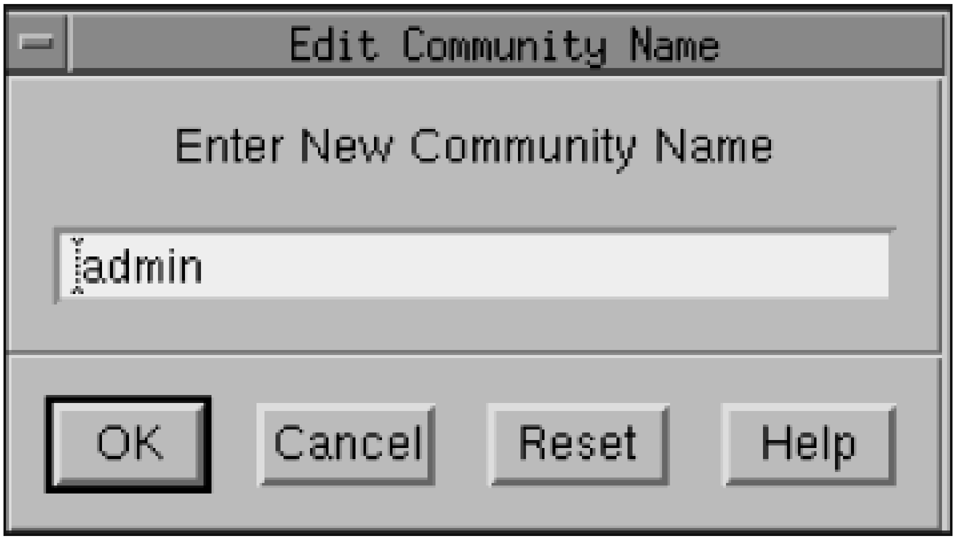


Figure 22. Edit Community Name Dialog Box

1) Type the new community name.
2) Click **OK** to save your changes and return to the Modify Current View dialog box. The new community name will be used in subsequent communication with the device.
3) If required, to revert to the default community name contained in the `probe.map` file, open the Edit Community Name dialog box and click **Reset**. Click **OK** and the community name stored on the device will be used.

4. Select the graphs and the refresh rate:
   a. Select the graphs that should be displayed in the Available Graphs area. By default all graphs are selected. The list of graphs varies according to the media type of the selected interface or device. Refer to "Description of Available Graphs" on page 56 for a definition of the available graphs.
   b. Set the rate in seconds at which the graphs should be refreshed with new data. This rate applies to all the graphs. The default value is 10 seconds.

   Click **OK** to confirm your selections. Nways Manager Remote Monitor will refresh the main window to focus on the selected network segment.

Accessing Multiple Windows

As well as customizing the active window from the Modify Current View dialog box, you can display a new window onto a different network segment. The steps are similar to those in the previous section, but you must select a different device or, for multi-interface devices, a different interface on the device.

1. Select **New** from the View menu or **New View** in the toolbar to open the Create New View dialog box.

   An asterisk (*) is appended to the device and interface name for any entries currently being used for monitoring in a main window.
2. To select the segment to be monitored, select a device in the Devices area. Then select an interface from the Interfaces area.
3. The community name currently being used is displayed in the Community field. To change the community name, follow the instructions in "Customizing the Main Window" on page 54.
4. Select the graphs and the refresh rate by following the instructions in step 4 of "Customizing the Main Window" on page 54.
5. To open a new window with the selected configuration, click **New**.

   New windows contain the same functionality as the initial main window.

Reading the Main Window

This section describes:

1. Pausing and restarting the main window.
2. The different LAN graphs that may be displayed in the main window.

Pausing the Main Window

You can temporarily pause the main window and prevent data updates from being displayed.

Note: If you have more than one main window open, only the current window is paused.

To pause the main window display, click on the toolbar or select Pause from the View menu. To restart the main window display update, click or select Restart from the View menu.

When you restart the data display update, the graphs are updated at the end of the current update period to reflect all data gathered since the pause point.

Note: Data collection continues while the main window is paused.

Description of Available Graphs

The list of graphs that are available will vary according to the media type of the selected device or, in the case of multi-interface devices, of the selected interface. Graphs are shown in Table 15 on page 57.

Table 15. Available Graphs by Media Type

List of Graphs	Media Type		
	Ethernet	**Token Ring**	**FDDI**
Packet Size Distribution	■	■	■
Packet Rates	■	■	■
Network Statistics	■	■	■
Top 10 Hosts by Packet Rate	■	■	■
Top 10 Hosts by Error Rate	■	■	
Top 10 Receivers			■
Event Distribution	■		
Token Ring Status		■	■

This section gives a definition of each graph and how it can be used to monitor your network.

Packet Size Distribution

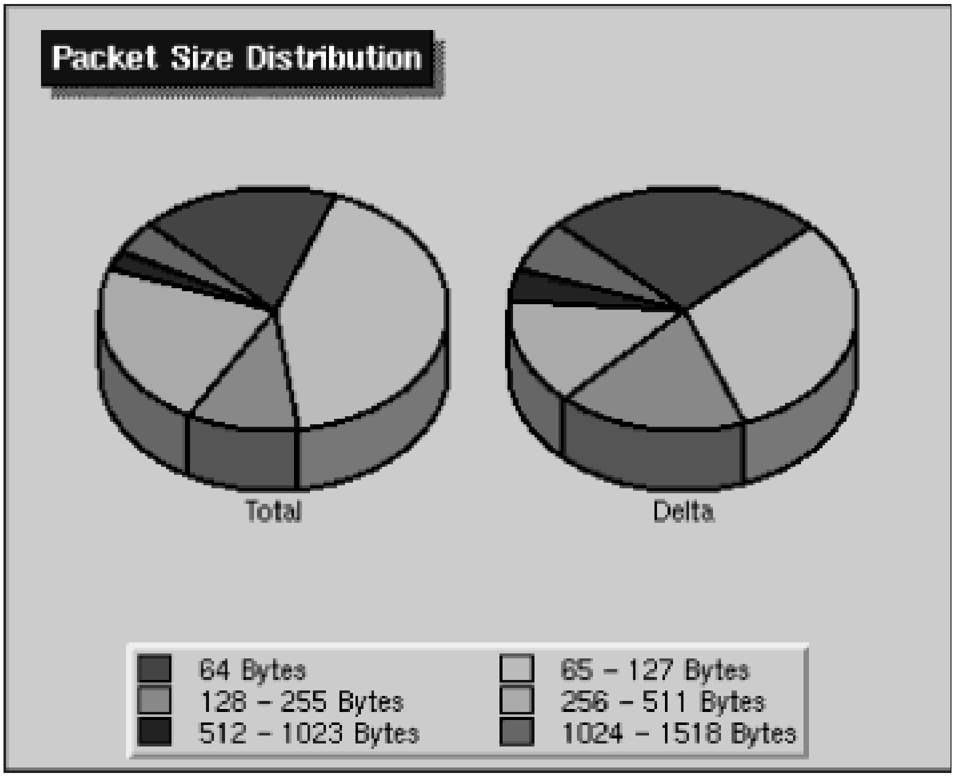


Figure 23. Packet Size Distribution Graph

The Packet Size Distribution graph Figure 23 illustrates the composition of network traffic. It shows whether the segment is transmitting lots of small packets or is saturated with large packets.

Total shows the trend of packet sizes seen since the statistics table was created. Delta displays the packet size distribution over the last sample interval.

Packet or Frame Rates

Figure 24 on page 59 shows a sample Packet Rates graph.

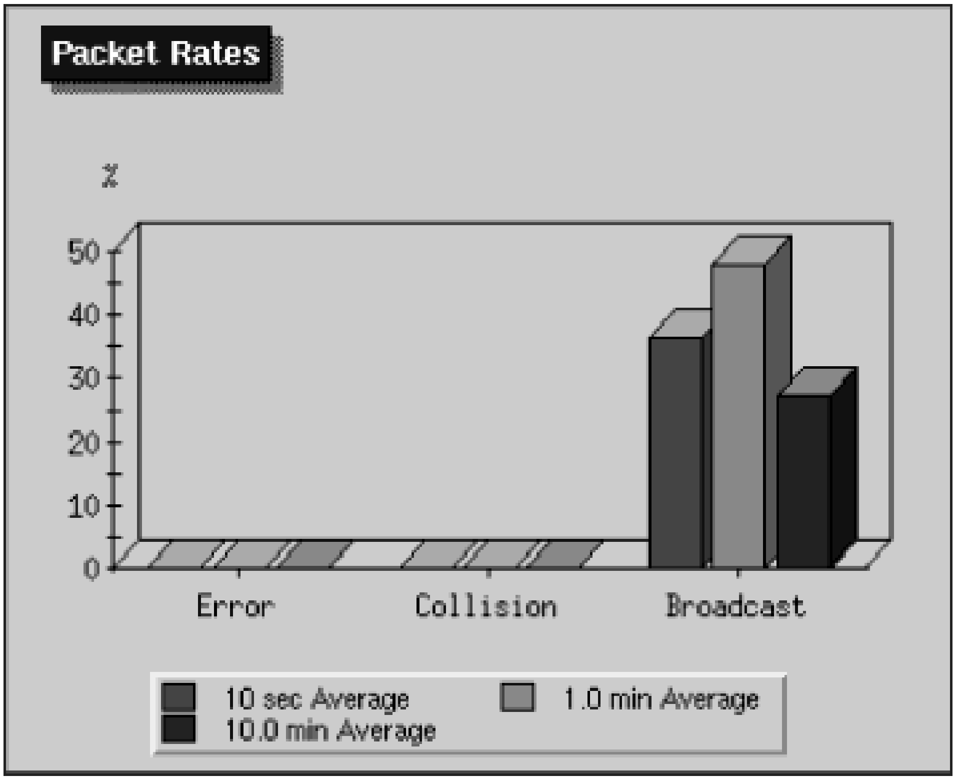


Figure 24. Packet Rates Graph

The Packet or Frame Rates graph shows how many broadcast packets, errors, collisions, purges or SMT frames (FDDI only) have been detected on the network. This allows you to quickly assess network performance. It shows both current and previous network activity.

Network Statistics

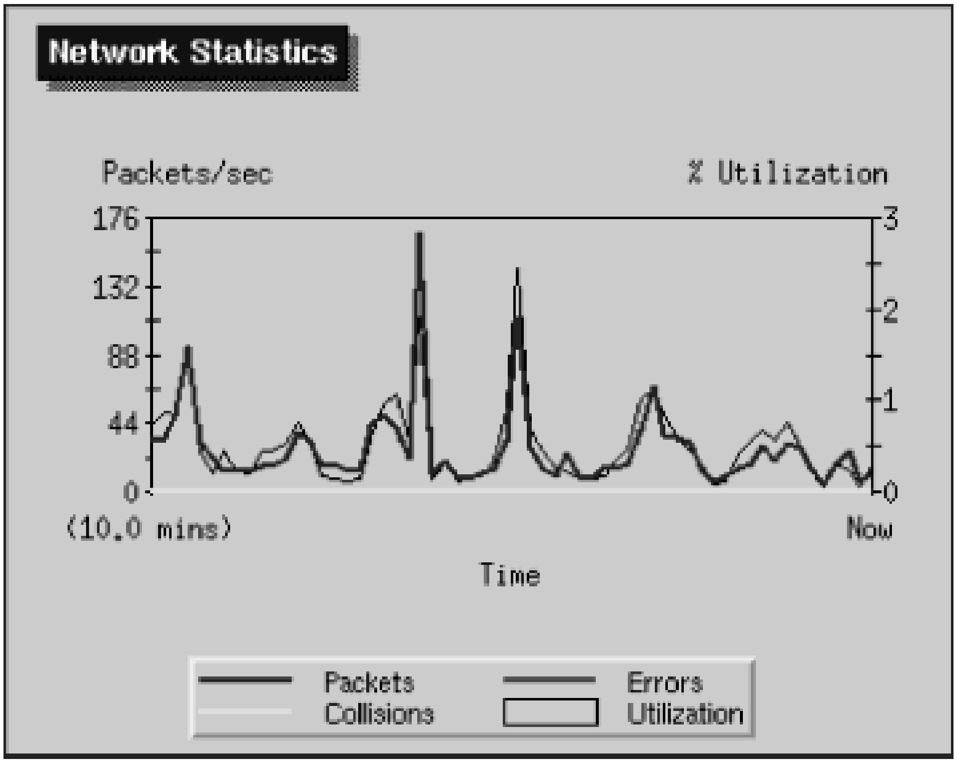


Figure 25. Network Statistics Graph

The Network Statistics Graph Figure 25 shows a network performance over the last n minutes (where n is the update rate) and allows you to determine short-term trending. By comparing the number of packets with Utilization levels, you can gain an understanding of the number of packets commonly seen on the network.Table 16 shows which network statistics are available for each media type:

Table 16. Network Statistics Graph Variables by Media Type

Variables	**Media Type**		
	Ethernet	**Token Ring**	**FDDI**
Collisions	■		
Aborts	■	■	■
Packets	■	■	■
Purges		■	
SMT Frames			■
Utilization	■	■	■

Top 10 Hosts by Packet Rate

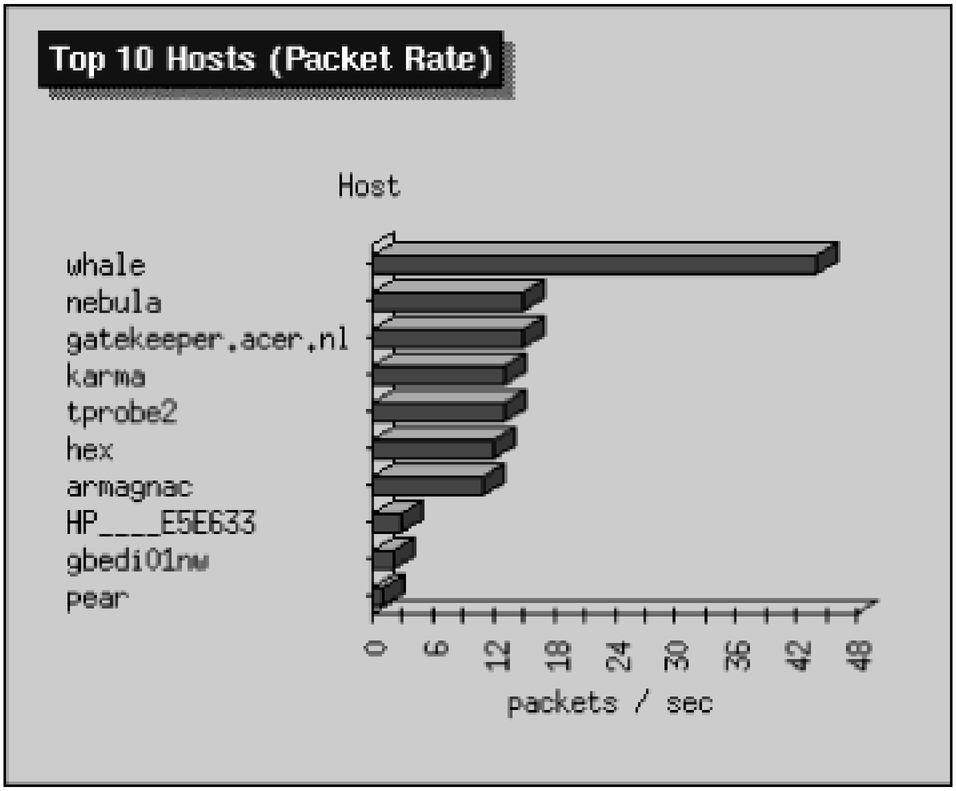


Figure 26. Top 10 hosts by Packet Rate Graph

The Top 10 Hosts by Packet Rate graph (Figure 26) identifies the busiest hosts on the segment, and shows which hosts or stations on the network are generating most traffic. It is available for Ethernet, Token Ring and FDDI.

Click the appropriate bar to display an ordered list of conversations for the host. This shows if the host is involved in high volumes of traffic with a number of stations (which may simply indicate a busy station), or with one or two devices only (which may indicate client/server activity).

Top 10 hosts by Error Rate (Ethernet and Token Ring)

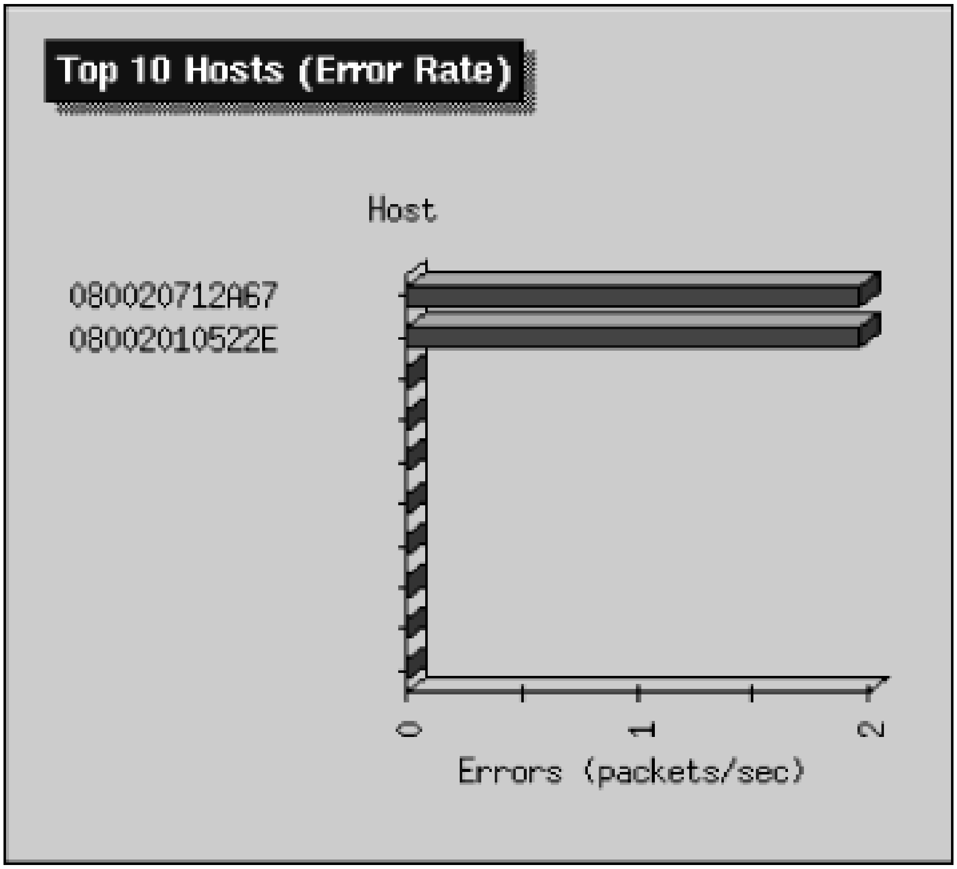


Figure 27. Top 10 Hosts by Error Rate

The Top 10 Hosts by Error Rate graph (Figure 27) shows where most error packets are coming from and to whom these stations are talking. It is available for Ethernet and Token Ring.

Click a bar on the histogram for more detailed information on the possible source of network problems.

Top 10 Receivers (FDDI)

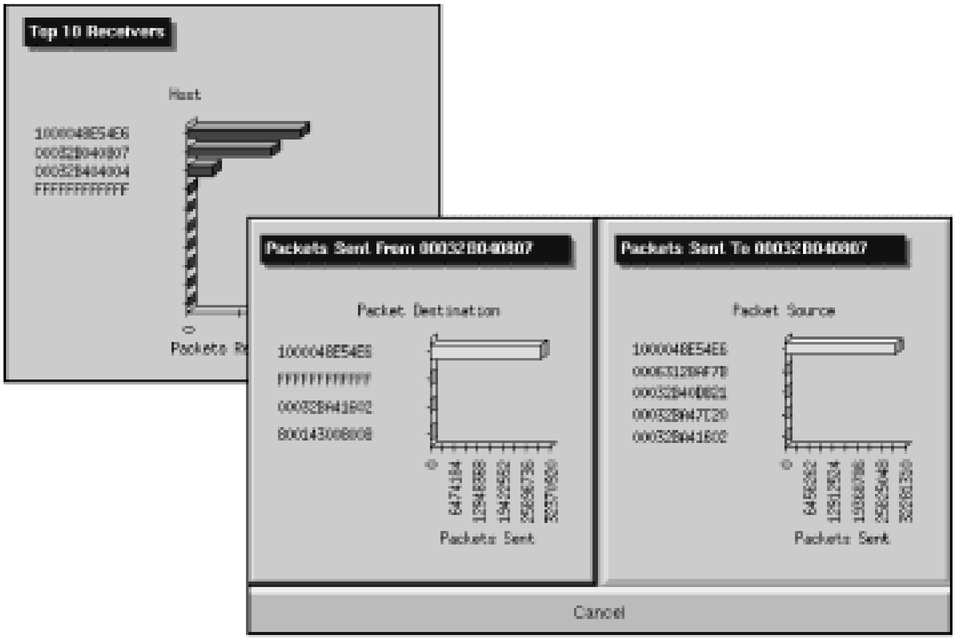


Figure 28. Top 10 Receivers

The Top 10 Receivers (Figure 28) appears for FDDI interfaces instead of the Top 10 Hosts by Error Rate graph displayed for Ethernet and Token Ring interfaces. It displays the top 10 destinations for traffic on the network.

Event Distribution (Ethernet)

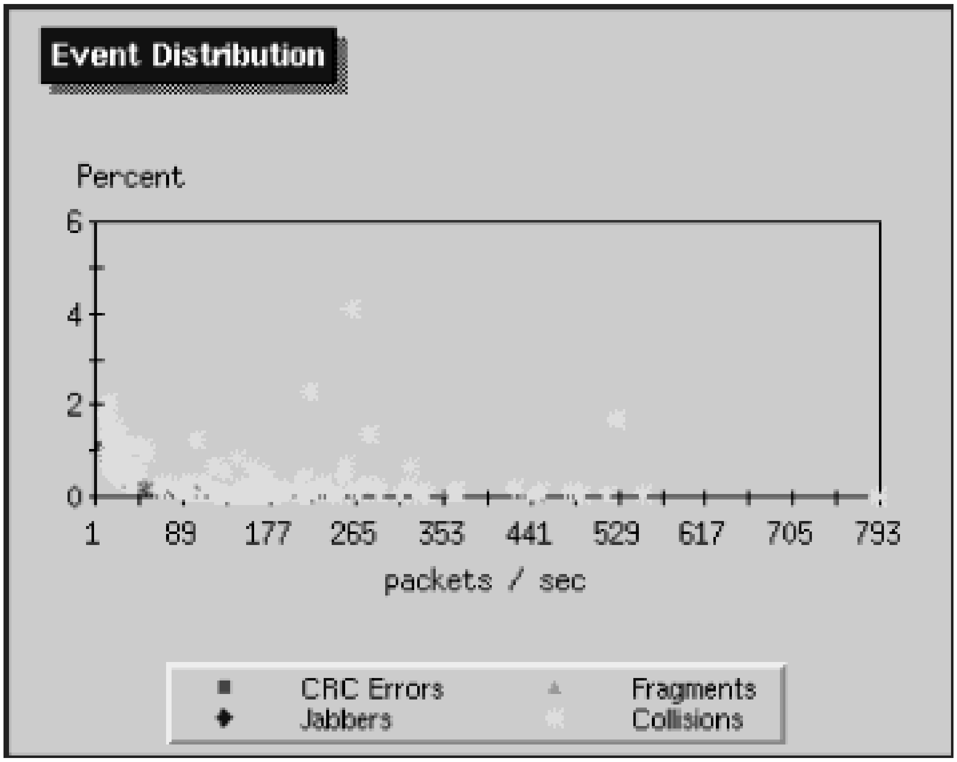
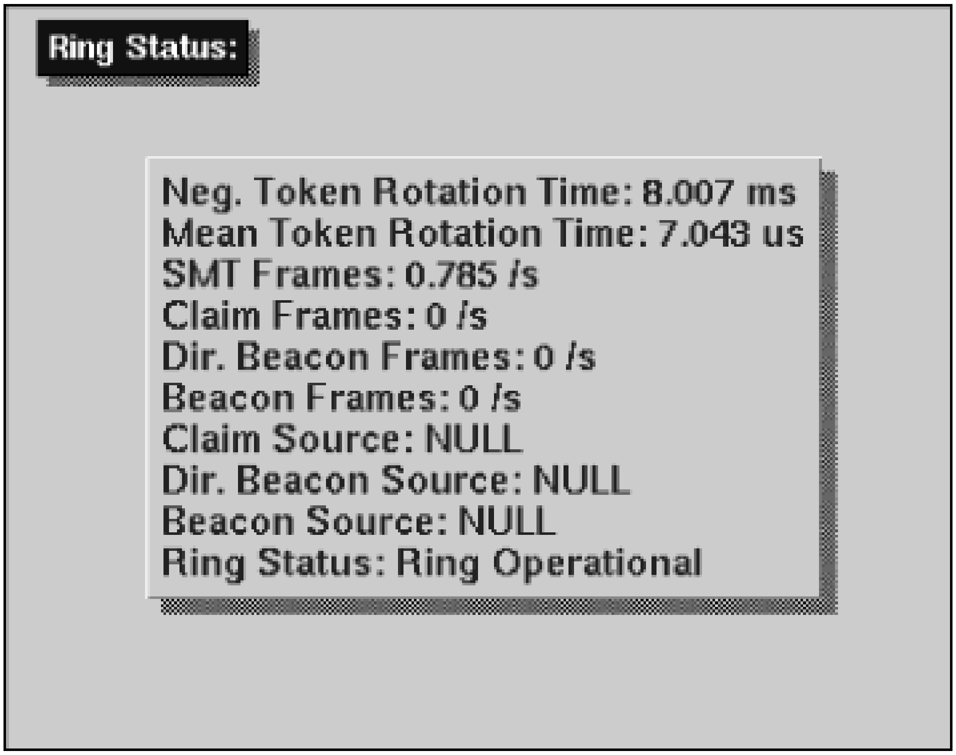


Figure 29. Event Distribution

The Event Distribution graph Figure 29 shows the relationship between packet rate and errors seen on a segment. For example, it could indicate that at 200 packets per second, 2% of all packets are collisions.

Ring Status


Ring Status:

Neg. Token Rotation Time: 8.007 ms
Mean Token Rotation Time: 7.043 us
SMT Frames: 0.785 /s
Claim Frames: 0 /s
Dir. Beacon Frames: 0 /s
Beacon Frames: 0 /s
Claim Source: NULL
Dir. Beacon Source: NULL
Beacon Source: NULL
Ring Status: Ring Operational

Figure 30. Ring Status

The Ring Status panel (Figure 30) gives a constantly updated summary of ring information for either FDDI (Table 17) or Token Ring (Table 18 on page 66).

Table 17. FDDI Variables in the Ring Status Panel

Variable	Definition
Neg. Token Rotation Time	Rotation time offered by the winner of the bidding process.
Mean Token Rotation Time	Average token rotation time in the last sample period.
SMT Frames	Rate of SMT frames seen on this ring in frames per second.
Claim Frames	Rate of claim frames seen on this ring in frames per second.
Dir. Beacon Frames	Rate of directed beacons seen on this ring in frames per second.
Beacon Frames	Rate of beacons seen on this ring in frames per second.
Claim Source	Address of the host that sent the last claim frame. This will be the host that won the bidding process. This is currently unsupported and will be displayed with a Null value.
Dir. Beacon Source	Address of the host that sent the last directed beacon.

Table 17. FDDI Variables in the Ring Status Panel (continued)

Variable	Definition
Beacon Source	Address of the host that sent the last beacon.
Ring Status	Current operational status of the FDDI ring: 1. Ring Operational 2. Non Operational Claim 3. Non Operational Beacon 4. Non Operational Directed beacon 5. Unknown

Table 18. Token Ring Variables in the Ring Status Panel

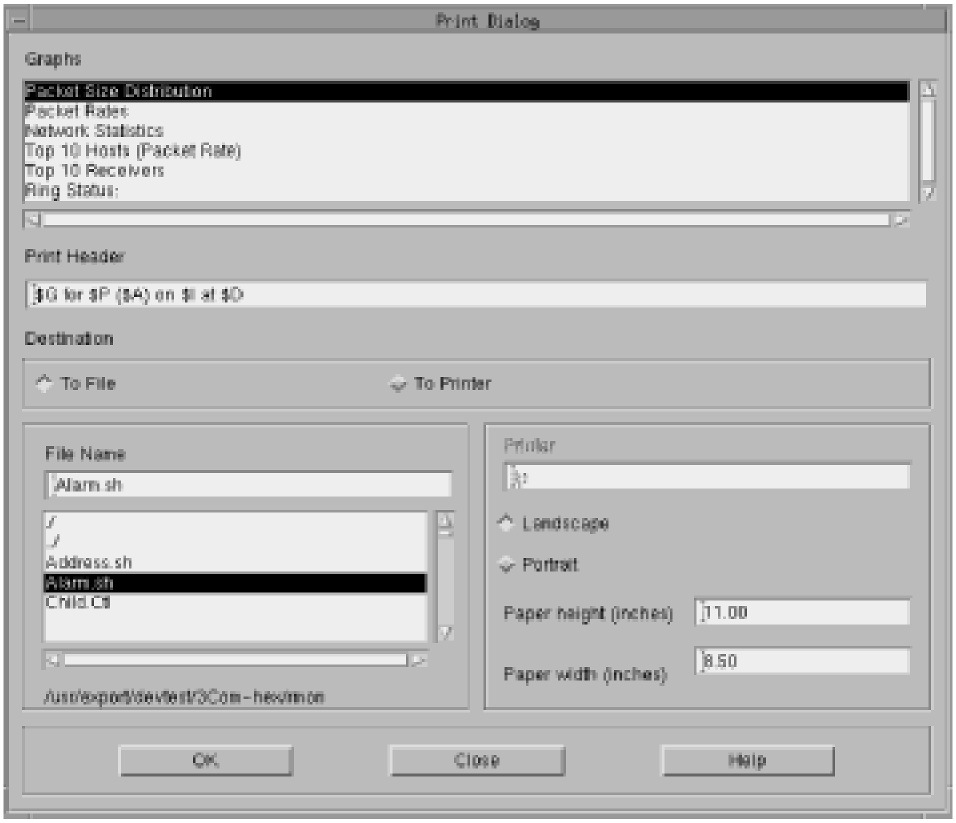
Variable	Definition
Ring Number	The ring number of this ring segment.
Ring Status	The current overall staus of the ring.
Active Stations	The number of active stations on the ring.
Active Monitor	The current Active Monitor on the ring.
Beacon Sender	The last station fo broadcast Beacon frames onto the ring.
Beacon NAUN	The last beaconing station's Nearest Active Upstream Neighbor.

Printing from Nways Manager Remote Monitor

The Print dialog box lets you print any graph, from a View or Application display or from the main window, to file or directly to your printer.

To launch the Print dialog box (Figure 31 on page 67), do one of the following:

- From the Nways Manager Remote Monitor main window, select **Print** from the View menu or click **Print View** on the toolbar.
- From a history graph display, select **Print** from the File menu.



Print Dialog

Graphs

Packet Size Distribution
Packet Rates
Network Statistics
Top 10 Hosts (Packet Rate)
Top 10 Receivers
Ring Status:

Print Header: $G for $P ($A) on $I at $D

Destination: ○ To File ◇ To Printer

File Name: Alarm.sh

./
../
Address.sh
Alarm.sh
Child.Ctl

/usr/export/devtest/3Com-hew/rmon

Printer: 3:

○ Landscape
◇ Portrait

Paper height (inches): 11.00

Paper width (inches): 8.50

Figure 31. Print Dialog Box

Note: The Graphs list does not appear if you launch the Print dialog box from a history graph display.

When printing graphs from the main window, you can select any combination of graphs from the Graphs area and specify a print header. To do this, follow these steps:

1. Select the graphs to be printed in the Graphs area. Each graph will be printed on a single page.
2. In the Print Header area, you can tailor the header to your own requirements. Enter your own combination of text and the predefined variables shown in Table 19.

   Note: If the header text exceeds the width of the page setup, it will be incomplete when printed.

Table 19. Print Header Variables

Variable	Description
$A	Device IP address

Table 19. Print Header Variables (continued)

Variable	Description
$D	Date and Time
$G	Date and Time
$I	Device interface description
$P	Device Name

3. To save the graphs to file, activate **To File** and complete the File Name area.
4. To print out the graphs, activate **To Printer**, then edit the printer name and page setup in the Printer area.
5. Click **OK** to send the report to the specified file or to the printer.

Setting Print Preferences

As you use the printing facility over time, you may find it useful to change the defaults that appear in the Print dialog box to show your most commonly used settings. For instance, you may wish to set the default header string to your own standard header, perhaps to include a company name or department title. These can be set by editing the View or Application resource file.

The following lines marked with an asterisk (*) may be edited in the X resource files named Ecam, Rmon, Viewport, and Proto contained in the `/usr/LANReMon/rmon/locale/C/app-defaults` directory:

```
!Default printer commands
*.printCommand: lpr -P
*.paperWidth: 8.5
*.paperHeight: 11.0
*.printerName: lp

! valid paper orientations are - portrait or landscape
*.paperOrientation:  landscape

! header formatting
! $G - graph name, $P - device name, $A - probe ip address,
! $D - date and time stamp
*.headerFormat: $G for $P ($A) at $D
```

Chapter 5. Using RMON Views

This chapter tells you how to use Nways Manager Remote Monitor RMON Views to collect predefined or user-defined data about your network. It contains the following sections:

- Dialog Box Format
- Editing and Creating Customized Views
- Statistical Displays
- Using the Statistics View
- Using the History View
- Using the Host View
- Using the Matrix View
- Using the Ring Station View

Dialog Box Format

Nways Manager Remote Monitor uses a standard layout for most View dialog boxes, as shown in Figure 32.

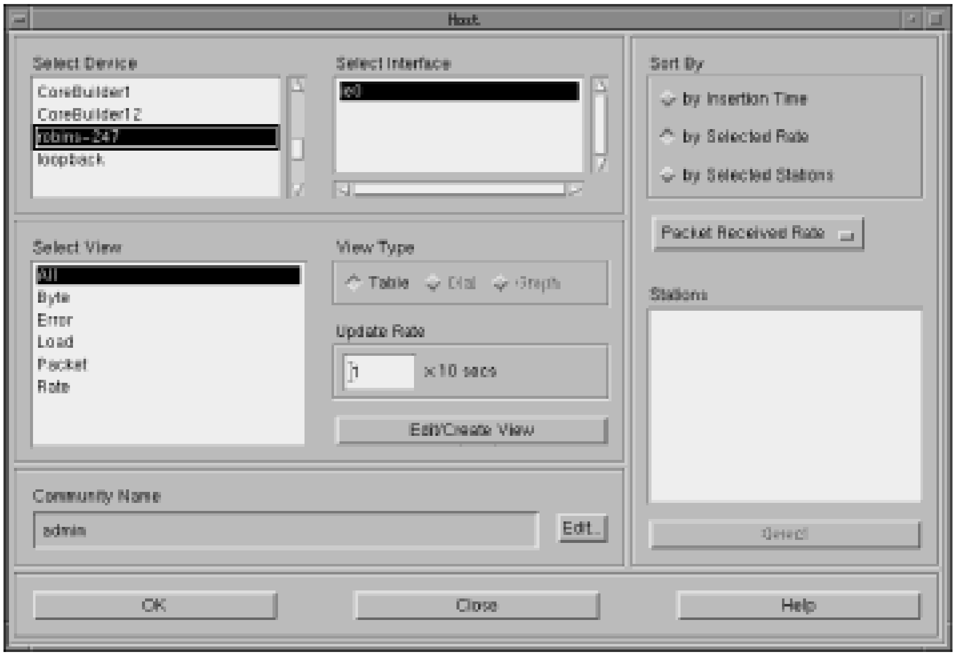


Figure 32. Example of a View Dialog Box

All RMON Views allow you to select from a number of predefined views, or to create your own from a list of variables. Some Views have extra configuration options which let you set up additional parameters - these are described in the relevant sections.

To set up an RMON View, follow these steps:

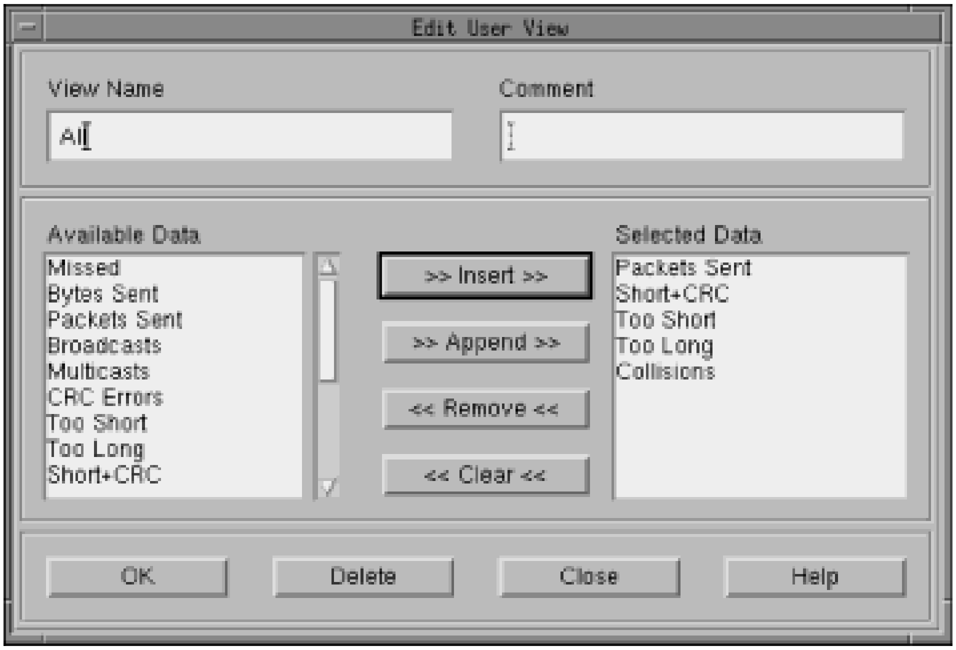
1. Select a device from the Select Device area. This area contains a list of all configured devices (refer to “Setting Up and Verifying Devices” on page 9). The device highlighted is the current selection.
2. Select an interface from the Select Interface area. This area contains a list of available interfaces (if the selected device is accessible).
3. Select a predefined view from the Select View area, or create your own (refer to “Editing and Creating Customized Views” on page 70). This view determines the statistical elements that are displayed.
4. Use the View Type area to specify how you would like to display this view: as a table, dial or graph.
5. Use the Update Rate area to specify how often to update the display with new data.
6. SNMP devices on the network use community names to restrict access to information on the device to specified groups of workstations. The Community Name area shows the community name that is currently used with this device. To change the community name, click **Edit...** and refer to 3 on page 54.

Editing and Creating Customized Views

Nways Manager Remote Monitor allows you to create new data views, and to edit existing ones.

For example, you might find that file servers on your factory floor are frequently generating short packets on an Ethernet segment. To examine this particular set of statistics, you can create a customized view. This section explains how to create a view called factory short stats.

1. Select a view in the Select View list of the View dialog box.
2. Click **Edit/Create View** to open the Edit User View dialog box, shown in Figure 33 on page 71.



View Name: All

Comment:

Available Data:
Missed
Bytes Sent
Packets Sent
Broadcasts
Multicasts
CRC Errors
Too Short
Too Long
Short+CRC

Selected Data:
Packets Sent
Short+CRC
Too Short
Too Long
Collisions

Figure 33. Edit User View Dialog Box

3. Enter a new name for this view in the View Name field - in this case, you would enter `factory short stats`.
4. Click **Clear** to clear the existing set of statistical variables from the Selected Data list.
5. Click the required variables in the Available Data list to include them in the view. To deselect a variable simply click it again.
6. For the factory short stats example, you could use the following variables:
   - Collisions
   - Too Long
   - Too Short
   - Short + CRC
   - Packets Sent (Utilization)
   - CRC
7. Add any notes you required in the Comment field.
8. Click **Insert** or **Append** to add these selections to the Selected Data list. The order in the Selected Data list defines the order in which categories are displayed on screen. **Insert** adds a new entry to the beginning of the list or before a selected entry in the list. **Append** adds it to the end of the list or after a selected entry.
9. Click **OK** to create a customized data view and return to the View dialog box.

Using the Station Select Dialog Box

The Station Select dialog box is used by the following RMON Views:

- Host
- Matrix
- Ring Station

This dialog box allows you to select stations and modify existing station entries. To access it, click **Select** in the relevant View dialog box.

Note: In the Host and Ring Station Views, **Select** only becomes available when you chose to sort entries ″by Selected Station″.

Figure 34 shows the Station Select dialog box.

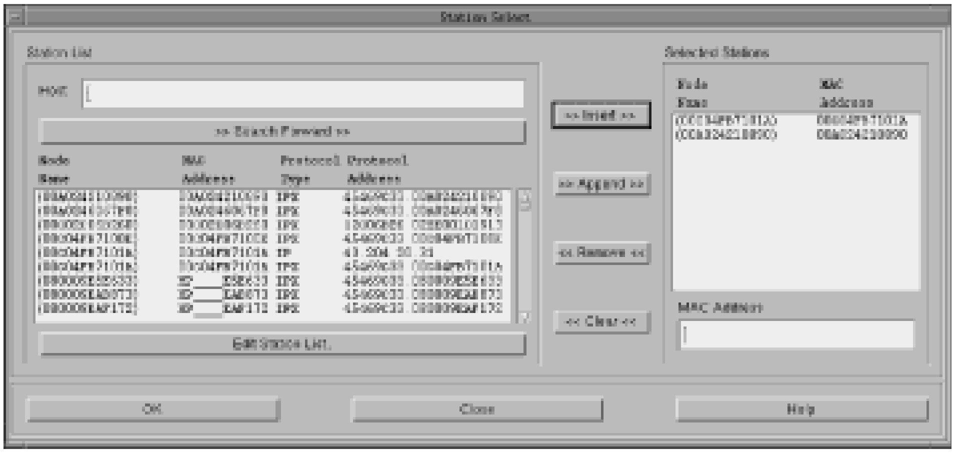


Figure 34. Station Select Dialog Box

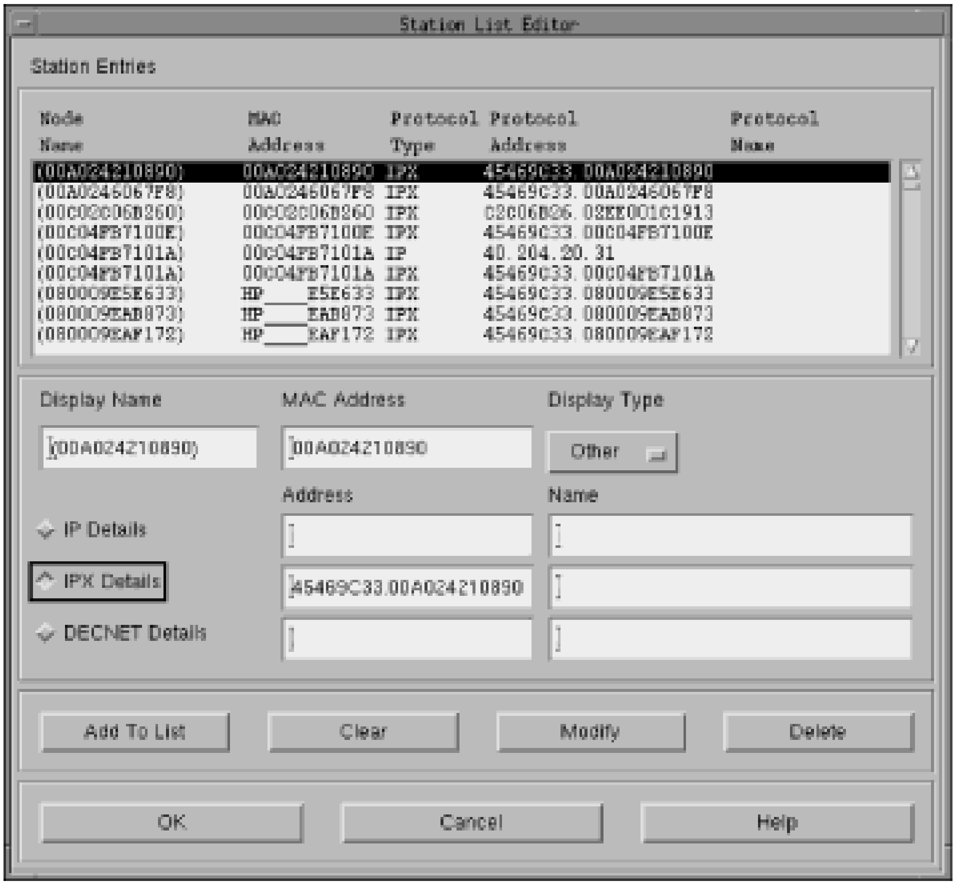
1. Select one or more station entries in the Station area, then click **Insert** or **Append** to add the stations to the Selected Stations area.
   - To select a station, click it in the list. (The red search bar highlights but does not select the entry.)
   - To search for a station in the Station List, enter characters or digits (for instance the first letters of a host name or the first digits of a MAC address) in the Host field. The first occurrence of that string at any point in the station list will be highlighted by a red bar. Continue adding characters or digits to narrow down the search.
   - To find the next occurrence of a string, click **>>Search Forward>>**. If there is only one occurrence in the list, the red bar will remain on the current entry. The search function will search for the contents of the Host field in any column of the list.

- For example, you may be searching for a host called pear and you typed pe in the Host field. The search list could highlight the host opera first. Click **Search Forward** to jump to the next occurrence of the pe string, or narrow the search by adding additional characters or digits to the string in the Host field.
- To remove stations from the Selected Stations list, select the stations and click **Remove**. To clear the Selected Stations list, click **Clear**.
- To modify the list of stations that appear in the list, refer to “Modifying the Station List” on page 73.

2. In the Station Select dialog box, click **OK** to accept the list of selected stations.

Modifying the Station List

To modify station entries in the list, click **Edit Station List...** in the Station Select dialog box to bring up the Station List Editor dialog box (Figure 35).



Node Name	MAC Address	Protocol Type	Protocol Address	Protocol Name
(00A024210890)	00A024210890	IPX	45469C33.00A024210890	
(00A0246067F8)	00A0246067F8	IPX	45469C33.00A0246067F8	
(00C02C06D260)	00C02C06D260	IPX	C2C06D26.02EE001C1913	
(00C04FB7100E)	00C04FB7100E	IPX	45469C33.00C04FB7100E	
(00C04FB7101A)	00C04FB7101A	IP	40.204.20.31	
(00C04FB7101A)	00C04FB7101A	IPX	45469C33.00C04FB7101A	
(080009E5E633)	HP____E5E633	IPX	45469C33.080009E5E633	
(080009EAD873)	HP____EAD873	IPX	45469C33.080009EAD873	
(080009EAF172)	HP____EAF172	IPX	45469C33.080009EAF172	

Display Name: (00A024210890)
MAC Address: 00A024210890
Display Type: Other

	Address	Name
◇ IP Details		
◆ IPX Details	45469C33.00A024210890	
◇ DECNET Details		

Figure 35. Station List Editor Dialog Box

Known stations are listed alphabetically by display name in the Station Entries area, with separate entries for each protocol type.

When you select a station entry, the detailed information for all protocols is shown.

Nways Manager Remote Monitor automatically lists all available stations. However, you may need to add a station to the list. For example, you may be using a device onto which you cannot load SmartAgent software and which is not an RMON2 device, or you may want to create a station entry in advance for a device which you have not yet added to your network.

Adding a New Station Entry

To add a new entry, follow these steps:

1. Click **Clear** to present an empty station template.
2. Enter the station’s MAC address.
3. To add the IP, IPX or DECnet information, activate the appropriate protocol button. Then enter the protocol address and a name.
4. To select the Display Name for the station, click **Display Type** and select either IP, IPX, DECnet or Other.
5. Click **Add To List** to create this new entry.
6. Click **OK** to return to the Station Select dialog box.

Modifying a Station Entry

To modify an entry, follow these steps:

1. Select the entry in the list. All protocol entries for this station are highlighted in the list.
2. To add or change protocol entries, activate the appropriate protocol button and modify the values in the Address and Name fields.
3. To remove a protocol-specific entry for the selected station, simply deactivate the protocol button.
4. Click **Modify** to accept these changes.
5. Click **OK** to return to the Station Select dialog box.

Deleting a Station Entry

To delete an entry, follow these steps:

1. Select the entry in the list. All protocol entries for this station will be highlighted in the list.
2. Click **Delete**.

   Note: All occurrences of this station for the different protocol types will be deleted.
3. Click **OK** to return to the Station Select dialog box.

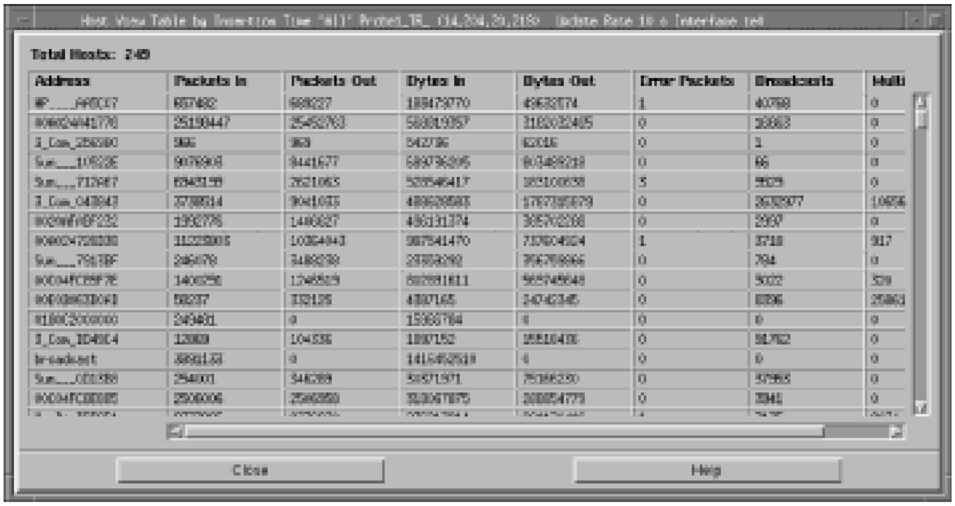
Statistical Displays

Nways Manager Remote Monitor supports multiple displays on screen at any one time. The formats available are table, dial and graph.

Table Display

The table display presents statistics in tabular form, updating itself in real-time as specified in the Update Rate field (refer to “Dialog Box Format” on page 69). Table displays show absolute values, not delta values. Use the scroll bars to move through the view. Figure 36 shows a sample Table display.

Note: Entries in the Matrix table are not updated in real-time, though they can be updated manually by using the **Update** button.



Host View Table by Insertion Time "all" Probe1_TR_ (14.204.20.218) Update Rate 10 s Interface 1e0

Total Hosts: 248

Address	Packets In	Packets Out	Bytes In	Bytes Out	Error Packets	Broadcasts	Multi
HP____AA5C07	657482	688227	188479770	45632574	1	40788	0
000024941776	25190447	25452763	588819357	3182032405	0	38863	0
3_Com_256980	986	969	542796	62016	0	1	0
Sun___10522E	9076908	9441677	689796205	803489218	0	66	0
Sun___712687	6945159	2621065	528546417	182100658	5	5929	0
3_Com_043843	3738514	9041033	488620583	1767385879	0	2632977	10656
0020AFABF232	1352776	1446627	486131374	385702288	0	2557	0
0000247200D0	11228805	10064043	987541470	737604024	1	3718	917
Sun___7917BF	246078	3488239	27858292	756709666	0	784	0
00004FC85F7E	1400250	1246519	802881611	565745648	0	5022	329
0040086300F0	58237	332125	4807165	24742345	0	8396	25063
0180C2000000	245481	0	15368784	6	0	0	0
3_Com_1D48C4	12089	104536	1897152	15510436	0	51762	0
broadcast	4860133	0	1416452518	6	0	0	0
Sun___0D1388	254001	546289	50871971	75366250	0	57565	0
00004FC0E085	2508006	2560850	310067875	200854779	0	3841	0

Figure 36. Table Display

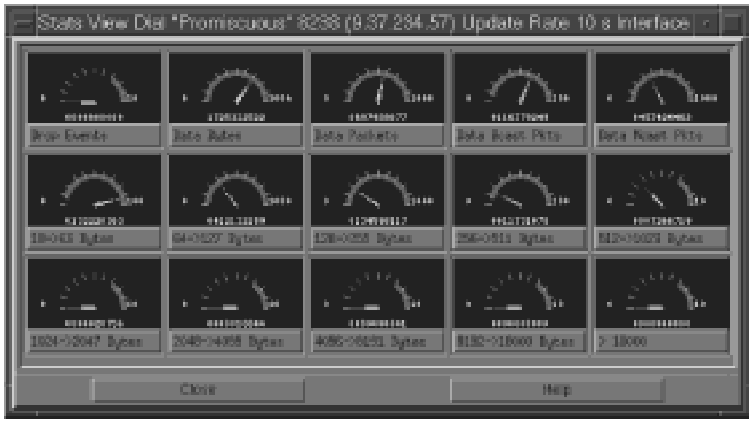
The Host and Matrix tables also include a count of the number of entries in the top left corner. The Host table is refreshed at the same rate as the data in the table. For further information, refer to “Configuring the Host View” on page 86 and “Configuring the Matrix View” on page 88.

Dial Display

The Dial display presents statistics in real time. A yellow pointer indicates the current value per second, while a red pointer shows the maximum level reached since the display was opened. The red zone, indicating unusual activity levels, can be set by the user. The number beneath the dials reflects the cumulative value over the monitored period. Table 20 on page 76 shows a sample Dial display.

Because the norm varies from LAN to LAN, you can tailor the red zone value to suit your own environment. You may even want to map the red zones to your own thresholds set up in Alarms (see Chapter 6). The dial threshold settings are contained in the Rmon file for RMON Views and in the ECAM file for the ECAM Application (see Appendix G). Both files are contained in the /usr/LANReMon/rmon/locale/C/app-defaults directory and can be edited using any text editor.

Table 20. Dial Display

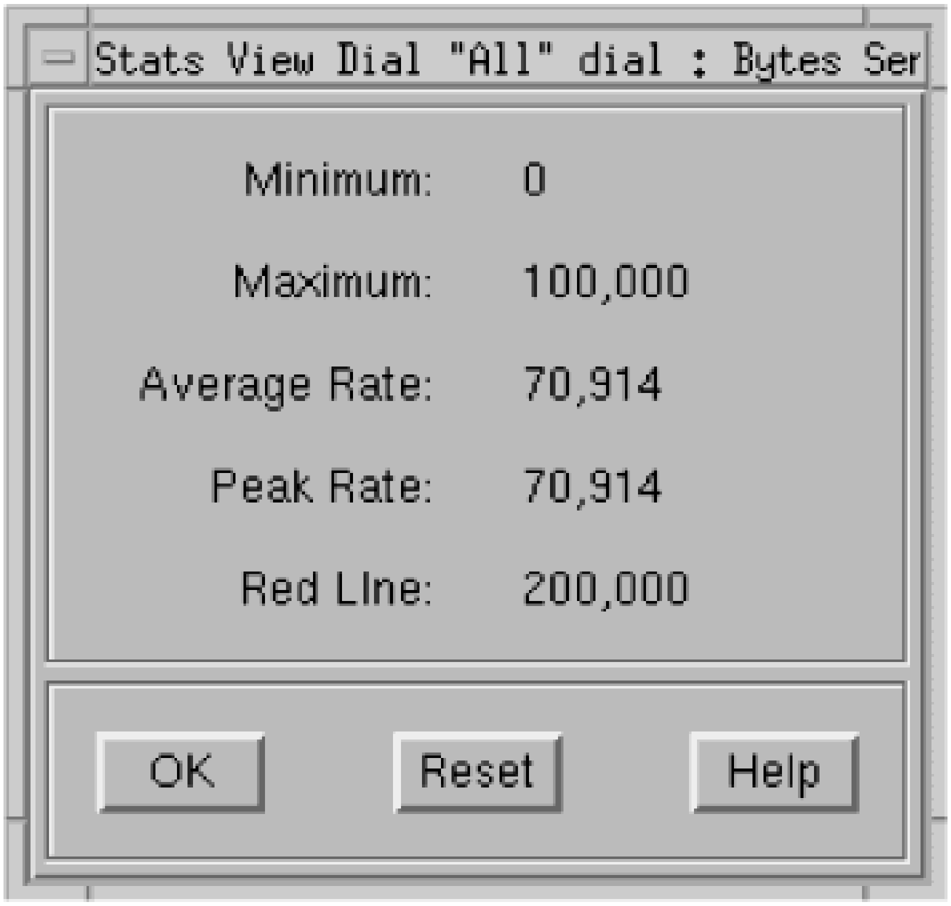


Yellow pointer: current value

Red Pointer: maximum level reached this session

Red zone: indicates unusual activity levels

Click any of the dial names to display the Dial Reset dialog box, shown in Figure 37 on page 77. This displays the minimum, maximum, average and red line (red zone) values in the dial. Click **Reset** to reset the values for that dial to 0. The dial will display refreshed data at the end of the update period you have set.



Stats View Dial "All" dial : Bytes Ser

Minimum: 0

Maximum: 100,000

Average Rate: 70,914

Peak Rate: 70,914

Red LIne: 200,000

Figure 37. Dial Reset Dialog Box

Graph Display

The Graph display lets you choose from the following graph types: bar, pie, 3D bar, line, area and scatter. The first three present the latest statistical sample. The others present historical statistics over time. All graphs are updated at the update rate specified in the Update Rate field (refer to “Dialog Box Format” on page 69). The Statistics View allows you to generate comparative graphs of statistics from several interfaces. Figure 38 on page 78 shows a sample Graph display.

Table 21 on page 78 shows which menus can be accessed from within the Graph display.

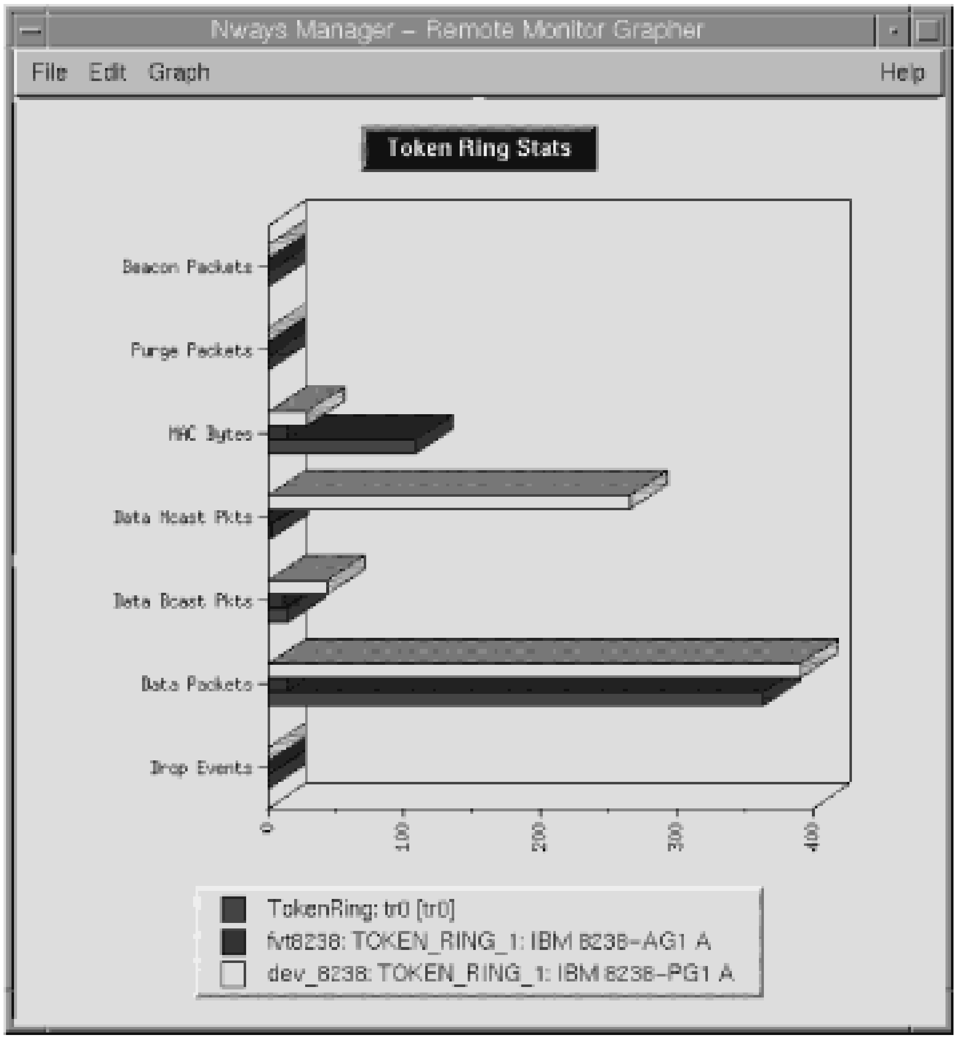


Figure 38. Graph Display

Table 21. Graph Display Menus

Menu	Option	Description
File	Print	Prints the statistical content of the display to file or to a printer.
	Exit	Closes the display.
Edit	Transpose*	Toggles between grouping statistics by sample point and grouping them by RMON variable.
	Delta Values*	Use absolute (total) values or delta (change) values.
	Select Columns...	Select which variables you want to display.

Table 21. Graph Display Menus (continued)

Menu	Option	Description
Graph	Bar*	Shows real-time statistics values. Useful for comparison of statistics.
	PieA	Shows proportion of each statistic to the whole.
	Bar 3DA	Shows real-time statistics values. Useful for comparison of statistics.
	LineB	Shows trends over time. Emphasizes rate of change over time, rather than magnitude of change.
	AreaB	Shows trends over time. Emphasizes rate of change over time, rather than magnitude of change.
	ScatterB	Shows trends over time. Emphasizes rate of change over time, rather than magnitude of change.

*Displays time-line (historical) statistics

ADisplays the latest set of statistics

BDisplays time-line (historical) statistics

Using the Statistics View

The Statistics View displays a real-time report of activity on your chosen network segment and is the first place you should look if you suspect there are problems on a particular segment. Use this View to display statistics on any combination of packets, bytes, errors, size distributions or multicasts.

Configuring the Statistics View

Use the Statistics dialog box to create a Statistics View. To access the Statistics dialog box, select **RMON Views** from the Analysis menu, then **Statistics**, or click the **RMON Statistics** button in the toolbar.

This View allows you to:

- View statistics from a single LAN segment.
- View and compare statistics gathered from multiple interfaces on different LAN segments.

Viewing Single Segment Statistics

To view single segment statistics, follow these steps:

1. Set up the basic View parameters as described in “Dialog Box Format” on page 69.

   Note: You can view statistics for a single LAN segment as a table, dial or graph (refer to “Statistical Displays” on page 75 for an explanation of the different display types).

2. Click **OK** to display the Statistics View.

Viewing Comparative Segment Statistics

You can view several device/interface combinations simultaneously and display this information in a single graph. This is useful if:

- You want to look at statistics gathered from interfaces of the same type on different devices.
- You want to compare statistics gathered from two or more interfaces of the same type on a single device.

To view several segment statistics, follow these steps:

1. Click **Graph** in the View Type area (refer to “Statistical Displays” on page 75 for a description of graphical displays).
2. Select the required device and interface and click **Add**. The selected items appear in the Graph Sample Points field. Repeat this procedure to add as many device/interface combinations as you require.

   Note: You must select interfaces of the same media type, such as all Ethernet or all FDDI. All interfaces should also have the same media speed.
3. To delete an individual device/interface combination from the Graph Sample Points field, select the item and click **Delete**. To remove all items, click **Clear**.
4. Configure the other areas as described in “Dialog Box Format” on page 69.
5. Click **OK** to display the Statistics View (Figure 39 on page 81).

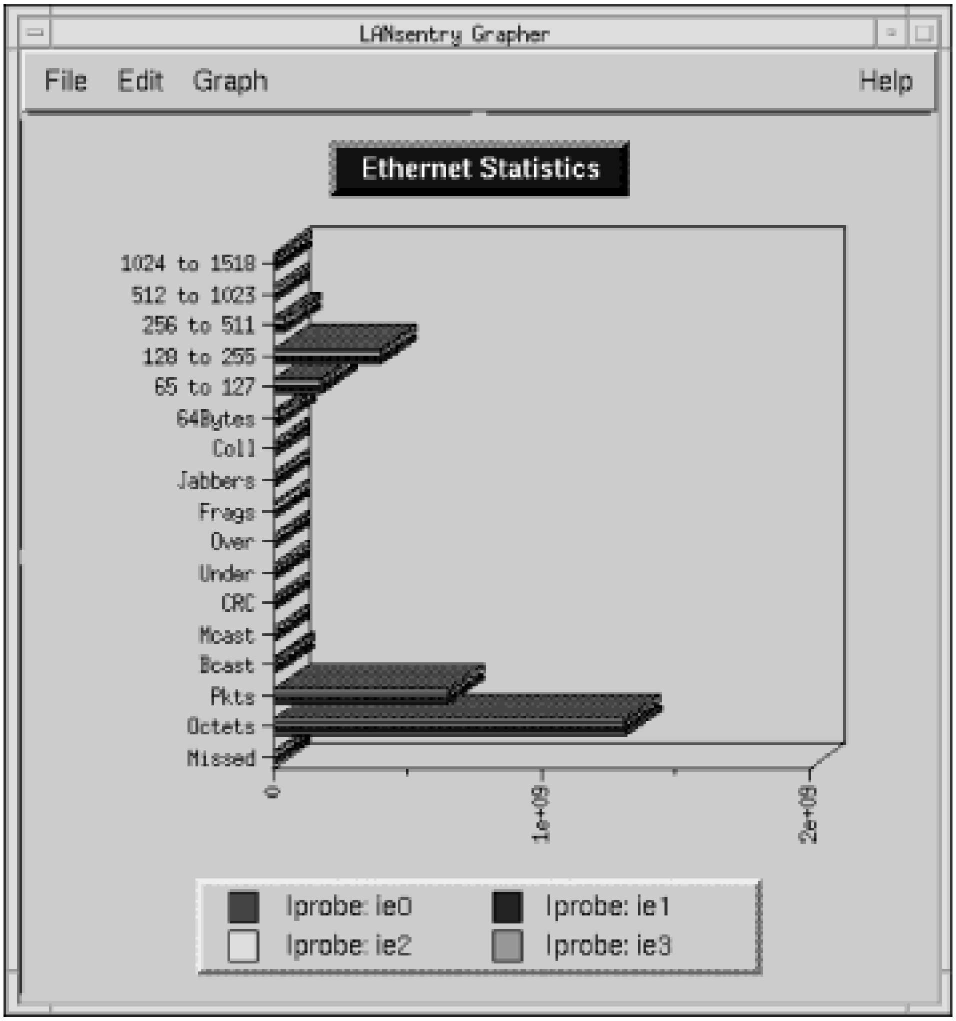


Figure 39. Example of a Comparative Statistics Graph

Predefined Statistics Views

Table 22 on page 82 describes the Statistics Views available for Ethernet, Token Ring and FDDI. Refer to Appendix F for a list of the variables available in the Statistics View.

Table 22. Predefined Statistics View

View	Media Type			Description
	Ethernet	**Token Ring**	**FDDI**	
All	■		■	Contains all variables.
Bytes	■		■	The number of bytes making up these packets (in other words, the total number of bytes of traffic on that segment).
Distribution	■	■		Packets classified into specific size categories, for either media type.
Errors	■	■	■	The number of errors detected on the segment.
Events			■	Ring Polls, Beacon Events and Purge Events on the ring.
MAC			■	All MAC layer traffic on a segment - packets, bytes making up these packets, MAC layer beacon information, various soft errors, the number of ring polls, and so on.
Multicast	■	■		The total number of good packets directed to the multicast address. Includes broadcast packets.
Packets	■	■	■	The total number of packets detected - including error packets - on the network segment.
Promiscuous			■	Data layer traffic on a segment.
Source Routing			■	Ring number, frame in and out, through frames, octets in and out, octets through, all route and single route broadcasts and octets, local LLC frames and hop counters.

*Contains some variables only suitable for table displays. Refer to “Appendix F. View and Application Variables” on page 167, for a list of variables available on FDDI.

Using the History View

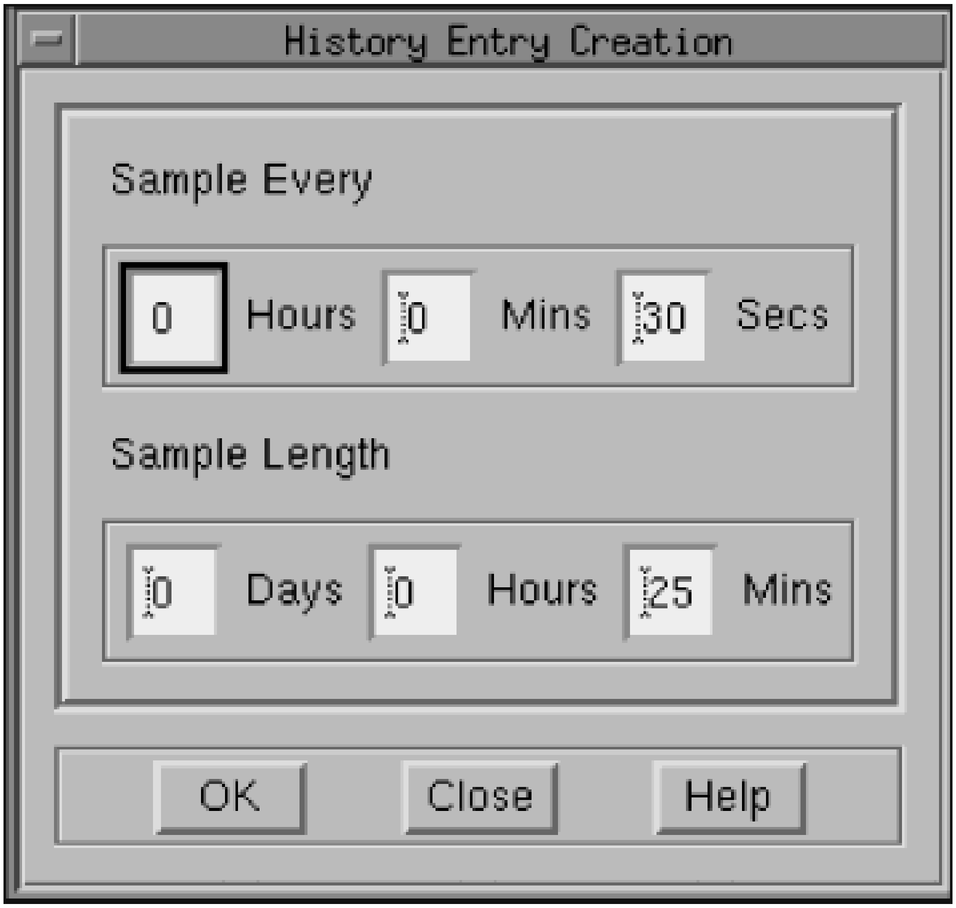
The History View complements the Statistics View. It allows you to gather data on your network’s normal trends. When you have determined your network’s normal activity, you can use the Alarms View to set alarms which trigger when network activity deviates from the norm. Use the History View to specify a sample period and spot trends over hours, days, weeks or even months.

Historical information is displayed as a table or graph over time. If you spot an unusual spike or dip in network activity, simply click that part of the line graph to find out when the event occurred.

Configuring the History View

Use the History dialog box to configure the History View. To access this dialog box, select **RMON Views** from the Analysis menu, and select **History**, or click **RMON History** in the toolbar.

1. Set up the basic View parameters as described in “Dialog Box Format” on page 69.
2. In the History Entries list, select a sample period. If the sample period you want does not already appear in the History Entries list, follow these steps:
   a. Click **Add** to create a new sample period. The History Entry Creation dialog box appears, as shown in Figure 40.



History Entry Creation

Sample Every

0 Hours 0 Mins 30 Secs

Sample Length

0 Days 0 Hours 25 Mins

Figure 40. History Entry Creation Dialog Box

   b. Specify how often to sample statistics on the segment (up to 1 hour at a time) and for how long.

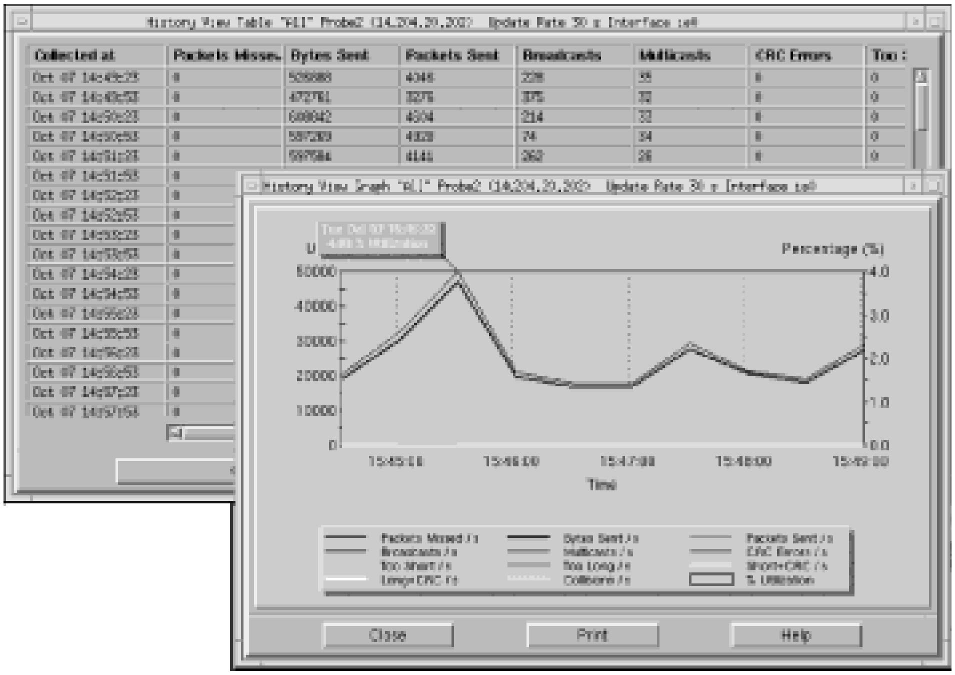
If you select once an hour, every point on the graph reflects events at an hourly interval.

c. To add this entry, click **OK**.

The device stores each history entry in a specific memory location or bucket, and has a maximum number of buckets. For example, if we chose to sample every 30 minutes for 8 hours, this would take up 16 buckets (2 buckets per hour for each sample type).

Note: If you have specified a very large number of samples, Nways Manager Remote Monitor may warn you that the device has insufficient resources to handle your new entry. If this happens, delete an old sample you no longer need from the History Entries list and then recreate the history entry.

3. Click **OK** to start the History View.



History View Table "ALL" Probe2 (14.204.20.202) Update Rate 30 s Interface is#

Collected at	Packets Misse.	Bytes Sent	Packets Sent	Broadcasts	Multicasts	CRC Errors	Too :
Oct 07 14:49:23	0	509888	4346	228	35	0	0
Oct 07 14:49:53	0	472761	3276	375	32	0	0
Oct 07 14:50:23	0	608042	4504	214	32	0	0
Oct 07 14:50:53	0	597289	4828	74	34	0	0
Oct 07 14:51:23	0	597584	4141	262	26	0	0
Oct 07 14:51:53	0						
Oct 07 14:52:23	0						
Oct 07 14:52:53	0						
Oct 07 14:53:23	0						
Oct 07 14:53:53	0						
Oct 07 14:54:23	0						
Oct 07 14:54:53	0						
Oct 07 14:55:23	0						
Oct 07 14:55:53	0						
Oct 07 14:56:23	0						
Oct 07 14:56:53	0						
Oct 07 14:57:23	0						
Oct 07 14:57:53	0						

History View Graph "ALL" Probe2 (14.204.20.202) Update Rate 30 s Interface is#

Figure 41. Example of History Table and Graph Displays

Refer to “Statistical Displays” on page 75 for a description of table displays.

The Graph window provides a pictorial display of historical events over time. A time axis is shown along the bottom of the graph, scrolling with the graph as new data is displayed. Vertical grid lines mark the times labeled on this axis.

Each history variable is color-coded, and events are plotted against packet rates and utilization on the segment. Token Ring utilization rates are calculated using the interface speed value from the interface table. If the value is unavailable, a 16 MB ring speed is assumed for the calculation.

To find out when a particular event occurred on the network, click that point in the graph. A data description label appears. To remove the data description label, click the point in the graph again.

Predefined History Views

Table 23 describes the History Views available for Ethernet, Token Ring and FDDI. Refer to Appendix G. Enterprise Communications Analysis Module (ECAM) for a list of variables available in the History View.

Table 23. Predefined History Views

	Media Type			
View	**Ethernet**	**Token Ring**	**FDDI**	**Description**
All	■		■	Contains all variables.
Byte	■		■	The number of bytes making up the packets seen on the segment (in other words, the total number of bytes traffic on that segment).
Error	■	■	■	The number of error packets detected on the segment.
Events		■		Purge events, beacon events, claim token events and ring polls.
Load	■		■	The percentage of network utilization at the time of this sample period.
Multicast	■		■	The total number of good packets directed to the multicast address. Includes broadcast packets.
Packet	■	■	■	The total number of packets detected—including error packets—on the network segment.
Size Distribution		■	■	Packets classified into specific size categories.

Using the Host View

The Host View is useful when determining which nodes are on your network, the state of those nodes, and which nodes may be causing problems. For example, you may be fairly sure that as broadcast rates increase on a segment the number of errors on your router is increasing too, but it can often be difficult to collect the hard facts required to back up the theory.

The Host View has been designed to help you access the appropriate information to get to the heart of this sort of problem. Information is presented from the Host and Host TopN RMON groups. Depending on your line of investigation, results can be sorted in different ways to help highlight the relevant information:

- By insertion time
- By selected rate
- By selected stations

Configuring the Host View

Use the Host dialog box to configure the Host View. To access this dialog box, select **RMON Views** from the Analysis menu, then **Host**, or click the **RMON Host** button in the toolbar.

- Set up the basic View parameters as described in “Dialog Box Format” on page 69.
- The **Sort By** area allows you to view the host entries in three ways:

  By Instertion Time
  This lists the hosts in the order in which they appeared in the RMON Host table.

  By Selected Rate
  If you choose this option, Packet Received Rate becomes active. This is a default value only.

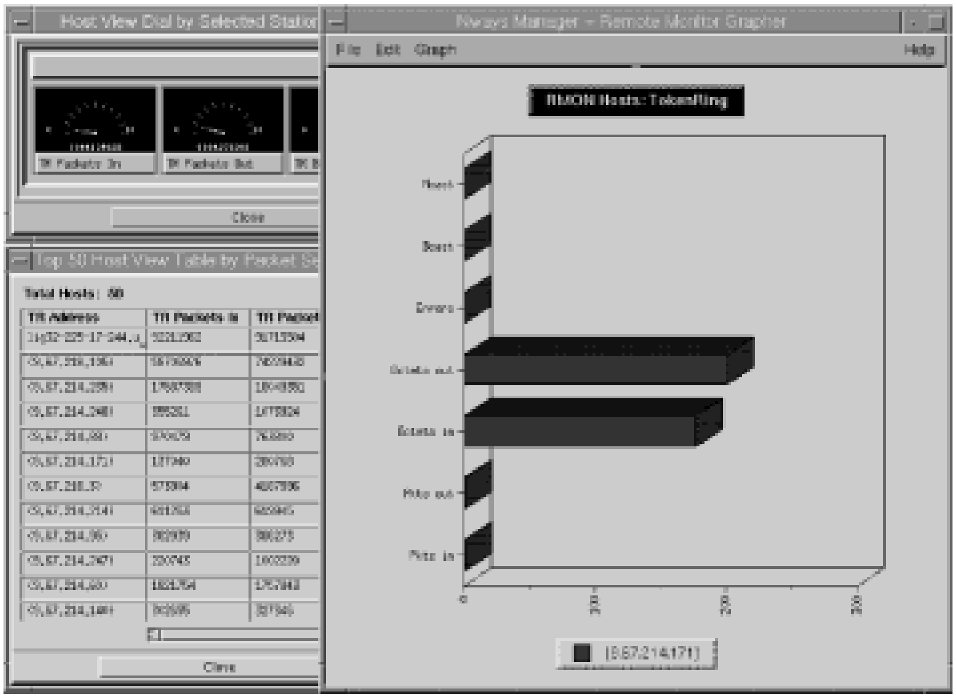
  You can choose from:

  – Packet received rate
  – Packet sent rate
  – Bytes received rate
  – Bytes sent rate
  – Error packet rate
  – Broadcast packet rate
  – Multicast packet rate

  By Selected Station
  If you choose this option, the Select button becomes active and any currently selected stations will be shown in the Stations list.

  You can modify the stations in this list by clicking Select to open the Station Select dialog box. Refer to Using the Figure 34 on page 72 for a description of adding, modifying and deleting station entries.

- Click **OK** to start the Host View.



Total Hosts : 50

TR Address	TR Packets In	TR Packet
1s(32-225-17-244..	5221.2582	51715504
(9.67.218.136)	18730926	74029440
(9.67.214.239)	17587308	18048582
(9.67.214.248)	995261	1075824
(9.67.218.88)	970479	763080
(9.67.214.171)	127340	280760
(9.67.218.3)	575084	4007806
(9.67.214.214)	601203	620945
(9.67.214.95)	302939	300275
(9.67.214.247)	220745	1602239
(9.67.214.60)	1821754	1757843
(9.67.214.148)	202695	327546

Figure 42. Example of a Host Table, Dial and Graph Display

Refer to “Statistical Displays” on page 75 for a description of the table, dial, and graph displays.

The total number of hosts in the table is displayed below the title bar. This number is refreshed at the same time as the rest of the table. Nways Manager Remote Monitor displays the host in the Address column as either its name, protocol address or MAC address depending on the selected Address Translation Level. For more information, refer to “Setting the Address Translation Level” on page 43.

Predefined Host Views

Table 24 describes the Host Views available for Ethernet, Token Ring and FDDI. Refer to Appendix G. Enterprise Communications Analysis Module (ECAM) for a list of variables available in the Host View.

Table 24. Predefined Host Views

	Media Type			
View	Ethernet	Token Ring	FDDI	Description
All	■	■	■	Contains all variables.
Broadcast		■		The number of broadcasts seen.

Table 24. Predefined Host Views (continued)

	Media Type			
View	**Ethernet**	**Token Ring**	**FDDI**	**Description**
Byte	■	■	■	The number of bytes making up the packets seen on the segment (in other words, the total number of bytes traffic on that segment).
Error	■		■	The number of error packets detected on the segment.
Load	■		■	The number of multicasts seen.
Packet	■	■	■	The total number of packets detected—including error packets—on the network segment.
Rate	■		■	The number of broadcasts and multicasts seen.

Using the Matrix View

The Matrix View shows the amount of traffic and number of errors between a pair of stations on the network. This allows you to single out stations that might be responsible for generating problems.

You can use the Matrix View to determine:

- Who is talking to whom on the network.
- How much traffic is flowing between two stations.

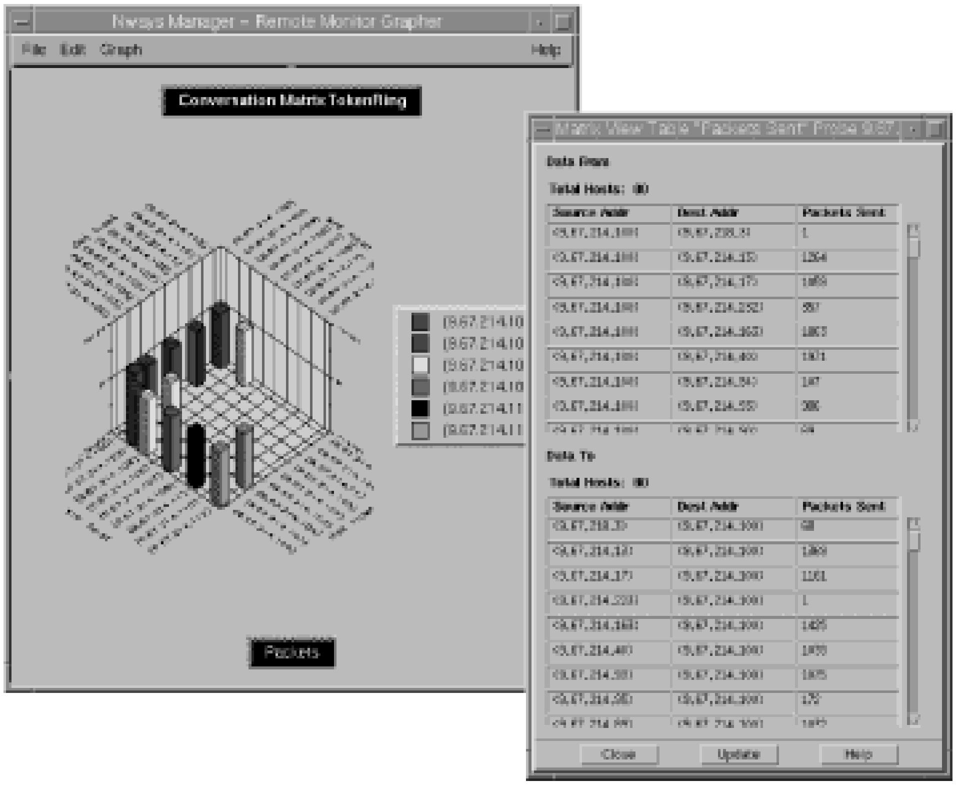
Configuring the Matrix View

Use the Matrix dialog box to configure the Matrix View. To access this dialog box, select **RMON Views** from the Analysis menu, and select **Matrix**, or click **RMON Matrix** in the toolbar.

1. Set up the basic View parameters as described in “Dialog Box Format” on page 69.

   Note: There must be at least one station in the Stations list.

2. In the Matrix dialog box, click **OK** to start the Matrix View.


Nways Manager – Remote Monitor Grapher
File
Edit
Graph
Help
Conversation Matrix Tokenring
(9.67.214.10
(9.67.214.10
(9.67.214.10
(9.67.214.10
(9.67.214.11
(9.67.214.11
Packets
Matrix View Table "Packets Sent" Probe 9.67.
Close
Update
Help

Data From

Total Hosts: (8)

Source Addr	Dest Addr	Packets Sent
<9.67.214.100>	<9.67.238.3>	1
<9.67.214.100>	<9.67.214.15>	1264
<9.67.214.100>	<9.67.214.17>	1069
<9.67.214.100>	<9.67.214.252>	557
<9.67.214.100>	<9.67.214.163>	1803
<9.67.214.100>	<9.67.214.40>	1871
<9.67.214.100>	<9.67.214.54>	147
<9.67.214.100>	<9.67.214.55>	306
<9.67.214.100>	<9.67.214.56>	64

Data To

Total Hosts: (8)

Source Addr	Dest Addr	Packets Sent
<9.67.218.3>	<9.67.214.100>	68
<9.67.214.12>	<9.67.214.100>	1269
<9.67.214.17>	<9.67.214.100>	1101
<9.67.214.228>	<9.67.214.100>	1
<9.67.214.163>	<9.67.214.100>	1435
<9.67.214.40>	<9.67.214.100>	1855
<9.67.214.58>	<9.67.214.100>	1905
<9.67.214.28>	<9.67.214.100>	179
<9.67.214.99>	<9.67.214.100>	1872

Figure 43. Example of Matrix Table and Graph Displays

Reading the Matrix Display

Nways Manager Remote Monitor displays all hosts which are either receiving data from, or sending data to, the stations in your selection. The total number of hosts in the table is displayed for both the Data From table and the Data To table. This number is refreshed at the same time as the rest of the table. The table is displayed in the form of a matrix, as shown in Figure 43. Table 25 describes the columns of the matrix.

Table 25. Matrix Columns

Column	Description
Source Address	The station sending the data.
Destination Address	The station data is being sent to.
Packets Sent	The number of packets of data sent by the source host.
Bytes Sent	The number of bytes making up these packets.
Error Packets	The number of error packets generated by the source host.

Note: As the Matrix table is not updated automatically, you must click **Update** to upload data from the device.

Predefined Matrix Views

Table 26 describes the Matrix Views available for Ethernet, Token Ring and FDDI. Refer to Appendix G for a list of variables available in the Matrix View.

Table 26. Predefined Matrix Views

	Media Type			
View	**Ethernet**	**Token Ring**	**FDDI**	**Description**
All	■	■	■	Contains all variables.
Bytes	■	■	■	The total number of bytes of traffic on that segment.
Errors	■	■	■	The number of error packets detected on the segment.
Packets	■	■	■	The total number of packets detected, including error packets, on the network segment.

Using the Ring Station View

The Ring Station generates a table of statistics and status information associated with each station on the ring, including station status and last entered and last exited times.

For example, a disruption is caused every time a station inserts onto the ring. This results in a ring purge event and a new token is issued by the active monitor. You can use the Ring Station View to track which station is doing this and to discover the active monitor issuing the new token.

Using the Ring Station View you can:

- Learn to spot patterns on your own Token Ring.
- Home in on isolating errors and non-isolating errors.
- See which devices are currently active on the ring.

Configuring the Ring Station View

Use the Ring Station dialog box to configure the Ring Station View. To access this dialog box, select **RMON Views** from the Analysis menu, and select **Ring Station**, or click **RMON Ring Station** in the toolbar.

1. Set up the basic View parameters as described in “Dialog Box Format” on page 69.

   Note: Ensure that you select a Token Ring device or, in the case of multi-interface devices, a device that contains a Token Ring interface, as Ring Station statistics are particular to Token Ring.

2. Depending on your line of inquiry, you can choose to view the Ring Station entries in three ways:

   By Ring Order
   This lets you view active stations on the ring in order of their physical connection to the ring, starting with the Active Monitor.

   By Address
   This shows all devices currently or previously attached to the Ring.

   By Selected Station
   If you choose this option, Select becomes active.

   Click **Select** to open the Station Select dialog box. Refer to Figure 34 on page 72 for a description of adding, modifying and deleting station entries.

3. In the View Type area, select the required display type. The Table display is available at all times, while the Dial and Graph displays are available when Sort View is set to by Selected Stations.
4. Click **OK** to start the Ring Station View.

Predefined Views

Table 27 describes the Ring Station Views available for Token Ring. Refer to Appendix F for a list of available variables.

Table 27. Predefined Ring Station Views

View	Token Ring	Description
All	■	Contains all variables.
Errors	■	Errors detected on the ring, including duplicate addresses, AC errors, and abort frames.
Events	■	Includes last NAUN, station status, last entered, and last exited.

Chapter 6. Alarms

This chapter tells you how to set up and configure alarms on Nways Manager Remote Monitor. It contains the following sections:

- Alarms Overview
- Configuring Alarms

Alarms Overview

Nways Manager Remote Monitor lets you set alarms for specific network events and then informs you as soon as they occur. Consider the following examples:

- The router on your network is capable of forwarding at 3000 packets per second (pps). It appears to have problems forwarding at the top of its specification. You want to know as soon as the traffic rate gets near 3000 pps.
- Your network is running at 1400 pps. Typically, a CRC rate of more than 1% of network traffic is considered excessive. You want to know as soon as the CRC rate climbs above 14 pps.

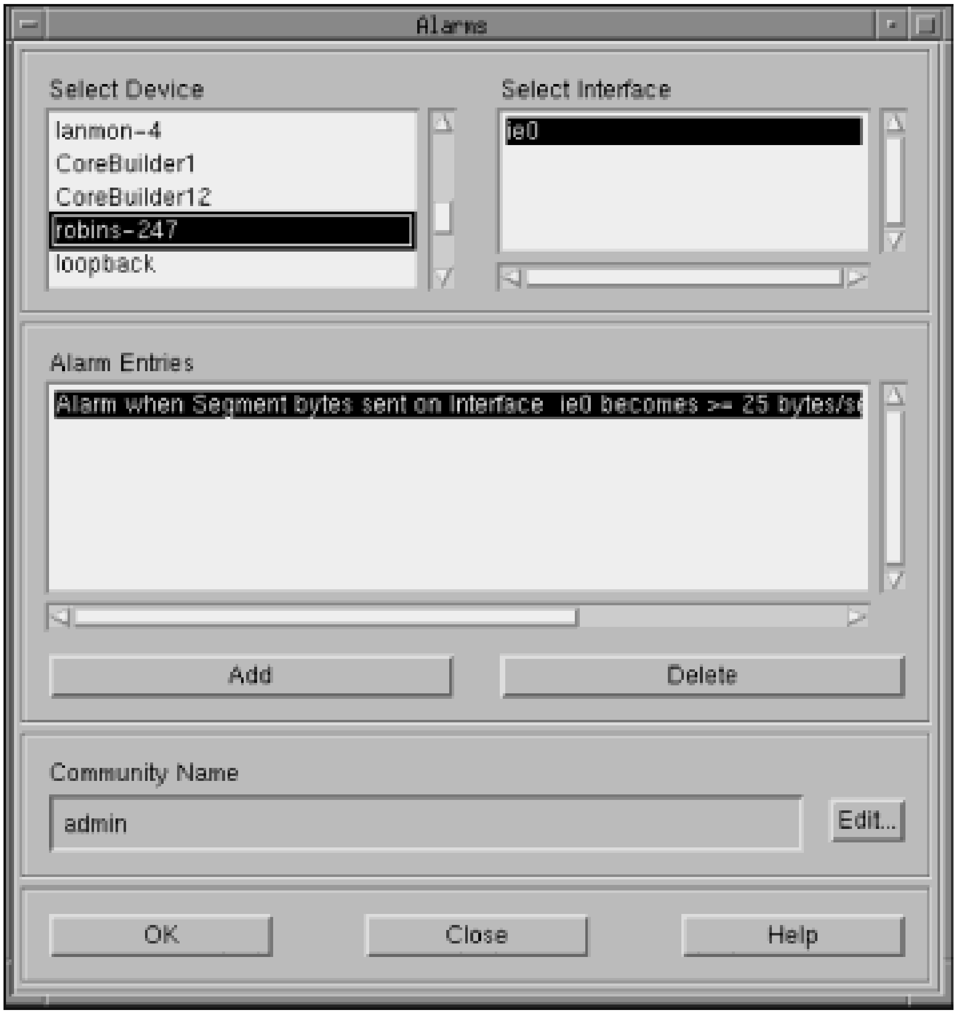
Over time you will build up a library of alarms tailored to your own network.

As well as using alarms on their own, you can use them as Start or Stop events when capturing packets with the Capture application (refer to Chapter 7). Taking our first example above, you might start capturing all packets transmitted by the router whenever the traffic rate gets above 2800 packets per second, then stop capturing when it drops below this level again.

Configuring Alarms

To configure alarms, follow these steps:

1. Select **Alarms** from the Analysis menu, or click **Alarms** in the toolbar to open the Alarms dialog box, shown in Figure 44 on page 94.



Alarm when Segment bytes sent on Interface ie0 becomes >= 25 bytes/s

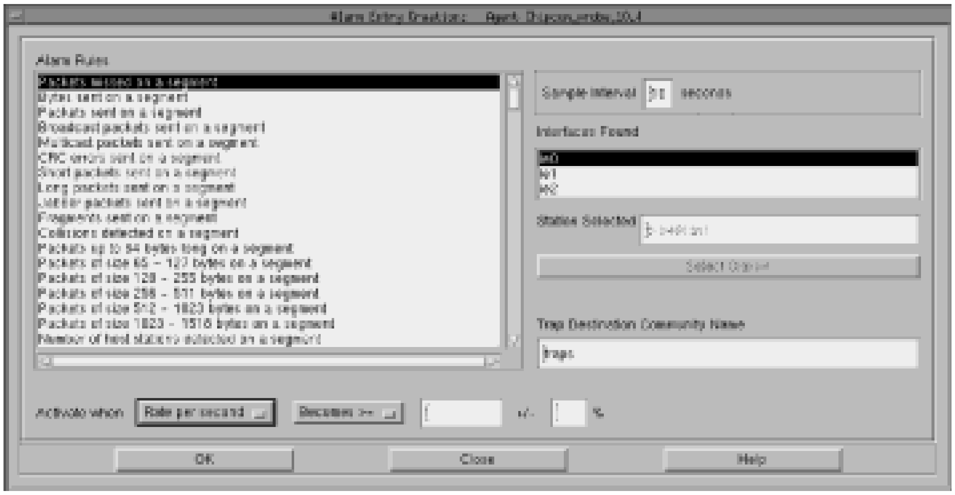
Community Name: admin

Figure 44. Alarms Dialog Box

2. Select a device and interface.

   If this is the first time you have set alarms on this device or if you have deleted all of the old alarms, there will be no existing entries in the Alarm Entries list and the message ″No entries found on that device″ is displayed.

3. To add a new entry to the Alarms list, click **Add** to open the Alarm Entry Creation dialog box, shown in Figure 45 on page 95.



Alarm Rules

- Packets missed on a segment
- Bytes sent on a segment
- Packets sent on a segment
- Broadcast packets sent on a segment
- Multicast packets sent on a segment
- CRC errors sent on a segment
- Short packets sent on a segment
- Long packets sent on a segment
- Jabber packets sent on a segment
- Fragments sent on a segment
- Collisions detected on a segment
- Packets up to 64 bytes long on a segment
- Packets of size 65 – 127 bytes on a segment
- Packets of size 128 – 255 bytes on a segment
- Packets of size 256 – 511 bytes on a segment
- Packets of size 512 – 1023 bytes on a segment
- Packets of size 1023 – 1518 bytes on a segment
- Number of host stations detected on a segment

Sample interval [illegible] seconds

Interfaces Found

- le0
- le1
- le2

Station Selected [illegible]

Trap Destination Community Name: traps

Activate when: Rate per second, Becomes >=, +/- %

Figure 45. Alarm Entry Creation Dialog Box

a. In the Alarm Rules area, select the type of alarm required. The Alarms View offers a wide range of alarm types. The list of Alarm Rules varies according to the type of the interfaces available. The Interfaces Found list will show the permissible interfaces for the selected Alarm Rule. Select the Alarm Rule you require.

b. In the Sample Interval area, specify how often you would like the View to check for this event.

c. If you have selected a station-specific alarm type, then Select Station will be active. Click this to select a station. This procedure is described in “Using the Stations Dialog Box” on page 96.

d. If desired, change the Trap Destination Community Name. If an alarm triggers, an SNMP trap is sent to all devices associated with that community. For more information on trap communities, refer to “Setting Up Trap Communities” on page 34.

e. Some alarms require further selection of objects to complete the alarm description. An example would be an alarm on a network hub counting the number of packets sent on one port in a particular group or on any port in a group.

   If more information is required to complete the alarm, Additional Parameters will be active. Click **Additional Parameters** to open the Alarm Variables dialog box. Enter values in the appropriate variables fields and then click **OK** to return to the Alarm Entry Creation dialog box.

f. Use the Activate When area to specify when the alarm should trigger. Most alarm types center around the frequency or rate of a specific event, for example when the CRC rate gets above an acceptable level on a segment. On occasions they may center around a specific value, for example when your new router has forwarded its first 1 million packets.

The Activate When area allows you to select the event on either the value of the selected variable, or the packet rate for it.

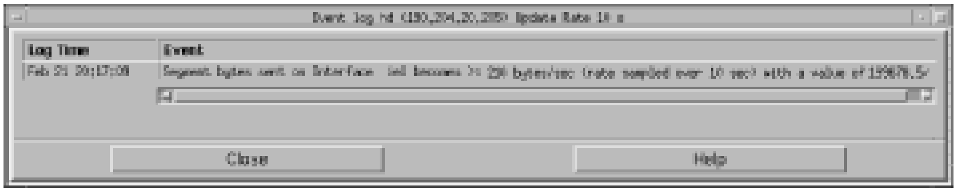
For the variable value you can specify the condition it should trigger on. There are three conditions:

Becomes >= The packet rate or value is greater than or equal to a specified value.

Becomes <= The packet rate or value is less than or equal to the specified value.

Crosses The packet rate or value falls below or rises above the set threshold. This will only trigger when the value or rate is crossed, but not when the rate or value remains above or below the threshold.

In Figure 46, the horizontal line represents the alarm rate being monitored, and the shaded area represents the specified hysteresis zone.



Event log hd (150,204,20,205) Update Rate 10 s

Log Time	Event
Feb 21 20;17;08	Segment bytes sent on Interface (all becomes >= 250 bytes/sec (rate sampled over 10 sec) with a value of 159878.5/

Figure 46. Hysteresis Zone

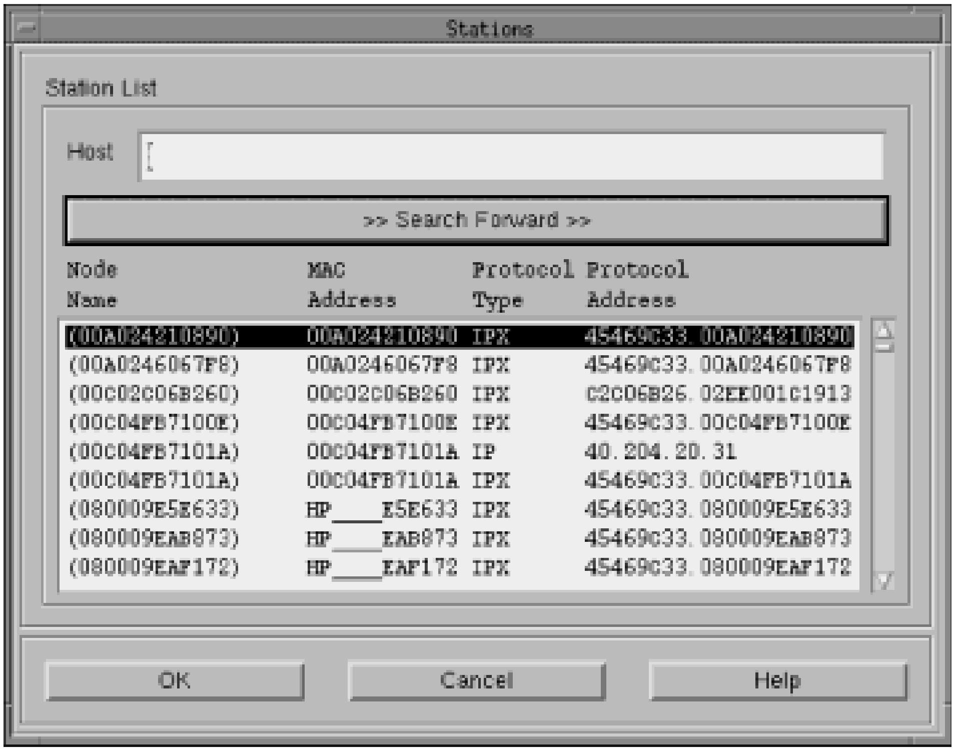
The black line notionally shows the actual network values for the variable setup. For the three condition types detailed above, the following results would be given:

- For an alarm specified as `Becomes >=`, the <u>circles</u> in the diagram show when this event would trigger.
- For an alarm specified as `Becomes <=`, the <u>squares</u> in the diagram show when this event would trigger.
- For an alarm specified as `Crosses`, <u>both the circles and the squares</u> in the diagram show when this event would trigger.

4. To accept the alarm settings in the Alarm Entry Creation dialog box, click **OK**. Your new entry now appears in the Alarm Entries list in the Alarms dialog box.
5. Click **OK** in the Alarms dialog box to set up this alarm condition. When an alarm triggers, an alarm icon will appear in the alarm bar in the main window and a new entry will appear in the Event Log.

Using the Stations Dialog Box

The Station dialog box is used to specify a station for an alarm. Figure 47 on page 97 shows an example of a Stations dialog box.



Node Name	MAC Address	Protocol Type	Protocol Address
(00A024210890)	00A024210890	IPX	45469C33.00A024210890
(00A0246067F8)	00A0246067F8	IPX	45469C33.00A0246067F8
(00C02C06B260)	00C02C06B260	IPX	C2C06B26.02EE001C1913
(00C04FB7100E)	00C04FB7100E	IPX	45469C33.00C04FB7100E
(00C04FB7101A)	00C04FB7101A	IP	40.204.20.31
(00C04FB7101A)	00C04FB7101A	IPX	45469C33.00C04FB7101A
(080009E5E633)	HP____E5E633	IPX	45469C33.080009E5E633
(080009EAB873)	HP____EAB873	IPX	45469C33.080009EAB873
(080009EAF172)	HP____EAF172	IPX	45469C33.080009EAF172

Figure 47. Stations Dialog Box

- To search for a station, enter characters or digits (for instance the first letters of a host name or the first digits of a MAC address) in the Host field. The first occurrence of that string at any point in the station list will be highlighted by a red bar. Continue adding characters or digits to narrow down the search.
- To find the next occurrence of a string, click **Search Forward**. If there is only one occurrence in the list, the red bar will remain on the current entry.

  The search function will search for the contents of the Host field in any column of the list. For example, you may be searching for a host called pear and you type pe in the Host field. The search list would highlight the host opera first. Click **Search Forward** to jump to the next occurrence of the pe string, or narrow the search by adding additional characters or digits to the string in the Host field.
- To select a station, you must click it in the list. The red search bar does not select the highlighted entry.
- Click **OK** or **Cancel** to return to the Alarm Entry Creation dialog box.

]

Chapter 7. Packet Capture and Decode

This chapter tells you how to use the Capture and Decode Applications on Nways Manager Remote Monitor. It contains the following sections:

- Capture and Decode Overview
- Using the Capture Application
- Decoding Captured Packets

Capture and Decode Overview

The Capture Application captures packets from the network using predefined patterns and start and stop conditions. You can setup a library of commonly used configuration criteria by saving each one to file. You can then reuse them on the same device when necessary, or load them onto different devices.

The Decode Application decodes all major protocols and provides a split-window display showing views of packet contents at three levels of detail: summary information, header information, and actual packet content.

With the unique Conversation Trace and Analysis feature, you can click on a specific packet and see all other packets in that conversation.

Packet Structure Overview

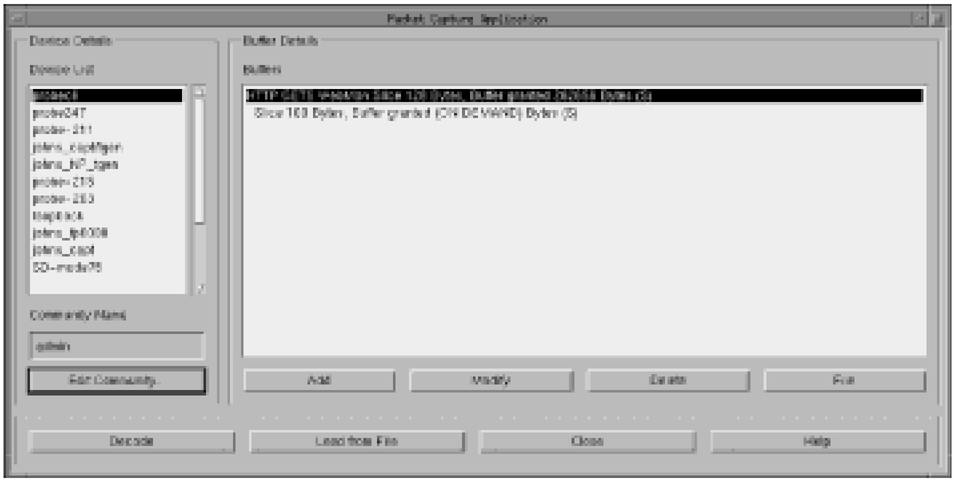
Before you start to set up Capture Buffers, it is important to understand the basic structure of network packets.

Packets are composed of two parts - header and data. The header section contains packet type and protocol information in a standard format. This is the part of the packet on which capture filters operate. The data section has no predefined structure.

The header section of a packet typically contains many different headers. These provide the information for the different layers within the protocol hierarchy. When filling in a template, you need to provide sufficient header information to identify these protocol layers within a packet. We recommend that you consult documentation on the relevant protocol for further details.

Using the Capture Application

You carry out packet capture configuration from the Capture Application dialog box, shown in Figure 48 on page 100. To run the Capture Application, select **Capture** from the Analysis menu, or click **Capture** in the toolbar.



probe8
probe247
probe-211
johns_capbfgen
johns_NP_tgen
probe-215
probe-253
nagtrack
johns_tp8008
johns_capt
SD-mode75

admin

HTTP GETS [illegible] Slice 128 Bytes, Buffer granted 262658 Bytes (S)
Slice 100 Bytes, Buffer granted (ON DEMAND) Bytes (S)

Figure 48. Capture Main Dialog Box

You can carry out the following functions from this dialog box:

- Select the device you want to use to capture packets in the Device Details area.
- Create, modify and save capture buffers, load your own buffers from file or use predefined protocol-specific capture buffers.
- Launch the Decode Application to display captured packets and carry out conversation trace analysis of packet contents.

Working with Capture Buffers

A buffer is the space allocated to the storage of packets as they are captured from the network.

The Buffer Details area allows you to see the names of any predefined capture criteria running on the device and defines who owns these buffers.

In addition, the buffer description contains the following information:

Slice Size Shows the amount of space allocated to each captured packet, followed by the total buffer size.

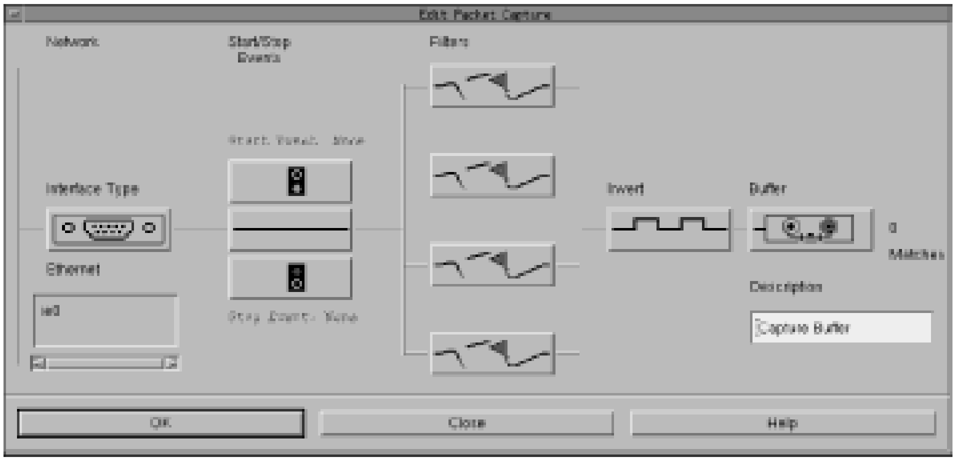
Buffer Size You can also see whether the buffer has space available to hold more packets, denoted by the symbol (S) at the end of the description line, or is full, shown by the symbol (F).

Note: The device only has a limited set of resources to hold buffer data. If one of the buffers uses all of the device’s resources, it will stop the other buffers from storing captured packets. To conserve resources you can choose to slice packets or assign maximum sizes to buffers as described in Creating New Capture Buffers.

Creating New Capture Buffers

You create new capture buffers from the Edit Packet Capture dialog box. To create new capture buffers, follow these steps:

1. Click **Add** in the Capture Application main dialog box to open the Edit Packet Capture dialog box, shown in 49.



ie0

Start Event: None

Stop Event: None

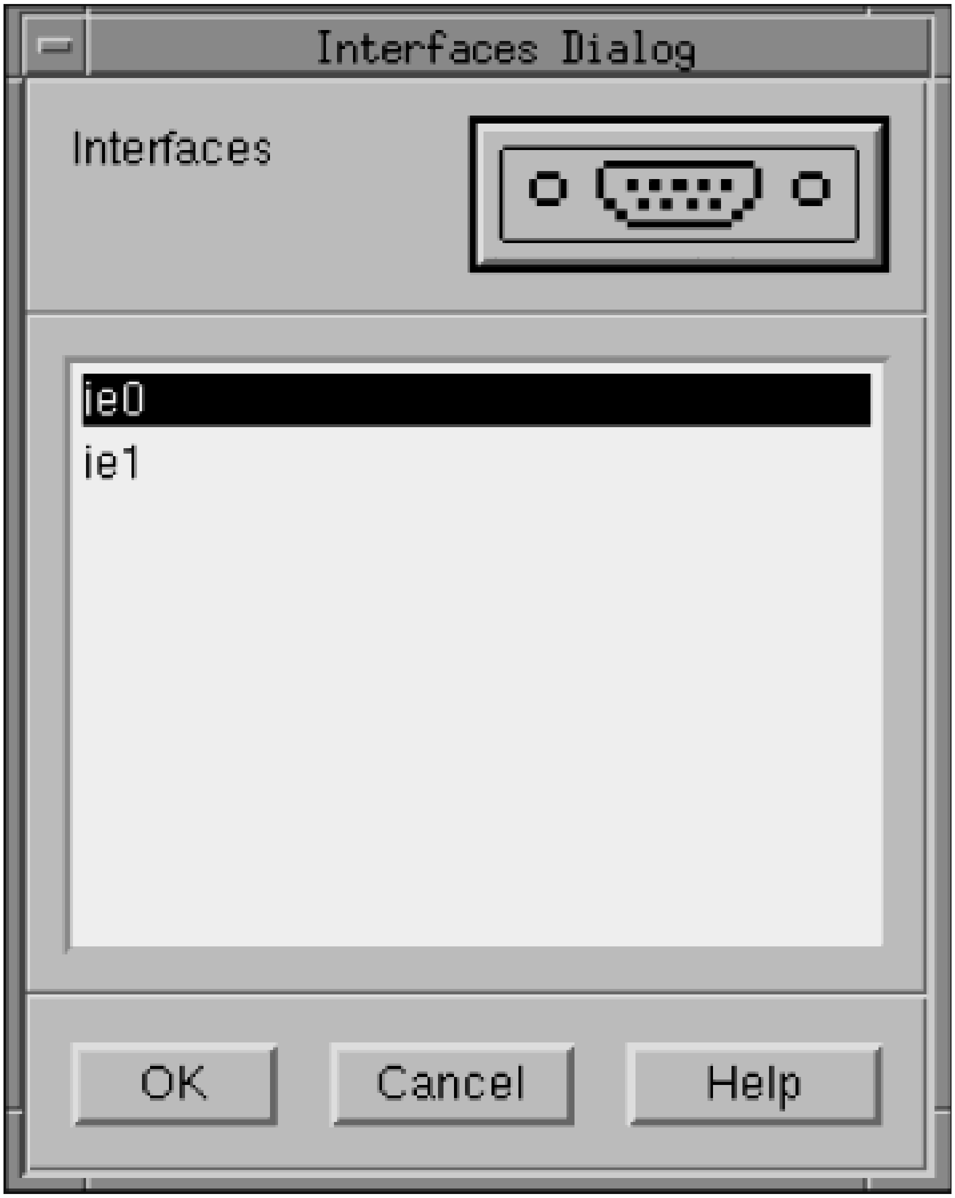
0 Matches

Description

Capture Buffer

Figure 49. Edit Packet Capture Dialog Box

2. Click Interface Type to open the Interfaces dialog box, shown in 50. Use this dialog box to select the interface to be used for packet capture. Click **OK** to return to the Edit Packet Capture dialog box.



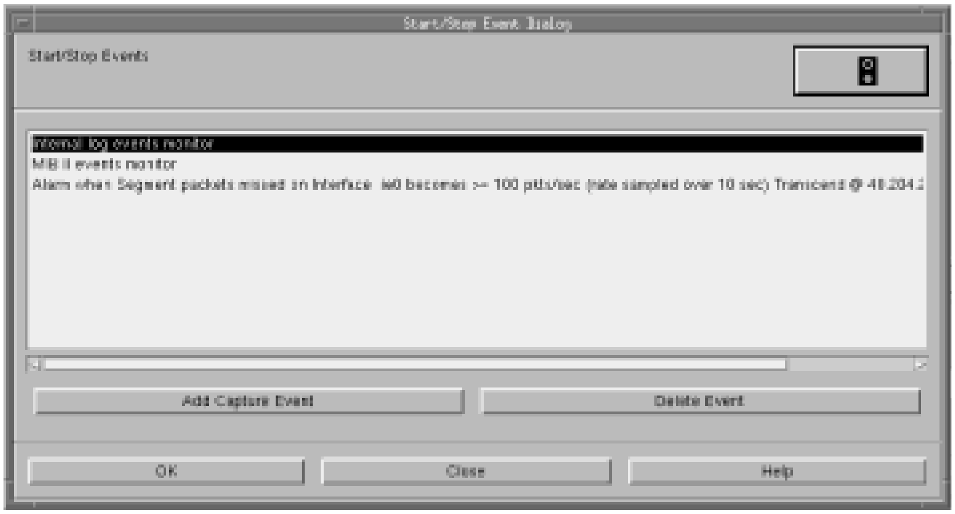
ie0
ie1

Figure 50. Interfaces Dialog Box

3. You may want to start or stop capturing packets automatically whenever a certain Alarm event occurs (for more information, refer to Chapter 6), or whenever a set of packets match a particular pattern. This is called the trigger.

   a. To select a trigger event, follow these steps:

b. Click **Start Event** or **Stop Event** to open the Start/Stop Event dialog box, shown in Figure 51.



Internal log events monitor
MIB II events monitor
Alarm when Segment packets missed on Interface le0 becomes >= 100 pkts/sec (rate sampled over 10 sec) Transcend @ 48.204.2

Figure 51. Start/Stop Events Dialog Box

- To use an Alarm or an existing event, simply select it from the list and click **OK**.
- To add a new capture event, click **Add Capture Event** to open the Edit Start Event or Edit Stop Event dialog box. Refer to “Creating New Start and Stop Events” on page 110.
- To delete a capture event, select it in the Start/Stop Event dialog box and click **Delete Event**. To delete an alarm, you must use the Alarms View.

c. To make the Start Event and/or Stop Event active, click the **Activate** button, located between the Start Event and Stop Event buttons. This will activate either event or both events, as shown in Table 28.

Table 28. Activate Buttons

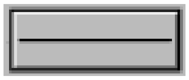
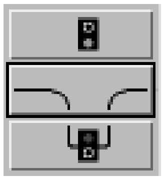
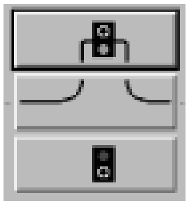
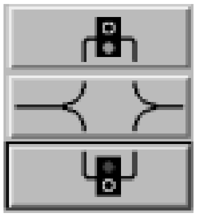
Activate Button	Status	Activate Button	Status
	No start or stop event activated.		Only stop event activated.

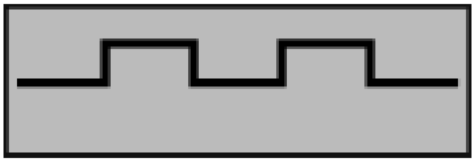
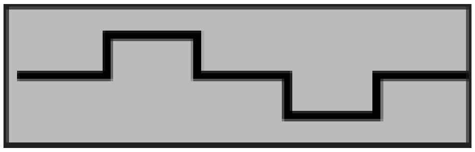
Table 28. Activate Buttons (continued)

Activate Button	Status	Activate Button	Status
	Only start event activated.		Both start and stop event activated.

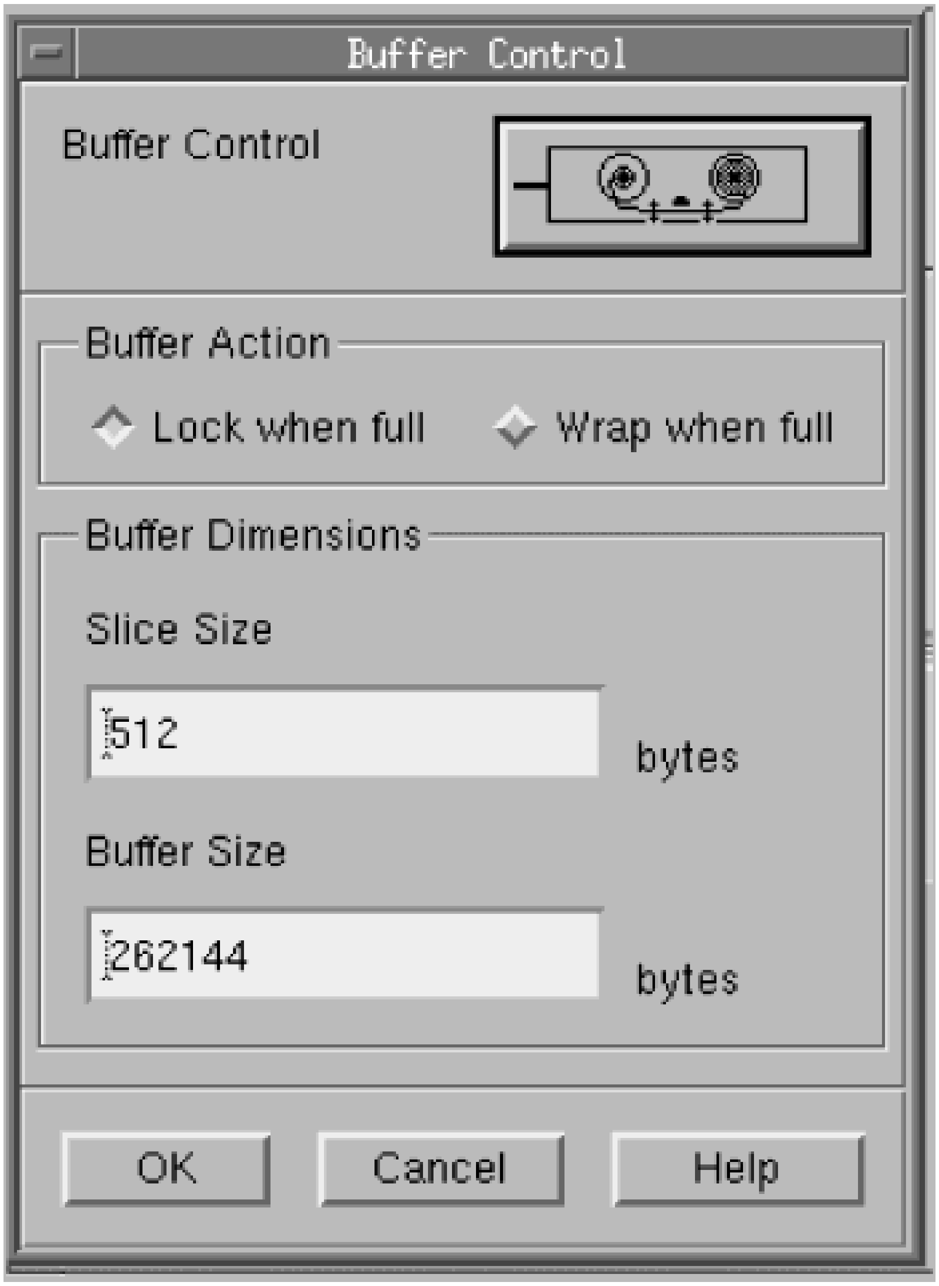
4. Click one of the **Filter** buttons to specify what type of packet you are watching for. You can specify up to four filters by clicking any of the Filter buttons. Refer to "Using the Filter Editor" on page 111 for details.

5. Click **Invert** (Table 29) if required to invert the logic of the channel.

Table 29. Invert Button

Invert Button	Description
	Collects the specified packets.
	Collects everything except the specified packets.

6. Click **Buffer** to specify how you would like the buffer to behave when storing packets. The Buffer Control dialog box opens, as shown in Figure 52 on page 105.



Slice Size 512 bytes

Buffer Size 262144 bytes

Figure 52. Buffer Control Dialog Box

a. Use the fields on the Buffer Control dialog box to specify how to store packets on the device.

Wrap Captures packets continuously, throwing away old packets when the buffer is full.

Lock Stops capturing once the buffer is full.

Slice Size Indicates how much of the packet to capture - depending on the amount of information you want to gather, keep this as small as is reasonable - however, ensure you have a large enough sample for the Decode application to work on. The larger the slice size the quicker the buffer will fill up.

Buffer Size Lets you specify the size of the capture buffer in bytes. If you wish the device to allocate as much memory as is available, set this value to be -1. This will show the buffer as being `ON DEMAND` in the Buffers list.

b. Click **OK** to return to the Edit Packet Capture dialog box.

7. Enter a name for your capture configuration in the Event Description field. If you have set it up to capture all TCP/IP packets for example, you might call it `TCP Buffer`.
8. Click **OK** to create this new capture buffer on the selected device.

Saving a Capture Buffer

When you have configured a capture buffer and it appears in the Buffers list in the Packet Capture Application dialog box (Figure 48 on page 100), you can save the buffer to file and reload it onto any device at a later date. To save a capture buffer, follow these steps:

1. Select a buffer entry in the list.
2. Click **File** in the Buffer Details area to open the Buffer Save/Load dialog box, as shown in Figure 53 on page 108.
3. Click **Save**.
4. Enter a file name in the Selection area.
5. Click **OK** to save the file or **Cancel** to abandon the save.

Modifying Capture Buffers

You can modify existing capture buffers at any time as your requirements change. To modify a capture buffer, follow these steps:

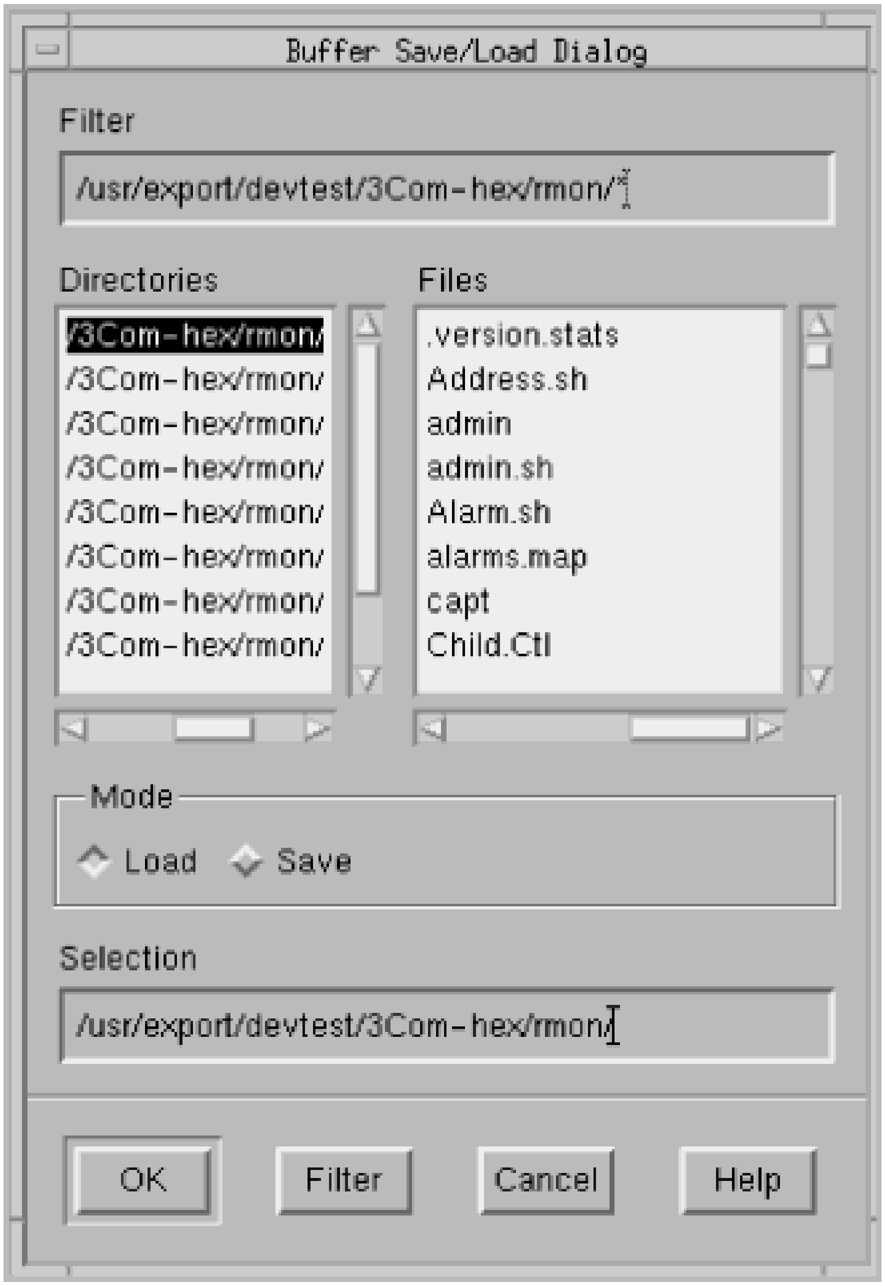
1. Select a buffer entry in the list.
2. Click Modify in the Buffer Details area to open the Edit Packet Capture dialog box, as shown in Figure 49 on page 101.
3. Follow the procedures from step 6 onwards in “Creating New Capture Buffers” on page 101 to make changes to the existing capture configuration.
4. Click **OK** in the Edit Packet Capture dialog box to accept your changes, or **Cancel** to abandon them.

Working with Predefined Capture Buffers

Nways Manager Remote Monitor simplifies setting up capture buffers by providing a number of predefined protocol-specific buffers. The filter templates in these buffers are preconfigured with the header information required for each of the protocol layers. These buffers can be loaded from file and then modified as required.

To load a predefined capture buffer, follow these steps:

1. In the Capture Application main dialog box, click **File** in the Buffer Details area to open the Buffer Save/Load dialog box, as shown in Figure 53 on page 108.



Filter: /usr/export/devtest/3Com-hex/rmon/*

Directories:
/3Com-hex/rmon/
/3Com-hex/rmon/
/3Com-hex/rmon/
/3Com-hex/rmon/
/3Com-hex/rmon/
/3Com-hex/rmon/
/3Com-hex/rmon/
/3Com-hex/rmon/

Files:
.version.stats
Address.sh
admin
admin.sh
Alarm.sh
alarms.map
capt
Child.Ctl

Selection: /usr/export/devtest/3Com-hex/rmon/

Figure 53. Buffer Save/Load Dialog Box

2. Locate the predefined buffers by doing one of the following:
   - Enter

     `/usr/LANReMon/rmon/vi_chans/*`

  in the Filter field.

- Use the Directories list to locate the

  ```
  /usr/LANReMon/rmon/vi_chans
  ```

  directory.

3. Select a predefined buffer from the Files list. The list of predefined filters will vary according to the media type of the selected physical interface, as shown in Table 30.

Table 30. Predefined Filters Description

Filter	Media Type			Description
	Ethernet	**Token Ring**	**FDDI**	
AppleTalk	■	■	■	Pass AppleTalk packets only
FTP	■	■	■	Pass FTP packets only
ICMP	■	■	■	Pass ICMP packets only
IP	■	■	■	Pass IP packets only
LLC Frames		■		Pass LLC packets only
MAC Frames		■		Pass MAC packets only
Netware	■	■	■	Pass Netware packets only
NFS	■	■	■	Pass NFS packets only
Non-SNMP	■	■	■	Pass all packets except SNMP
SMTP	■	■	■	Pass SMTP packets only
SNMP	■	■	■	Pass SNMP packets only
TCP	■	■	■	Pass all TCP packets
Telnet	■	■	■	Pass Telnet packets only
UDP	■	■	■	Pass all UDP packets
WWW	■	■	■	Pass WWW packets only
XNS	■			Pass XNS packets only

4. Click **Load**.

5. Click **OK** to load this buffer, or **Cancel** to abandon, and return to the Capture Application main dialog box.

   If you clicked **OK**, the capture buffer will be displayed in the Buffer Details area.

   Select the capture buffer and click **Modify** in the Buffer Details area to open the Edit Packet Capture dialog box, shown in Figure 49 on page 101.

6. Follow the steps in “Creating New Capture Buffers” on page 101.

Loading Capture Buffers from File

If you have previously saved a capture buffer to file, you can load it onto any device at a later date. The selected interface on the destination device must be of the same media type as the original interface on which the buffer was created.

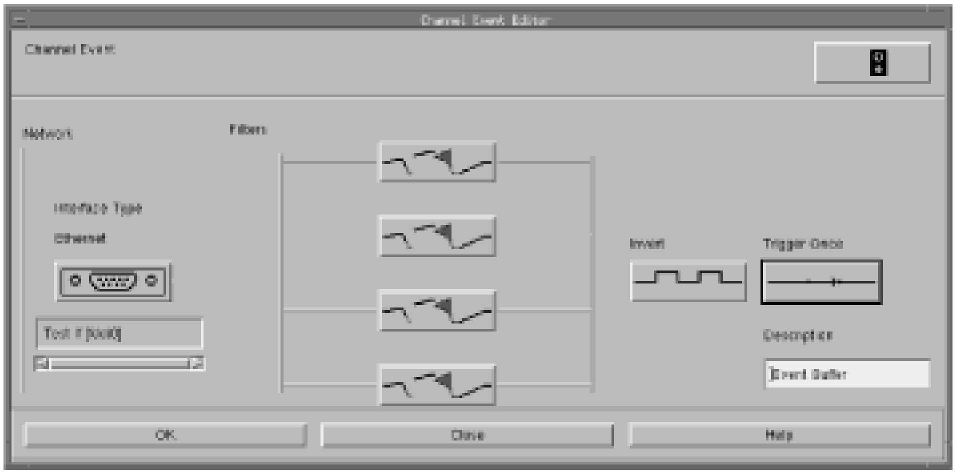
1. In the Device area, select the device that the buffer is to be loaded onto.
2. Click **File** in the Buffer Details area to open the Buffer Save/Load dialog box (53).
3. Select the buffer file you want to use.
4. Click **Load**.
5. Click **OK** to load the file or **Cancel** to abandon the load.Click **OK** to load the file or **Cancel** to abandon the load.

The buffer is loaded directly onto the device. When this is complete, the buffer entry appears in the Buffers list in the Capture Application main dialog box.

Creating New Start and Stop Events

To create a trigger that will start or stop the collection of packets from the network:

1. Click **Add** in the Capture main dialog box to display the Edit Packet Capture dialog box.
2. Click either **Start Event** or **Stop Event** to display the list of alarms and events available.
3. Click **Add Capture Event** to open the Channel Event Editor dialog box (Figure 54 on page 111).



Interface Type

Ethernet

Description

Event Buffer

Figure 54. Channel Event Editor Dialog Box

Use this dialog box to create a new set of capture criteria and store it under its own event name. Using events in this way allows you set up more detailed trigger conditions than are possible using Alarms alone.

4. Click Interface Type to open the Interfaces dialog box and specify the interface on the device you would like to use.

   This does not have to be the same as the interface you will be capturing on - so you might watch for a particular packet or type of packet on one interface, then start capturing on another.
5. Click one of the Filter buttons to specify what type of packet you are watching for. You can specify up to four filters by clicking any of the Filter buttons. This is covered in “Using the Filter Editor”.
6. If required, click **Invert** to invert the logic of the original operation.
7. Click trigger to set the trigger. Trigger Once means that only one event will be generated. Trigger Many means that an event will be generated every time a packet passes the channel.
8. Enter a name for this event in the Description field.
9. Click **OK** to save this new event. It now forms part of your own event library.

Using the Filter Editor

The Filter Editor allows you to capture anything from a certain type of packet right down to a specific packet itself. You can specify up to four filters to run simultaneously on each packet.

Nways Manager Remote Monitor’s Capture Application comes with a number of protocol templates ready for use. Each of these templates is designed to let you specify the type of packets you want to filter from the network. A wide variety of protocol families are supported.

Using Wildcards in Filter Templates

When filling in templates, you can use an X as a wildcard. For example, imagine you are trying to capture all packets issued by Sun workstations on your network. Because you know that all Sun products have a vendor prefix of

```
080020
```

in their MAC address, you might fill in the Source Address field with `080020XXXXXX`.

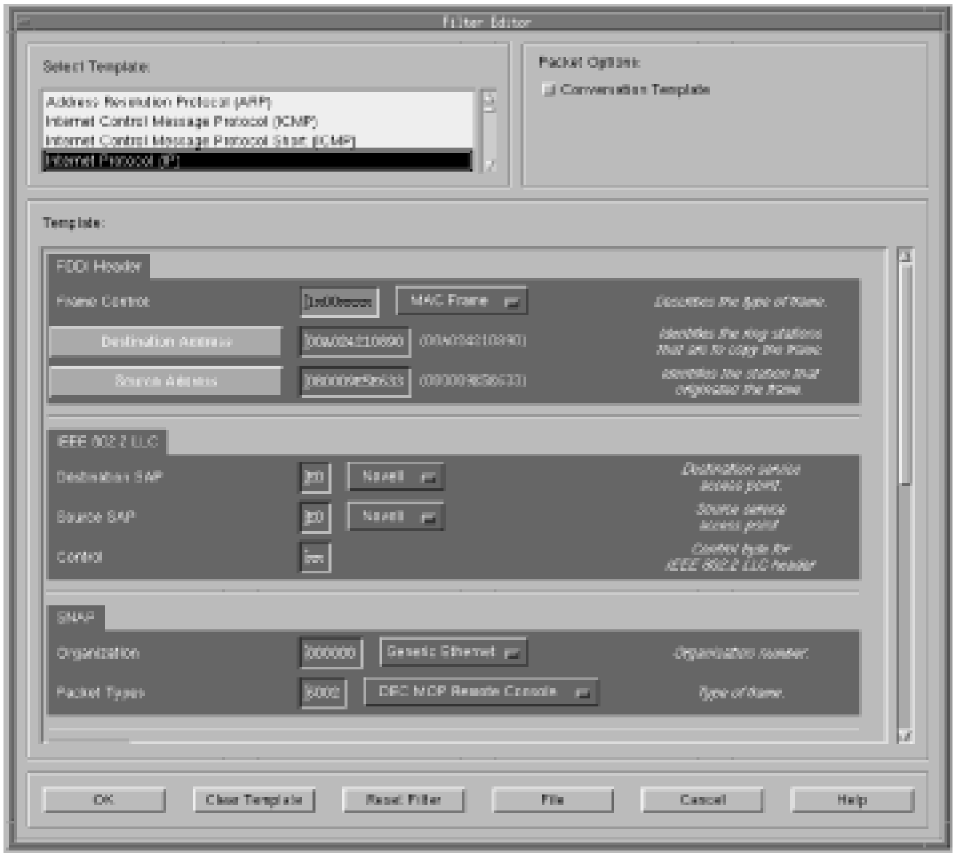
Setting Up a Filter

To set up a filter, follow these steps:

1. Click **Filter** in the Edit Packet Capture dialog box to bring up the Filter Editor, as shown in Figure 55 on page 113.

   The Filter Editor offers a selection of protocol templates from which you can choose. The list of templates varies according to the media type of the selected interface.

   Note: You must fill in the relevant fields for each of the header types. This ensures that Nways Manager Remote Monitor filters the correct packet type.



□ Conversation Template

Frame Control: 1x00xxxxx — MAC Frame — Describes the type of frame.

Destination Address: 00A024210890 (00A024210890) — Identifies the ring stations that are to copy the frame.

Source Address: 08000098586633 (08000098586633) — Identifies the station that originated the frame.

Destination SAP: E0 — Novell — Destination service access point.

Source SAP: E0 — Novell — Source service access point

Control: [illegible] — Control byte for IEEE 802.2 LLC header

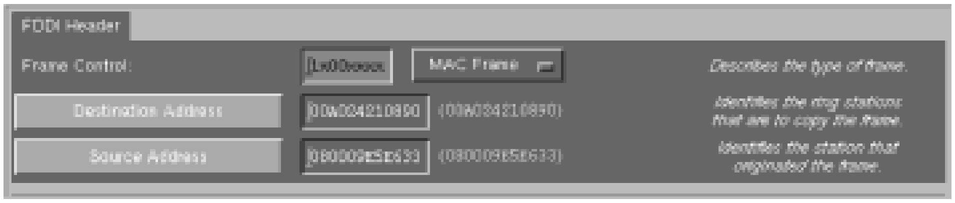
Organization: 000000 — Generic Ethernet — Organization number.

Packet Types: 6002 — DEC MOP Remote Console — Type of frame.

Figure 55. Filter Editor Dialog Box

2. Choose the required template from the Select Template area.
3. In the Packet Options area, click the **any size**or **any packets** popups to set general packet constraints, such as the length of the packet, or whether the packet has a CRC error or is well formed. The size and type conditions are combined using a logical AND.
4. The templates provide source and destination fields to capture traffic from one address to another at network and device level. However, with Conversation Template enabled, the application will capture traffic going in both directions between the specified points.

   For example, destination and source MAC addresses are entered in the Ethernet Header area of an Internet Protocol template, as shown in Figure 56 on page 114.



FDDI Header

Frame Control: 1x00xxxx MAC Frame — Describes the type of frame.

Destination Address 00A024210890 (00A024210890) — Identifies the ring stations that are to copy the frame.

Source Address 080009E5E633 (080009E5E633) — Identifies the station that originated the frame.

Figure 56. Entering Destination and Source MAC Addresses

The application will capture traffic directed from source to destination address.

Note: When activated, the Conversation Template will invert addresses at any point in the filter template.

The Capture Application simplifies the process of entering Destination and Source addresses by providing a list of available stations. Click Destination Address or Source Address to open the Stations dialog box. This procedure is described in “Using the Stations Dialog Box” on page 96.

5. Complete the rest of the Filter Editor dialog box. The fields displayed vary from protocol to protocol and are color-coded as shown in Table 31:

Table 31. Field Type Color-coding Field

Field Type	Color
Binary	Green
Decimal	Pink
Hexadecimal	Purple

In some cases a field may have a popup menu for you to choose from.

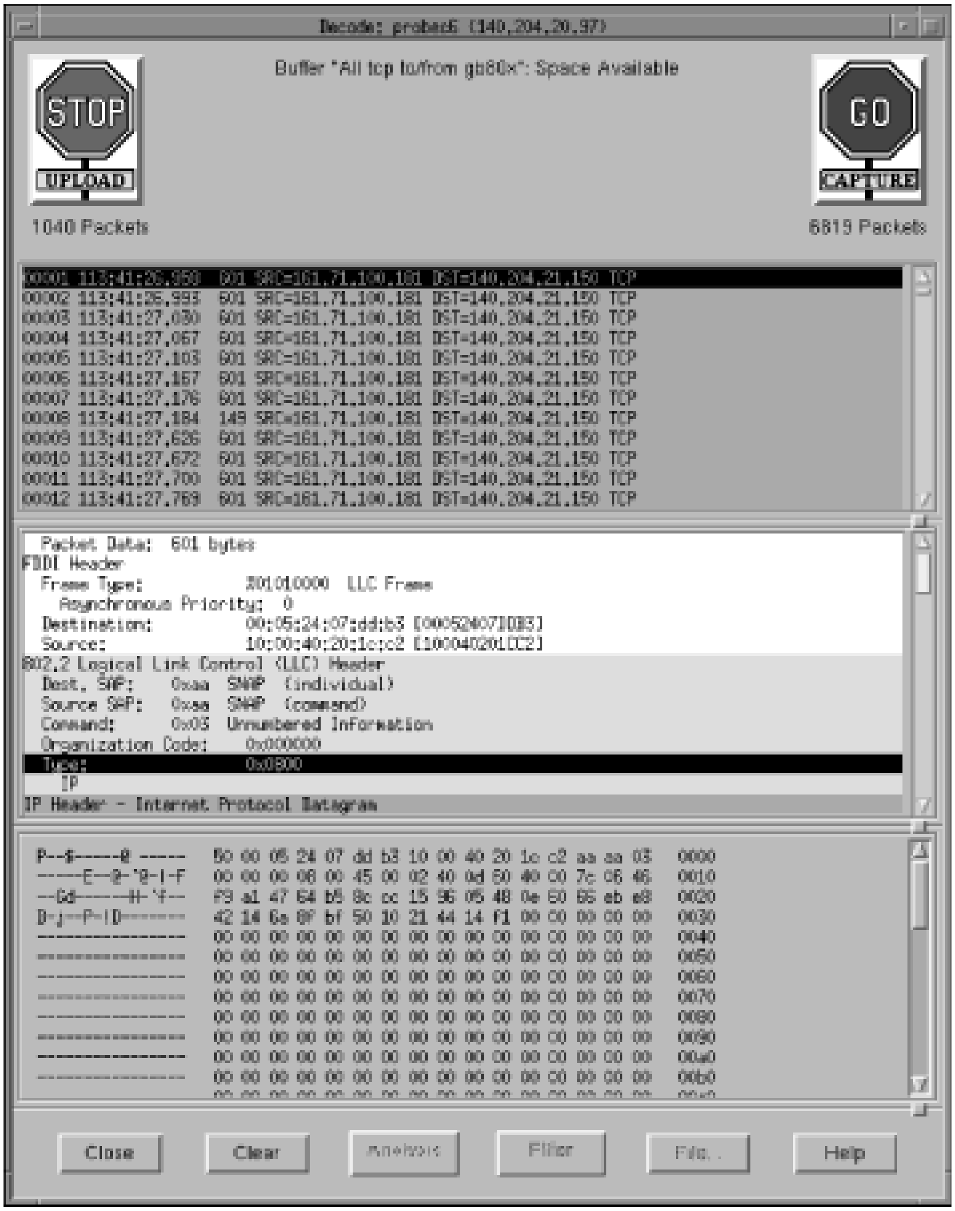
6. Click **OK** to make this filter active.

Using the Stations Dialog Box

The Stations dialog box is used to specify a station as a Source or Destination address. Refer to “Using the Stations Dialog Box” on page 96.

Decoding Captured Packets

To display the packets you have captured, click Decode in the Capture main dialog box and the Decode dialog box opens, as shown in Figure 57 on page 115.



Buffer "All tcp to/from gb80x": Space Available

1040 Packets

6815 Packets

```
00001 113:41:26.958  601 SRC=161.71.100.181 DST=140.204.21.150 TCP
00002 113:41:26.993  601 SRC=161.71.100.181 DST=140.204.21.150 TCP
00003 113:41:27.030  601 SRC=161.71.100.181 DST=140.204.21.150 TCP
00004 113:41:27.067  601 SRC=161.71.100.181 DST=140.204.21.150 TCP
00005 113:41:27.103  601 SRC=161.71.100.181 DST=140.204.21.150 TCP
00006 113:41:27.167  601 SRC=161.71.100.181 DST=140.204.21.150 TCP
00007 113:41:27.176  601 SRC=161.71.100.181 DST=140.204.21.150 TCP
00008 113:41:27.184  149 SRC=161.71.100.181 DST=140.204.21.150 TCP
00009 113:41:27.626  601 SRC=161.71.100.181 DST=140.204.21.150 TCP
00010 113:41:27.672  601 SRC=161.71.100.181 DST=140.204.21.150 TCP
00011 113:41:27.700  601 SRC=161.71.100.181 DST=140.204.21.150 TCP
00012 113:41:27.769  601 SRC=161.71.100.181 DST=140.204.21.150 TCP
```

```
  Packet Data:  601 bytes
FDDI Header
  Frame Type:            01010000  LLC Frame
    Asynchronous Priority:  0
  Destination:           00:05:24:07:dd:b3 [00052407DDB3]
  Source:                10:00:40:20:1c:c2 [100040201CC2]
802.2 Logical Link Control (LLC) Header
  Dest. SAP:     0xaa  SNAP  (individual)
  Source SAP:    0xaa  SNAP  (command)
  Command:       0x03  Unnumbered Information
  Organization Code:     0x000000
  Type:                  0x0800
    IP
IP Header - Internet Protocol Datagram
```

```
P--$-----@ -----     50 00 05 24 07 dd b3 10 00 40 20 1c c2 aa aa 03    0000
-----E--@-'@-|-F     00 00 00 08 00 45 00 02 40 0d 60 40 00 7c 06 46    0010
--Gd------H-'f--     f9 a1 47 64 b5 8c cc 15 96 05 48 0e 60 66 eb e8    0020
B-j--P-!D-------     42 14 6a 8f bf 50 10 21 44 14 f1 00 00 00 00 00    0030
----------------     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    0040
----------------     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    0050
----------------     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    0060
----------------     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    0070
----------------     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    0080
----------------     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    0090
----------------     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    00a0
----------------     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    00b0
```

Figure 57. Decode Dialog Box

The Decode Application dialog box is split into three views so that you can view detailed information about a given packet.

- The top view provides a summary decode of packets. Select the required packet here.
- The middle view provides a detailed decode of the selected packet.

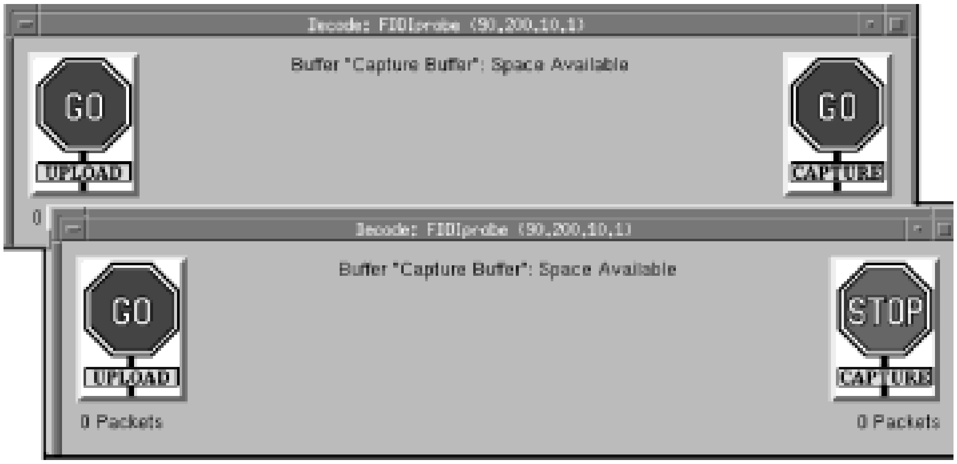
- The bottom view displays the selected packet in hex format.

Each protocol is color-coded for easy identification. (A complete list of supported decodes is given in Appendix D.).

You can resize each of the views to suit your own requirements. Click and drag the sashes at the bottom right hand corner of each pane to resize the view.

Capturing Packets Using the Decode Application

This dialog box allows you to control when the device should start or stop capturing packets and when to upload the captured packets for analysis. Capture controls when packet capture starts and stops on the device (Figure 58).



Decode: FDDIprobe (90.200.10.1)

Buffer "Capture Buffer": Space Available

Decode: FDDIprobe (90.200.10.1)

Buffer "Capture Buffer": Space Available

0 Packets

0 Packets

Figure 58. Capture Button

To capture packets, follow these steps:

1. Click **Go Capture** and Nways Manager Remote Monitor clears the existing buffer contents from the device, resets any capture triggers set and starts capturing a completely fresh set of packets. Previously uploaded packets are unaffected. The button will toggle to **Stop Capture**. The total number of captured packets is shown beneath the button.
2. To stop capturing packets, click **Stop Capture**.

Uploading Packets Using the Decode Application

1. To upload packets from the capture buffer on a device, follow these steps: Upload starts or stops the uploading of packets from the device. Click **Go Upload** and Nways Manager Remote Monitor will start adding packets from the capture buffer to the list of packets loaded in the Decode dialog box. The button will toggle to **Stop Upload**.

The number of packets that have been uploaded is shown beneath Upload. As the application uploads more packets into the dialog box, you will notice the slider bar in the top dialog box shortening to reflect this.

2. To stop the upload of packets from the device, click **Stop Upload**.

   Note: If Nways Manager Remote Monitor loses contact with the device during packet upload, you will be asked if you want to try to contact the device again. Click **Retry** and Nways Manager Remote Monitor will try to contact the device. The Retry dialog box will be displayed until Nways Manager Remote Monitor is able to contact the device or until you cancel the upload attempt.

3. At any time, you can empty the contents of the Decode dialog box by clicking **Clear**.

Post-Capture Filtering

When you have uploaded captured packets, you can filter these packets even further to search for any subset of the captured data.

1. Click **Filter** in the Decode dialog box and select **Specify** to open the Channel Editor.
2. The interface and channel settings are set automatically and cannot be changed.
3. From the Channel Editor, you can then specify up to four filters by clicking one of the Filter buttons. Refer to “Using the Filter Editor” on page 111 for instructions on setting up a filter.
4. Click **Invert** if desired, to invert the logic of the channel.
5. Click **OK** to start the packet filtering and return to the Decode dialog box, where only packets meeting your filter specifications will be displayed. The number of filtered packets is displayed beneath the buffer description in the header area.
6. To abandon the post-filtering and return to the original display of packets, click **Filter** and select **Reset**.

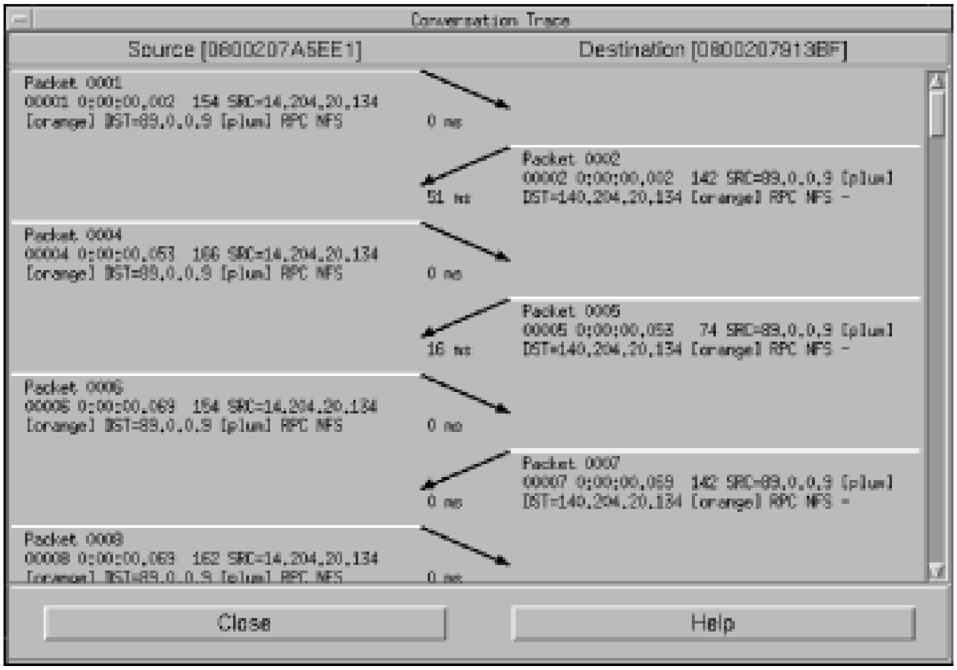
Conversation Trace and Analysis

Some packet displays show conversations between machines on the network. Use Conversation Trace and Analysis to focus on those displays in more detail.

1. Select the packet from sthe top view in the Decode dialog box.
2. Click **Analysis**. This allows you to select a time-stamped trace of the conversation based on either the MAC addresses or IP addresses.

   Note: The IP layer conversation is particularly useful if your IP hosts are on different sides of a router and the router’s MAC address is in the packet.

3. Nways Manager Remote Monitor then uses the packet selected in the summary view as the key to the conversation you want to watch. The packets involved in that conversation are filtered out and displayed in the Conversation Trace dialog box, shown in Figure 59 on page 118.



```
Source [0800207A5EE1]                                   Destination [0800207913BF]

Packet 0001
00001 0:00:00.002  154 SRC=14.204.20.134
[orange] DST=89.0.0.9 [plum] RPC NFS          0 ms
                                                   Packet 0002
                                                   00002 0:00:00.002  142 SRC=89.0.0.9 [plum]
                                              51 ms DST=140.204.20.134 [orange] RPC NFS -
Packet 0004
00004 0:00:00.053  166 SRC=14.204.20.134
[orange] DST=89.0.0.9 [plum] RPC NFS          0 ms
                                                   Packet 0005
                                                   00005 0:00:00.053   74 SRC=89.0.0.9 [plum]
                                              16 ms DST=140.204.20.134 [orange] RPC NFS -
Packet 0006
00006 0:00:00.069  154 SRC=14.204.20.134
[orange] DST=89.0.0.9 [plum] RPC NFS          0 ms
                                                   Packet 0007
                                                   00007 0:00:00.069  142 SRC=89.0.0.9 [plum]
                                              0 ms  DST=140.204.20.134 [orange] RPC NFS -
Packet 0008
00008 0:00:00.069  162 SRC=14.204.20.134
[orange] DST=89.0.0.9 [plum] RPC NFS          0 ms
```

Figure 59. Conversation Trace Dialog Box

The Conversation Trace dialog box highlights the relationship between packets in the selected conversation. It provides an overall view of the conversation.

The times beneath the arrows in the centre of the view show the inter-packet delays in milliseconds.

An interesting point to look for is packets being sent by one side repeatedly before the other responds - this can point to congestion problems.

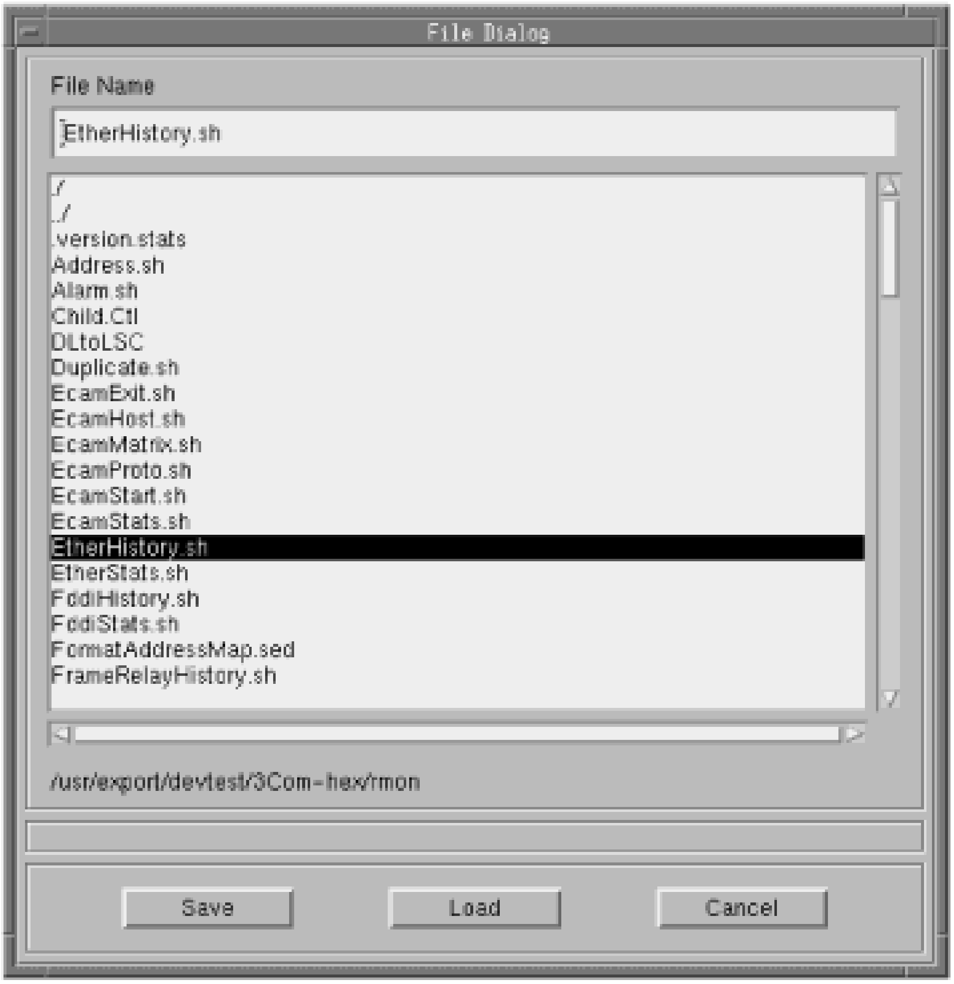
Saving and Loading Captured Packets

The following sections tell you how to save and load packet samples.

Saving Packets

To save a packet sample, follow these steps:

1. Click **File** in the Decode dialog box (Figure 57 on page 115) to open the File dialog box. Figure 60 on page 119 shows an example of the File dialog box.



EtherHistory.sh

```
./
../
.version.stats
Address.sh
Alarm.sh
Child.Ctl
DLtoLSC
Duplicate.sh
EcamExit.sh
EcamHost.sh
EcamMatrix.sh
EcamProto.sh
EcamStart.sh
EcamStats.sh
EtherHistory.sh
EtherStats.sh
FddiHistory.sh
FddiStats.sh
FormatAddressMap.sed
FrameRelayHistory.sh
```

/usr/export/devtest/3Com-hex/rmon

Figure 60. File Dialog Box

2. You can save the packets in the following file formats:

   Network General Sniffer
   The resulting file can be loaded into a Network General Sniffer.

   ASCII The resulting file can be loaded into a text editor or printed.

   Attention: Because ASCII files can be very large, ensure that you have sufficient disk space before saving the packets in ASCII format.

   W&G DA-30 Capture File
   The file can be loaded into a Wandel & Goltermann DA-30 analyzer.

   Note: FDDI is not supported on DA-30 analyzer.

Nways Manager Remote Monitor
The file can be loaded back into the Packet Decode dialog box for further analysis.

3. Type a filename into the File Name area, then click **Save**.

Loading Packet Samples

To load a packet sample you saved earlier, repeat the above process but click **Load** instead of **Save** in step3. This allows you to load in packets which were previously saved with this application in Nways Manager Remote Monitor format, from a Network General Sniffer or a Wandel & Goltermann DA-30 analyzer.

Chapter 8. Additional Nways Manager Remote Monitor Functionality

This chapter looks at the additional functionality available with Nways Manager Remote Monitor. It contains the following sections:

- Address Mapping
- Protocol Distribution
- Data Export Application
- Using the Data Collector Application

Address Mapping and Protocol Distribution can either run with SmartAgent software or with RMON2. For instructions on how to enable SmartAgent Applications, refer to “Downloading SmartAgent Software” on page 179. Roving Analysis Port Application and Using PACMIB Functionality are discussed in Appendix E.

Address Mapping

The Address Map application displays tables which show mappings of MAC addresses and network layer addresses. Nways Manager Remote Monitor uses these tables to translate the addresses into names. For information on Address Translation, refer to “Setting the Address Translation Level” on page 43.

You must be using one of the following to view this application:

- An RMON2-compliant device.
- An RMON device with RMON2 (ECAM) SmartAgent software loaded.

Functionality

The Address Map application allows you to do the following:

- View the address map tables for the current device.
- Check for duplicate addresses in the device’s address map table. This could, for example, immediately highlight a networking problem if two devices have the same IP address. This table is only available if you are using an RMON device with RMON2 (ECAM) SmartAgent software downloaded.

Viewing Address Map Tables

To display the Address Map tables:

1. Select **Address Map** from the Analysis menu.
2. Select either **Address Table** or **Duplicate Addresses**. Address Map data will be retrieved from the device and displayed as a table.
3. To export the contents of the tables, click **Export** to open the Data Export dialog box and refer to “Protocol Distribution” on page 123.

4. To close the table display, click **Close**.

Address Table

The address table indicates the mapping between MAC address and network layer address, and is used for name translations. Its display differs depending on whether you are using an RMON2-compliant probe or a device with RMON2 (ECAM) SmartAgent downloaded.

Using an RMON2-compliant Device

The RMON2 Address Map Table contains the following information:

PhysicalAddress
This is the MAC address of the station.

ProtocolName
The address type.

NetworkAddress
The network address of the station.

Interface
Indicates which interface last received data from this address.

LastChange
The time, measured from when the device was last reset, that this table entry last changed.

Using RMON2 (ECAM) SmartAgent Software

The RMON2 (ECAM) SmartAgent software Address Map Table contains the following information:

MacAddress
The MAC address of the station.

NetAddrType
The address type.

ChangeRate
Each entry has a change rate variable to indicate which stations have multiple protocol addresses for a single MAC address. Any devices with a high change rate are usually routers and are identified by `RTR=` in front of the MAC address.

NetAddress
The network address of the station.

IsDuplicate
Lists stations where more than one MAC address has been assigned the same network layer address. These stations are marked in red. This occurrence is

usually regarded as an error which might arise from someone assigning the same protocol address to two machines.

Name The name of the station.

Duplicate Addresses Table

This table is available on devices with RMON2 (ECAM) SmartAgent software downloaded.

It compiles a list of all stations marked as duplicates in the Address Table, making it easy to see them at a glance.

Protocol Distribution

The Protocol Distribution application shows the types of traffic that are present on the LAN segment being monitored by the selected device. The Protocol Distribution application allows you to do the following:

- Display Protocol Distribution data as a table, bar graph or pie chart.
- Print the contents of a Protocol Distribution graph to file or direct to a printer.
- Export the contents of a Protocol Distribution table to another application as an ASCII or CSV format file.

Attention:: You must be using one of the following devices to view this application:

- An RMON2-compliant device.
- An RMON device with RMON2 (ECAM) SmartAgent software loaded.

Displaying Protocol Distribution Data

To display protocol distribution data, follow these steps:

1. Select **Protocol Distribution** from the Analysis menu and then **Table** or **Graph**. If you choose Graph, select one of the graph types.
2. After a short delay, Protocol Distribution data is loaded from the device and displayed in the selected format.
3. To close the display, click **Close**.

Working with Protocol Distribution Data

The Protocol Distribution display allows you to:

Export the contents of a table display
Select **Export** from the Option menu. Data can be saved in either ASCII or CSV format.

Export the contents of a graph display

Select **Print** from the Option menu. Activate the **To File** option and graph will be saved as Postscript. Refer to "Setting Print Preferences" on page 68 for more information on using the Print dialog box.

Print graph data

Select **Print** from the Option menu. Activate the **To Printer** option and specify the correct printer settings.

Update the displayed data

Click **Update**.

Display Options

Each display type has a number of available options. The functions provided for each of the display types are shown in Table 32.

Table 32. Display Options

Display Options	Description
Export	For Table displays, this function saves data to file for export to other applications or for printing. The data may be saved in either Flat ASCII or Comma Separated Variable file format. Selecting this option displays a file dialog box allowing the data format and file name to be specified.
Print	For Graph displays, this function allows graphs to be printed on a Postscript printer. Selecting this option displays a print dialog box allowing the user to designate a printer to send the data to or a file to save the data in and the paper layout and size.
Grid On/Off	For Graph displays, this function toggles the display of grid lines on the graphs.
Display Style	For Graph displays, the data can be displayed as either a bar graph, stacked bar graph or pie chart. Selecting one of these options changes the current display style.

Data Export Application

The Data Export Application lets you select a specific RMON statistical group to view and export from the device as an ASCII or CSV format file.

The groups available are:

Statistics	Ethernet, Token Ring, FDDI.
History	Ethernet, Token Ring, FDDI.
Host	Predefined host variables.
Matrix	Source to Destination or Destination to Source.

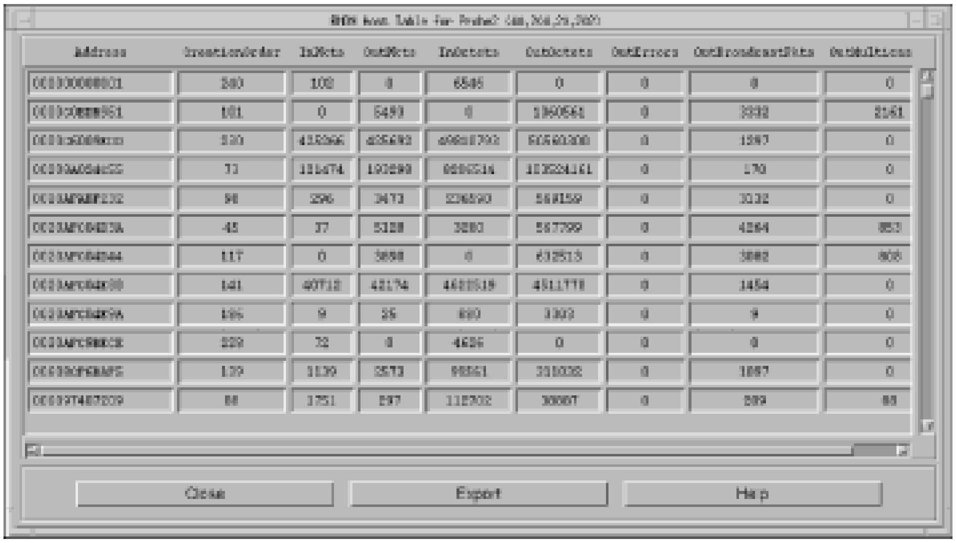
For the Statistics and History groups, the following Token Ring data can be selected:

Token Ring Statistics
Promiscuous, MAC Layer, Source Routing, Ring Station Control and Ring Station Table.

Token Ring History
Promiscuous and MAC Layer.

To display data:

1. Select a data group from the **Export** menu in the Nways Manager Remote Monitor menu bar. The selected data is loaded from the device and displayed as a table, as shown in Figure 61.

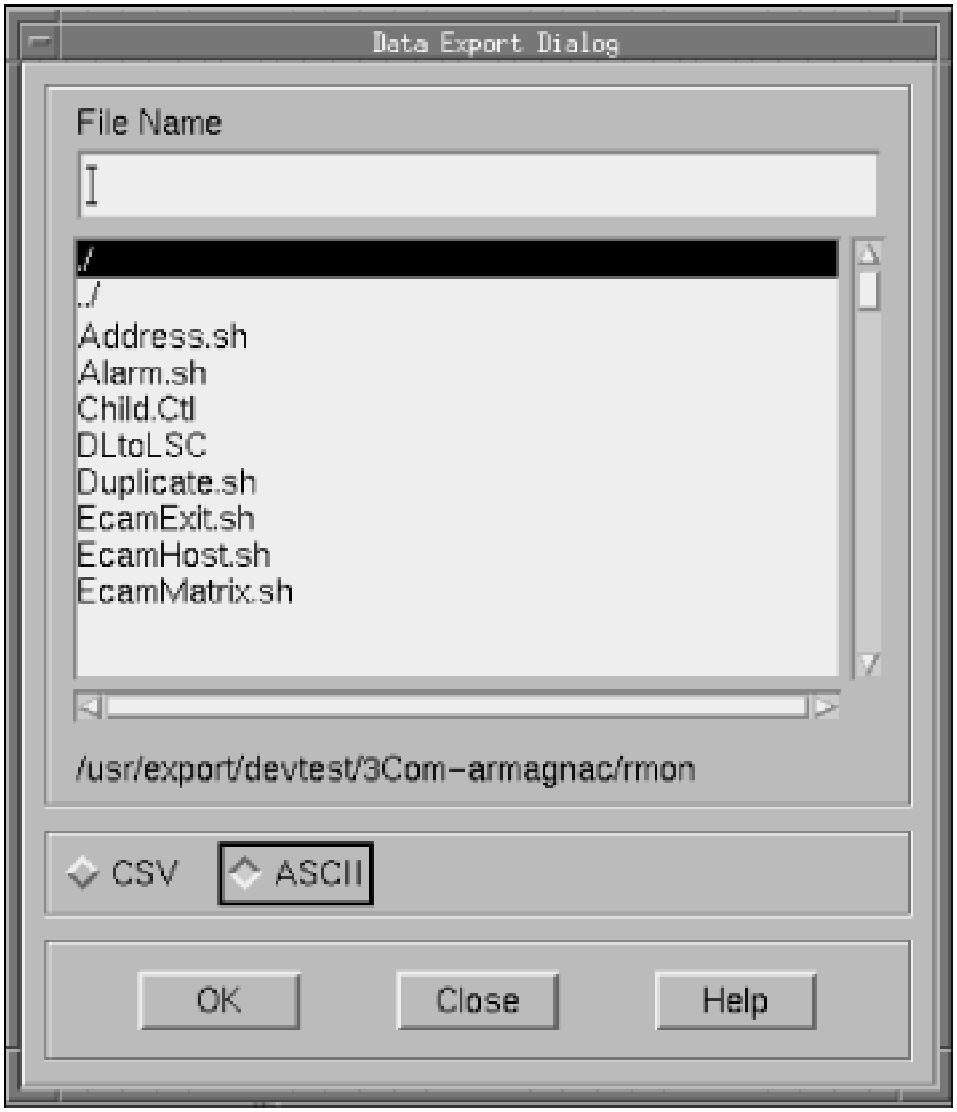


RMON Host Table for Probe2 [illegible]

Address	CreationOrder	InPkts	OutPkts	InOctets	OutOctets	OutErrors	OutBroadcastPkts	OutMulticast
000000000001	240	108	0	6546	0	0	0	0
0000c0[illegible]951	101	0	5493	0	1360561	0	3332	2161
[illegible]	320	435266	405682	40818792	60560308	0	1287	0
00000A05[illegible]	73	131474	193898	6006516	103224161	0	170	0
0002AF[illegible]232	98	296	3473	236590	568159	0	3132	0
0002AFC04E3A	45	37	5128	3280	567799	0	4264	853
0002AFC04D44	117	0	3858	0	632513	0	3882	808
0002AFC04E30	141	40712	42174	4622519	4511778	0	1454	0
0002AFC04E9A	186	9	26	880	3303	0	9	0
0002AFC0BEC8	229	72	0	4626	0	0	0	0
00030CF6BAF5	139	1139	2573	98561	310032	0	1097	0
0009[illegible]	88	1751	297	112702	38087	0	289	88

Figure 61. Example of Data Export Table

2. To export the data contained in the table, click **Export** to open the Data Export dialog box. Figure 62 on page 126 shows a sample Data Export dialog box.



```
./
../
Address.sh
Alarm.sh
Child.Ctl
DLtoLSC
Duplicate.sh
EcamExit.sh
EcamHost.sh
EcamMatrix.sh
```

/usr/export/devtest/3Com–armagnac/rmon

Figure 62. Data Export Dialog Box

a. Enter the file name and specify the appropriate file type.

b. CSV files can be read into databases and spreadsheets for presentation style reports and more detailed analysis, while ASCII files can be loaded into any text editor, or printed directly.

c. Click **OK** to export the data to file and return to the table display.

3. To close the table display, click **Close**.

Using the Data Collector Application

This section explains how to collect RMON data from devices on your network using the Collector application.

Note: Access permissions for the creation and modification of configurations within the Collector are limited to one user id.

Starting the Collector

To start the Collector, follow these steps:

1. Select **Data Collector** from the Tools menu in the menu bar in Nways Manager Remote Monitor's main window. Open the Collector main dialog box (See Figure 63).
   Before you can start data collection, you will need to build a list of logging points.

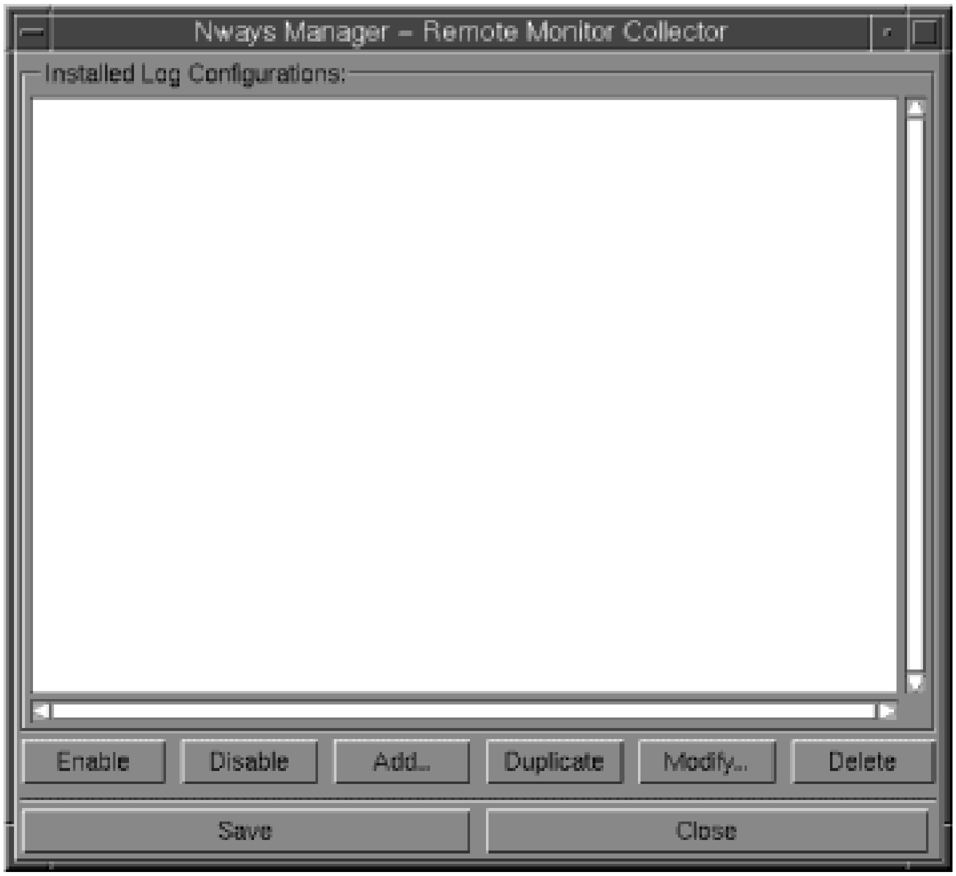

Nways Manager – Remote Monitor Collector
Installed Log Configurations:
Enable
Disable
Add...
Duplicate
Modify...
Delete
Save
Close

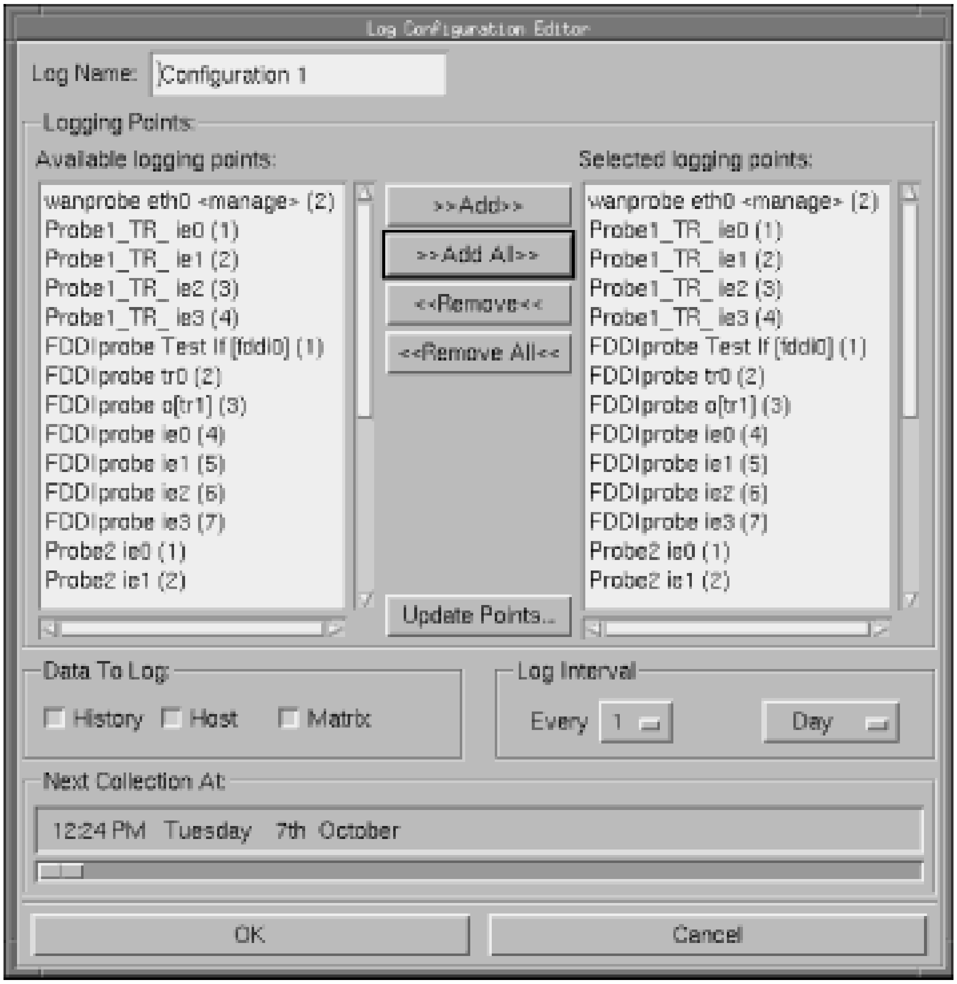
Figure 63. Collector Main Dialog Box

Setting Up Logging Points

A logging point consists of a device name and the name and physical number of each interface on that device.

To set up the list of logging points:

1. In the Collector main dialog box, click **Add**... to open the Log Configuration Editor dialog box (See Figure 64).



Log Name: Configuration 1

Available logging points:

wanprobe eth0 <manage> (2)
Probe1_TR_ ie0 (1)
Probe1_TR_ ie1 (2)
Probe1_TR_ ie2 (3)
Probe1_TR_ ie3 (4)
FDDIprobe Test If [fddi0] (1)
FDDIprobe tr0 (2)
FDDIprobe o[tr1] (3)
FDDIprobe ie0 (4)
FDDIprobe ie1 (5)
FDDIprobe ie2 (6)
FDDIprobe ie3 (7)
Probe2 ie0 (1)
Probe2 ie1 (2)

Selected logging points:

wanprobe eth0 <manage> (2)
Probe1_TR_ ie0 (1)
Probe1_TR_ ie1 (2)
Probe1_TR_ ie2 (3)
Probe1_TR_ ie3 (4)
FDDIprobe Test If [fddi0] (1)
FDDIprobe tr0 (2)
FDDIprobe o[tr1] (3)
FDDIprobe ie0 (4)
FDDIprobe ie1 (5)
FDDIprobe ie2 (6)
FDDIprobe ie3 (7)
Probe2 ie0 (1)
Probe2 ie1 (2)

Every 1 Day

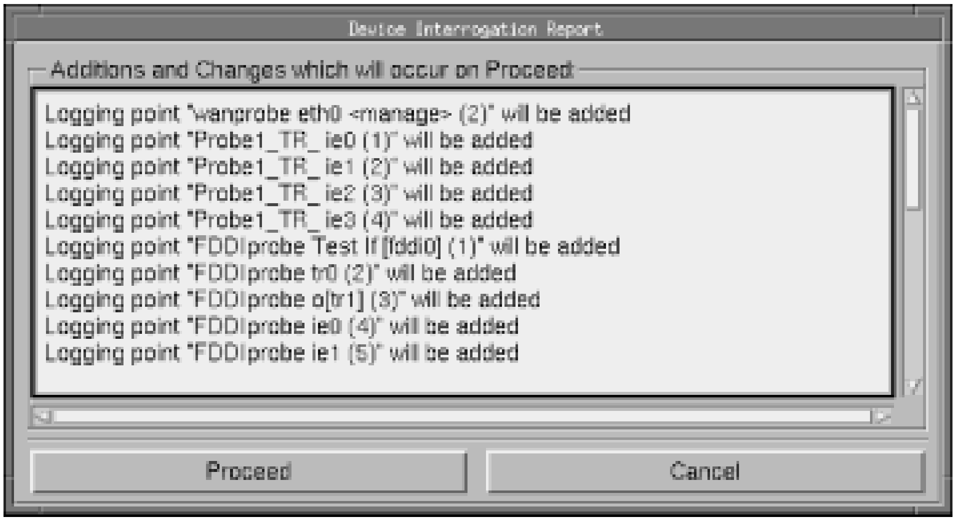
Next Collection At:

12:24 PM Tuesday 7th October

Figure 64. Log Configuration Editor Dialog Box

2. Enter a log name in the Log Name field. The logging points that you set up in the Log Configuration Editor dialog box will appear in the Installed Log Configurations dialog box under this name.

3. Click **Update Points**... to display the Device Interrogation Progress dialog box (See Figure 65).


Device Interrogation Report
Additions and Changes which will occur on Proceed
Proceed
Cancel

```
Logging point "wanprobe eth0 <manage> (2)" will be added
Logging point "Probe1_TR_ ie0 (1)" will be added
Logging point "Probe1_TR_ ie1 (2)" will be added
Logging point "Probe1_TR_ ie2 (3)" will be added
Logging point "Probe1_TR_ ie3 (4)" will be added
Logging point "FDDIprobe Test If [fddi0] (1)" will be added
Logging point "FDDIprobe tr0 (2)" will be added
Logging point "FDDIprobe o[tr1] (3)" will be added
Logging point "FDDIprobe ie0 (4)" will be added
Logging point "FDDIprobe ie1 (5)" will be added
```

Figure 65. Device Interrogation Progress Dialog Box

4. Select **Yes** to start the interrogation process. This process may take a few minutes, depending on the number of devices on your network.
5. The list of logging points will remain static until you choose to update it again. The Collector will then refresh the contents of the list by comparing entries with those in the `probe.map` file and making a new interrogation of each device and interface.
6. The contents of the probe.map file are assumed to be an accurate representation of the network, as this file contains the device listing created from Nways Manager Remote Monitor. As a result, the Collector will make the following changes to the Available Logging Points list:
   - If a device or interface no longer exists in the probe.map file, it will automatically be deleted from the Available Logging Points list. For example, if you take a device off the network and remove it from within Nways Manager Remote Monitor, it will be removed from the Available Logging Points list in the Collector at the next update.
   - Any new entries in the probe.map file will be added to the Available Logging Points list.

   Once the Collector has compared and interrogated every device, it will advise you of any configurations that will be affected by changes to the Available Logging Points list. If a device has been removed from this list, it will also be removed from any configurations; otherwise, the configurations will remain unchanged.
7. To implement any changes made to the configurations, click **OK** in the Log Configuration Editor dialog box. You are returned to the Collector main dialog box.

8. To save the current Available Logging Points list, click **Save** in the Installed Log Configurations. (Refer to “Activating Data Collection” on page 133).

Creating Data Collection Configurations

When you start the Collector, the application’s main dialog box will open showing a list of existing configurations (See Figure 63 on page 127). When you run the Collector for the first time, this list will be empty.

The functions available from the main dialog box are summarized in Table 33.

Table 33. Collector Main Dialog Box Functionality

Function	Description
Enable	Activate collection of data for selected configurations at next save point.
Disable	Stop collection of data for selected configurations at next save point.
Add	Create new configuration.
Duplicate	Copy selected configuration(s).
Modify	Edit selected configuration.
Delete	Delete selected configuration(s).
Save	Save changes to Collector and update cron entry to start data collection
Close	Exit Collector with option to save or abandon changes.

Adding a New Collection Configuration

1. Click **Add...** to open the Log Configuration Editor dialog box, shown in Figure 64 on page 128.
2. Enter a name for this collection in the Log Name field.
3. The Selected Logging Points list contains the currently selected interfaces and devices.
   a. To add entries from the Available logging points list:
      - Select an entry by clicking it.
      - To select multiple entries, hold down the [**Ctrl**] key while you click the entries in the list.
      - Click **Add**.
      - Click **Add All** to add all the available devices.
      - To remove entries from the Selected logging points list:
        – Select an entry by clicking it.
        – To select multiple entries, hold down the [Ctrl] button while you click the entries in the list.
        – Click **Remove**.
   b. Click **Remove All** to remove all the available devices.

c. To update the list of Available Logging Points, click **Update Points**.... This process may take some time and may affect other configurations (refer to “Setting Up Logging Points” on page 128 for more information).

4. Select which data should be logged: History, Host and/or Matrix.

   History data will only be collected from those devices for which you have previously set up a History View in the Nways Manager Remote Monitor. Refer to “Using the History View” on page 82.

5. Choose an interval period for data logging. By default, the Log Interval is set to a daily collection.
6. To set the exact time at which the collection should take place, use the time bar in the Next Collection area of the dialog box.

   For a log interval of once a day, you can specify the exact minute the collection should start and, with log intervals of longer than one day, you can specify both the day and the minute that the collection should start.

   Attention: You should carry out only one data collection at any given time of day. The collection process writes its data to common (and non-unique) filenames. If more than one data collection is running at any given time, there could be interference between the processes. This would invalidate the data for the collections.

   To set a new time, do one of the following:

   - Click the slider and drag it to the left or right.
   - Click at any point in the scroll bar with the middle mouse button — the scroll button will jump to that point.
   - Click at any point in the scroll bar with the left mouse button and hold the mouse button down — the scroll button will move towards that point.

   The collection time displayed will update as the scroll button moves.
7. Click **OK** to accept these changes and return to the Collector’s main dialog box. Clicking **Cancel**will abandon any changes you have made to the configuration.

   The new collection configuration is shown in the Installed Log Configurations list in the main dialog box.
8. To start data collection for a configuration, you must save your changes to the Collector. Refer to “Enabling and Disabling Collections” on page 132 and “Activating Data Collection” on page 133.

Duplicating and Modifying Configurations

Another way to create a new configuration is to duplicate an existing one and then modify it. To do this, follow these steps:

1. Select one or more collection configurations in the Installed Log Configurations list and click **Duplicate** to create a copy of the selected configurations. Duplicates are identified by quotation marks at the end of the log name.
2. Select a duplicate configuration and click **Modify**... to open the Log Configuration Editor dialog box.

3. Follow the instructions for “Adding a New Collection Configuration” on page 130 to change any of the duplicate configuration’s details.
4. Click **OK** to accept these changes and return to the Collector Configuration dialog box. Clicking **Cancel** will abandon any changes you have made to the configuration.

The modified collection configuration will be shown in the Installed Log Configurations list in the main dialog box.

To start data collection for a configuration, you must save your changes to the Collector. Refer to “Enabling and Disabling Collections” and “Activating Data Collection” on page 133.

Deleting Configurations

You can also delete any configurations that you have created.

If you make a mistake, for instance by deleting the wrong configuration, you can quit the application without saving your changes. When you reopen the Collector, the list of configurations will revert to that at the last save point. However, you will have lost all the changes that you made after this point.

1. Select one or multiple collection configurations in the Installed Log Configurations list.
2. Click **Delete**.

Enabling and Disabling Collections

The Collector is designed to let you set up any number of collections, activating some immediately and keeping others inactive until they are required.

Enabling Collections

When you add new collections to the Installed Log Configurations list, by default they will be enabled immediately. Duplicate configurations will be disabled by default. An enabled collection configuration is denoted by the ’>>’ prefix.

To enable a currently inactive configuration:

1. Select that entry in the Installed Log Configurations list.
2. Click **Enable** to activate the selected collection.

Disabling Collections

To disable a collection configuration:

1. Select the collection that is to be disabled from the Installed Log Configurations list.
2. Click **Disable** to deactivate the selected collection. The enabled symbol ’>>’ will be removed from the start of the collection entry.

Activating Data Collection

The Installed Log Configurations list shows all the configurations that you have created. Saving the Collector Configuration as a whole will activate data collection for all the enabled configurations.

- When you choose **Save** or **Quit** and then **Save Settings Before Quitting**, the Collector will create an entry in your `crontab` file for each enabled collection configuration. At the designated time, `cron` will run the data collection program.
- If you select **Quit** and then **Quit without Saving**, you will lose all of the changes you made to the Collector since the last save point.

CSV Files

The Collector stores collected data in the `/usr/LANReMon/rmon/LOGDIR` directory in CSV format files. As new collections are made, new data is appended to the existing files.

The files created are shown in Table 34:

Table 34. CSV Files

File Name	Description
hist.csv	Ethernet History data
host.csv	Host data
matrix.csv	Matrix data
trml.csv	Token Ring MAC-Layer History data
trp.csv	Token Ring Promiscuous History data
fddihist.csv	FDDI History data

The size of the CSV files in the `/usr/LANReMon/rmon/LOGDIR` directory will depend on the amount of data being collected; so if you have set up frequent collections of large amounts of data from large numbers of devices on your network, you can expect the CSV files to grow quickly.

Appendix A. Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area.

References in this publication to IBM products, programs, and services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not that only IBM's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program, or service. Evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, are the user's responsibility.

IBM may have patents or pending patent applications covering the subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION ″AS IS″ WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

Trademarks

The following terms are trademarks of the IBM Corporation in the United States, or other countries, or both:

IBM	Nways	AIX	NetView

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Ltd.

Microsoft, Windows, Windows NT, and the Windows 95 logo are trademarks or registered trademarks of Microsoft Corporation.

Pentium® is a trademark or registered trademark of Intel Corporation in the U.S. and other countries.

Other company product and service names may be trademarks or service marks of others.

Appendix B. NetView for AIX Integration

This appendix describes:

- Setting Up Probes in IBM NetView
- Using RMON Applications in IBM NetView.

IBM NetView must be installed before you install the Nways Manager Remote Monitor. During installation, the Nways Manager Remote Monitor will integrate with IBM NetView automatically.

Integration with NetView allows you to set up RMON devices, such as the IBM RMON probe, in IBM NetView and then view statistical information regarding the monitored segment in either graphical or tabular format.

In addition, all the functionality of the Nways RMON can be accessed from within NetView. This allows applications such as Packet Capture and Decode to be used form within NetView.

Setting Up Probes in IBM NetView

Within IBM NetView, each probe should be set up for the segment that it is monitoring as follows:

1. When starting IBM NetView, the discovery program may have found the selected probe and inserted it into the map as a Generic Computer object. If this is the case the Net Device symbol class may need to be changed to Analyzer as follows:
   a. Select the object in the map.
   b. With the right mouse button, click **Change Symbol Type** in the menu bar.
   c. Set the Net Device symbol class to *Analyzer.*
   d. Set the probe's object attributes as described in step 3
2. If the IBM probes have not yet been discovered, use the ping command to verify their connection to the network. Usually after a few moments a network analyzer device (signifying an IBM probe) will appear on the map. If the probe does not appear, you can add it manually by doing the following:
   a. Select **Edit**from the menu bar.
   b. Select the **Add Object** menu option.
   c. Select the Net Device symbol class.
   d. With the middle mouse button, pick up an Analyzer and drop it onto the map.

      A dialog box will be displayed allowing the name associated with the probe to be set up. This should be the name that has been set up in the /etc/hosts system file.
   e. Set the probe's object attributes as described in Step 3.
3. To set up the probe's object attributes:

a. With the right mouse button, click **Describe/Modify Object** in the menu bar. There are three categories to be set: Capabilities, General Attributes and IP Map.

b. Double-click **IP Map** and enter the host name as it appears in the /etc/hosts system file. Press **Return** and the host's IP address will be displayed. Check that this address is correct and is not a duplicate IP address, then click**OK** to save the new IP Map setting.

c. Double-click **General Attributes** and set the *SNMPSupported* flag to **true**.

d. From the pull-down SNMPAgent menu, select a Nways Manager Remote Monitor device. For the vendor, select **IBM.**

e. Click **OK**to save the new General Attributes setting.

f. Double-click **Capabilities** and check that the `isAnalyzer` and the `isSNMPSupported` flags are both set to **true**. Then check that the SNMPAgent and vendor information have been set up correctly. If either of the flags are not set then the **General Attributes** should be set up again.

Using RMON Applications in IBM NetView

Once you have completed setting up your probes, it is then possible to view network statistics for the monitored segments. This may be done using IBM NetView graphs and Nways Manager Remote Monitor. All of the functionality provided by Nways Manager Remote Monitor can be launched from within IBM NetView.

Starting Nways Manager Remote Monitor Applications

To access Nways Manager Remote Monitor Applications:

1. Select a probe.
2. Select Monitor from the main menu.
3. Select Nways Manager Remote Monitor.
4. Select one of the Nways Manager Remote Monitor menu options:

IBM Tools
From this menu option it is possible to execute all of Nways Manager Remote Monitor Applications, either individually by selecting RMON Segment Statistics, RMON History View, and so on, or collectively by selecting the RMON Summary Viewport option which displays the main window.

OpenView Tools
From this menu option various graphs and tables can be viewed showing information currently held on the probe. These menu options are available for both Ethernet and Token-Ring and are explained in Nways Manager Remote Monitor below.

Stop RMON Tools
Exits any NetView Tools that are currently active.

5. When returning to IBM NetView, either iconify the viewport, leaving it running for rapid start up the next time you need to use it, or use the Exit button on the main viewport to close down Nways Manager Remote Monitor.

NetView Tools

Table 35 lists the options available from the NetView Tools menu.

Table 35. NetView Tools Options

Options	Description
Ethernet Packet Size Distribution	This graphs the distribution of traffic for different packet sizes on an Ethernet segment.
Ethernet Segment Statistics	This graphs statistics for various types of packets, including different types of error packets, collisions, broadcasts, and so on. This is only for an Ethernet segment.
Token-Ring Packet Size Distribution	This graphs the distribution of traffic for different packet sizes on a Token-Ring segment.
Token-Ring Packet Rate	This graphs statistics for the LLC packets and the MAC packets, and shows the rate of dropped events for a Token-Ring segment.
Token-Ring MAC Error Rates	This graphs statistics for various types of errors on a Token-Ring segment. This includes such information as the number of Beacon packets or Congestion errors that may have occurred.
Token-Ring Routing Statistics	This graphs statistics on routing information for a Token-Ring segment. This includes such information as Local LLC Frames, Through Frames, Single Route Broadcast packets, and so on.
Token-Ring Hop Statistics	This graphs statistics for frames which have traversed over more than one Token-Ring segment. This shows statistics for packets of various numbers of hops.
Host Table by Selected Station	This displays a table of all of the hosts the selected probe has seen. From this table any host of interest may be selected by clicking the left mouse button in any field in its row, and from this an NetView graph will update with the statistics of packets being sent from and being received by that host. This is available for both Ethernet and Token-Ring probes.
Matrix Table by Selected Station	This displays a table of all of the conversations that have been seen by the selected probe. Any conversation between two particular devices may be selected by clicking the left mouse button in the relevant row. From this a NetView graph will be displayed showing the conversation between these two devices. This is available for both Ethernet and Token-Ring probes.

Appendix C. OpenView Integration

This appendix describes:

- Setting Up Probes in HP OpenView
- Using RMON Applications in HP OpenView

HP OpenView must be installed before you install the Nways Manager Remote Monitor. During installation, the Nways Manager Remote Monitor will integrate with HP OpenView automatically.

Integration with OpenView allows you to set up RMON devices, such as the IBM RMON probe, in HP OpenView and then view statistical information regarding the monitored segment in either graphical or tabular format.

In addition, all Nways Manager Remote Monitor functionality can be accessed from within OpenView. This allows applications such as Packet Capture and Decode to be used form within OpenView.

Setting Up Probes in HP OpenView

Within HP OpenView, each probe should be set up for the segment that it is monitoring as follows:

1. When starting HP OpenView, the discovery program may have found the selected probe and inserted it into the map as a Generic Computer object. If this is the case the Net Device symbol class may need to be changed to **Analyer** as follows:
   a. Select the object in the map.
   b. With the right mouse button, click **Change Symbol Type** in the menu bar.
   c. Set the Net Device symbol class to **Analyer**
   d. Set the probe’s object attributes as described in step 3
2. If the IBM probes have not yet been discovered, use the ping command to verify their connection to the network. Usually after a few moments a network analyzer device (signifying an IBM probe) will appear on the map. If the probe does not appear, you can add it manually by doing the following:
   a. Select **Edit**from the menu bar.
   b. Select the **Add Object** menu option.
   c. Select the Net Device symbol class.
   d. With the middle mouse button, pick up an Analyzer and drop it onto the map.

      A dialog box will be displayed allowing the name associated with the probe to be set up. This should be the name that has been set up in the /etc/hosts system file.
   e. Set the probe’s object attributes as described in Step 3.
3. To set up the probe’s object attributes:
   a. With the right mouse button, click **Describe/Modify Object** in the menu bar.

There are three categories to be set: Capabilities, General Attributes and IP Map.

b. Double-click **IP Map** and enter the host name as it appears in the /etc/hosts system file. Press **Return** and the host's IP address will be displayed. Check that this address is correct and is not a duplicate IP address, then click **OK** to save the new IP Map setting.

c. Double-click **General Attributes** and set the *SNMPSupported* flag to **true**.

d. From the pull-down SNMPAgent menu, select a Nways Manager Remote Monitor device. For the vendor, select **IBM.**

e. Click **OK**to save the new General Attributes setting.

f. Double-click **Capabilities** and check that the `isAnalyzer` and the `isSNMPSupported` flags are both set to **true**. Then check that the SNMPAgent and vendor information have been set up correctly. If either of the flags are not set then the **General Attributes** should be set up again.

Using RMON Applications in HP OpenView

Once you have completed setting up your probes, it is then possible to view network statistics for the monitored segments. This may be done using HP OpenView graphs and Nways Manager Remote Monitor. All of the functionality provided by Nways Manager Remote Monitor can be launched from within HP OpenView.

Starting Nways Manager Remote Monitor Applications

To access Nways Manager Remote Monitor Applications:

1. Select a probe.
2. Select Monitor from the main menu.
3. Select Nways Manager Remote Monitor.
4. Select one of the Nways Manager Remote Monitor menu options:

IBM Tools
From this menu option it is possible to execute all of Nways Manager Remote Monitor Applications, either individually by selecting RMON Segment Statistics, RMON History View, and so on, or collectively by selecting the RMON Summary Viewport option which displays the main window.

OpenView Tools
From this menu option various graphs and tables can be viewed showing information currently held on the probe. These menu options are available for both Ethernet and Token-Ring and are explained in OpenView Tools below.

Stop RMON Tools
Exits any Nways Manager Remote Monitor tools that are currently active.

5. When returning to HP OpenView, either iconify the viewport, leaving it running for rapid start up the next time you need to use it, or use the Exit button on the main viewport to close down Nways Manager Remote Monitor.

Openview Tools

Table 36 lists the options available from the Openview Tools menu.

Table 36. Openview Tools Options

Options	Description
Ethernet Packet Size Distribution	This graphs the distribution of traffic for different packet sizes on an Ethernet segment.
Ethernet Segment Statistics	This graphs statistics for various types of packets, including different types of error packets, collisions, broadcasts, and so on. This is only for an Ethernet segment.
Token-Ring Packet Size Distribution	This graphs the distribution of traffic for different packet sizes on a Token-Ring segment.
Token-Ring Packet Rate	This graphs statistics for the LLC packets and the MAC packets, and shows the rate of dropped events for a Token-Ring segment.
Token-Ring MAC Error Rates	This graphs statistics for various types of errors on a Token-Ring segment. This includes such information as the number of Beacon packets or Congestion errors that may have occurred.
Token-Ring Routing Statistics	This graphs statistics on routing information for a Token-Ring segment. This includes such information as Local LLC Frames, Through Frames, Single Route Broadcast packets, and so on.
Token-Ring Hop Statistics	This graphs statistics for frames which have traversed over more than one Token-Ring segment. This shows statistics for packets of various numbers of hops.
Host Table by Selected Station	This displays a table of all of the hosts the selected probe has seen. From this table any host of interest may be selected by clicking the left mouse button in any field in its row, and from this an NetView graph will update with the statistics of packets being sent from and being received by that host. This is available for both Ethernet and Token-Ring probes.
Matrix Table by Selected Station	This displays a table of all of the conversations that have been seen by the selected probe. Any conversation between two particular devices may be selected by clicking the left mouse button in the relevant row. From this a NetView graph will be displayed showing the conversation between these two devices. This is available for both Ethernet and Token-Ring probes.

Appendix D. List of Protocols and Protocol Decodes

This appendix lists the protocol decodes supported for the RMON Views and ECAM Applications.

RMON Application Decodes

Table 37. List of Supported Protocol Decodes by Protocol Family

Protocol Family	Protocol
AppleTalk	AARP, ADSP, AEP, AFP, ASP, ATP, DDP, MacIP, MacIP config, NBP, PAP, RTMP, ZIP.
TCP/IP	AppleTalk in Cayman IP Tunnel, ARP, AURP (IPTALK routing information), BOOTP, DNS, EGP, FTP, ICMP, IGMP, IP, IPTALK (AppleTalk in IP Tunnel), LPR/LPD, NetBIOS (TCP), NFS, OSPF, POP, RARP, RIP, RIP2, RLOGIN, RPC, RSH, SMTP, SNMP, TCP, Telnet., TFTP, UDP.
DECNet (Phrase IV & V)	Control, DRP, NSP, LAT, MOP, SCP.
Novell NetWare	IPX, NCP, RIP, SAP, SNMP (over IPX), SPX.
Banyan VINES	ARP, Echo, ICP, IPC, RTP, SPP.
IBM SNA	DLC, XID (TH, RH, RU).
Xerox XNS	Echo, Error, PEP, RIP, SPP.
ISO	CLNP, ESIS, ISIS, LLC 1 & 2, TP0 through TP4
LAN Manager	NetBEUI, NetBIOS, SMB.
LAN Encapsulations	Ethernet Type II, IEEE 802.1, IEEE 802.2, IEEE 802.3, IEEE 802.5, LLC1, LLC2, LSAP, MAC, SNAP, Spanning Tree.
FDDI	LLC, MAC, SMT.

ECAM Application Decodes

This section lists the protocols supported by RMON2 (ECAM) SmartAgent software version 0.21. The protocols have been grouped into two tables to show:

- Those protocols which are associated with only one protocol family.
- All encapsulations of protocols which are associated with more than one protocol family.

Note: For clarity, each protocol appears once only.

Table 38. Protocols Associated with One Protocol Family

Protocol Family	Protocol	Description
AppleTalk Phase I & II	AARP	AppleTalk Address Resolution Protocol
	ADSP	AppleTalk Data Stream Protocol
	AEP	AppleTalk Echo Protocol
	ATP	AppleTalk Transaction Protocol
	DDP1	AppleTalk Datagram Delivery Protocol - short header formats
	DDP2	AppleTalk Datagram Delivery Protocol - long header formats
	NBP	AppleTalk Name Binding Protocol
	RTMP	AppleTalk Routing Table Maintenance Protocol
	ZIP	AppleTalk Zone Information Protocol
Banyan VINES	VINES	Banyan VINES Internet Protocol catch-all group
	VINES (ARP)	Banyan VINES Address Resolution Protocol
	VINES (ICP)	Banyan VINES Internet Control Protocol
	VINES (IPC)	Banyan VINES InterProcess Communications Protocol
	VINES (RTP)	Banyan VINES Routing Update Protocol
	VINES (SPP)	Banyan VINES Sequenced Packet Protocol
DECnet	DEC	DECnet catch-all group*
	DRP	DECnet (Phase IV) Routing Protocol
	LANBridge	Digital's Bridge Management Protocol
	LAT	DECnet Local Area Transport Protocol
	LAVC/SCA	Local Area Vax Cluster/System Communication Architecture
	MOP	DECnet Maintenance Operations Protocol
	PathWorks	PC to Digital Server Protocol
IBM SNA	SNA	Systems Network Architecture catch-all group*
	SNA (data)	SNA End User and Network Services Data
	SNA (flow control)	SNA Data Flow Control
	SNA (network control)	SNA Network Control
	SNA (session control)	SNA Session Control
LAN Manager	NetBIOS/NETBEUI	Network Basic Input/Output System
NetWare	IPX	Internet Packet Exchange
	NetBIOS/IPX	IPX implementations of NetBIOS
	NCP	NCP Netware Core Protocol
	RIP	Routing Information Protocol
	SAP	Service Advertising Protocol
	SPX	Sequenced Packet Exchange

Table 38. Protocols Associated with One Protocol Family (continued)

Protocol Family	Protocol	Description
TCP/IP	AFS	Andrew File System
	ARP	Address Resolution Protocol
	DNS	Domain Name Service Protocol
	FTP	File Transfer Protocol
	GOPHER	Internet Document Search and Retrieval
	ICMP	Internet Control Message Protocol
	IGRP	Inter-Gateway Routing Protocol
	IP	Internet Protocol*
	LPR/LPD	Printer
	NetBIOS/IP (datagram)	NetBIOS datagram support
	NetBIOS/IP (name)	NetBIOS Name Support
	NetBIOS/IP (session)	NetBIOS Session Support
	NeWS	Network Window Service
	NFS	Network File Service
	NNTP	Network News Transfer Protocol
	NTP	Network Time Protocol
	OSPF	Open Shortest Path First
	RCMD	Remote Command
	REXEC	Remote Process Execution
	RLOGIN	Remote Login
	Router	Local Routing Processes (520/udp)
	RWHO	Remote Who
	SMTP	Simple Mail Transfer Protocol
	SOCKS	Secure Socket Server
	SUNPRC	SUN Remote Procedure Call Protocol
	TCP	Transmission Control Protocol
	TELNET	Network Virtual Terminal Protocol
	TFTP	Trivial File Transfer Protocol
	UDP	User Datagram Protocol
	WWW	World Wide Web
	X	X Windows

*The RMON2 (ECAM) SmartAgent software tries to identify each packet in as much detail as possible. However, fragmented packets cannot be fully classified and these are counted instead in a 'catch-all' class.

Table 39. Protocols Associated with Multiple Protocol Families

Protocol	Description	Supported Transports
Notes	Lotus Notes	NETBEUI, NetBIOS/IP (datagram and session), NetBIOS/IPX, SPX, TCP
SMB	Microsoft's Server Message Block Protocol	IPX, NETBEUI, NetBIOS/IP (datagram and session), NetBIOS/IPX

Table 39. Protocols Associated with Multiple Protocol Families (continued)

Protocol	Description	Supported Transports
SNMP	Simple Network Management Protocol	DDP1, DDP2, IPX, UDP
SNMPTRAP	Simple Network Management Protocol TRAPS	DDP1, DDP2, IPX, UDP

RMON2 Protocols Overview

Each entry in the protocol directory table on a device represents a protocol that the device can decode and count. These may be standard or custom protocols.

The entries within the table are indexed by each data-link layer protocol: first by MAC-layer protocol and then by each level of encapsulated protocol. For example:

`ether2` denotes the Ethernet MAC protocol.

`ether2.ip` denotes IP running over the Ethernet MAC protocol.

`ether2.ip.udp` denotes UDP running over IP on an Ethernet LAN.

`ether2.ip.udp.snmp` identifies the application-level protocol SNMP operating over Ethernet.

The MAC-layer protocols consist of:

ether2 Denotes Ethernet II.

llc Denotes the LLC (802.2) protocol.

snap Denotes the sub-network access protocol.

vsnap Denotes the pseudo protocol associated with snap.

wgAssigned Denotes those protocols which don’t easily conform to the format of the other link-layer branches.

anyLink Denotes a wildcard protocol, identified by the ′*’ prefix, that aggregates all link-layer protocols by their layer 2 encapsulated protocol. For example, if IPX is the layer 2 encapsulated protocol:

*.ipx Ξ ether2.ipx + llc.ipx + snap.ipx + wgAssigned.ipx

RMON2 Predefined Protocols

This section shows predefined protocols supported by firmware version 4.10 and above for IBM devices. Encapsulated protocols are listed alphabetically and the MAC-layer protocols over which they run are marked. For example, the 802.1-bridge protocol appears as *.802.1-bridge and llc.802.1-bridge.

Table 40. Protocol Names

Protocols	Protocol Name
802.1-bridge	802.1D Bridge Spanning Tree Protocol
aarp	AppleTalk Address Resolution Protocol
adsp	AppleTalk Data Stream Protocol
aep	AppleTalk Echo Protocol
arp	Address Resolution Protocol
atalk	AppleTalk Datagram Delivery Protocol (short and long headers)
atp	AppleTalk Transaction Protocol
bootpc	Bootstrap Protocol Client
bootps	Bootstrap Protocol Server
ccmail	Lotus cc-Mail Protocol
dec-diag	DEC Diagnostic Protocol
dns	Domain Name Service Protocol
drp	DECnet (Phase IV) Routing Protocol
ftp	File Transfer Protocol Control Port
ftp-data	File Transfer Protocol Data Port
gopher	Internet Document Search and Retrieval
icmp	Internet Control Message Protocol
idp	XNS Internet Datagram Protocol
igrp	Inter-Gateway Routing Protocol
ip	Internet Protocol
ipx	Internet Packet Exchange
nbp	AppleTalk Name Binding Protocol
lat	DECnet Local Area Transport Protocol
lavc	Local Area Vax Cluster
mop	DECnet Maintenance Operations Protocol
nbt_data	NetBIOS Datagram Support
nbt_name	NetBIOS Name Support
nbt_session	NetBIOS Session Support
netbeui	LAN Manager Netbeui Protocol
netbios-IBM	IBM NetBIOS Protocol
news	Network Window Service
nfs	Network File Service
nntp	Network News Transfer Protocol
notes	Lotus Notes Protocol
nov-bcast	Novell Broadcast Protocol
nov-diag	Novell Diagnostic Protocol
nov-echo	Novell Echo Protocol
nov-error	Novell Error-Handler Protocol
nov-ncp	Novell Netware Core Protocol
nov-netbios	Novell Network Basic Input/Output System
nov-pep	Novell Packet Exchange Protocol
nov-rip	Novell Routing Information Protocol
nov-sap	Novell Service Advertising Protocol
nov-sec	Novell Security Protocol
nov-spx	Novell Sequenced Packet Exchange
nov-watchdog	Novell Watchdog Protocol

Table 40. Protocol Names (continued)

Protocols	Protocol Name
nsp	DECnet Network Services Protocol
ntp	Network Time Protocol
ospf	Open Shortest Path First
pop3	Post Office Protocol Version 3
printer	Printer
rcmd	Remote Command
rexec	Remote Process Execution
rlogin	Remote Login
router	Local Routing Processes (520/udp)
rtmp	AppleTalk Routing Table Maintenance Protocol
rwho	Remote Who
smb	Microsoft Server Message Block Protocol
smtp	Simple Mail Transfer Protocol
sna	Systems Network Architecture
snmp	Simple Network Management Protocol
snmptrap	Simple Network Management Protocol TRAPS
sunrpc	SUN Remote Procedure Call Protocol
tcp	Transmission Control Protocol
telnet	Network Virtual Terminal Protocol
tftp	Trivial File Transfer Protocol
udp	User Datagram Protocol
varp	Banyan VINES Address Resolution Protocol
vecho	Banyan VINES Data Link Level Echo Protocol
vicp	Banyan VINES Internet Control Protocol
vip	Banyan VINES Internet Protocol
vipc	Banyan VINES InterProcess Communications Protocol
vipc-dgp	Banyan VINES Unreliable Datagram Protocol
vipc-rdp	Banyan VINES Reliable Datagram Protocol
vrtp	Banyan VINES Routing Update Protocol
vspp	Banyan VINES Sequenced Packet Protocol
www-http	World Wide Web HTTP
X	X Windows
xns-echo	XNS Echo Protocol
xns-error	XNS Error-Handler Protocol
xns-pep	XNS Packet Exchange Protocol
xns-rip	XNS Routing Information Protocol
xns-spp	XNS Sequenced Packet Protocol
zip	Zone Information Protocol

Table 41. Predefined Protocols

MAC-Layer Protocol						Encapsulated Protocols
*.	ether2.	llc	snap.	vsnap_ether2.	wgAssigned.	
■		■				802.1-bridge
■	■		■			aarp
■	■		■			arp

Table 41. Predefined Protocols (continued)

MAC-Layer Protocol						Encapsulated Protocols
***.**	**ether2.**	**llc**	**snap.**	**vsnap_ether2.**	**wgAssigned.**	
■	■		■	■		atalk
■	■		■	■		atalk.adsp
■	■		■	■		atalk.aep
■	■		■	■		atalk.atp
■	■		■	■		atalk.atp.zip
■	■		■	■		atalk.nbp
■	■		■	■		atalk.rtmp
■	■		■	■		atalk.snmp
■	■		■	■		atalk.snmptrap
■	■		■	■		atalk.zip
■	■		■			dec-diag
■	■		■			drp
■	■		■			drp.nsp
■	■		■			idp
■	■		■			idp.xns-echo
■	■		■			idp.xns-error
■	■		■			idp.xns-pep
■	■		■			idp.xns-rip
■	■		■			idp.xns-spp
■	■	■	■			ip
■	■	■	■			ip.icmp
■	■	■	■			ip.igrp
■	■	■	■			ip.ip
■	■	■	■			ip.ip.icmp
■	■	■	■			ip.ip.igrp
■	■	■	■			ip.ip.opsf
■	■	■	■			ip.ip.udp.ccmail
■	■	■	■			ip.ip.udp.dns
■	■	■	■			ip.ip.udp.nbt_data
■	■	■	■			ip.ip.udp.nbt_data.smp
■	■	■	■			ip.ip.udp.nbt_name
■	■	■	■			ip.ip.udp.nbt_session

Table 41. Predefined Protocols (continued)

MAC-Layer Protocol						**Encapsulated Protocols**
***.**	**ether2.**	**llc**	**snap.**	**vsnap_ether2.**	**wgAssigned.**	
■	■	■	■			ip.ip.udp.nbt_session.smp
■	■	■	■			ip.ip.udp.notes
■	■	■	■			ip.ip.udp.ntp
■	■	■	■			ip.ip.udp.printer
■	■	■	■			ip.ip.udp.router
■	■	■	■			ip.ip.udp.rwho
■	■	■	■			ip.ip.udp.snmp
■	■	■	■			ip.ip.udp.snmptrap
■	■	■	■			ip.ip.udp.sunrpc
■	■	■	■			ip.ip.udp.sunrpc.nfs
■	■	■	■			ip.ip.udp.tftp
■	■	■	■			ip.ospf
■	■	■	■			ip.tcp
■	■	■	■			ip.tcp.X
■	■	■	■			ip.tcp.ccmail
■	■	■	■			ip.tcp.dns
■	■	■	■			ip.tcp.ftp
■	■	■	■			ip.tcp.ftp-data
■	■	■	■			ip.tcp.gopher
■	■	■	■			ip.tcp.nbt_data
■	■	■	■			ip.tcp.nbt_data.smb
■	■	■	■			ip.tcp.nbt_name
■	■	■	■			ip.tcp.nbt_session
■	■	■	■			ip.udp.rwho
■	■	■	■			ip.udp.snmp
■	■	■	■			ip.udp.snmptrap
■	■	■	■			ip.udp.sunrpc
■	■	■	■			ip.udp..sunrpc.nfs
■	■	■	■			ip.udp.tftp
■	■	■	■		■	ipx
■	■	■	■		■	ipx.nov-echo

Table 41. Predefined Protocols (continued)

MAC-Layer Protocol						Encapsulated Protocols
*.	ether2.	llc	snap.	vsnap_ether2.	wgAssigned.	
■	■	■	■		■	ipx.nov-error
■	■	■	■		■	ipx.nov-netbios
■	■	■	■		■	ipx.nov-netbios.notes
■	■	■	■		■	ipx.nov-netbios.smb
■	■	■	■		■	ipx.nov-pep
■	■	■	■		■	ipx.nov-pep.nov-bcast
■	■	■	■		■	ipx.nov-pep.nov-diag
■	■	■	■		■	ipx.nov-pep.nov-netbios
■	■	■	■		■	ipx.nov-pep.nov-netbios.notes
■	■	■	■		■	ipx.nov-pep.nov-netbios.smb
■	■	■	■		■	ipx.nov-pep.nov-rip
■	■	■	■		■	ipx.nov-pep.nov-sap
■	■	■	■		■	ipx.nov-pep.nov-sap.notes
■	■	■	■		■	ipx.nov-pep.nov-sap.nov-ncp
■	■	■	■		■	ipx.nov-pep.nov-sec
■	■	■	■			ip.ip.tcp
■	■	■	■			ip.ip.tcp.X
■	■	■	■			ip.ip.tcp.ccmail
■	■	■	■			ip.ip.tcp.dns
■	■	■	■			ip.ip.tcp.ftp
■	■	■	■			ip.ip.tcp.ftp-data
■	■	■	■			ip.ip.tcp.gopher
■	■	■	■			ip.ip.tcp.nbt_data
■	■	■	■			ip.ip.tcp.nbt_data.smb
■	■	■	■			ip.ip.tcp.nbt_name
■	■	■	■			ip.ip.tcp.nbt_session
■	■	■	■			ip.ip.tcp.nbt_session.smb
■	■	■	■			ip.ip.tcp.news
■	■	■	■			ip.ip.tcp.nntp
■	■	■	■			ip.ip.tcp.notes
■	■	■	■			ip.ip.tcp.pop3

Table 41. Predefined Protocols (continued)

MAC-Layer Protocol						Encapsulated Protocols
***.**	**ether2.**	**llc**	**snap.**	**vsnap_ether2.**	**wgAssigned.**	
■	■	■	■			ip.ip.tcp.printer
■	■	■	■			ip.ip.tcp.rcmd
■	■	■	■			ip.ip.tcp.rexec
■	■	■	■			ip.ip.tcp.rlogin
■	■	■	■			ip.ip.tcp.smtp
■	■	■	■			ip.ip.tcp.snmp
■	■	■	■			ip.ip.tcp.snmptrap
■	■	■	■			ip.ip.tcp.telnet
■	■	■	■			ip.ip.tcp.www-http
■	■	■	■			ip.ip.udp
■	■	■	■			ip.ip.udp.X
■	■	■	■			ip.ip.udp.bootpc
■	■	■	■			ip.ip.udp.bootps
■	■	■	■			ip.tcp.nbt_session.smb
■	■	■	■			ip.tcp.news
■	■	■	■			ip.tcp.nntp
■	■	■	■			ip.tcp.notes
■	■	■	■			ip.tcp.pop3
■	■	■	■			ip.tcp.printer
■	■	■	■			ip.tcp.rcmd
■	■	■	■			ip.tcp.rexec
■	■	■	■			ip.tcp.rlogin
■	■	■	■			ip.tcp.smtp
■	■	■	■			ip.tcp.snmp
■	■	■	■			ip.tcp.snmptrap
■	■	■	■			ip.tcp.telnet
■	■	■	■			ip.tcp.www-http
■	■	■	■			ip.udp
■	■	■	■			ip.udp.X
■	■	■	■			ip.udp.bootpc
■	■	■	■			ip.udp.bootps

Table 41. Predefined Protocols (continued)

MAC-Layer Protocol						**Encapsulated Protocols**
***.**	**ether2.**	**llc**	**snap.**	**vsnap_ether2.**	**wgAssigned.**	
■	■	■	■			ip.udp.ccmail
■	■	■	■			ip.udp.dns
■	■	■	■			ip.udp.nbt_data
■	■	■	■			ip.udp.nbt_data.smb
■	■	■	■			ip.udp.nbt_name
■	■	■	■			ip.udp.nbt_session
■	■	■	■			ip.udp.nbt_session.smb
■	■	■	■			ip.udp.notes
■	■	■	■			ip.udp.ntp
■	■	■	■			ip.udp.printer
■	■	■	■			ip.udp.router
■	■	■	■		■	ipx.nov-pep.nov-watchdog
■	■	■	■		■	ipx.nov-pep.smb
■	■	■	■		■	ipx.nov-pep.snmp
■	■	■	■		■	ipx.nov-pep.snmptrap
■	■	■	■		■	ipx.nov-rip
■	■	■	■		■	ipx.nov-spx
■	■		■			lat
■	■		■			lavc
■	■		■			mop
■		■				netbeui
■		■				netbeui.notes
■		■				netbeui.smb
■	■					netbios-IBM
■		■				sna
■	■	■	■			vecho
■	■	■	■			vip
■	■	■	■			vip.varp
■	■	■	■			vip.vicp
■	■	■	■			vip.vipc
■	■	■	■			vip.vipc.vipc-dgp

Table 41. Predefined Protocols (continued)

MAC-Layer Protocol						Encapsulated Protocols
*.	ether2.	llc	snap.	vsnap_ether2.	wgAssigned.	
■	■	■	■			vip.vipc.vipc-rdp
■	■	■	■			vip.vrtp
■	■	■	■			vip.vspp

*These products running over llc will be displayed as llc.vtr.vecho, and so on, where vtr is an additional protocol layer.

User-Defined Protocols

Note: This section is specific to V4.10.

If you are using customized protocols or protocol encapsulations on your network, you may want to add these to your protocol directory using a management application such as Nways Manager Remote Monitor.

With firmware version 4.10 installed on your device, you can specify at least 64 wildcard protocols or 256 non-wildcard protocols. (Refer to the list of MAC-layer protocols in “RMON2 Protocols Overview” on page 148 for a description of the anyLink or wildcard protocol.) You may be able to specify additional protocols on devices with more memory available.

Firmware version 4.10 supports a number of extensible protocols (see Table 42) with the following exceptions:

- ipx is not extensible by either values 0 or 17.
- llc is not extensible by odd-numbered children.
- nov-sap, nsp, sunrpc, vip, vipc and vsnap are not extensible.

The maxChildren value shows the total number of child protocols that may be defined. This is calculated irrespective of the encapsulation used. For example, ether2.ip.udp and ip.ip.udp would be counted as one child only.

Table 42. Extensible Protocols and maxChildren Values

	maxChildren				maxChildren		
Protocol	Total	Pre-Defined	User-Defined	Protocol	Total	Pre-Defined	User-Defined
atalk	16	9	7	snap	32	14	18
ether2	32	28	4	tcp	64	22	42
idp	8	5	3	udp	64	17	47
ip	32	7	25	vipc-dgp	4	0	4
ip.ip	16	7	9	vipc-rdp	0	4	
ipx	256	5*	249	vspp	4	0	4

Table 42. Extensible Protocols and maxChildren Values (continued)

	maxChildren				maxChildren		
Protocol	Total	Pre-Defined	User-Defined	Protocol	Total	Pre-Defined	User-Defined
llc	256	8	120**	xns-pep	0	4	
nov-pep	16	11	5	xns-spp	4	0	4
nov-spx	16	0	16				

*ipx is not extensible by either values 0 or 1. **llc is not extensible by odd-numbered children.

Appendix E. Roving Analysis Port Application and PACMIB

As part of IBM's relationship with 3Com, Nways Manager Remote Monitor supports the management of some 3Com proprietary monitoring functions.

This appendix looks at the functionality of:

- Roving Analysis Port Application
- Using PACMIB Functionality

Roving Analysis Port Application

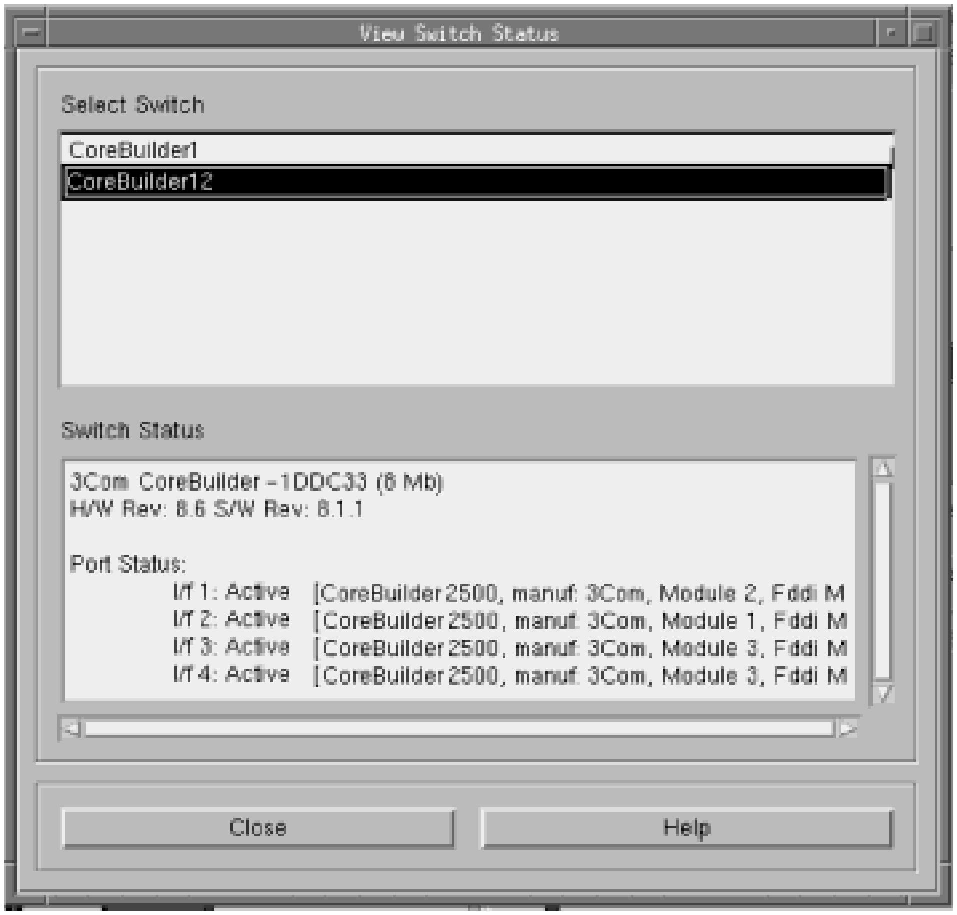
The Roving Analysis Port Application lets you view the status of 3Com CoreBuilder switches on your network. You can also configure Analyzer and Monitor ports on these switches, to use for the monitoring of port traffic for network management purposes. You can choose any network segment attached to a 3Com CoreBuilder device and monitor its activity using a network analyzer, such as a device or sniffer.

This application only supports 3Com CoreBuilder family of switches.

Status

To view a summary of information about the status of a 3Com CoreBuilder and the ports on that switch, follow these steps.

1. In Nways Manager Remote Monitor's main window, select RAP Status from the Configure menu to open the View Switch Status dialog box. (Figure 66 on page 160).
2. This dialog box contains a list of the switches on your network. (These are the devices for which the Device Type has been set to 3Com CoreBuilder in the Device List Editor dialog box - refer to "Setting Up and Verifying Devices" on page 9.)



CoreBuilder1
CoreBuilder12

```
3Com CoreBuilder - 1DDC33 (8 Mb)
H/W Rev: 8.6 S/W Rev: 8.1.1

Port Status:
               I/f 1: Active   [CoreBuilder 2500, manuf: 3Com, Module 2, Fddi M
               I/f 2: Active   [CoreBuilder 2500, manuf: 3Com, Module 1, Fddi M
               I/f 3: Active   [CoreBuilder 2500, manuf: 3Com, Module 3, Fddi M
               I/f 4: Active   [CoreBuilder 2500, manuf: 3Com, Module 3, Fddi M
```

Figure 66. View Switch Status Dialog Box

3. To view the status of a switch, select it in the Select Switch area. The switch information will appear in the Switch Status area.

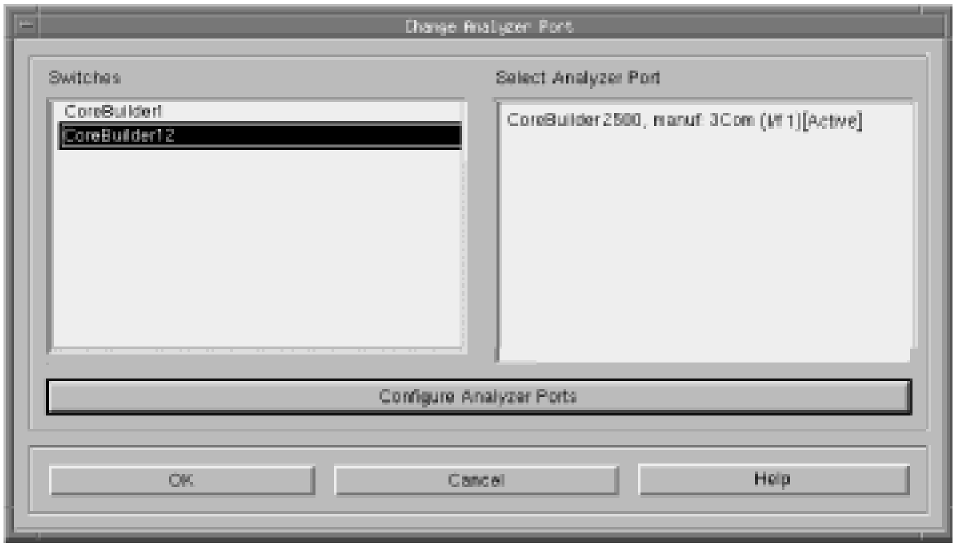
Configuration

When you set up a Monitor port, data switched over that port is copied and forwarded to the Analyzer port - without disrupting the regular processing of packets. By attaching a device to the Analyzer port, you can use this feature to monitor traffic from any 3Com CoreBuilder port.

Configuring an Analyzer Port

Configuration of Analyzer ports should be carried out when a device has been newly attached to a port on the switch.

1. In Nways Manager Remote Monitor's main window, select RAP Configuration from the Configure menu.
2. The Change Analyzer Port dialog box is displayed (Figure 67).



Switches:

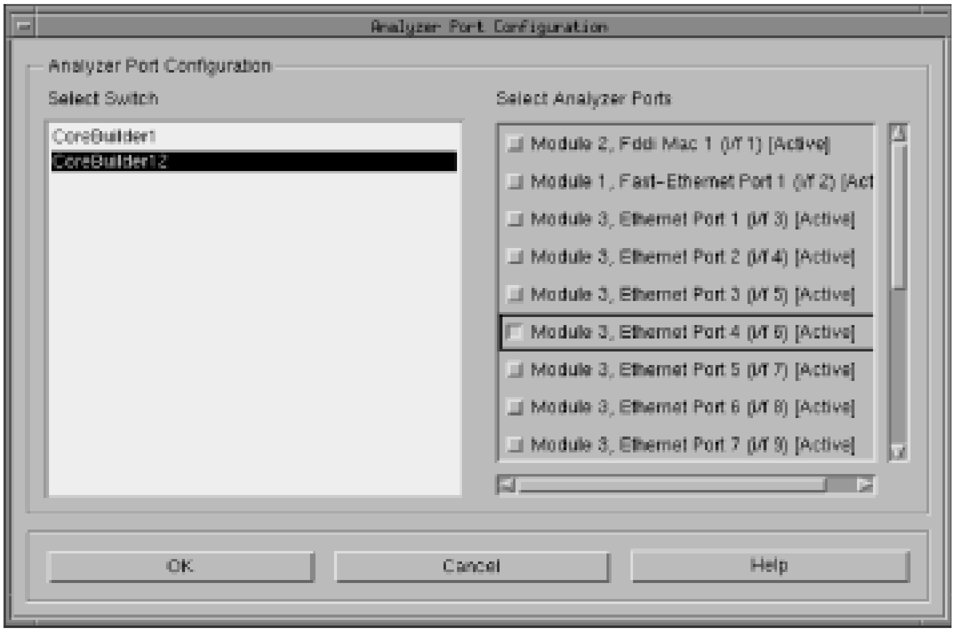
CoreBuilder1
CoreBuilder12

Select Analyzer Port:

CoreBuilder2500, manuf: 3Com (M 1)[Active]

Figure 67. Change Analyzer Port Dialog Box

3. Select a switch from the Switches area. If the switch is available, a list of the Analyzer ports that exist on the switch will be displayed in the Select Analyzer Port area. If it is unavailable, the message `No response from switch` will be displayed.
4. Select an Analyzer port from the Select Analyzer Port area. Note: You should only select ports to which a network analyzer is attached.
5. To change the current configuration of Analyzer ports on the selected switch or any other available switch, click **Configure Analyzer Ports**. The Analyzer Port Configuration dialog box is displayed, as shown in Figure 68 on page 162.



Analyzer Port Configuration

Analyzer Port Configuration

Select Switch

CoreBuilder1
CoreBuilder12

Select Analyzer Ports

- □ Module 2, Fddi Mac 1 (i/f 1) [Active]
- □ Module 1, Fast-Ethernet Port 1 (i/f 2) [Act
- □ Module 3, Ethernet Port 1 (i/f 3) [Active]
- □ Module 3, Ethernet Port 2 (i/f 4) [Active]
- □ Module 3, Ethernet Port 3 (i/f 5) [Active]
- □ Module 3, Ethernet Port 4 (i/f 6) [Active]
- □ Module 3, Ethernet Port 5 (i/f 7) [Active]
- □ Module 3, Ethernet Port 6 (i/f 8) [Active]
- □ Module 3, Ethernet Port 7 (i/f 9) [Active]

Figure 68. Analyzer Port Configuration Dialog Box

a. If required, change the currently selected switch in the Select Switch area. A list of the ports available on the switch will be displayed in the Select Analyzer Port area. Ports currently selected as Analyzer ports are identified by the red button proceeding the port name.

b. To select or deselect ports as Analyzer ports, enable or disable the button preceding the port name.

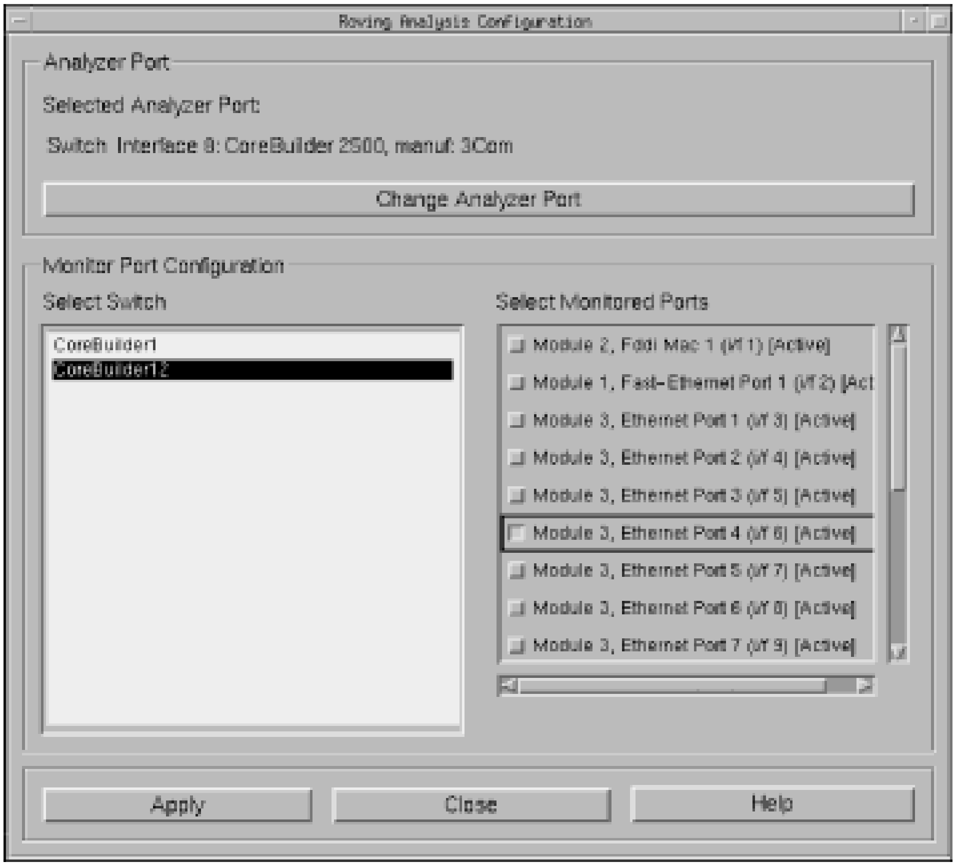
   You should only select ports to which a network analyzer is attached.

c. Click **OK** to save your changes and return to the Change Analyzer Port dialog box, or click **Cancel** to abandon your changes.

Configuring Monitor Ports

Configuring Monitor ports can be carried out at any time as your monitoring requirements change.

1. With an Analyzer port selected in the Change Analyzer Port dialog box, click **OK** to launch the Roving Analysis Configuration dialog box (Figure 69 on page 163). From this dialog box you can set up the ports that are to be monitored.



Selected Analyzer Port:

Switch Interface 8: CoreBuilder 2500, manuf: 3Com

CoreBuilder1
CoreBuilder12

□ Module 2, Fddi Mac 1 (i/f 1) [Active]
□ Module 1, Fast-Ethernet Port 1 (i/f 2) [Act
□ Module 3, Ethernet Port 1 (i/f 3) [Active]
□ Module 3, Ethernet Port 2 (i/f 4) [Active]
□ Module 3, Ethernet Port 3 (i/f 5) [Active]
□ Module 3, Ethernet Port 4 (i/f 6) [Active]
□ Module 3, Ethernet Port 5 (i/f 7) [Active]
□ Module 3, Ethernet Port 6 (i/f 8) [Active]
□ Module 3, Ethernet Port 7 (i/f 9) [Active]

Figure 69. Roving Analysis Configuration Dialog Box

a. If required, select a different Analyzer port to which the traffic on the Monitor port will be copied. Click **Change Analyzer Port** and follow the instructions in step 5 on page 161.

b. To set up the Monitor ports on a switch, select a switch from the Select Switch area. A list of the ports available on that switch will be displayed in the Select Monitored Ports area. Any ports currently being monitored will be highlighted in blue and the button preceding the port name will be selected.

c. To select or deselect a Monitor port, enable or disable the button proceeding the port name in the Select Monitored Ports list.

d. Click **Apply** to configure these ports on the selected switch. Packets from these ports will now be copied and forward to the network analyzer on the specified Analyzer port.

Refer to the documentation accompanying the 3Com CoreBuilder device for more information on Roving Analysis and 3Com CoreBuilder configuration.

Using PACMIB Functionality

The Port Address Correlation MIB (PACMIB) maps port to host data and gathers port statistics for 3Com CoreBuilder 5000 devices on your network. Using the PACMIB function you can generate a table of the MAC addresses of devices connected to each port on a hub.

3Com CoreBuilder 5000 devices with the following cards are supported as shown in Table 43.

Table 43. 3Com CoreBuilder 5000 Supported Cards

Product	Model Number	Module	Version
3Com CoreBuilder 5000 Ethernet Network Monitoring Card	6100-MGT	EMAC	3.0 or higher
3Com CoreBuilder 5000 Advanced Ethernet Network Monitoring Card	6100D-AMGT	GEMINI	2.0 or higher
3Com CoreBuilder 5000 Token Ring Network Monitoring Card	6200-MGT	TRMAC	3.0 or higher

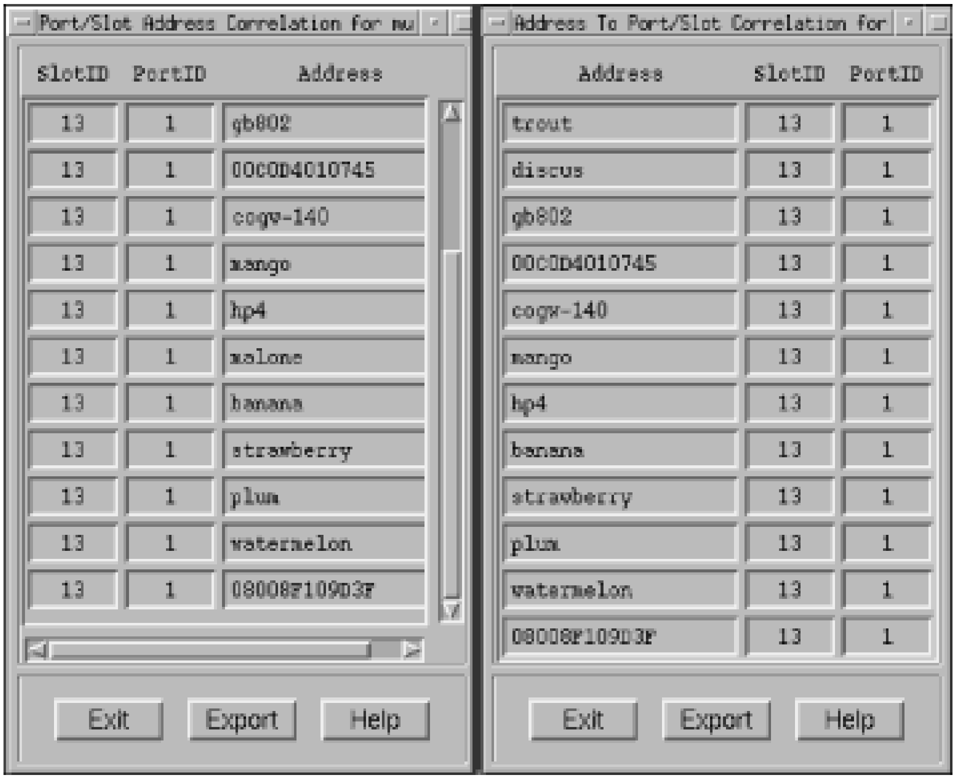
PACMIB data can be viewed in two ways:

- Host to port, sorted by the connected devices’ MAC address.
- Port to host, sorted by the port on the hub.

A table of statistics for each port can also be displayed by clicking an entry in the table.

1. PACMIB will use the device currently being used for monitoring in the main window. If required, follow the procedures in Chapter 4 to select a device and interface for monitoring.
2. To start PACMIB for the monitored device, click PACMIB in the Analysis menu of Nways Manager Remote Monitor’s main window and select Enable/Disable.

   When PACMIB is enabled on the selected device, the device will be reset.
3. From the PACMIB Enable/Disable dialog box, click **Enable**. You will be returned to the main window while the device is warm reset. Refer to “Setting System Parameters” on page 19 for a description of the warm reset process.
4. When the device has been reset and monitoring has been resumed in the main window, select either the Port Host Table or Host Port Table from the PACMIB menu. Figure 70 on page 165 shows examples of the Port to Host and Host to Port Tables.


Port/Slot Address Correlation for mu
Exit
Export
Help
Address To Port/Slot Correlation for
Exit
Export
Help

SlotID	PortID	Address
13	1	gb802
13	1	00C0D4010745
13	1	cogw-140
13	1	mango
13	1	hp4
13	1	malone
13	1	banana
13	1	strawberry
13	1	plum
13	1	watermelon
13	1	08008F109D3F

Address	SlotID	PortID
trout	13	1
discus	13	1
gb802	13	1
00C0D4010745	13	1
cogw-140	13	1
mango	13	1
hp4	13	1
banana	13	1
strawberry	13	1
plum	13	1
watermelon	13	1
08008F109D3F	13	1

Figure 70. Examples of the Port to Host and Host to Port Tables

5. The contents of a PACMIB table can be exported to file, for export to other applications or for printing. The data may be saved in either Flat ASCII or CSV file format. Click **Export** to open the File dialog box and specify the data format and file name.
6. To close a PACMIB Table, click **Exit**.

Appendix F. View and Application Variables

This appendix contains definitions of the variables that may be selected in Nways Manager Remote Monitor's Views and Applications. It contains the following sections:

- Statistics Variables
- History Variables
- Host Variables
- Ring Station Variables
- ECAM Variables

Statistics Variables

The Statistics View presents the following variables on Ethernet, FDDI, and Token Ring.

Variables Available on Ethernet

Table 44. Statistics Variables Available on Ethernet

Bytes Sent	The total number of bytes making up all packets detected on this segment.
Broadcasts	Good packets directed to the broadcast address.
Collisions	The best estimate of the number of collisions on this segment.
CRC Errors	A packet is not an integral number of octets in length or has a bad FCS.
Packets Missed	The number of times the probe detected a lack of resources and so may have missed counting some packets.
Packets Sent	The total number of packets detected - on this segment - including error packets.
Multicasts	Good packets directed to the multicast address. Does not include broadcast packets.
Too Long	Longer than 1518 octets (including FCS octets) but otherwise well formed.
Too Short	Less than 64 octets long (including FCS octets) but otherwise well formed.
Long + CRC	Too long and CRC error. Short + CRC Too short and CRC error. 64 Bytes Packets exactly 64 bytes long. 65 to 127, and so on Packet sizes are inclusive, and include FCS octets.
Short + CRC	Too short and CRC error. 64 Bytes Packets exactly 64 bytes long. 65 to 127, and so on Packet sizes are inclusive, and include FCS octets.
64 Bytes	Packets exactly 64 bytes long.
65 to 127, and so on	Packet sizes are inclusive, and include FCS octets.

Variables Available on FDDI

Table 45. Statistics Variables Available on FDDI

Variable	Description
Beacons	The number of Beacons seen on the ring.
Beacon Src.*	The address of the host that sent the last Beacon.
Broadcasts	Good packets directed to the broadcast address.
Bytes Sent	The total number of bytes making up all packets detected on the ring.
Claim Frames	The number of Claim frames seen on the ring.
Dir. Beacons	The number of Directed Beacons seen on the ring.
Dir. Beacon Src.*	The address of the host that sent the last Directed Beacon.
Errors	A frame with the error indication set.
Missed	The number of times the probe detected a lack of resources and so may have missed counting some packets.
Multicasts	Good packets, excluding broadcast packets, directed to the multicast address.
Packets Sent	Total number of packets detected on this ring, including error packets.
Ring State*	The current operational status of the FDDI ring: 1. Ring Operational 2. Non Operation Claim 3. Non Operational Beacon 4. Non Operational Dir. Beacon 5. Unknown
SMT Frames	The number of SMT frames seen on the ring.
TNEG*	Negotiated token rotation time TNEG. This is the TNEG that succeeded in the bidding process.
Tokens	The number of tokens on the ring.
22 Bytes	Packets exactly 22 bytes long.
23 to 63 etc.	Packet sizes are inclusive and include FCS octets

* Not suitable for graph or dial displays.

Table 46. Statics Variables Available on Token Ring

Variable	Description
Abort Errors	The total number of abort delimiters reported in error reporting packets identified by the probe. A problem was detected by a station while trying to transmit a frame
AC Errors	The total number of AC (Address Copied) errors reported in error reporting packets identified by the probe.
All Route Bcasts	The number of broadcasts issued to any and all addresses on all rings.
All Route Octets	The number of octets making up broadcasts issued to any and all addresses.

Table 46. Statics Variables Available on Token Ring (continued)

Variable	Description
Beacon Events	The total number of times the ring goes into a beaconing state (changing the source address of a beacon packet does not constitute a new beacon event).
Beacon Packets	The total number of beacon MAC packets detected by the probe.
Beacon Time	The total amount of time that the ring has been in a beaconing state.
Burst Errors	The total number of burst errors reported in error reporting packets identified by the probe. Often caused by a very brief disconnection in the cable or a very brief surge of electronic noise.
Claim Token Events	The number of times the ring has gone into the claim token process.
Claim Token Pkts	The total number of claim token packets detected by the probe.
Congestion Errors	The total number of receive congestion errors reported in error reporting packets detected by the probe. A station received a frame and did not have the buffer space to store it.
Data Bytes	The total number of bytes making up all promiscuous data packets detected on this segment.
Data Packets	The total number of promiscuous data packets detected on this segment.
Data Bcast Pkts	Good packets directed to the broadcast address. Does not include multicast packets.
Data Mcast Pkts	Good packets directed to the multicast address. Does not include broadcast packets.
Drop Events	The number of times the probe detected a lack of resources and so may have missed counting some LLC packets or MAC packets.
Error Reports	The total number of soft error report frames detected by the probe. Soft errors are not severe enough to stop the ring functioning - includes line, burst, internal, abort, ACE, lost frame, token, frequency and frame copied errors.
Frames Copied	The total number of frame copied errors reported in error reporting packets detected by the probe. A station believes that another station on the ring has the same address (not usually a problem - refer to the Glossary)..
Frames In	The number of frames coming onto this ring segment from another segment.
Frames Out	The number of frames passing from this ring segment onto another.
Frequency Errors	The total number of frequency errors reported in error reporting packets detected by the probe. A timing error often caused by hooking up more than 72 stations on the ring.
Internal Errors	The total number of adapter internal errors reported in error reporting packets detected by the probe. Often caused by overheating in an overloaded system.
Line Errors	The total number of line errors reported in error reporting packets detected by the probe. Normally caused by electronic noise or cable problems.

Table 46. Statics Variables Available on Token Ring (continued)

Variable	Description
Local LLC Frames	The total number of frames received which had no RIF field (or had a RIF field that only included the local ring's number) and were not All Route Broadcast Frames.
Lost Frames	Lost Frames The total number of lost frame errors reported in error reporting packets detected by the probe. A station transmitted a frame and didn't see it again.
MAC Bytes	The total number of bytes making up all MAC packets detected on this segment.
MAC Packets	The total number of MAC packets detected - including error packets - on this segment.
NAUN Changes	The total number of NAUN changes detected by the probe, caused by a new station opening onto the ring or a station taking itself off the ring.
Octets In	Octets In The number of octets making up frames coming onto this ring segment from another segment.
Octets Out	The number of octets making up frames passing from this ring segment onto another.
Octets Through	The number of octets making up frames passing across this ring segment on the way to their destination.this ring segment on the way to their destination.
Purge Events	The total number of times the ring goes into a ring purge state from a normal ring state (excludes any ring purge states that arise as a result of claim token or beacon states).
Purge Packets	The total number of ring purge MAC packets detected by the probe. This ring's numerical identifier.
Ring Number	This ring's numerical identifier.
Ring Polls	The total number of ring poll events detected by the probe (in other words, the number of ring polls initiated by the Active Monitor).
Sgl Route Bcasts	The number of broadcasts issued to a limited number of recipients - usually the local ring segment.
Sgl Route Octets	The number of octets making up broadcasts issued to a limited number of recipients - usually the local ring segment.
Through Frames	The number of frames passing across this ring segment on the way to their destination.
Token Errors	The total number of token errors reported in error reporting packets detected by the probe. Reported by the Active Monitor when the token gets corrupted.
1 Hop Frames, and so on	The total number of frames that will make either 1, 2, 3, 4, 5, 6, 7, 8, or more than 8 ″hops″ (across bridges between ring segments) to reach their destination.
18 - 63 Bytes, and so on	Packet size distribution.

History Variables

The following tables list the variables available on Ethernet, FDDI and Token Ring.

Table 47. History Variables Available on Ethernet

Variable	Description
Broadcasts	Good packets directed to the broadcast address.
Bytes Sent	The total number of bytes making up all packets detected on this segment.
Collisions	The best estimate of the number of collisions on this segment.
CRC Errors	A packet is not an integral number of octets in length or has a bad FCS.
Long + CRC	Too long and CRC error.
Multicasts	Good packets directed to the multicast address. Does not include broadcast packets.
Packets Missed	The number of times the probe detected a lack of resources and so may have missed counting some packets.
Packets Sent	The total number of packets detected - on this segment - including error packets.
Too Long	Longer than 1518 octets (including FCS octets) but otherwise well formed.
Too Short	Less than 64 octets long (including FCS octets) but otherwise well formed.
Utilization	The percentage of network capacity at the time of this sample period.

Variables Available on FDDI

Table 48. History Variables Available on FDDI

Variable	Description
Beacons	The number of Beacons seen on the ring.
Broadcasts	Good packets directed to the broadcast address.
Bytes Sent	The total number of bytes making up all packets detected on the ring.
Claim Frames	The number of Claim frames seen on the ring.
Dir. Beacons	The number of Directed Beacons seen on the ring.
Errors	A frame with the error indication set.
Mean TRT	Calculated mean time for a token to rotate.
Missed	The number of times the probe detected a lack of resources and so may have missed counting some packets.
Multicasts	Good packets, excluding broadcast packets, directed to the multicast address.
Packets Sent	Total number of packets detected on this ring, including error packets.
SMT Frames	The number of SMT frames seen on the ring.

Table 48. History Variables Available on FDDI (continued)

TNEG	Negotiated token rotation time. This is the TNEG that succeeded in the bidding process.
Utilization	Percentage of network capacity at the time of this sample period.
22 Bytes	Packets exactly 22 bytes long.
22 Bytes	Packets exactly 22 bytes long.
23 to 63 etc.	Packet sizes are inclusive and include FCS octets.

Variables Available on Token Ring

Table 49. History Variables Available on Token Ring

Variable	Description
Abort Errors	The total number of abort delimiters reported in error reporting packets identified by the probe. A problem was detected by a station while trying to transmit a frame.
AC Errors	The total number of AC (Address Copied) errors reported in error reporting packets identified by the probe.
Active Stations	The number of active stations on this ring segment, in other words those taking part in the ring poll.
Beacon Events	The total number of times the ring goes into a beaconing state (changing the source address of a beacon packet does not constitute a new beacon event).
Beacon Packets	The total number of beacon MAC packets detected by the probe.
Beacon Time	The total amount of time that the ring has been in a beaconing state.
Burst Errors	The total number of burst errors reported in error reporting packets identified by the probe. Often caused by a very brief disconnection in the cable or a very brief surge of electronic noise.
Claim Token Events	The number of times the ring has gone into the claim token process.
Claim Token Packets	The total number of claim token packets detected by the probe.
Congestion Errors	The total number of receive congestion errors reported in error reporting packets detected by the probe. A station received a frame and did not have the buffer space to store it.
Data Bcast Packets	Good packets directed to the broadcast address.
Data Bytes	The total number of bytes making up all promiscuous data packets detected on this segment.
Data Mcast Packets	Good packets directed to the multicast address. Does not include broadcast packets.
Data Packets	The total number of promiscuous data packets detected on this segment.
Drop Events	The number of times the probe detected a lack of resources and so may have missed counting some packets.

Table 49. History Variables Available on Token Ring (continued)

Variable	Description
Error Reports	The total number of soft error report frames detected by the probe. Soft errors are not severe enough to stop the ring functioning - includes line, burst, internal, abort, ACE, lost frame, token, frequency and frame copied errors.
Frames Copied	The total number of frame copied errors reported in error reporting packets detected by the probe. A station believes that another station on the ring has the same address (not usually a problem - refer to the Glossary).
Frequency Errors	The total number of frequency errors reported in error reporting packets detected by the probe. A timing error often caused by hooking up more than 72 stations on the ring.
Internal Errors	The total number of adapter internal errors reported in error reporting packets detected by the probe. Often caused by overheating in an overloaded system.
Line Errors	The total number of line errors reported in error reporting packets detected by the probe. Normally caused by electronic noise or cable problems.
Lost Frames	The total number of lost frame errors reported in error reporting packets detected by the probe. A station transmitted a frame and did not see it again.
MAC Bytes	The total number of bytes making up all MAC packets detected on this segment.
MAC Packets	The total number of MAC layer packets detected - including error packets - on this segment.
NAUN Changes	The total number of NAUN changes detected by the probe, caused by a new station opening onto the ring or the current NAUN taking itself off the ring.
Purge Events	The total number of times the ring goes into a ring purge state from a normal ring state (excludes any ring purge states that arise as a result of claim token or beacon states).
Purge Packets	The total number of ring purge MAC packets detected by the probe.
Ring Polls	The total number of ring poll events detected by the probe (in other words, the number of ring polls initiated by the Active Monitor).
Token Errors	The total number of token errors reported in error reporting packets detected by the probe. Reported by the Active Monitor when the token gets corrupted.
18 - 63 and so on	Packet sizes are inclusive, and include FCS octets.
Utilization	Token Ring utilization calculations are based on using the ifSpeed variable from the interface table. If the value is zero, a 16 Mbps ring speed is assumed for the calculation.

Host Variables

The following list of variables is available for the Host View on Ethernet, Token Ring, and FDDI.

Table 50. Host Variables Available on Ethernet, Token Ring and FDDI

Variable	Description
Packets In	The number of packets seen on the segment - including error packets - destined for this station.
Packets Out	The number of packets - including error packets - this station was responsible for sending.
Bytes In	The total number of bytes making up all packets destined for this station.
Bytes Out	The total number of bytes making up all packets this station was responsible for sending.
Error Packets	The number of error packets this station was responsible for generating.
Broadcasts	Good packets transmitted by this station and directed to the broadcast address.
Multicasts	Good packets transmitted by this station and directed to the multicast address. Does not include broadcast packets.

Ring Station Variables

The following variables are available for the Ring Station View on Token Ring.

Table 51. Ring Station Variables Available on Token Ring

Variable	Description
Last NAUN	The physical address of the last known NAUN (Nearest Active Upstream Neighbor) of this station.
Station Status	This station’s status on the ring - either active, inactive or forced off the ring.
Last Entered	The time when this station entered the ring.
Last Exited	The time when this station last exited the ring.
Duplicate Address	The number of times this station experienced a duplicate address error.
In-line Errors	The total number of line errors detected upstream of this station in error reporting packets detected by the probe. Normally caused by electronic noise or cable problems.
Out-line Errors	The total number of line errors detected downstream of this station in error reporting packets detected by the probe. Normally caused by electronic noise or cable problems.
Internal Errors	The total number of adapter internal errors reported in error reporting packets detected by the probe. Normally caused by overheating in an overloaded system.

Table 51. Ring Station Variables Available on Token Ring (continued)

Variable	Description
Inburst Errors	The total number of burst errors detected upstream of this station in error reporting packets detected by the probe. Normally caused by a very brief disconnection in the cable or a very brief surge of electronic noise.
Out Burst Errors	The total number of burst errors detected downstream of this station in error reporting packets detected by the probe. Normally caused by a very brief disconnection in the cable or a very brief surge of electronic noise.
AC Errors	The total number of Address Copied (AC) errors reporting packets sent by the enarest active downstream neighbor of this station.
Abort Errors	The total number of abort delimiters reported by this station in error reporting packets detected by the probe. Similar to an internal error but in this case the fault occurred while transmitting a frame.
Lost Frames	The total number of lost frame errors reported by this station in error reporting packets detected by the probe.
Congestion Errors	The total number of receive congestion errors. Caused when a station receives a frame and does not have the buffer space to store it.
Frame Copied Errors	The total number of frame copied errors reported by this station. A station believes that another station has the same address (often not the case - refer to the Glossary).
Frequency Errors	The total number of frequency errors reported by this station. Caused by large differences between an adaptor’s clock and its NAUN’s clock.
Token Errors	The total number of token errors reported by this station. Similar to a line error, but in this case the token itself is damaged.
In Beacon Errors	The total number of beacon frames detected upstream of this station - refer to the Glossary.
Out Beacon Errors	The total number of beacon frames detected downstream of this station (by the station naming this station as the NAUN) - refer to the Glossary.
Insertions	The number of times the probe detected this station inserting into the ring.

ECAM Variables

This section describes the variables available for the Statistics, Host, Matrix, and Protocol Distribution modules in the ECAM application. Refer to Appendix H for a description of the ECAM application.

Protocol Statistics Variables

The variables common to all Statistics protocols are described below:

Table 52. ECAM Protocol Statistics Variables

Variable	Description
Packets	The total number of packets for this protocol detected on the network.
Bytes	The total number of bytes for this protocol on the network.

Table 52. ECAM Protocol Statistics Variables (continued)

Variable	Description
Fragment Packets	The total number of packets for this protocol that have been fragmented, detected on the network.
Fragment Bytes	The total number of bytes that make up the fragment packets detected on the network.
Broadcast Packets	The total number of packets for this protocol directed to the broadcast address on the network.
Broadcast Bytes	The total number of bytes that make up the broadcast packets detected on the network.

Host Protocol Variables

The variables common to all Host protocols are described below:

Table 53. ECAM Host Protocol Variables

Variable	Description
In Packets	The total number of packets of this protocol type detected on the network, destined for this station.
Out Packets	The total number of packets of this protocol type detected on the network, sent by this station.
In Bytes	The total number of bytes for this protocol on the network, destined for this station.
Out Bytes	The total number of bytes for this protocol on the network, sent by this station.
In Fragment Packets	The total number of packets for this protocol which have been fragmented, detected on the network, destined for this station.
Out Fragment Packets	The total number of packets sent by this station for this protocol which have been fragmented on the network.
In Fragment Bytes	The total number of bytes making up the fragment packets detected on the network, destined for this station.
Out Fragment Bytes	The total number of bytes making up the fragment packets detected on the network, sent by this station.
Out Broadcast Packets	The total number of packets for this protocol directed to the broadcast address on the network, sent by this station.
Out Broadcast Bytes	The total number of bytes making up these broadcast packets detected on the network, sent by this station

Matrix Protocol Variables

The variables common to all Matrix protocols are described below:

Table 54. ECAM Matrix Protocol Variables

Variable	Description
Packets	The total number of packets for this conversation and protocol, detected on the network.

Table 54. ECAM Matrix Protocol Variables (continued)

Variable	**Description**
Bytes	Bytes The total number of bytes for this conversation and protocol detected on the network.
Fragment Packets	The total number of packets for this conversation and protocol that have been fragmented, detected on the network.
Fragment Bytes	The total number of bytes that make up the fragment packets for this conversation and protocol, detected on the network.
Broadcast Packets	The total number of packets for this conversation and protocol directed to the broadcast address on the network.
Broadcast Bytes	The total number of bytes that make up the broadcast packets for this conversation and protocol, detected on the network.

Appendix G. Enterprise Communications Analysis Module (ECAM)

This chapter tells you how to use Nways Manager Remote Monitor's RMON2 (ECAM) Application, which is available when the RMON2 (ECAM) SmartAgent software has been downloaded. It contains the following sections:

- ECAM Application Overview
- Downloading SmartAgent Software
- ECAM Display
- Collecting ECAM Statistics
- Protocol Statistics
- Host Protocol Statistics
- Matrix Protocol Statistics
- Protocol Distribution

Traditional protocol analyzers and RMON give the network manager an in-depth view of a single segment. ECAM allows the network manager to view internetwork traffic for troubleshooting and other operations

Where the term ECAM is used in this chapter, this implies RMON2 (ECAM).

ECAM Application Overview

The Enterprise Communications Analysis Module (ECAM) Application lets you collect and view protocol statistics and filtered protocol statistics. You can go beyond the original RMON standard to full seven layer data collection, including segment, host and conversation statistics for the major protocols and application types. Data collected can be exported in either ASCII or CSV format.

ECAM statistics can only be gathered from devices which have the RMON2 (ECAM) SmartAgent software downloaded. Refer to "Downloading SmartAgent Software" for instructions.

Downloading SmartAgent Software

SmartAgent software can be loaded or unloaded from a device to make additional functionality available in Nways Manager Remote Monitor's main window. The software can be started and stopped as required, depending on the type of data you wish to collect with the device.

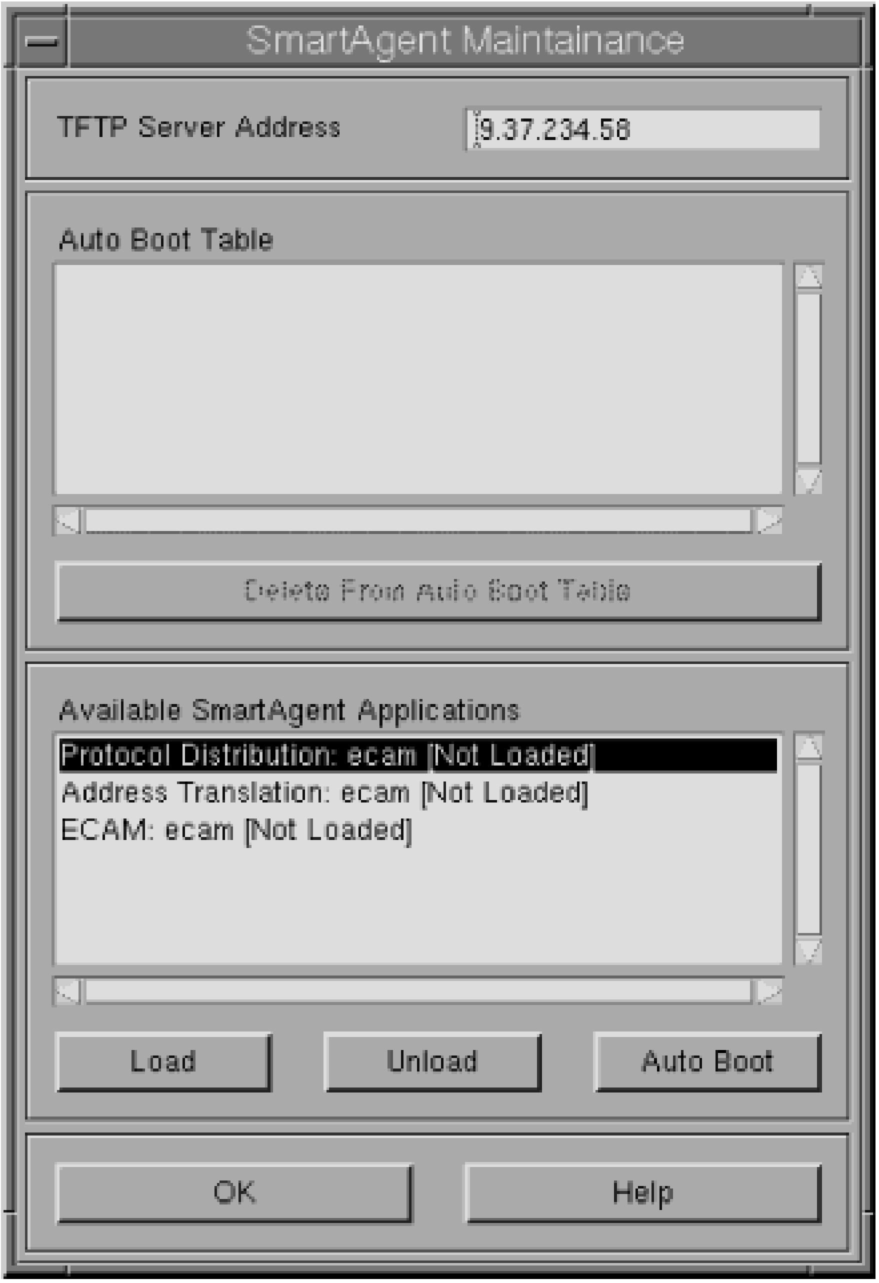
RMON2 (ECAM) SmartAgent software is shipped with Nways Manager Remote Monitor.

- If you are using an RMON2-compliant device, the RMON2 standard provides this functionality by default, and you do not need to download the software. Refer to "RMON2 Functionality" on page 21.

- If you are using a supported RMON device that does not have RMON2 functionality, you need to download the RMON2 (ECAM) SmartAgent software to get this functionality. The following sections describe how to do this.

Download Procedure

Use the SmartAgent Maintenance dialog box, shown in Figure 71 on page 181, to load or unload SmartAgent software. To access the dialog box, click **SmartAgent Administration** in the Device Administration dialog box.



TFTP Server Address: 9.37.234.58

Protocol Distribution: ecam [Not Loaded]
Address Translation: ecam [Not Loaded]
ECAM: ecam [Not Loaded]

Figure 71. SmartAgent Maintenance Dialog Box

The Available SmartAgent Applications area displays a list of available applications, as the application name followed by the name of the underlying software. The status of an application is displayed after the application name. If the software for any listed applications is already downloaded to the device, the status `[Loaded]` is displayed, followed by the version number and size of the application.

The number of times that this software has been loaded to the device without unloading is also displayed as `# References`.

Enabling Applications

A TFTP server must be active before you can load SmartAgent software. Refer to “Downloading Firmware” on page 22 for instructions on starting the TFTP server.

To load SmartAgent software, follow these steps:

1. Make sure that the SmartAgent software is available on the TFTP server.
2. If required, change the address in the TFTP Server area. By default, the software is stored in the installation directory and the TFTP server address is set to your host’s address.
3. Select an application from the Available SmartAgent Applications area. When the software for this application is loaded to the device, all applications based on the same underlying software will be available in the main window.
4. Click **Load**. The device contacts the TFTP server and, if it is available, loads the selected software. If successful, the status of the applications changes to [Loaded].

If the device is unable to load the software, this may be because:

- The selected software is not stored on the specified TFTP server.
- The device has become unavailable.
- RMON2 is still enabled on the device.
- The TFTP server is unavailable or the TFTP server address has been entered incorrectly.

To resolve this, check the following and then repeat the procedure above.

- TFTP is enabled on your system (setting up TFTP on your system is described in the Release Notes)
- You have disabled RMON2 on the device.
- The SmartAgent software is stored in the TFTP area.
- The community name being used gives sufficient access rights (refer to “Setting Up Trap Communities” on page 34 for more information on community names).
- The selected device supports SmartAgent software.

If you are still unable to load the SmartAgent software, return to the Device Administration dialog box and try reselecting the device to check that it is available.

Disabling Applications

To disable SmartAgent applications, follow these steps:

1. Select an application in the Available SmartAgent Applications list. You must select an entry that has the [Loaded] status.

   Disabling an application also disables all other applications based on the same software.
2. Click **Unload**.
   - If the software has only been loaded on the device once previously, the status of the applications is set to `[Not Loaded]`.
   - If the software has been loaded on the device more than once, then the status of the application will remain as `[Loaded]` but the References number at the end of the application entry will be reduced by one. To unload the software, press **Unload** as many times as required to set the status to `[Not Loaded]`.

     If the status remains as `[Loaded]` and the References number does not decrease, check that you are using a community name with sufficient access rights.

Auto Boot Table

If you require SmartAgent software on a device at all times, you can register it in the device's Auto Boot table. The Auto Boot table contains the name of software to load automatically when the device is warm reset. It also shows the TFTP server address the device will contact to find the software.

Registering Software

To register software in the Auto Boot table, follow these steps:

1. Select an application in the Available SmartAgent Applications list.
2. Click **Auto Boot**. Registered software is displayed in the Auto Boot table with the initial status of `[Not Loaded - Idle]`.

Please note that although the application name appears in the Auto Boot table, you are in fact registering the SmartAgent software to be loaded the next time the device is restarted. When the device is reset, all the functionality for that software is enabled.

When the device is warm reset, it attempts to contact the appropriate TFTP server to load that software. If it is successful, the status of the SmartAgent software in the Auto Boot table is set to `[Autoboot Succeeded]`.

If the attempt to load the software is unsuccessful, the message `[Autoboot Failed]` is displayed.

Disabling Software

To disable applications and remove SmartAgent software from the Auto Boot table, follow these steps:

1. Select the application in the Auto Boot table list.
2. Click **Delete** from Auto Boot Table.

The software is still available to its associated applications in the Available SmartAgent Applications list, but the applications are no longer reloaded onto the device when the device is rebooted.

Launching ECAM

Select ECAM Views from the Tools menu in Nways Manager Remote Monitor's main window. The ECAM Views menu contains the following options:

- Statistics
- Host
- Matrix
- Protocol

These are described later in this chapter.

ECAM Display

Table 55 shows the different display types available in ECAM.

Table 55. ECAM Displays

Function	Table	Dial	Line Graph	Stacked Bar	Pie Chart	Bar Chart
Statistics	■	■	■			
Host	■	■	■			
Matrix	■	■	■			
Protocol Distribution				■	■	■

These different display types and their available display options are explained in the following sections.

Table (Statistics, Host, and Matrix)

The Table display allows you to view segment, host and conversation statistics as absolute, delta or rate based values. You can save the data in either ASCII or CSV file format.

Dial (Statistics, Host, and Matrix)

The Dial display shows the rate of change for each of the protocol data sets. A dial is displayed for each of the statistics gathered.

Line Graph (Statistics, Host, and Matrix)

The Line Graph display plots the statistics being gathered. By selecting an item in the key, the value of the selected variable can be multiplied by a factor to rescale the graph. This allows you to promote or demote the display of individual statistics.

Bar, Stacked Bar, and Pie Chart (Protocol Distribution only)

The Bar Chart displays data in vertical bars placed side by side for easy analysis. To allow a quick determination of the relative protocol breakdowns, the Stacked Bar and Pie Chart displays can be used.

Click an area within the graph to display a label showing the protocol name and what percentage it makes of the total traffic seen on the network. Click again on the area to remove the data label.

Display Options

Each display type has a number of options available. The functions provided for each of the display types are shown in Table 56.

Table 56. Display Options

Display Options	Description
Export	For table displays, this function saves data to file for export to other applications or for printing. The data may be saved in either ASCII or Comma Separated Variable file format. Selecting this option displays a file dialog box allowing the data format and file name to be specified.
Print	For Protocol Distribution and graph displays, this function allows graphs to be printed on a Postscript printer. Selecting this option displays a print dialog box which allows you to designate a printer to send the data to or a file to save the data in and the paper layout and size.
Grid On/Off	For Protocol Distribution and graph displays, this function toggles the display of grid lines on the graphs.
Address Display Mode	For the Host and Matrix Views, the address information may be displayed either by Name, by Network Layer Address or by MAC Address. Selecting one of these options defines how the addresses will be displayed for subsequent updates.
Displayed Data Value	For table displays, the format of the displayed data can be modified to display either Absolute Value, Delta Value or Rate per Second. Selecting one of these options defines how the data will be displayed for subsequent updates.
Display Style	For Protocol Distribution displays, the data can be displayed as either a bar graph, stacked bar graph or pie chart. Selecting one of these options changes the current display style.

To calculate the Rate per Second, ECAM uses the value of each statistic at the last update and the present value. When a new entry is created in a table display, for instance if a previously unseen protocol appears on the network, ECAM will not have a previous value to refer to. In this case, the whole table will default to display the absolute value. At the next update, if no new entries are made to the table, the table will revert to display the Rate per Second.

Update

In addition to the update rate specified in the module’s Configuration dialog box, you can force an update at any time by clicking **Update**.

Collecting ECAM Statistics

Collecting ECAM Statistics ECAM gives you full control over both the source and protocols for which statistics are gathered. The data source can be one of the following:

- Physical interface
- Virtual interface
- Capture configuration

For example, using a virtual interface you can filter for the traffic going to or coming from a network router. By using ECAM to analyze this filtered data, you can see which protocols are being sent via the router. Where the router is connecting LANs via an expensive WAN link, this information lets you establish who is using the link and for what functions. The host and conversation information can then be used as the basis for accounting and performance analysis.

Adding or Modifying a Data Source

Data sources can be added and modified for all of the ECAM functions in the same way.

1. In the ECAM function’s Configuration dialog box, select a device in the Select Device list.
2. Click **Add** to create a new data source, or **Modify** to edit a data source. The Data Source dialog box is displayed.
3. Select a physical or virtual interface from the list of available interfaces displayed in the Select Interface list. Refer to “Setting the IP Address and Subnet Mask” on page 24 for more information on virtual interfaces.
4. By default, all protocols available on the selected interface are selected in the Select Protocols list.
   - To deselect all protocols, click **Clear**.
   - To select all protocols, click **Select All**.
   - To select or deselect specific protocols, click each protocol button.
5. Click **OK** to create this data source, or **Cancel** to abandon your selections, and return to the Configuration dialog box.

When you create a data source, it is displayed in the Data Source list as the interface name followed by a list of the selected protocols.

Protocol Statistics

The Statistics display presents information about the protocols detected on the network segment. For each protocol a set of statistics variables are monitored, some of which are common to all protocols, while others are specific to a particular protocol. Refer to “ECAM Variables” on page 175 for a list of the variables available in the ECAM Statistics module.

Configuring the Protocol Statistics View

To open the ECAM Statistics Configuration dialog box, select Statistics from the ECAM menu in the Nways Manager Remote Monitor main window.

1. In the Select Device list, select the device whose statistics you want to analyze.

   If the RMON2 (ECAM) SmartAgent software is not downloaded, then a dialog box will be displayed allowing the software to be loaded. Please refer to “Downloading SmartAgent Software” on page 179 for an explanation of the loading and unloading of SmartAgent software.

2. In the Select Source list, select the data source whose statistics you want to analyze. To create a new data source or modify an existing one, click **Add** or **Modify** and refer to “Adding or Modifying a Data Source” on page 186.

3. A list of the protocols specified in the Data Source dialog box is displayed in the View area. The selection to be used in this display can be narrowed without affecting the list of protocols configured for the selected Data Source.

   a. Click **Edit View...** to open the Protocol Selection dialog box.

   b. Deselect any of the configured protocols by clicking the protocol button. You cannot select any protocols that were not configured for this data source.

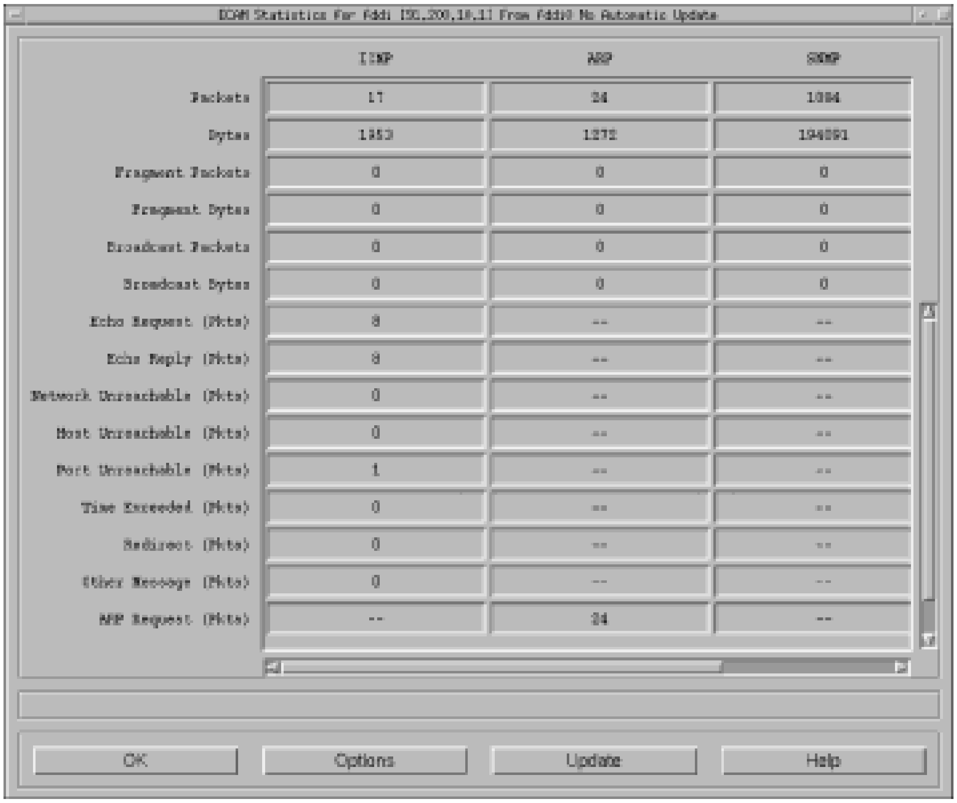
   c. Click **OK** to save your changes or **Cancel** to abandon them.

4. You can display the Statistics view in one of three ways - as a table, dials or graphs (refer to Table 55 on page 184). Click the View Type required.

5. In the Update Rate area, specify how often to update the displays. This option is only available for dial and graph displays and determines how often the displays are refreshed with new data.

   You can also force an update of data in the Statistics display by clicking **Update**.

6. Click **OK** to start the Statistics dialog box, shown in Figure 72 on page 188.



ECAM Statistics For fddi [151.200.10.1] From fddi0 No Automatic Update

	ICMP	ARP	SNMP
Packets	17	24	1084
Bytes	1353	1272	194091
Fragment Packets	0	0	0
Fragment Bytes	0	0	0
Broadcast Packets	0	0	0
Broadcast Bytes	0	0	0
Echo Request (Pkts)	8	--	--
Echo Reply (Pkts)	8	--	--
Network Unreachable (Pkts)	0	--	--
Host Unreachable (Pkts)	0	--	--
Port Unreachable (Pkts)	1	--	--
Time Exceeded (Pkts)	0	--	--
Redirect (Pkts)	0	--	--
Other Message (Pkts)	0	--	--
ARP Request (Pkts)	--	24	--

Figure 72. ECAM Statistics Dialog Box

Refer to “Line Graph (Statistics, Host, and Matrix)” on page 185 for a description of the multiplier function available for the graph display.

Host Protocol Statistics

Like the Statistics function, the Host function monitors protocol statistics detected on the network segment. However, statistics are gathered for each host rather than just for the segment.

Host information may be displayed as a table or - for station displays - dials or graphs. Per host information allows the performance of specific protocols to be monitored for that device.

Configuring the Host Protocol Statistics View

To open the ECAM Host Configuration dialog box, select **ECAM View** from the Tools menu, then select **Host**.

1. In the Select Device list, select the device whose host protocol statistics you want to analyze.

   If the RMON2 (ECAM) SmartAgent software is not downloaded, then a dialog box will be displayed allowing the software to be loaded. Please refer to “Downloading SmartAgent Software” on page 179 for an explanation of the loading and unloading of SmartAgent software.

2. In the Select Source list, select the data source whose host statistics you want to analyze. To create a new data source or modify an existing one, click **Add** or **Modify** and refer to “Adding or Modifying a Data Source” on page 186.

3. Depending on your line of investigation you can sort host entries in a number of different ways:

   By Protocol
   Sorts hosts entries by protocol type in table format only.

   By Address
   Sorts host entries by IP address and then by protocol, in table format only.

   By Selected Stations
   Sorts entries by the specified station and then by protocol, in table, dial or graph format.

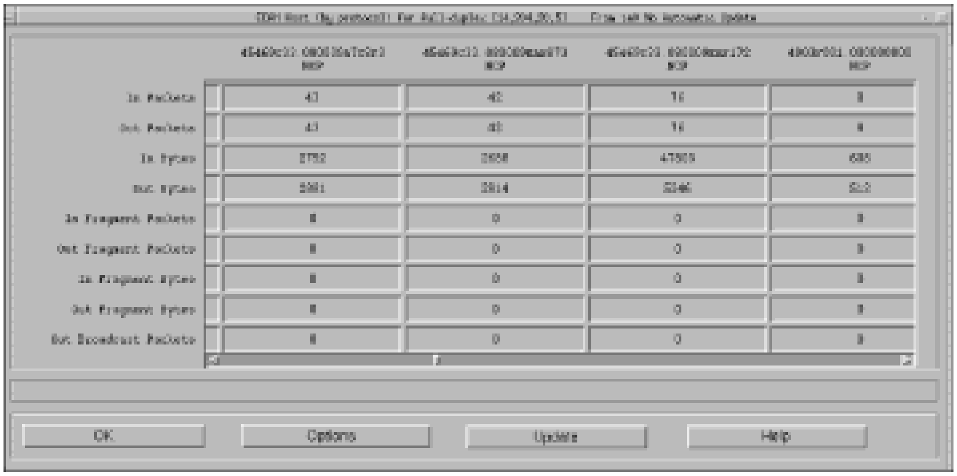
   When the by Selected Stations option is selected, the Select button becomes active. Click Select to open the Station Select dialog box and specify the stations that are to be included in this view. Refer to “Using the Station Select Dialog Box” on page 72 for a description of the station selection process.

4. You can display the Host view as a table or, for by Selected Station displays, as graphs or dials. Click a View Type to select it.

5. In the Update Rate area, specify how often to update the displays. This option is only available for dial and graph views and determines how often the displays are refreshed with new data.

   You can also force an update of data in the Host display by clicking **Update**.

6. Click **OK** to start the Host dialog box, shown in Figure 73 on page 190.



	[illegible]	[illegible]	[illegible]	[illegible]
In Packets	43	42	76	8
Out Packets	43	42	76	8
In Bytes	2752	2658	47509	686
Out Bytes	5381	2814	5246	512
In Fragment Packets	0	0	0	0
Out Fragment Packets	0	0	0	0
In Fragment Bytes	0	0	0	0
Out Fragment Bytes	0	0	0	0
Out Broadcast Packets	0	0	0	0

Figure 73. ECAM Host Dialog Box

Refer to “Line Graph (Statistics, Host, and Matrix)” on page 185 for a description of the multiplier function available for the graph display.

Matrix Protocol Statistics

Like the Statistics function, the Matrix function monitors protocol statistics detected on the network segment. However, the statistics are gathered for each host-to-host conversation rather than for the segment.

Configuring the Matrix Protocol Statistics View

To open the ECAM Matrix Configuration dialog box, select ECAM Views from the Tools menu, then select Matrix.

1. In the Select Device list, select the device whose statistics you want to analyze.

   If the RMON2 (ECAM) SmartAgent software is not downloaded, then a dialog box will be displayed allowing the software to be loaded. Please refer to “Downloading SmartAgent Software” on page 179 for an explanation of the loading and unloading of SmartAgent software.

2. In the Select Source list, select the data source whose statistics you want to analyze. To create a new data source or modify an existing one, click **Add** or **Modify** and refer to “Adding or Modifying a Data Source” on page 186.

3. Depending on your line of investigation you may sort Matrix entries by Address or by Selected Station:

   By Address

   Sorts host entries by IP address and then by protocol, in table format only.

By Selected Stations
Sorts entries by the specified station and then by protocol, in table, dial or graph format.

When the by Selected Stations option is selected, the Select button becomes active. Click **Select** to open the Station Select dialog box and specify the stations that are to be included in this view. Refer to “Using the Station Select Dialog Box” on page 72 for a description of the station selection process.

4. You can display the Matrix view as a table or, for by Selected Station displays, as graphs or dials. Select the View Type you require.
5. In the Update Rate area, specify how often to update the displays. This option is only available for dial and graph views and determines how often the displays are refreshed with new data.

   You can also force an update of data in the Matrix display by clicking **Update**.
6. Click **OK** to start the Matrix display.

Refer to “Line Graph (Statistics, Host, and Matrix)” on page 185 for a description of the multiplier function available for the graph display.

Protocol Distribution

The Protocol Distribution function presents a summarized view of the protocols detected, both on an individual network segment and specific to a particular host. The display shows the relative usage of each of the monitored protocols by packet and byte rate.

Using the ECAM Protocol Distribution function you can quickly see the protocols and applications using the network and from there, focus on the applications being used by a particular host.

Configuring the Protocol Distribution View

To open the ECAM Protocol Distribution Configuration dialog box, select ECAM Views from the Tools menu, then select Protocol.

1. In the Select Device list, select the device whose statistics you want to analyze.

   If the RMON2 (ECAM) SmartAgent software is not downloaded, then a dialog box will be displayed allowing you to load the software. Please refer to “Downloading SmartAgent Software” on page 179 for an explanation of the loading and unloading of SmartAgent software.
2. In the Select Source list, select the data source whose statistics you want to analyze. To create a new data source or modify an existing one, click **Add** or **Modify** and refer to “Adding or Modifying a Data Source” on page 186.
3. In the Calculate Distribution area, choose the way the Protocol Distribution should be calculated:

By Selected Source
The overall protocol distribution for the monitored network will be displayed.

By Selected Stations
Protocol distribution for each of the selected stations will be displayed.

When the by Selected Stations option is selected, the Select button becomes active. Click Select to open the Station Select dialog box and specify the stations that are to be included in this view. Refer to “Using the Station Select Dialog Box” on page 72 for a description of the station selection process.

4. Select the initial display style for the Protocol Distribution view - as a pie chart, a bar graph or a stacked bar graph (refer to “ECAM Display” on page 184). The view type can be changed later from the Option menu in the display window.
5. In the Update Rate area, specify how often to update the displays.

   You can also force an update of data in the Protocol Distribution display by clicking **Update**.
6. Click **OK** to start the Protocol Distribution display, as shown in Figure F-6.

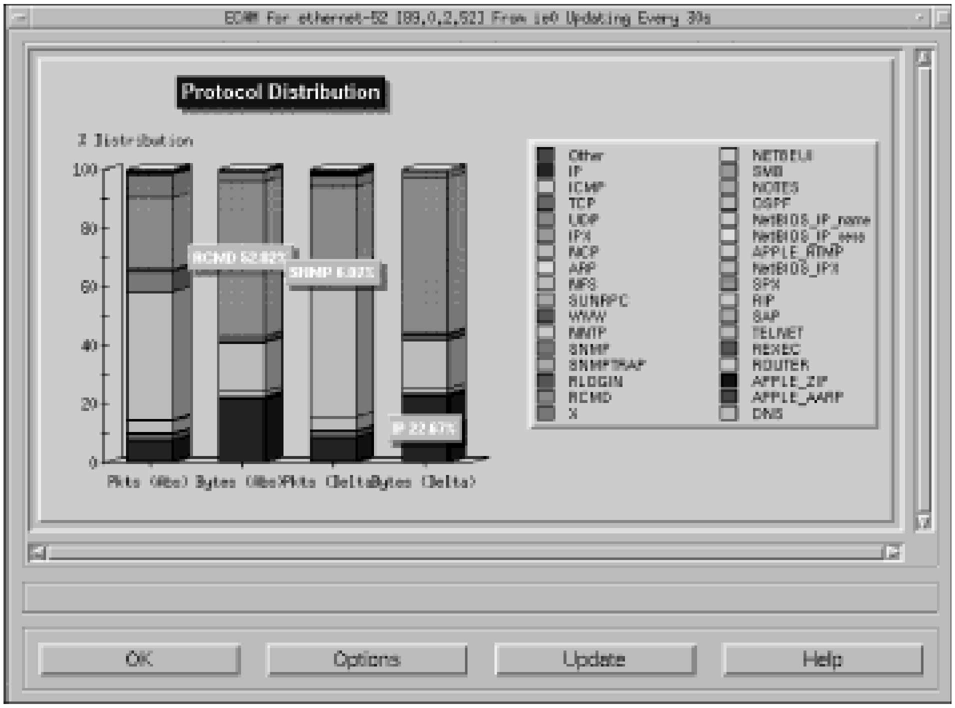


Figure 74. Example of a Protocol Distribution Graph with Data Labels

Protocol Distribution Display

The Protocol Distribution Graphs display the percentage of the total network traffic generated for each selected protocol. The display will refresh automatically during viewing according to the Update Rate specified in the Protocol Distribution view.

Click **Update** at any time to refresh the data.

To switch between display types, use the Display Style option available from the Options menu. Refer to Table 56 on page 185 for an explanation of the functions available from the Options menu.

Protocols are color-coded for easy identification. In addition, clicking the appropriate part of the graph will post a data label for that protocol, giving the protocol name and its distribution percentage. To remove the data label, click the graph again.

Selected software will be loaded if the device reboots. Software for the selected applications will be loaded to the device.

Appendix H. Known Problems

This section describes the known problems and limitations that have been identified for Nways Manager Remote Monitor.

NMDsc06794

When upgrading Nways Manager Remote Monitor, you may see the following warning message during the install process: The dcserver is still running. If you continue the installation it will be shut down. Do you want to continue? This message may appear even if Nways Manager Remote Monitor has been completely shut down.

Workaround: The dcserver process is never killed, even if you have shut down Nways Manager Remote Monitor. If you are not running any copies of Nways Manager Remote Monitor or Nways Manager - Traffic Monitor, it is safe to allow the install process to kill the dcserver process by answering yes to the warning shown above.

NMDsc06879

When launching Nways Manager Remote Monitor from OpenView, the selected device may not be recognized immediately by Nways Manager Remote Monitor - The modify current View dialog box opens, and the main widow graphs show the message No Device Selected. This is because OpenView does not make available enough information about the device to allow Nways Manager Remote Monitor to sue it immediately.

Workaround: To resolve this problem, add the device's IP address and community name manually in the Device List Editor dialog box. This is accessible from the Device Administration dialog box. You only need to add these details the first time the device is accessed from Nways Manager Remote Monitor.

Additional Online Help Viewers May Appear

A new viewer may open each time that online help is launched within the application.

Workaround: Close each online help viewer by selecting File and Exit from the viewer menu bar.

″Error - Can't contact dcserver″ or ″bad address″ error appears when launching Nways Manager Remote Monitor

This error is caused by a socket file, .dcserver, that has been left in the /tmp directory from an earlier session where the system has not shut down properly or the dcserver has crashed. Nways Manager Remote Monitor will start, but multi-segment graphs cannot be generated.

Workaround: To resolve this problem:

1. Quit Nways Manager Remote Monitor by clicking **Exit**.
2. Determine if the socket file is owned by someone other than the current user by entering the following command:

```
ls -1 /tmp/.dcserver
```

If someone else owns the file, check with the owner before proceeding.

3. Change to superuser: su and enter the password when prompted.
4. Delete the .dcserver file: rm /tmp/.dcserver
5. Start Nways Manager Remote Monitor.

Removing columns in graphs confuses scales on axis

If you remove columns from a graph, the scales that appear on the graph axis may be set to an inappropriate scale and could appear unreadable.

Glossary

AC. The Access Control field in frame header.

ACE. Address Copied Error. When a station reports this it indicates a problem with the station upstream rather than with itself, normally someone else on the Token Ring with this station’s address. An isolating error.

AMP. Active Monitor Present - a frame broadcast periodically by the Active Monitor on a Token Ring to start the Ring Poll process.

Abort. The same as a Token Ring internal error except the fault occurred while transmitting a frame. An isolating error.

Active Monitor. Chosen at random, the Active Monitor is the adaptor responsible for generating the token when it is lost or corrupted on a Token Ring.

Adapter. Each station on a Token Ring connects to the ring through a Token Ring adaptor. The adaptor has its own microprocessor and runs its own software. So, ring-specific processing - for example, the responsibilities of being Active Monitor - does not affect the performance of the station.

Application Layer. Layer seven, the uppermost part of the OSI network layer model. This layer contains the user and application programs.

Backbone. The part of a network used as the primary path for transporting traffic between network segments.

Bandwidth. Information capacity, measured in bits per second, that a channel can transmit. The bandwidth of Ethernet is 10 Mbps, the bandwidth of Fast Ethernet is 100 Mbps. FDDI bandwidth is 100 Mbps. Token Ring bandwidth is 4/16 Mbps.

Beacon. If a problem arises on a Token Ring a station may start receiving garbage packets (streaming signal error) or nothing at all (signal loss error). This station then broadcasts a beacon to repeat the error frame containing the address of its Nearest Active Upstream Neighbor (NAUN). When the NAUN recognizes itself in the beacon frame it removes itself from the ring and tests itself. If it detects an error it cannot fix it stays off the ring, otherwise it comes back on. If there is no error, the beaconing station then tests itself to see if it is causing the error. Beaconing is a level 1 error.

Bit. Either of the digits 0 or 1 when used in the binary numeration system. Eight bits equals a single byte. Broadcast . All good frames destined for the broadcast address, in other words sent out to all stations on the network. Some broadcasts are limited to the local network, and some broadcasts may cross onto other networks.

Broadcast. All good frames destined for the broadcast address, in other words, sent out to all stations on the network. Some broadcasts are limited to the local network, and some broadcasts may cross onto other networks.

Buffer. The space allocated to the storage of filtered packets as they are captured from the network. A probe only has a limited set of resources to hold buffer data. If one of the buffers uses all of the probe’s resources, it will stop the other buffers from capturing packets. To conserve resources, you can slice packets or assign maximum sizes to buffers.

Burst Error. More severe than a line error, burst errors are normally caused by either a very brief disconnection in the Token Ring cable or a very brief surge of electronic noise that was not severe enough to result in beaconing. An isolating error.

Bytes. The total number of bytes making up a frame - includes FCS octets.

Client. Any application that retrieves and displays data from probes or agents.

Collision. The best estimate of the number of collisions on an Ethernet segment.

Community Name. Also known as Community String. SNMP uses community names to limit access to certain device management functions. The Community Name used when accessing a device determines which functions may be accessed.

Congestion. Reported by a station on a Token Ring when it receives a frame and doesn't have the buffer space to store it. Because we don't report who is flooding this adaptor, this is a non-isolating error.

Contention. The process used to select a new Active Monitor on a Token Ring - normally selects the station with the lowest address. A level 3 error.

CRC Align Error. An Ethernet packet between 64 and 1518 octets long inclusive (includes FCS octets) - not an integral number of octets in length or has a bad FCS.

CSMA/CD Carrier. Carrier Sense Multiple Access with Collision Detection. The Ethernet protocol that allows each device to create and send its own data packets. CSMA/CD is used to avoid excessive collisions between packets as they are randomly transmitted. A CSMA/CD device first listens for other carriers, if it detects no other carriers, it will then allow the data packet to be transmitted. If a collision is detected, the device stops transmitting, waits a random length of time, and begins transmitting again

Data Link Layer. The second layer of the OSI reference model. This layer is responsible for controlling message traffic.

Data Packet (Packet). A sequence of binary digits, including data and control signals that is transmitted across a LAN.

Default Gateway. The IP address of a device, usually a router or gateway, to which the probe directs all packets not destined for its subnet.

ED. Ending Delimiter - a distinctive byte marking the end of a frame or a token.

Errors. Token Ring defines 4 error levels. At the highest (or most severe) level is beaconing. Monitor contention is the next highest, followed by ring purge. The least severe errors - at level 1 - are soft errors.

Forwarding. The process of sending a frame towards its destination by an intranet working device.

Fragment Packet. An Ethernet packet less than 64 octets long (excludes frame bits but includes FCS octets) - not an integral number of packets in length or has a bad FCS.

Frame. A collection of data (otherwise known as a packet). On Token Ring, token frames are only 3 bytes long while information frames can be over 18000 bytes.

Frame Copy Error. Reported by a station on a Token Ring when it believes another station may have the same address. Usually this is due to transparent bridges opening onto the ring and is very seldom a real problem. A non-isolating error.

Frequency Error. Occurs when the signal received by an adaptor on a Token Ring - from its NAUN - differs from its own internal clock by too much. Often caused by hooking up more than 72 stations and more prevalent in 16 Mbps operations. Also known as a jitter. A non-isolating error.

HDLC. High-Level Data Link Control. OSI bit-orientated protocol.

Host. A device or computer on an IP network to which you can connect.

Hop. The process of crossing a bridge between Token Rings - a count from 1 to 8. The number of hops and the hops themselves are stored in a frame's header.

Jabber Packet. An Ethernet packet longer than 1518 octets (excludes frame bits but includes FCS octets) - not an integral number of octets in length or has a bad FCS.

Internal Error. There was a problem with the originating station on a Token Ring, since recovered. Often caused by overheating in an overloaded system. An isolating error.

ICMP. Internet Control Message Protocol. Internet protocol that reports errors and provides other information relevant to IP packet processing.

IEEE. Institute of Electrical and Electronics Engineers.

IETF. Internet Engineering Task Force, whose responsibilities include specification of protocols and recommendation of Internet standards via the Request for Comment (RFC) process.

Isolating Error. An error that can be pinpointed to a specific station or location on a Token Ring (see also non-isolating error).

Line Error. On Token Ring, a packet is detected which is not an integral number of octets in length or has a bad FCS. Normally caused by electronic noise or cable problems. An isolating error.

Long Packet. See oversize packet.

Lost Frame. When a station transmits a frame around a Token Ring and doesn't get it back. Reported by the originating station. A non-isolating error.

MAC Frames. Token Ring defines two main frame types - data frames and ring management frames. MAC (Media Access Control) frames are used to maintain the health of the network and to help isolate errors on the network. The LANServant Manager lets you monitor MAC layer (ML) frames as well as data frames (see also Token Frames).

MIB. Management Information Base.

NAUN. Nearest Active Upstream Neighbor on a Token Ring (see beacon).

Multicast. Good packets directed to the multicast address. Does not include broadcast packets. Multicasts are similar to broadcasts but have a more limited scope, for example they may be directed to all bridges on a ring.

Oversize Packet. An Ethernet packet longer than 1518 octets (including FCS octets) but otherwise well formed.

Network Layer. The third layer of the OSI reference model. This layer is responsible for controlling message traffic.

Non-Isolating Error. A Token Ring error that cannot be pinpointed to a specific station or location on the ring (see also isolating error).

Octet. A digital unit of information comprising eight binary digits (bits) equivalent to a byte.

OSI. Open Systems Interconnection, a body of standards set by the International Standards Organization to define the activities that must occur when computers communicate. In the OSI Reference Model there are seven layers, and each contains a specific set of rules to follow at that point in the communication.

Packet. A unit of information that contains data, origin information; and destination information, which is switched as a whole through a network.

PACMIB. Port Address Correlation MIB maps port to host data and gathers port statistics for 3Com CoreBuilder devices on your network.

Probe. Station (or agent) responsible for gathering network data on a remote segment and passing it up to a central management station (or client). Usually configured and controlled by the client.

PDN. Public Data Network.

Physical Layer. The first layer of the OSI network layer model. This layer manages the transfer of individual bits of data over wires, or whatever medium, that is used to connect workstations and peripherals.

Presentation Layer. The sixth layer of the OSI network layer model. This layer controls the formatting and translation of data.

Protocol. A set of rules and procedures that govern the exchange of data between two communicating systems.

Protocol Number. The port or program number as defined by the parent protocol. For example, if you are adding a TCP child protocol, the protocol number will be the TCP port number.

Purge. On Token Ring, sent out by the Active Monitor after a monitor contention. Ring Purge frames tidy up the ring segment and signal the start of normal operations. A level 2 error.

PSTN. Public switched telephone network.

REM. On Token Ring, the Ring Error Monitor - the functional address that error reports are addressed to.

RMON. Remote MONitoring. Subset of SNMP MIB II which allows monitoring and management capabilities by addressing up to ten different groups of information. Defined in IETF document RFC 1757.

RMON2. Extends the capability of RMON to include protocols above the MAC layer.

Ring Poll. All stations report their presence on a Token Ring every 7 seconds. In this way stations are kept aware of their NAUNs. Also known as neighbor notification.

Ring Purge Event. A disruption is caused every time a station inserts onto a Token Ring. This results in a ring purge event.

SD. Starting Delimiter - a distinctive byte marking the start of a frame or a token.

Short Packet. See undersize packets.

SMP. Standby Monitor Present - a frame transmitted on a Token Ring by a ring station in response to an AMP frame as part of the neighbor notification process.

SMT. FDDI Station Management. This protocol is intended for use in a high-performance multi-station network. It is designed to be effective at 100Mbps using a Token Ring architecture and fiber optics as the transmission medium over distances of several kilometers.

Soft Error. On Token Ring, errors not severe enough to stop the ring functioning (level 1 errors). There are 10 soft errors - line, burst, congestion, internal, abort, ACE, lost frame, token, frequency and frame copied errors. Soft errors can be isolating or non-isolating.

Station. Any machine connected to the network - for example a fileserver, PC, workstation, printer or probe.

Subnet Mask. A filtering system for IP addresses. It defines the portion of the IP address used to identify the subnet. The remaining portion is used to represent host information. Devices and routers use the mask to identify the subnet on which a probe resides.

System Descriptor. A free-form field on RMON devices used by vendors to supply basic information about the device.

Token Error. Reported by the Active Monitor when the token gets corrupted. Similar to a line error, token errors are also non-isolating errors. A station which transmits a lot of token errors is often not at fault - it is probably the active monitor.

Token Frame. A station wishing to transmit must first grab the token before doing so. When it has finished it sends the token to its downstream neighbor which in turn may hold it or simply pass it on. Token frames are 3 bytes long.

Transport Layer. The fourth layer of the OSI network layer model. This is responsible for error checking and correction, and some message flow control.

Trigger. A trigger represents a sequence of events that may occur on a network. When these events occur, an alarm is triggered.

Undersize Packets. An Ethernet packet less than 64 octets long (excluding frame bits but including FCS octets) but otherwise well formed.

Virtual Circuit. Circuit-like service provided by the software protocols of a network, enabling two end points to communicate as though connected by a physical circuit. Network nodes provide the addressing information needed in the packets that carry the source data to the destination.

Readers' Comments — We'd Like to Hear from You

Nways Manager Remote Monitor
User's Guide

Publication No. SA33-0367-04

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	□	□	□	□	□

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	□	□	□	□	□
Complete	□	□	□	□	□
Easy to find	□	□	□	□	□
Easy to understand	□	□	□	□	□
Well organized	□	□	□	□	□
Applicable to your tasks	□	□	□	□	□

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? □ Yes □ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name

Address

Company or Organization

Phone No.

Readers' Comments — We'd Like to Hear from You
SA33-0367-04

Cut or Fold
Along Line

Fold and Tape **Please do not staple** Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

Department CGFA
Design & Information Development
IBM Corporation
P.O. Box 12195
RESEARCH TRIANGLE PARK, NC
USA 27709-9990

Fold and Tape **Please do not staple** Fold and Tape

SA33-0367-04

Cut or Fold
Along Line

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

SA33-0367-04