



Nways Remote Monitor For Windows NT

User's Guide

Version 2.0



Nways Remote Monitor For Windows NT

User's Guide

Version 2.0

Note

Before using this information and the product it supports, be sure to read the general information under "Appendix A. Notices" on page 155.

Third Edition (May 1999)

This edition applies to Version 2, of the Nways 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 CGF
Design & Information Development
IBM Corporation
PO Box 12195
RESEARCH TRIANGLE PARK NC 27709
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.

© **Copyright International Business Machines Corporation 1997, 1999. All rights reserved.**

US Government Users Restricted Rights – Use duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Figures	ix
Tables	xiii
About This Guide	xv
Who Should Read This Book	xv
New Features in This Release	xv
Conventions	xv
Terminology	xvi
Chapter 1. Nways Remote Monitor Overview	1
Introducing Nways Remote Monitor	1
Using Nways Remote Monitor for Network Management.	2
Theory of Operation.	2
RMON Overview.	2
Nways Remote Monitor Basics	3
New Features in This Release	4
Chapter 2. Using the Nways Remote Monitor Interface	7
Viewman Interface	7
Menu Bar	8
Toolbar	8
Summary Area	8
Alarm Bar	9
Status Bar	9
Rmonview Interface.	9
Dialog View	9
The Rmonview Main Window	10
Toolbar	13
Application Display Area	14
Status Bar	15
Collector Interface	16
Menu Bar	16
Status Log	17
Status Bar	17
Reporter Interface	17
Main Window Options	18
Menu Bar Options	18
Chapter 3. Setting Up Probes	21
Launching the Device Configuration Dialog	21
From Viewman	22
From Collector and Translator	22
From Windows NT Start Menu	22
Setting Up Probes	22
Managing Probes	24
Hardware and Firmware Versions	26

Downloading Firmware	27
Date/Time and Echo Interval	27
IP Address, Subnet Mask, and Default Gateway	28
Resetting a Probe	29
Access Control Tables	32
Opening Access Control Tables Dialog	32
Trap Communities	34
Opening the Trap Control Dialog	35
Setting Static Routes	37
Enabling and Disabling PACMIB	38
Setting the RMON2 Mode	39
Configuring Virtual Interfaces	40
Creating Virtual Interfaces	40
Deleting Virtual Interfaces	44
Managing RMON and RMON2 Tables	44
Managing RMON2 (ECAM) SmartAgent Firmware	46
Opening the SmartAgent Maintenance Dialog	46
Managing User-Defined Protocols	49
Viewing the Protocol Directory	49
Adding a Protocol	50
Deleting a Protocol	51
Updating Protocol RMON2 Tables	51
Chapter 4. Setting Up Station Names	53
Automatic Detection of Stations	53
SmartAgent Probes	53
RMON2 Probes	53
Launching the Translator	54
Start Menu	54
Translator Main Window	54
Importing Data	56
Starting Data Collection	57
Stopping Data Collection	59
Deleting a Data Collection	60
Manual Setup of Stations	60
Setting the Name Translation Level	62
Specifying Vendor Prefixes	63
Chapter 5. Viewman	65
Launching Viewman	65
Configuring the Main Window	66
Viewman Graphs	68
Packet Size Distribution	69
Packet Rates	70
Network Statistics	71
Top 10 Hosts by Packet Rate	72
Top 10 Hosts by Error Rate (Ethernet and Token Ring)	73
Top 10 Receivers (FDDI)	73
Event Distribution (Ethernet)	74
Ring Status (FDDI and Token Ring)	75

Chapter 6. Rmonview and RMON Applications	77
Launching Rmonview	77
Launching RMON Applications	77
Rmonview	77
Viewman	78
Configuring RMON Applications	79
Creating and Editing Views	79
Statistics View	81
Configuring Statistics View	82
History View	84
Configuring History View	84
Host View	86
Configuring Host View	87
Matrix View	90
Configuring Matrix View	90
Token Ring View	92
Configuring Ring Station View	92
Alarms View	94
Configuring Alarms View	94
Address Translation View	98
Address Translation Table Types	99
Viewing Address Translation Tables	99
Using the Protocol Distribution Application	100
Protocol Distribution View Types	101
Viewing Protocol Distribution Tables	101
Chapter 7. Packet Capture and Decode	103
Launching the Capture Application	103
Viewman	103
Start Menu.	104
Configuring Capture.	104
Working with Buffers	105
Creating New Capture Buffers	105
Modifying Capture Buffers.	111
Loading Capture Buffers from File	111
Creating New Start and Stop Events	111
Using the Filter Editor	113
List of Filter Templates	115
Launching the Decode Application	117
Capture.	117
Viewing a Capture Buffer on a Probe	117
Viewing a Saved Capture Buffer	117
Reading Captured Packets	118
Loading Probe Capture Buffer	119
Conversation Trace and Analysis	120
Saving and Loading Captured Packets	121
Saving Packets	121
Loading Packets	122
Chapter 8. Collector	123

Launching the Collector Application	123
Viewman	124
Start Menu.	124
Configuring Data Sources	125
Setting the Address Translation Level	126
Setting Up Data Collections	127
Adding a New Configuration	128
Modifying Configurations	130
Stopping Data Collection	130
Starting Data Collection	131
Collected Data Storage	131
Exiting the Collector.	132
Chapter 9. Reporter	133
Launching the Reporter Application	134
Viewman	134
Start Menu.	134
Selecting a Reporting Database.	135
Creating a New Database.	135
Opening an Existing Database	136
Importing Data	137
Viewing the Contents of a Database	138
Selecting and Generating Reports	139
Select Reports	140
Select Report Parameters.	140
Loading Saved Reports	145
Chapter 10. Data Management.	147
Managing Data	147
Consolidation Examples	148
Consolidating Data	149
Deleting Data	150
Archiving Data	151
To Archive Data	151
To Access Archived Data	151
Chapter 11. Compacting and Repairing the Application Database	153
Compacting the Application Database	153
Repairing the Application Database	154
Appendix A. Notices	155
Trademarks	156
Appendix B. List of Protocol Decodes	157
Appendix C. Application Variables	159
Statistics Variables	159
Variables Available on Ethernet	159
Variables Available on FDDI	159
Variables Available on Token Ring	160

History Variables	162
Variables Available on Ethernet	162
Variables Available on FDDI	163
Variables Available on Token Ring	164
Host Variables	165
Ring Station Variables	166
Appendix D. Performance Guidelines	169
Appendix E. CSV File Contents	171
History File Format	171
Host File Format	172
Matrix File Format	173
Token-Ring MAC-Layer Data	173
Token-Ring Promiscuous Data	175
Appendix F. Report Descriptions	177
Example of Report with Histogram	178
Example of Report with Line Graph	179
Appendix G. Customizing HTML Report Templates	181
Customizing the Default Template	181
Default HTML Template	181
Appendix H. RMON2 and ECAM Protocols	183
ECAM Application Decodes	183
RMON2 Protocols Overview	186
RMON2 Predefined Protocols	186
Glossary	195
Index	199

Figures

1. Viewman Main Window	8
2. Rmonview Main Window	11
3. Statistical Displays in Rmonview	15
4. Collector Main Window	16
5. Reporter Main Window	18
6. Probe List Editor	23
7. Agent Maintenance Dialog	26
8. Downloading Firmware	27
9. Date/Time and Echo Interval	28
10. IP Address, Subnet Mask, and Default Gateway.	29
11. Access Control Dialog	33
12. Trap Control Dialog	36
13. Static Routing Table	37
14. Edit Routing Entry Dialog	38
15. Enabling and Disabling PACMIB	38
16. RMON2 Config Dialog Box.	39
17. RMON2 Config Dialog Box.	40
18. Create Virtual Interfaces Dialog	41
19. Filters Dialog	43
20. RMON Tables Dialog.	45
21. RMON2 Tables Dialog	45
22. SmartAgent Maintenance Dialog	47
23. Protocol Directory Dialog Box	50
24. User-Defined Protocol Dialog	51
25. Example of a Protocol Properties Dialog.	52
26. Example of a Protocol Configure Dialog.	52
27. Nways Remote Monitor Menu and Toolbar	54
28. Translator Main Window	55
29. Import Host Map File Dialog	57
30. Data Collection Configurations Dialog	58
31. Data Collection Editor	58
32. Station List Editor	60
33. Add Station Dialog	61
34. Edit Station Dialog	62
35. Set Translation Level Dialog	63
36. Viewman.	65
37. View Menu	66
38. Display Options	67
39. Packet Size Distribution Graph on Token Ring	69
40. Packet Rates Graph on Token Ring	70
41. Network Statistics on Token Ring.	71
42. Top 10 Hosts by Packet Rate on Ethernet.	72
43. Top 10 Hosts by Error Rate on Ethernet	73
44. Event Distribution on Ethernet.	74
45. Ring Status	75
46. Opening an Application in Rmonview	78
47. Viewman Menu Bar and Toolbar	78

48. Application View Dialog	80
49. Edit User View Dialog	81
50. Application View Dialog	82
51. History View Dialog	84
52. History Entry Creation Dialog	86
53. Host View Dialog	87
54. Station Select Dialog	89
55. Matrix View	91
56. Ring Station View Dialog	93
57. Alarms View Dialog	95
58. Alarm Creation Dialog	96
59. Specifying Alarm Activation.	97
60. Hysteresis Zone	98
61. Current Device Shown in Viewman	100
62. Rmonview Applications Menu	100
63. Current Device Shown in Viewman	102
64. Rmonview Applications Menu	102
65. Viewman Menu Bar and Toolbar	104
66. Packet Capture Application Main Dialog	104
67. Edit Packet Capture Dialog.	106
68. Configure Interface Dialog	106
69. Start Events Dialog	107
70. Start Event Active	108
71. Stop Event Active	108
72. Start and Stop Events Active	109
73. Buffer Control Dialog	110
74. Edit Start Event Dialog	112
75. Edit Filter Dialog	114
76. Packet Decode Display	118
77. IP Conversation Trace View	121
78. Viewman Menu Bar and Toolbar	124
79. Collector Main Window	125
80. Mixed Address Translation Levels in the Reporter	126
81. Set Translation Level Dialog	127
82. Data Collection Configurations Dialog	128
83. Data Collection Editor Dialog	129
84. Reporter Main Window	135
85. New Database Dialog	136
86. Open Database Dialog	137
87. Import Files Dialog	138
88. Summary Data Dialog	139
89. Report Period Configuration Dialog	140
90. Report Configurations	141
91. Report Configuration Dialog	142
92. Selecting Report Output Options	143
93. Preview Tab.	144
94. Loading Saved Reports	145
95. Page Setup	146
96. Consolidation of Multiple Data Records.	148
97. Original Data Collections	148

98. After First Consolidation 149
99. After Second Consolidation 149
100. Data Management Dialog 150

Tables

1. Text Conventions	xv
2. Rmonview Tools	13
3. RMON Data Preserved and Lost	30
4. RMON2 Data Preserved and Lost	31
5. Security Access Levels	33
6. Predefined Channels (Filters)	41
7. Invert Button	43
8. Name Translation Levels	62
9. Available Graphs by Media Type	68
10. Packet Rate Graph Variables by Media Type	70
11. Network Statistics Graph Variables by Media Type	71
12. FDDI Ring Status Panel Variables	75
13. Token-Ring Status Panel Variables	76
14. Predefined Statistics Views.	83
15. Predefined History Views	85
16. Predefined Host Views	88
17. Predefined Matrix Views	91
18. Predefined Ring Station Views	93
19. Address Translation Display	99
20. Protocol Distribution Display	101
21. Invert Button	109
22. Filter Templates by Interface Media Type	115
23. Packet Decode File Formats	122
24. CSV Format Files Created by the Collector	131
25. List of Supported Protocol Decodes by Protocol Family	157
26. Statistics Variables Available on Ethernet	159
27. Statistics Variables Available on FDDI	159
28. Statistics Variables Available on Token Ring	160
29. History Variables Available on Ethernet.	162
30. History Variables Available on FDDI	163
31. History Variables Available on Token Ring.	164
32. Host Variables Available on Ethernet, FDDI, and token ring	165
33. Ring Station Variables Available on token ring	166
34. Example of Operation Times in Reporter	169
35. CSV Format Files Created by the Collector	171
36. History CSV Format File Contents	171
37. Host CSV Format File Contents	172
38. Matrix CSV Format File Contents	173
39. Token-Ring MAC-Layer CSV Format File Contents	173
40. Token-Ring Promiscuous CSV Format File Contents	175
41. History Reports	177
42. Host Reports	177
43. Matrix Reports	177
44. Noneditable HTML comments	181
45. Protocols Associated with One Protocol Family	183
46. Statistics Variables Available on Ethernet	186
47. Predefined Protocols-MAC-Layer Protocol.	189

About This Guide

This guide describes IBM Nways® Remote Monitor for Windows NT® (Nways Remote Monitor) and explains how you can use this application to monitor and gather statistical and historical information on your network.

If the information in the README file shipped with this product differs from the information in this guide, follow the README file.

For a description of the minimum system configuration and supported operating systems, as well as minimum probe firmware and SmartAgent software versions, refer to the README file shipped with this product.

Who Should Read This Book

This book is intended for people responsible for monitoring and maintaining network segments using the Nways Remote Monitor for Windows NT.

New Features in This Release

This release of Nways Remote Monitor for Windows NT offers the following new features:

- Support for RMON2 Address Translation and Protocol Distribution
- Ability to customize the Viewman main window and enable or disable particular graphs
- Ability to display multiple Viewman main windows
- Ability to set up user-defined protocols using the RMON2 Protocol Directory Manager
- Ability to generate HTML-based reports in Nways Remote Monitor Reporter

Conventions

Table 1 lists conventions that are used throughout this guide.

Table 1. Text Conventions

Convention	Description
"Enter" vs. "Type"	When the word "enter" is used in this guide, it means 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 special type	This typeface is used to represent messages and displays that appear on your terminal screen, for example: NetLogin:
Text represented as commands	This typeface is used to represent commands that you enter, for example: <code>SETDefault !0 -IP NETaddr = 0.0.0.0</code>

Table 1. Text Conventions (continued)

Convention	Description
Keys	<p>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.</p> <p>If two or more keys are to be pressed simultaneously, the keys are linked with a plus sign (+), for example:</p> <p>Press Ctrl+Alt+Del.</p>
<i>Italics</i>	<i>Italics</i> are used to denote <i>new terms</i> .

Terminology

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

Device, agent, or probe	A generic term used to refer to RMON probes or agents installed on your network.
Ethernet	This refers to both Ethernet and Fast Ethernet, unless otherwise stated in the guide.
Firmware	This is the software running in a device, also sometimes referred to as agent, or probe software.
Station	A generic term used to refer to workstations or other network equipment installed on your network, also referred to as host.

Chapter 1. Nways Remote Monitor Overview

This chapter introduces you to Nways Remote Monitor for Windows NT (Nways Remote Monitor). It is divided into two main parts:

- Introducing Nways Remote Monitor

A brief overview of Nways Remote Monitor, its component applications, and features, and the benefits it brings to network management.

- Theory of Operation

A summary of the RMON standard and an introduction to how Nways Remote Monitor works with RMON.

- Nways Remote Monitor Basics
- New Features in this Release

Introducing Nways Remote Monitor

Nways 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-compliant devices on the network. You can also configure and direct those devices from Nways Remote Monitor.

Use Nways Remote Monitor to:

- Monitor current performance of network segments.
- See trends over time (Viewman, Nways Remote Monitor's main window, shows the short-term trends, while the History application 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 and capture and display packets using filtering and decode functions.

At specified intervals, Nways Remote Monitor will poll remote network probes to retrieve essential network data, which it then processes and displays live in the main window. From Viewman you can monitor the health of a segment, its current performance, and recent trends.

For in-depth investigation, you can launch Nways Remote Monitor's RMON and RMON2 applications from Viewman or independently from your system software. With these applications you can view statistical and historical data, set up alarm conditions, monitor conversations between stations on the network, and capture and display specific packets.

Additional applications can be added by downloading SmartAgent software to probes. This software can then be unloaded when the applications are no longer required. SmartAgent software can also be registered with a probe's auto-boot table, so that the probe will try to reload the software if it is rebooted.

Using Nways Remote Monitor for Network Management

Viewman and the RMON applications can be used singly or in combination for proactive network management, collecting statistics to identify and deal with imminent problems.

- Use Viewman and the Statistics application periodically to check network performance and utilization, watching for emerging problems and short-term trends.
- For specific problems, combine the Alarms and Packet Capture applications to collect packets leading up to or following a specified event. Then use the Packet Decode application and Trace Analysis function to expose the cause of the problem.
- Use the Host and Matrix applications to get information on the busiest stations on your network.
- Use the History application to view 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 application 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 Packet Capture to watch for a recurrence of this specific problem.

Theory of Operation

This section introduces some of the basic concepts of remote network monitoring with Nways Remote Monitor. This section is divided into two parts. The first part provides an overview of the RMON and RMON2 standards and ideas for remote network monitoring. The second part provides a short description of the tools and methods provided by Nways Remote Monitor for the management of the network.

RMON Overview

Prior to the RMON standard, management 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 provides an effective and efficient way to monitor the behavior of the entire LAN, while reducing the burden on both remote probes and management stations.

RMON probes are intelligent, remotely controlled devices that collect information about network behavior and transfer it on command to an analysis site. A probe can be deployed as a stand-alone device or as an agent in a hub, router, or switch. Use of RMON probes improves the efficiency of staff by allowing them to remain in a central site while collecting information from widely dispersed LAN segments. A further advantage of remote probes is that they can also continuously monitor and collect information and deliver it before problems occur, allowing administrators to take a proactive approach to managing their networks.

Each remote probe can handle requests from multiple management applications. A management application, such as Nways Remote Monitor, typically runs on the network management station. Using a management application, network administrators

responsible for specific aspects of the network's operation can make use of the probe's capabilities to meet their own data requirements.

The management application sets the appropriate RMON Management Information Base (MIB) variables to specify measurement intervals, monitored thresholds, and other operational parameters. The remote probe collects and stores information and delivers it to the management application on request. Probes can also send an SNMP Trap to a group of management stations when specified conditions have been detected, thereby 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 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.

RMON2 statistics let you see who is talking to whom on the network, and which applications are being used. They improve a network manager's ability to optimize performance of current network resources and manage client/server and switched network environments.

Nways Remote Monitor Basics

Nways Remote Monitor is made up of the following applications:

- | | |
|-------------------|--|
| Viewman | This consists of a main window from which you can monitor key parameters of network health. You can also launch all other applications from here. |
| Config | The Configuration application is used for setting address translation levels and editing the station information list. It can be launched from Viewman, Translator, Collector, and the system. |
| Translator | The Address Translation application collects station information from any probe with the ECAM (RMON2) SmartAgent software loaded. The resulting Address Translation table provides station information to all other Nways Remote Monitor applications. |
| Capture | This captures packets on specific alarm conditions and enables you to filter out only those packets you need and store them for analysis. |
| Decode | This decodes captured packets and displays all major protocols in easily readable format. Then use Trace Analysis to track the component packets, along with their transmission times. |
| Reporter | This is a data collection and reporting tool ideal for smaller networks or for reporting on a limited number of RMON devices in a larger network environment. It consists of two core components: the |

Collector and the Reporter, providing a streamlined approach to the gathering of essential statistics and the creation of valuable network reports.

The Collector and Reporter work in conjunction with Nways Remote Monitor and IBM's family of RMON Ethernet, Fast Ethernet, and token-ring probes and other RMON-compliant Ethernet, Fast Ethernet, and token-ring devices available on the network.

SmartAgents SmartAgents can be loaded or unloaded from a probe at any time to provide RMON2-like applications.

Rmonview This consists of nine RMON applications: Statistics, History, Host, Alarms, Matrix, Ring Station, Protocol Distribution, Address Translation, and the Rmonview window in which these applications are displayed.

Statistics Displays segment statistics on any combination of packets, bytes, errors, size distributions, or multicasts. Data is updated in real time.

History Specifies a sample period and spot trends over hours, days, weeks, or even months.

Host Displays detailed information about the hosts on a segment.

Alarms Monitor specific events on the network as they happen. Use alarms on their own, or in conjunction with the Capture application.

Matrix Determines which hosts are talking to each other on the network and how much traffic is flowing between them. Single out stations that might be responsible for generating problems.

Ring Station (Token Ring) Displays ring information, exclusive to a token ring, including station status and last-entered and last-exited times.

Protocol Distribution Displays protocol distribution as a table, bar graph, or pie chart.

Address Translation Displays a table indicating the mapping between MAC address and the network layer.

New Features in This Release

This release of Nways Remote Monitor for Windows NT offers the following new features:

- Support for RMON2 Address Translation and Protocol Distribution

- Ability to customize the Viewman main window and enable or disable particular graphs
- Ability to display multiple Viewman main windows
- Ability to set up user-defined protocols using the RMON2 Protocol Directory Manager
- Ability to generate HTML-based reports in Nways Remote Monitor Reporter

Chapter 2. Using the Nways Remote Monitor Interface

This chapter describes:

- Viewman and Rmonview interfaces

Both Viewman and Rmonview consist of one main window from which you can launch other Nways Remote Monitor applications. Although Viewman is a monitoring application in its own right, Rmonview acts simply as a launch and display area to Nways Remote Monitor's RMON applications and does not carry out any monitoring or statistics-gathering functions of its own.

- Collector and Reporter interfaces

These sections describe the interfaces for both the Collector and Reporter applications.

Viewman Interface

Viewman consists of one main window from which you can monitor the performance of a LAN segment. You can also launch all other Nways Remote Monitor applications and RMON2/SmartAgent applications from this window.

The main window is divided into five areas (see Figure 1 on page 8):

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

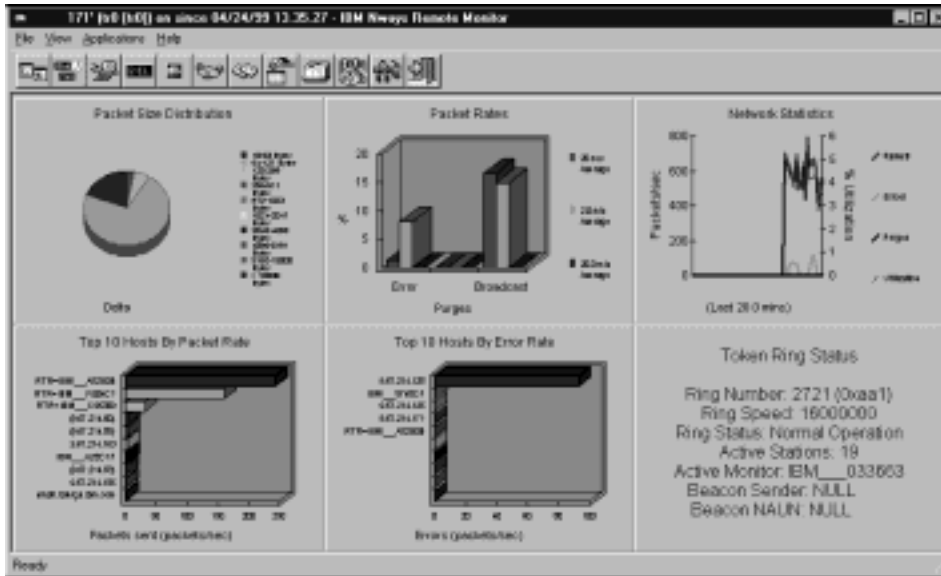


Figure 1. Viewman Main Window

Menu Bar

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

- File** The **New** command launches a new Viewman main window.
- View** Lets you turn on or off the display of any area within the main window, select **Device Options** to select the LAN segment to be monitored, refresh date for displayed data, or select the graphs to be displayed in the summary area.
- Applications** From this menu you can launch any Nways Remote Monitor application, including the Device Configuration Dialog.
- Help** Gives access to help on Viewman and to Nways Remote Monitor's full online help.

Toolbar

The toolbar, located beneath the menu bar, displays a partial list of available Nways Remote Monitor applications. Click a button to launch the corresponding application dialog. It also contains an Exit button with which you can quit Viewman.

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 will vary according to the media type of the monitored segment.

A guide to the different graphs is given in “Viewman Graphs” on page 68.

Alarm Bar

The alarm bar is located beneath the summary area. Alarm icons appearing in this bar will turn red whenever the alarm is triggered. When the mouse is passed over the top of an alarm icon, an alarm status message appears in the status bar.

Status Bar

Located beneath the alarm bar, the status bar displays system messages and alarm status information.

Rmonview Interface

Rmonview is Nways Remote Monitor’s RMON display. All RMON applications can be launched from the Rmonview window, and applications will also use this window to display data (see “Chapter 6. Rmonview and RMON Applications” on page 77). Each application will open a new window within the Rmonview display area, and any number of application windows can be open simultaneously. Rmonview can be iconised and left running in the background.

Dialog View

This dialog displays when you start a new Rmonview application. It allows you to select the RMON probe and interface for the application to analyze and display. This dialog also allows you to select the statistical elements that the application will display. These options allow you to customize the application view. Some of the sections of this dialog are described here. See “Configuring RMON Applications” on page 79 for more detailed information.

Probe	The Probe area contains a list of all configured probes (see “Chapter 3. Setting Up Probes” on page 21). The probe highlighted is the current selection. Click a probe to select it.
Interface	A list of available interfaces will appear in the Interface area if the selected probe is accessible. Click an interface to select it.
View	Select a predefined view or create your own. This view will determine the statistical elements that are displayed.
Update Rate	Specify how often to update the display with new data.
Community String	SNMP devices on the network use the community

string to restrict access to the probe. This can be modified for each probe (see “Community Access Names” on page 33).

OK, Close and Help

- Click **OK** to implement the choices made in the dialog.
- Click **Close** to abandon your choices and return to the previous level.
- Click **Help** for online help information.

Selecting Entries in Lists

To select a single entry in any list, simply click the entry.

To select multiple entries, where this function is supported, do one of the following actions:

- Press and hold **Ctrl** and click each entry in turn.
- Click the first entry and then drag the mouse to the last entry.
- Click the first entry and, holding down **Shift**, click the last entry.

The Rmonview Main Window

Rmonview’s main window is divided into four areas:

- Menu Bar
- Toolbar
- Application Display Area
- Status Bar

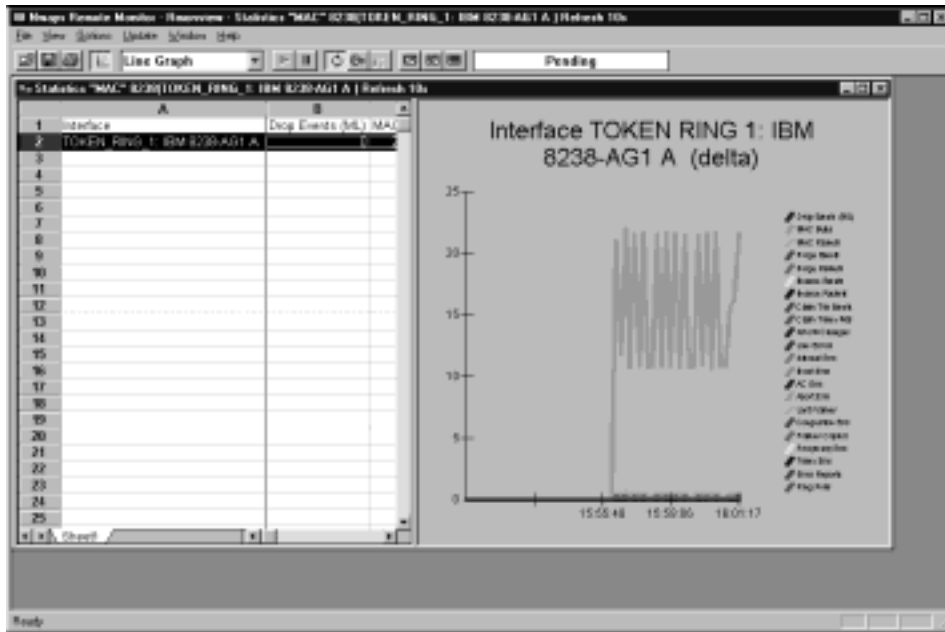


Figure 2. Rmonview Main Window

Menu Bar

The contents of the menu bar, located at the top of the window, will vary according to whether any RMON data is being displayed.

File

- | | |
|-------------------------|---|
| New | Gives access to all the RMON applications. Selecting an RMON application from this menu will launch the application's configuration dialog. |
| Open | Lets you select previously saved RMON application views. This item is also available from the toolbar. |
| Close | Closes the currently selected RMON application views. |
| Save and Save As | Let you save the configuration view of the current application window to file. |
| Print Graphic | Allows you to print the current display to your system's default printer. |
| Print Setup | Allows you to select the print properties of the current display to be printed. |
| Export | Lets you export the contents of displayed tables to ASCII or CSV format files. |

	Recent File	Lists recently saved application views. Select the file name to start the application. If the text Recent Files is grayed out, this indicates that there are no saved views.
	Exit	This menu item ends the Rmonview.
View	Toolbar	Allows you to toggle the toolbar area of the application window on and off.
	Status Bar	Allows you to toggle the status bar area of the application window on and off.
	Graph Only, Graph and Table, and Table Only	Let you reconfigure the application display to show either the graph or table, or both the graph and table in equal proportion. You can also resize the areas in the display by dragging the middle window bar to left or right with the mouse. These items are also available from the toolbar.
	Clear Flags	When you click data in a graph, a flag will be posted showing the exact date and time that the selected data was gathered, a variable description, and the value for that variable. This menu item will clear any flags from a graph.
	Pause Graph and Resume Graphing	Toggle refreshing of data in the graph on or off. If Auto Upload is running or Manual Update is selected, the data will still be uploaded from the probe but the display in the graph area will not be refreshed until Resume Graphing is selected.
Options	Display Graph	Toggles the display of the graph on and off in the selected view.
	Automatic Upload	When enabled, causes new data to be uploaded at the update rate specified in the View's configuration dialog box.
	Manual Upload	When enabled, disables automatic upload. New data is uploaded only when you press the Manual Upload button.
	Line Width	Specifies the width of the lines used on line graphs.
	Table Control	Displays a dialog box that enables you to set the size and wrap options for the active application display table.

Graphed Values









Lets you select the value to use for the graph. You can select either the values for the change over the specified time interval (delta) or the absolute totals since the probe was started.





- Update** Forces an update of the application display.
- Window** This menu contains standard Microsoft® Windows functions for manipulating windows.
- Help** Gives access to Nways Remote Monitor's full online help.

Toolbar

The toolbar contains the buttons described in Table 2.

Table 2. Rmonview Tools

Tool	Description
 Open	Opens a saved application file for viewing.
 Save	Saves the contents of the current display to file.
 Print Graph	Prints the current display to your system's default printer.
 Display Event Data	Toggles the graph display on and off.
 Resume Graphing	Causes graphing to resume.
 Pause Graph	Causes graphing to pause.
 Auto Upload	When on, causes new data to be uploaded at the Update Rate.
 Manual Upload	When on, disables automatic upload. New data will be uploaded only when you press the Manual Update button.

 Manual Update	Use with the Manual Upload tool to force a new update specified in the application's configuration dialog.
 Graph Only	Resizes the application window to display only the graph.
 Table & Graph	Resizes the application window to display graph and table.
 Table Only	Resizes the application window to display only the table.

The toolbar also contains two other functions:

Graph List Lets you select or change the format of the current graph display. Available display formats are: Line Graph, 3D Tape, Log/Lin, Histogram, and Pie.

Upload/Update Status Displays upload and update progress messages.

Application Display Area

RMON and RMON2/SmartAgent application windows will be displayed in this area. Any number of application windows can be open in this area at the same time. Use the Window menu options and the standard Minimize, Maximize, and Close buttons in the top right corner of each application window to manage the window display.

Statistical Displays

Rmonview supports multiple windows within its display area. All applications use a standard format.

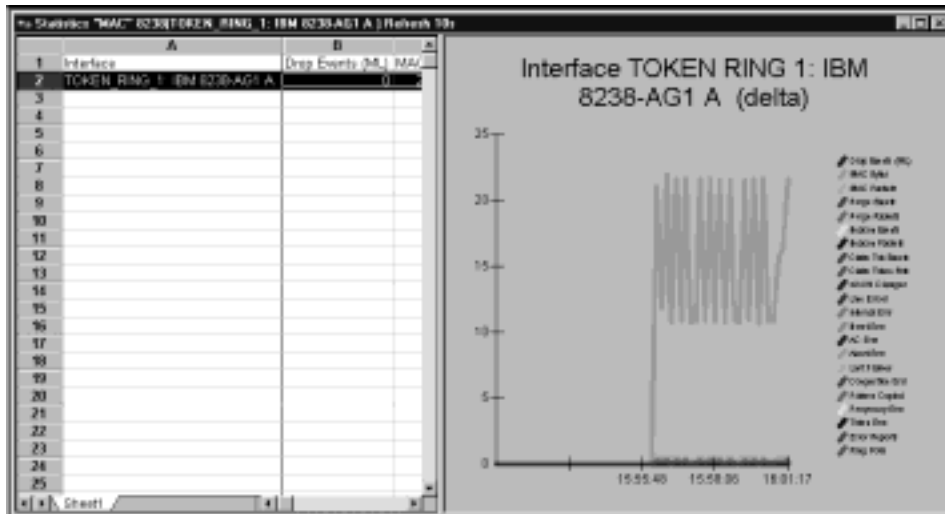


Figure 3. Statistical Displays in Rmonview

The display is divided into two sections:

Table

Statistics are displayed in tabular format in the left portion of the display. To select entries for graphing:

- Graph individual variables by selecting a single cell in the table.
- Graph multiple adjacent variables in a row or column by clicking the first cell and, with the **Shift** button depressed, clicking the last adjacent cell.
- Graph multiple variables in nonadjacent cells by keeping the **Ctrl** button pressed while clicking each cell.
- Graph the entries in an entire row or column by selecting the row or column header.

Graph

A graphical display of the selected data is displayed in the right portion of the display. Click the data in the graph to display a data label telling you the exact date and time the statistic was gathered, the type of statistic, and the exact value. To remove display labels use the clear flags menu item on the view menu.

Use the Graph Only, Table and Graph and Table Only buttons in the toolbar or from the View menu. To resize the display, click the middle bar with the mouse and drag to the left or right.

Status Bar

The status bar is located at the bottom of the main window, and displays any system messages.

Collector Interface

This section describes the interface for the Collector. Launching the Collector is described in “Chapter 8. Collector” on page 123. The main window is divided into three areas:

- Menu Bar
- Status Log
- Status Bar

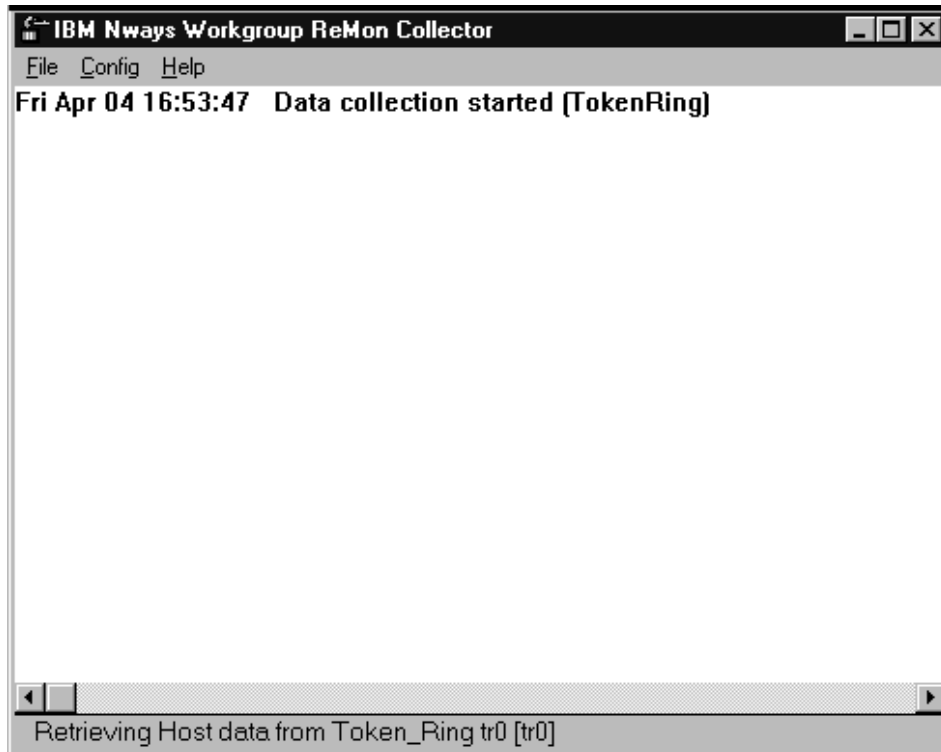


Figure 4. Collector Main Window

The main window displays the status log for all current collection configurations. The status bar at the bottom of the window gives real-time feedback, such as when the next collection is due to start.

Menu Bar

The menu options available from this window are:

File

- Save** Saves the contents of the status log to keep a record of collections made.
- Print** Prints the contents of the status log.
- Exit** Exits the Collector.

Config

Data Collections

Lets you create, modify, and delete configurations.

Address Translation Level

Lets you select the level of address information that the Collector should try to discover for devices and the preferred protocol.

RMON Devices

Gives access to the Device Configuration dialog, which is also available from the Viewman and Translator main windows and as a stand-alone application available from your system software. From this dialog box, you can set up the list of RMON-compliant devices available on the network.

Help

Contents

Launches the Remote Monitor online help system.

About Collector

Version and copyright information.

Status Log

The status log forms the largest area in the main window. While data collection is taking place, status messages will appear in this area. When the area becomes full of messages, you can scroll up and down through the log. The contents of the log can be saved to a file or printed from the File option in the menu bar.

Status Bar

The status bar, located at the bottom of the main window, is used to display the status of the current or next collection.

Reporter Interface

This section describes the interfaces for the Reporter. Launching the Reporter is described in "Chapter 9. Reporter" on page 133. The Reporter consists of one main window set in the Microsoft Access database environment.



Figure 5. Reporter Main Window

Main Window Options

The functions available from the Reporter main window are:

New Database	Create a new reporting database.
Open Database	Open an existing reporting database.
Import	Import contents of CSV files created in Collector into a database.
Data Management	Consolidate data on a regular basis or delete data.
Data Summary	View a summary of the current database.
Report	Generate reports from the current database.
Open Report	Load a saved report for printing.
Exit	Close the application.

Menu Bar Options

These are the menu options applicable to the Reporter in the menu bar:

File

New Database	Create a new reporting database from existing CSV files.
Open Database	Open an existing reporting database.

	Close Database	Close current database.
	Exit	Exit the database environment. In addition, when you are previewing a report (see page 144) or have loaded an existing report (see page 145), the following options are available:
	Print	Print current report.
	Print Setup	Change the current print setup.
Window		Tile, Cascade, or Arrange windows.
Help		About Reporter Version and copyright information.

Chapter 3. Setting Up Probes

To make Nways Remote Monitor operational, you must specify a list of the probes that are available to be used. When this is complete, you can immediately start to monitor the health of your network via Viewman and the Nways Remote Monitor applications.

Additional configuration, such as creating virtual interfaces and adding user-defined protocols, can be carried out at any time.

This chapter is divided into the following sections:

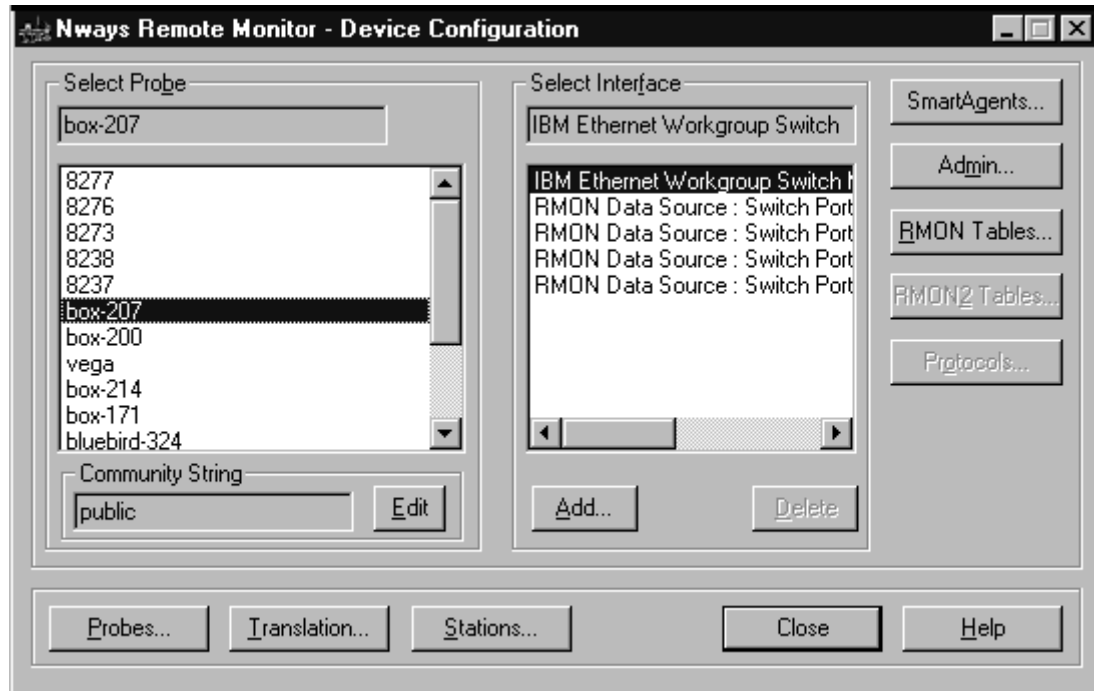
- Launching the Device Configuration Dialog
- Setting up and verifying probes
- Managing probes
- Enabling and disabling PACMIB
- Setting the RMON2 mode
- Configuring virtual interfaces
- Managing RMON and RMON2 tables
- Managing SmartAgent firmware
- Managing user-defined protocols
- Updating protocol RMON2 tables

Launching the Device Configuration Dialog

The Device Configuration dialog can be launched as follows:

From Viewman

To open the Device Configuration dialog, click



in the toolbar or select **Config** from the application menu bar drop-down item.

From Collector and Translator

Select **RMON Devices...** from the Config menu in the application's main window menu bar.

From Windows NT Start Menu

Select the **IBM Nways ReMon** Program Group from the Start menu and then choose **Config**.

All Nways Remote Monitor Device configuration is carried out from this dialog.

Setting Up Probes

You can specify which probes Nways Remote Monitor will use to monitor the network by doing the following steps from the Device Configuration Dialog:

1. Click **Probes** to open the Probe List Editor. By default, the first probe in the list will be selected.

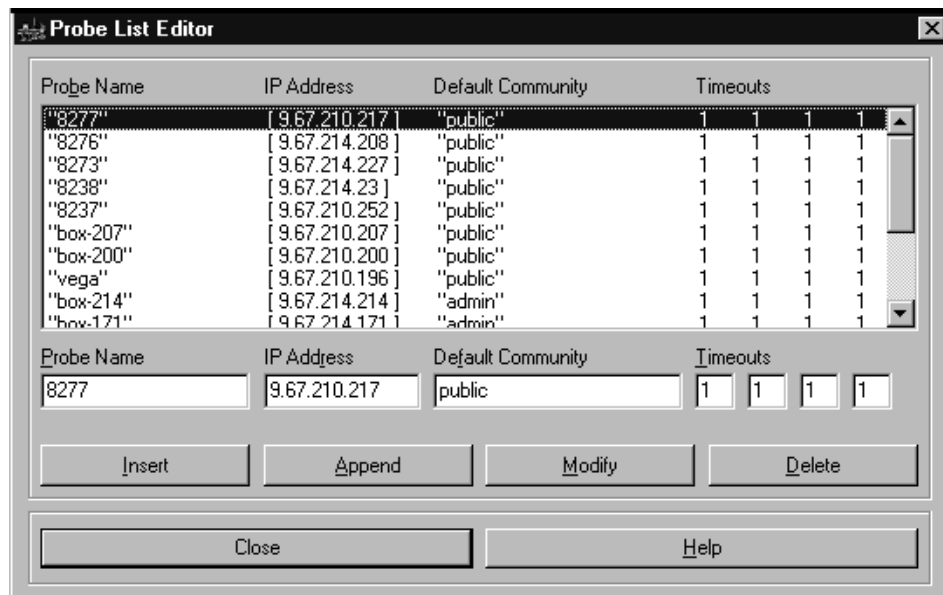


Figure 6. Probe List Editor

2. To set up a new probe:
 - a. Enter a unique name in the Probe Name field.
 - b. Enter the *IP Address* for the probe in the format n.n.n.n where n is a decimal number from 0 to 255. An example IP address is: 192.128.40.120. If you are unsure of the IP addresses allocated to the probe, consult your network administrator.
 - c. If appropriate, change the Community Name. Setting up community access tables is described in "Access Control Tables" on page 32.
 - d. If appropriate, change the Timeout values for the probe. All of the default values are 1 second.

The timeout values determine the intervals at which Nways Remote Monitor polls a probe before announcing that there is no response. The defaults are adequate for most installations. However, if you are running over serial cable or a slow link, the response will be slower and you may wish to increase the values, for example to 1, 2, 3, and 4 seconds.

- e. Click **Insert** or **Append** to add the new entry to the list.

If you have an entry selected, **Insert** will place the new entry in front of the current selection, while **Append** will add it after the current selection.

3. To modify an existing probe entry:

- a. Click an existing entry in the list. The details for the selected probe will appear in the fields beneath the Probe Entries list.
 - b. Change any of the entries, as described in step 2 on page 23 above.
 - c. Click **Modify** to apply these changes.
4. Click **Close** to return to the Configuration dialog.
The new probe will be shown in the **Select Probe** area of the Configuration dialog.
 5. To verify that the probe has been set up correctly and is contactable, select the probe by clicking on it in the **Select Probe** area.
 - a. If successful, a list of interfaces available on the probe will be displayed in the **Select Interface** area.
 - b. If the probe cannot be contacted, the message `Unavailable` will be displayed in the **Select Interface** area. This message may indicate that:
 - You have not set up the probe details correctly.
 - The probe 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 Probe List Editor is correct, and try to contact the probe again.

Once you have completed these steps, you can immediately start to monitor your network via the main window (described in Chapter 5. Viewman) and Nways Remote Monitor applications (described in Chapter 6. Rmonview and RMON Applications and Chapter 7. Packet Capture and Decode).

You can also carry out further configuration of remote probes at any time, as described in the following sections.

Managing Probes

For the IBM 8250 Ethernet Probe and IBM 8260 High-End Token-Ring Media Access Daughter Card, you can view and configure the following information from the Agent Maintenance dialog:

- View hardware and firmware versions, and download new firmware.
- View and set date and time details and echo interval.
- View and set PACMIB availability.
- View and set RMON2 availability.
- View and set a probe's IP address, subnet mask, and default gateway.
- Reset a probe using cold or warm starts.
- View and configure access control tables.
- View and configure trap communities.

This section applies only to RMON agents that implement the "Aspen" MIB.

To open the Agent Maintenance dialog:

1. In the Configuration dialog, select the probe you want to examine.
2. For probes that support multiple interfaces, such as the IBM 8250 Ethernet RMON Probe and IBM 8250 High-End Ethernet Media Access Daughter Card, you can set the IP address on any of the listed physical interfaces.

Select an interface by clicking on it in the **Select Interface** list.

You cannot set IP addresses on virtual interfaces (see “Configuring Virtual Interfaces” on page 40 for a description of virtual interfaces).

3. Click **Admin** and you will be prompted to supply the security level 4 Community Name, in order to gain access to the configuration information for the selected probe. (See “Access Control Tables” on page 32 for an explanation of community names.)

To gain access to the Agent Maintenance dialog, you must have the security level 4 Community Name (levels are defined in Table 5 on page 34). If you forget this name, you will need to cold-start the probe using a local terminal attached directly to the probe.

4. Click **OK** and the Agent Maintenance dialog will open.

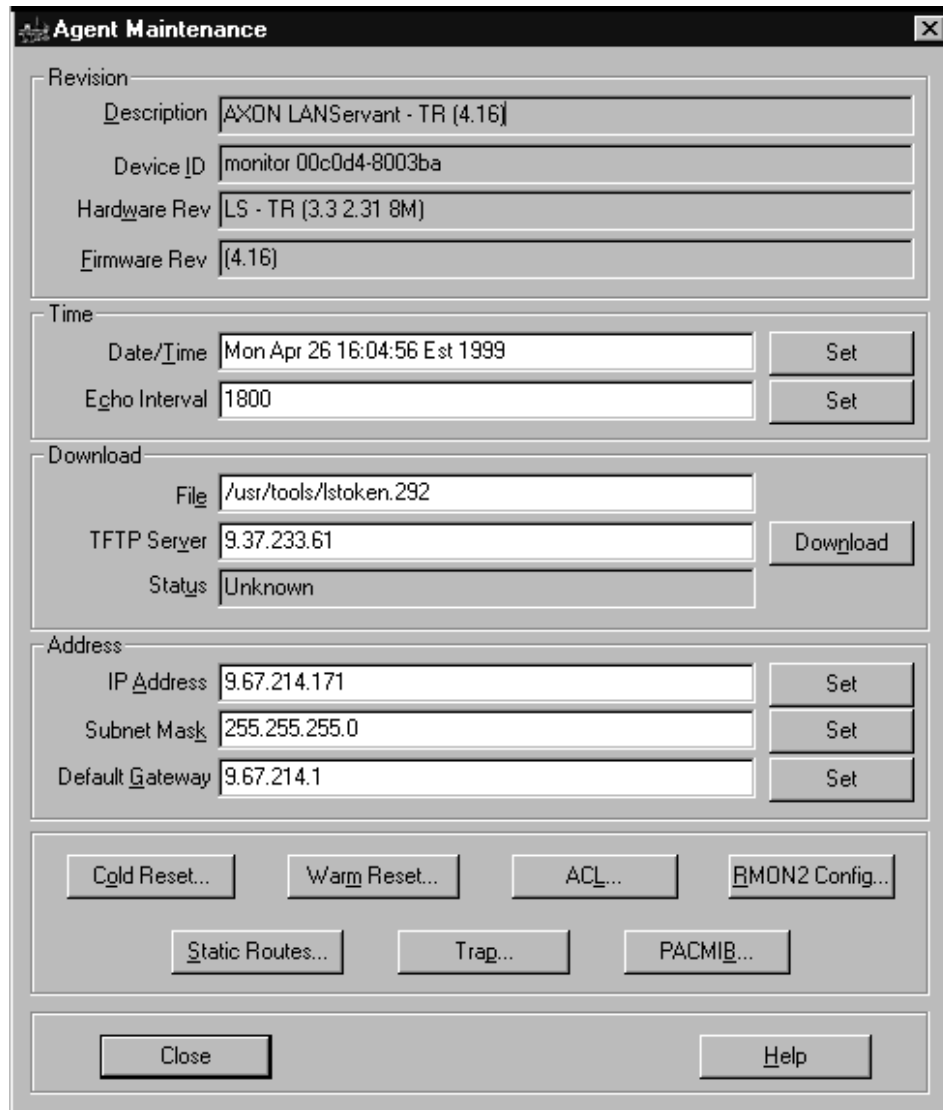


Figure 7. Agent Maintenance Dialog

Hardware and Firmware Versions

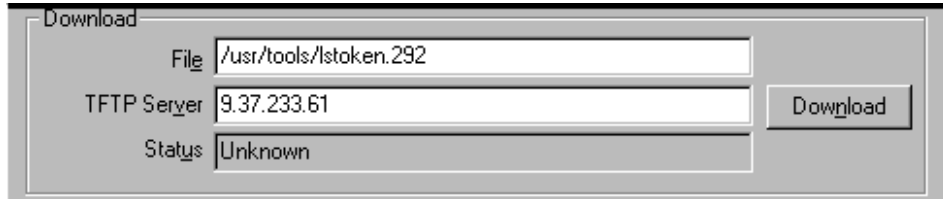
The first area in the Agent Maintenance dialog gives the probe identifier. The current hardware and firmware levels are shown in the *Hardware Rev.* and *Firmware Rev.* fields.

Downloading Firmware

To simplify probe administration, firmware files are generally stored on a TFTP server that can be accessed by the probes on the network. New versions of firmware can be quickly and simply downloaded to the probe from this server.

SmartAgent (ECAM) firmware downloads are initiated from the SmartAgent dialog. See “Managing RMON2 (ECAM) SmartAgent Firmware” on page 46 for more information.

The *Status* field in the Agent Maintenance dialog reflects the success of the last download made by Nways Remote Monitor.



Download	
File	/usr/tools/istoken.292
TFTP Server	9.37.233.61
Status	Unknown

Download

Figure 8. Downloading Firmware

1. A TFTP server must be active before you can load new firmware. To launch the TFTP server shipped with Nways Remote Monitor, select the **IBM Nways ReMon** Program Group from the start menu and then select **TFTP**.
The TFTP server starts when the Nways Remote Monitor workstation boots up.
2. In the Download File field, type the file name of the agent firmware. Nways Remote Monitor will use the installation directory as the location of this file. You do not need to specify a directory location in the Download File field.
3. In the TFTP Server field, type the IP address of the TFTP server to use.
4. To download the new firmware release to the probe, click **Download**.
The probe will automatically perform a cold reset, during which time you will lose your connection to the probe and will be returned to the Configuration dialog. When the probe has restarted, return to the Agent Maintenance dialog and check that the Status field has been set to **Success**.
If the Status field is set to **Failure**, check that the TFTP Server is running and correctly configured and repeat steps 1 to 3.

Date/Time and Echo Interval

Date/Time Settings

For probes that have a real-time clock, you can set the date and time on the probe from the Agent Maintenance dialog.

For probes that do not have real-time clocks, you cannot enter a date or time setting and the message *Unavailable* will be displayed in the Date/Time field.

Figure 9. Date/Time and Echo Interval

1. In the *Date/Time* field, enter the date and time in the format:

Day	First three letters of day: Mon, Tue, Wed, Thu, Fri, Sat, Sun.
Month	First three letters of month: Jan, Feb, Mar, Apr, and so on.
Date	Two-digit date: 01, 02, 03, and so on.
Time	Hours:minutes:seconds.
Time zone	BST, EST, GMT, or other.
Year	Four-digit year: 1996, 2000, or other.

2. To apply the new date and time to the probe, click **Set**.

Echo Interval

Probes can be set up to send a PING message to the default gateway periodically (see “Default Gateway” on page 29). If your router requires a shorter or longer interval between PING messages, to keep the probe in its routing tables, you may need to change the echo interval.

1. In the *Echo Interval* field, enter the PING rate in seconds. The default is 1800 seconds.
2. To apply the new rate to the probe, click **Set**.

IP Address, Subnet Mask, and Default Gateway

IP Address and Subnet Mask

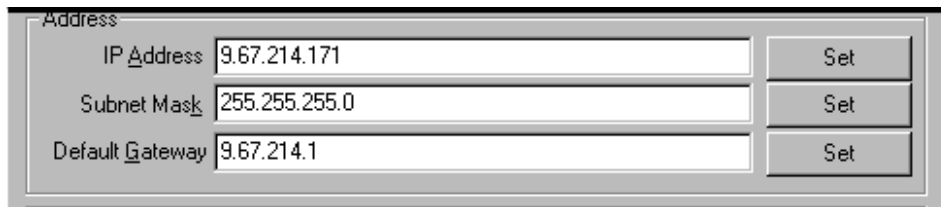
On multi-interface devices, you can set an IP address and subnet mask for each physical interface. The interface is selected in the Configuration dialog (see “Launching the Device Configuration Dialog” on page 21).

If you have selected a virtual interface or an interface for which the IP address and subnet mask cannot be set, these fields will be empty and cannot be edited.

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

Where two or more interfaces on a probe are monitoring the same subnet, each interface must be configured with a different IP address.

The subnet mask is a filtering system for IP addresses. It defines the first portion of the IP address used to identify the network, and the remainder is used to represent host information. Devices and routers use the mask to identify the subnet on which a probe resides.



Address		
IP Address	9.67.214.171	Set
Subnet Mask	255.255.255.0	Set
Default Gateway	9.67.214.1	Set

Figure 10. IP Address, Subnet Mask, and Default Gateway

1. To set the IP address:
 - a. In the *IP Address* field, enter the IP address for the probe or for the selected interface on the probe.
IP addresses have the format *n.n.n.n*, where *n* is a decimal number from 0 to 255. An example IP address is 91.1.1.9.
 - b. To apply the new IP address, click **Set** to the right of the IP Address field.
2. To set the subnet mask:
 - a. In the Subnet Mask field, enter a suitable subnet mask for the class of IP address. For more information, see your system administrator.
 - b. To apply the new subnet mask, click **Set** to the right of the Subnet Mask field.

Default Gateway

The default gateway is the IP address of a device, usually a router or gateway, to which the probe will direct all packets not destined for this subnet.

You can also define up to 16 routes to other subnets via the Static Routes menu in the main window. See “Setting Static Routes” on page 37.

1. In the *Default Gateway* field, enter the IP address for the router or gateway.
2. To apply the new setting, click **Set** to the right of the Default Gateway field.

Resetting a Probe

You can reset probes using either a warm reset or a cold reset. Both cause it to reinitialize, but there are differences in the effect each has on the probe. These differences are summarized for RMON and RMON2 variables in Table 3 on page 30 and Table 4 on page 31. Information is preserved but collected statistics stored in the probe’s RAM are lost.

Warm Reset

When you warm-reset a probe, all basic and additional configuration information is preserved but collected statistics stored in the probe's RAM are lost.

Cold Reset

When you cold-reset a probe, all network management information-except basic configuration information, such as IP address, subnet mask, and default gateway, stored in EEPROM-is lost.

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.

To warm- or cold-reset a probe, click **Warm Reset...** or **Cold Reset...** in the toolbar at the bottom of the Agent Maintenance dialog. You will be returned to the Device Configuration dialog and the probe will be temporarily unavailable while it is reset.

Both kinds of reset cause the probe to reinitialize, but there are differences in the effect each has on the probe. These differences are summarized for RMON and RMON2 variables in Table 3 and Table 4 on page 31.

Table 3. RMON Data Preserved and Lost

Data Type	Warm Reset	Cold Reset
Probe configuration information (IP address, and so on)	P	P
Tftp server address	P	P
Download filename	P	P
Date and time	P	P
Serial port configuration information	P	P
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 topN table	L	L
Alarm table	P	L
Event table	P	L ^a
Community access table entries	P	L ^a
Client table entries	P	L ^a
Serial connection table	P	L
Trap destination table	P	L
Captured packets	L	L

Table 3. RMON Data Preserved and Lost (continued)

Data Type	Warm Reset	Cold Reset
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

Note:

- P Data preserved
- L Data lost
- ^a Reverts to default
- ^b User-defined protocols preserved
- ^c Control information preserved
- ^d Token ring only

Table 4. RMON2 Data Preserved and Lost

Data Type	Warm Reset	Cold Reset
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
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

Access Control Tables

The Access Control window lets you set up community access names with appropriate security levels, then assign these names to specific end-user workstations. This lets you limit access to a probe's MIB to a selected set or community of management stations. By using more than one community, the probe can provide different levels of access to different management stations. Each time users attempt to carry out a sensitive function using Nways Remote Monitor, they must first provide a community name of the appropriate security level.

Opening Access Control Tables Dialog

In the Agent Maintenance dialog (Figure 7) click **ACL...** to open the Access Control dialog.

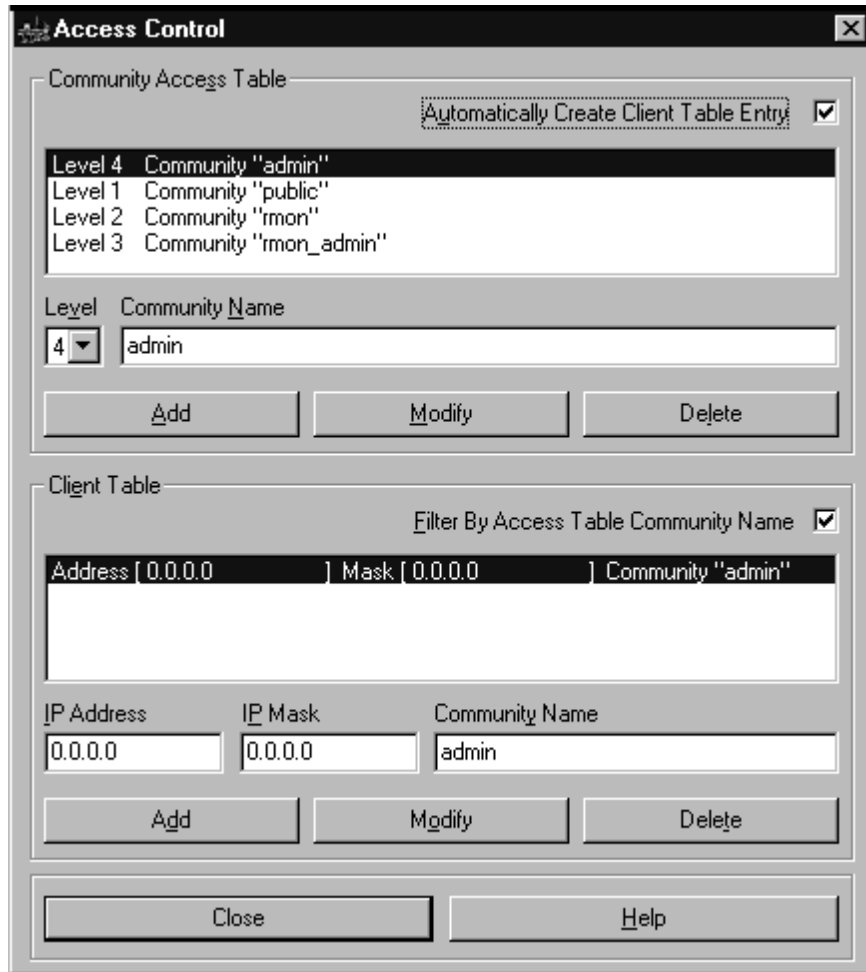


Figure 11. Access Control Dialog

Any changes you make to the Community Access and Client Tables will take effect immediately.

Community Access Names

To set up a new community access name with a specific security level:

If you want Nways Remote Monitor to automatically create an entry in the Client Table for this new entry, enable the Automatically Create Client Table Entry in the top right corner of the dialog. You can add the entry in the Client Table manually at any time (see “Security Levels for Specific End-User Workstations” on page 34).

1. Select the security level by clicking on the *Level* button and selecting the appropriate level from the drop-down menu (shown in Table 5).

Table 5. Security Access Levels

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

- a. To set the community name, type a new value in the Community Name field. The name must be unique.
- b. Click **Add** to create this new entry.

2. To change the settings for an existing community access entry:
 - a. Click an existing entry in the Community Access table. The current settings are displayed in the *Level* and Community Name fields.
 - b. Change the security level as described above, and then click **Modify** to apply the change.
 - c. Change the community name as described above, and then click **Modify** to apply the change.
3. To delete an existing entry, simply select the entry in the Table and click **Delete**.

Security Levels for Specific End-User Workstations

1. By default, all entries will be displayed in the Client Table. To filter the Client Table's contents, to display only the Client Table entries corresponding to the entry currently selected in the Community Access Table, click the **Filter by Community Access Table** button above the Client Table.
2. To add a new Client Table entry:
 - a. Type the IP address and subnet mask of the workstation in the IP Address and Mask fields.
 - b. Enter a unique community name in the Community Name field.
 - c. Click **Add** to create this new entry.
3. To modify a Client Table entry, change the IP address and Mask values, and then click **Modify**.
4. To delete a Client Table entry, simply select the entry and click **Delete**.

Trap Communities

When an alarm on a probe is triggered, the probe can inform other 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 requested previously that they want to be informed. This is controlled by assigning a trap community to each alarm on a probe and, for each trap community, assigning a list of workstations to be informed.

There are two ways to assign trap communities:

- Nways Remote Monitor automatically assigns traps as the default Community name to any new alarm you create. Nways Remote Monitor checks that this community exists on any probe it contacts and will also add the information for the workstation on which it is being run to the traps community.
- You can type in a different community name in the *Trap Configuration* field in the Alarm Creation dialog and editing the trap community names on the probe. In the *Trap Control Dialog*, you can control precisely which workstations on your network receive alarm events from the probe in question.

Assigning trap communities to an alarm is described in “Alarms View” on page 94.

Opening the Trap Control Dialog

In the Agent Maintenance dialog (Figure 7), click **trap...** in the box at the bottom of the dialog to open the Trap Control dialog.

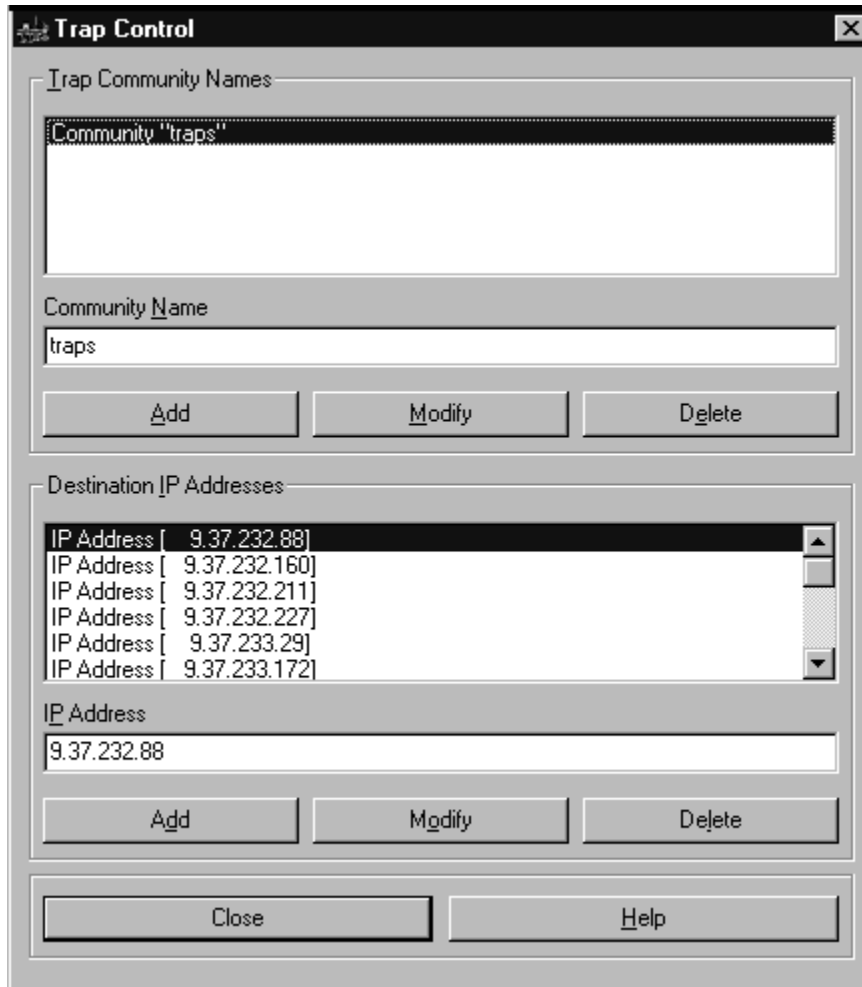


Figure 12. Trap Control Dialog

Trap Community Names

1. To create a trap community, type a unique name in the Community Name field below the Trap Community Names list and click **Add**.
2. To modify a community name, click the entry you want to change and the name will appear in the Community Name field. Edit this field and then click **Modify** to apply the change.
3. To delete a community, click the entry and then click **Delete**.

Destination IP Addresses

To change the list of workstation IP addresses assigned to a community:

1. Select the community by clicking on it in the Trap Community Names list. A list of existing IP addresses assigned to this community will be displayed in the Destination IP Addresses list.
2. To add a destination workstation, type the workstation's IP address in the *IP Address* field and click **Add**.
3. To modify an IP address for a destination workstation, click the entry you want to modify and change the value displayed in the *IP Address* field. Then click **Modify**.
4. To delete a destination workstation from a community, click the workstation IP address and then click **Delete**.

Setting Static Routes

Static routes are used to set up specific routes that the probe should use to reach other networks, overriding the default gateway (see "Default Gateway" on page 29). Up to 16 static routes can be set up on each probe.

1. In the Agent Maintenance dialog (Figure 7 on page 26), click **Static Routes...** to open the Static Routing Table.

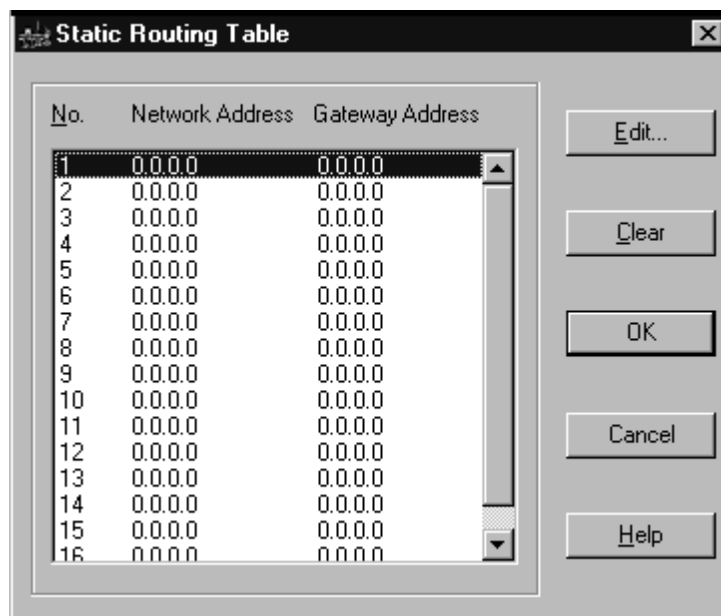


Figure 13. Static Routing Table

2. If you want to reset the contents of the Static Routing Table, press *Clear*. All values will be set to 0.0.0.0.
3. Click a static route to select it.
4. Click **Edit** to open the Edit Routing Entry dialog.

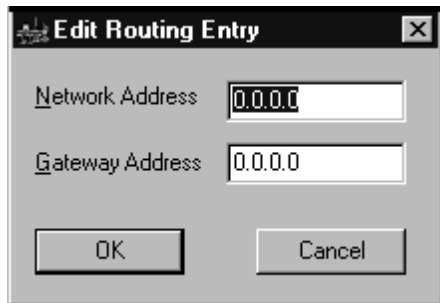


Figure 14. Edit Routing Entry Dialog

- The network address is the IP address of the destination network, for example 91.0.0.0.
 - The gateway address is 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 network as the probe.
5. Click a field and edit the values as appropriate.
 6. Click **OK** to save the new settings and return to the Static Routing table.
 7. Repeat steps 2 to 6 as many times as required.
 8. Click **OK** to return to the Agent Maintenance dialog.

Enabling and Disabling PACMIB

The Port Address Correlation MIB (PACMIB) maps port-to-host data and gathers port statistics for supported devices on your network. Using PACMIB you can gather port and slot statistics on a host using the Host View in Rmonview.

1. In the Agent Maintenance Dialog (Figure 7), click **PACMIB** button to open the PACMIB support dialog.

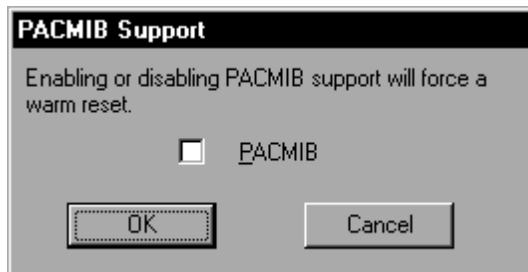


Figure 15. Enabling and Disabling PACMIB

2. If PACMIB is enabled on the current device, *PACMIB* is selected. To disable it, select *PACMIB*. If PACMIB is disabled on the current device, *PACMIB* is not selected. To enable it, select *PACMIB*.

3. Click **OK** to activate your changes and reset the device. You are returned to the Device Configuration dialog box, and the device is unavailable while it resets.
4. When the device is available again, you can use the Host View to gather port and slot statistics for supported devices.

Setting the RMON2 Mode

You can configure RMON2-compliant probes to use optimum table sizes for different applications. You can also disable RMON2 so that the probe can run SmartAgent software such as the RMON2 (ECAM) SmartAgent. ECAM is a precursor to the RMON2 standard.

To set the RMON2 mode, follow these steps:

1. Click **RMON2 Config** to open the RMON2 Config dialog box, shown in Figure 16.

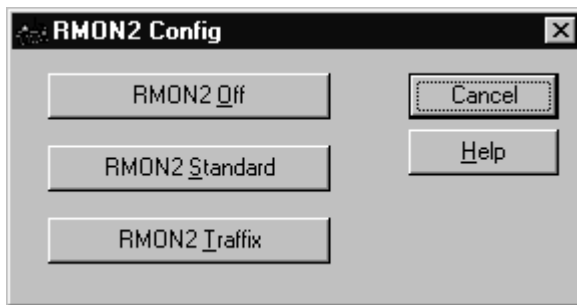


Figure 16. RMON2 Config Dialog Box

2. Choose one of the following settings:
 - RMON2 Off
Click **RMON2 Off** to disable RMON2. You should choose this setting for use with applications which use SmartAgent software.
 - RMON2 Standard Mode
You should select this mode to optimize RMON2's troubleshooting capabilities.
 - RMON2 Traffic Monitor Mode
This mode allocates more memory to Traffic Monitor functions and means that Traffic Monitor usage is optimized.

Note: IBM Nways Traffic Monitor is not currently provided on Windows NT.

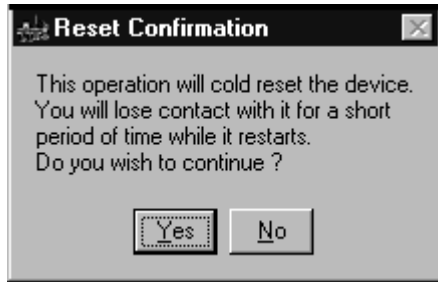


Figure 17. RMON2 Config Dialog Box

3. When you click **Yes**, the probe performs a cold reset and your changes are applied.

Configuring Virtual Interfaces

The physical interfaces on a probe can collect specific sets of data for instrumentation of network health parameters, such as total packets, total errors, and so on. Using the Packet Capture application, physical interfaces can also filter specific types of packets from the network for examination of the contents of those packets.

However, with virtual interfaces you can combine these filtering and instrumentation functions. Virtual interfaces are copies of a physical interface on a probe and are used 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 tables on the probe.

Creating Virtual Interfaces

To create a virtual interface, you must specify the probe and the physical interface it should be attached to, the filter to be used, and the RMON tables where the filtered data should be stored.

1. In the Device Configuration dialog, select the probe on which you want to create the virtual interface by clicking on it in the *Select Probe* list.
2. Select the physical interface to which the new virtual interface will be attached. You can change this selection later from within the Create Virtual Interfaces dialog.
3. Click **Add...** to open the Create Virtual Interfaces dialog.

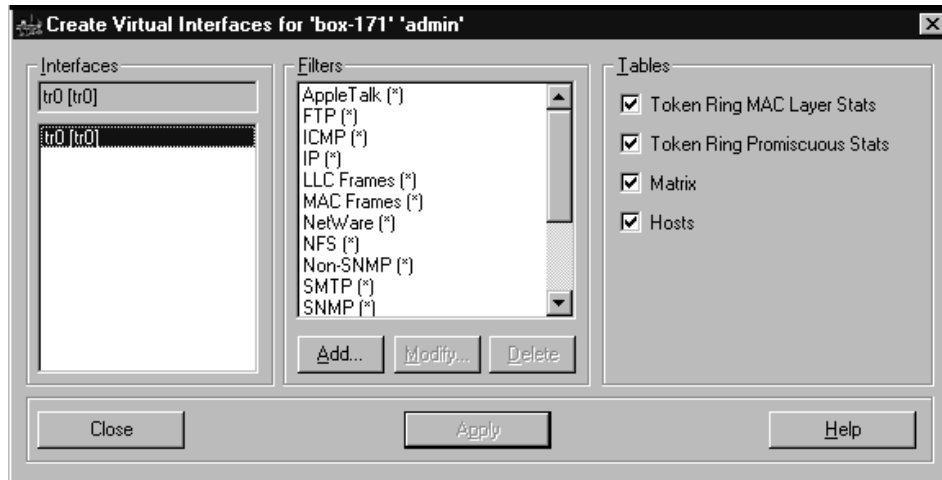


Figure 18. Create Virtual Interfaces Dialog

This dialog is divided into three areas:

- Interfaces** Select the physical interface to which the virtual interface should be attached.
- Filters** Add a filter according to the media type of the selected physical interface, or select one of the predefined ones.
- Tables** Specify which RMON tables should be attached to the virtual interface.

RMON2 tables can be selected once the interface is created using the RMON2 button on the Main Device Configuration dialog screen.

4. Select a physical interface on the probe by clicking on it in the *Interfaces* list. The virtual interface will be attached to the selected physical interface, so any changes made to the physical interface, such as name, will be replicated to the virtual interface.
5. To select a predefined filter, click an entry in the list. The list of predefined filters will vary according to the media type of the selected physical interface.
6. To create your own filters for use with this or any other interface, click **Add...** to open the Filters dialog.

Table 6. Predefined Channels (Filters)

Channel	Description	Physical Interface Media Type		
		Ethernet	FDDI	Token Ring
AppleTalk	Pass AppleTalk packets only	■	■	■
FTP	Pass FTP packets only	■	■	■
ICMP	Pass ICMP packets only	■	■	■

Table 6. Predefined Channels (Filters) (continued)

Channel	Description	Physical Interface Media Type		
		Ethernet	FDDI	Token Ring
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	■	■	■
Non-SNMP	Pass all packets except SNMP	■	■	■
SMTP	Pass SMTP packets only	■	■	■
SNMP	Pass SNMP packets only	■	■	■
Telnet	Pass Telnet packets only	■	■	■
UDP	Pass all UDP packets	■	■	■
WWW	Pass WWW packets only	■	■	■
XNS	Pass XNS packets only	■		
X-Windows	Pass X-Windows packets only	■	■	■

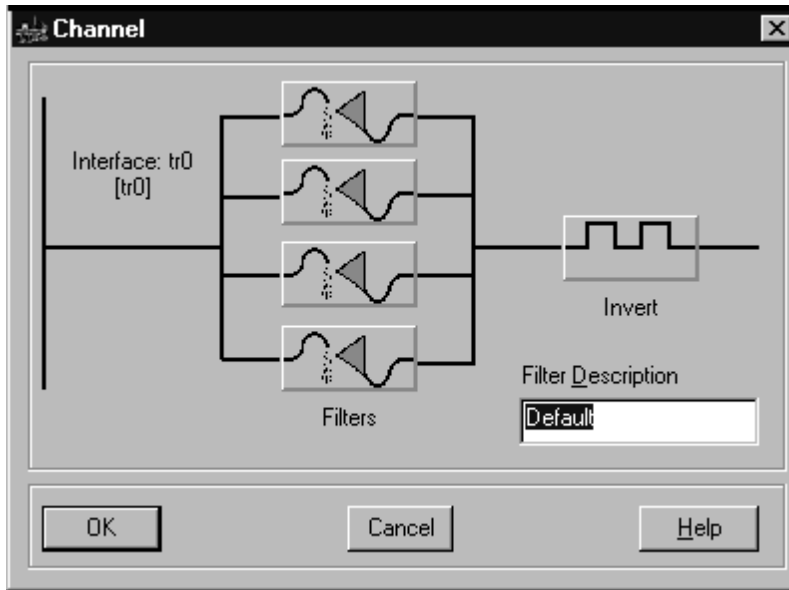


Figure 19. Filters Dialog

- a. You can include up to four sub-filters. To set up a filter, click one of the





Filter buttons and the Edit Filter dialog will open.

Setting up a filter is described in “Using the Filter Editor” on page 113. Click **OK** to return to the Filters dialog.

- b. The *Invert* button lets you invert the logic of the filter. For example, if you are capturing all TCP packets at the moment, simply click the button to start capturing everything except TCP packets.

Table 7. Invert Button

Level	Description
	Collects the specified packets.
	Collects everything except the specified packets.

- c. To create this filter, click **OK**. You will be returned to the Create Virtual Interfaces dialog and the new filter will be selected automatically.

7. Select which tables you want to create by clicking on the buttons for those tables. You can also select tables at a later time using the RMON Tables dialog, as described in “Managing RMON and RMON2 Tables”.
8. To create the virtual interface, click **Apply**. A message box will appear confirming that the virtual interface has been created.
9. Repeat steps 3 to 7 to create as many virtual interfaces as required. When you return to the Configuration dialog, the new virtual interface will be displayed in the *Select Interface* list. The virtual interface will appear as the name of the attached physical interface, followed by the description of the filter in brackets. For example: ie0 (All IP Packets).

Deleting Virtual Interfaces

Deletion of virtual interfaces is carried out from the Configuration dialog.

1. Select the probe from which the virtual interface is to be deleted by clicking on it in the *Select Probe* list.
2. Select the virtual interface to be deleted by clicking on it in the *Select Interface* list.
3. Click **Delete**.
4. If you have selected a virtual interface to which RMON tables are attached, you will be prompted to confirm the deletion. Click **Yes** to continue or **No** to leave the virtual interface unchanged.

Managing RMON and RMON2 Tables

You can view and reset the RMON tables for a physical or virtual interface on a probe from the Device Configuration Dialog.

1. Select a probe by clicking on it in the *Select Probe* list.
2. Click **RMON Tables...** to open the RMON tables dialog. Or Click **RMON2 Tables...** to open the RMON2 tables dialog.

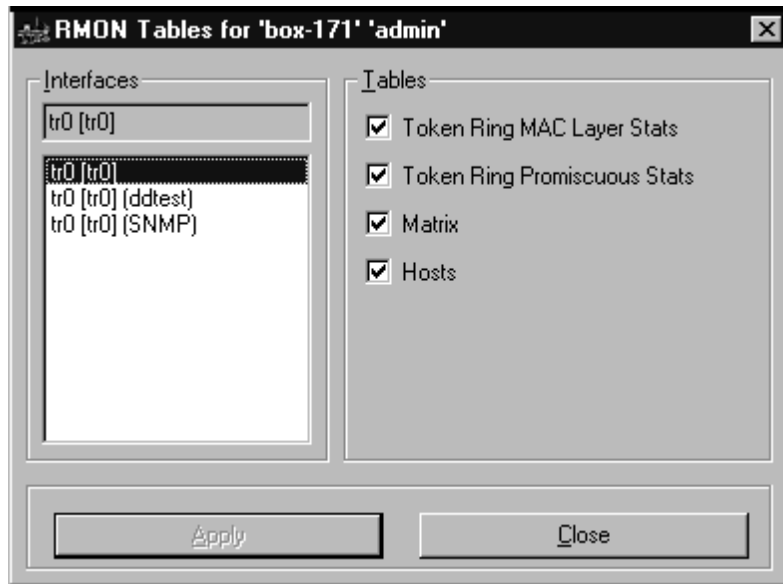


Figure 20. RMON Tables Dialog

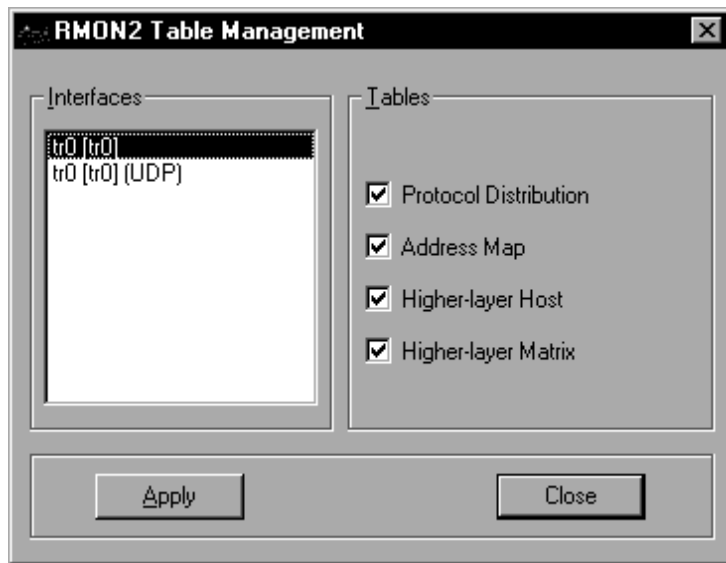


Figure 21. RMON2 Tables Dialog

3. Select the interface for which you want to view the current RMON tables by clicking on it in the *Interface* list. This can be a physical or a virtual interface.

4. To empty an active table of all currently collected statistics, click the check box to turn it off and click **Apply**.
5. To start collecting statistics for an inactive table, click the check box to turn it on and click **Apply**.
6. Click **Close** to return to the Configuration dialog.

Note: Selecting *close* without selecting *apply* first will not have changes effective.

Managing RMON2 (ECAM) SmartAgent Firmware

SmartAgent firmware can be loaded or unloaded from a probe at any time to enable functionality on the probe. The firmware can be started and stopped as required, depending on the type of data you want to collect with the probe.

You can also register SmartAgent firmware with a probe's auto-boot table so that the firmware will be reloaded by the probe on restart.

If you are using an RMON2-compliant probe, the RMON2 standard provides information for most applications and you do not need to download the firmware. To download the SmartAgent firmware, you must disable RMON2 on the probe. See "Setting the RMON2 Mode" on page 39 for more information.

Opening the SmartAgent Maintenance Dialog

Loading and unloading of SmartAgent firmware is carried out from the SmartAgent Maintenance dialog. To open, click **SmartAgents...** in the Device Configuration dialog.



Figure 22. SmartAgent Maintenance Dialog

One element of SmartAgent firmware can be the foundation for more than one application. When you select an application, the underlying firmware will be loaded to the probe and, as a result, *all applications* for that firmware will be made available in Viewman and Rmonview.

Enabling Applications

1. A TFTP server must be active before you can load SmartAgent firmware. See “Downloading Firmware” on page 27 for instructions on starting the TFTP server shipped with Nways Remote Monitor.
2. By default, the firmware is stored in Nways Remote Monitor’s installation directory and the TFTP server address will be set to your PC’s address. If required, change the address in the *TFTP Server Address field*.
3. The list of available applications is displayed as the application name followed by the name of the underlying firmware.

These are the applications that can be run from Viewman or Rmonview—they do not represent the firmware stored on the TFTP server.

The status of an application is displayed after the application name. If the firmware for any of the listed applications is already downloaded to the probe, the status [Loaded] will be displayed, followed by the version number and size.

The number of times that this firmware has been loaded to the probe without unloading is also displayed as # References.

Select an application from the *Available SmartAgent Applications* list. When the firmware for this application is loaded to the probe, all applications based on the same underlying firmware will be made available in the main window.

4. Click **Load**. The probe will contact the TFTP server and, if it is available, will load the selected firmware. If successful, the status of the applications will change to [Loaded].

If the probe is unable to load the firmware, this may be because:

- The TFTP server is unavailable or the TFTP server address has been entered incorrectly.
- The selected firmware is not stored on the specified TFTP server.
- The probe has become unavailable.
- RMON2 is still enabled on the probe. See “Setting the RMON2 Mode” on page 39 for more information.

Check the server details and try again. If still unsuccessful, return to the Configuration dialog and try reselecting the probe to check that it is available.

Disabling Applications

1. Select the application that is no longer required by clicking on it in the *Available SmartAgent Applications* list. You must select an entry that has the [Loaded] status. *Remember that a number of applications can have the same underlying firmware. Disabling one application will also disable all applications based on the same firmware.*
2. Click **Unload** and the status of the applications will be set to [Not Loaded].

Auto-Boot Table

If there are some applications that are required at all times, you can register the underlying firmware with the probe’s auto-boot table. The auto-boot table contains the names of the firmware that should be loaded automatically when the probe is warm-started or power-cycled.

1. To register the underlying firmware with the auto-boot table:
 - a. Click an application in the *Available SmartAgent Applications* list.
 - b. Click **Auto-Boot**. The firmware will be added to the *Auto-Boot* list with the initial status of [Not Loaded - Idle].

Remember that although the application name appears in the auto-boot table, you are in fact registering the underlying firmware. When the probe is restarted, all the applications for that firmware will be available in Viewman and Rmonview.

When the probe is restarted, the probe will attempt to contact the appropriate TFTP server to load the firmware. If successful, the status of the firmware in the auto-boot table will be set to [Autoboot Succeeded].

If the attempt to load the firmware is unsuccessful, the message [Autoboot failed] will be displayed.

2. To disable applications and remove SmartAgent firmware from the auto-boot table:
 - a. Select the application in the *Auto-Boot* list.
 - b. Click **Delete**.

The firmware is still available to its associated applications in the *Available SmartAgent Applications* list, but the applications will no longer be useable in Viewman if the probe is restarted.

Managing User-Defined Protocols

Nways Remote Monitor allows you to view the protocol directory on an RMON2 probe. The protocol directory forms part of the RMON2 standard, and lists all the protocols for which the device is gathering statistics.

If you are using customized protocols or protocol encapsulations on your network, you may want to define these protocols and add them to your protocol directory to enhance Nways Remote Monitor's Protocol Distribution view.

For examples of the protocols supported by an RMON2 compliant device, see Appendix H. RMON2 and ECAM Protocols.

Viewing the Protocol Directory

To view the protocol directory, follow these steps:

1. In the Device Configuration dialog box, select a probe from the Select Probe area.
2. Click **Protocols...** to open the Protocol Directory dialog box, shown in Figure 23 on page 50.

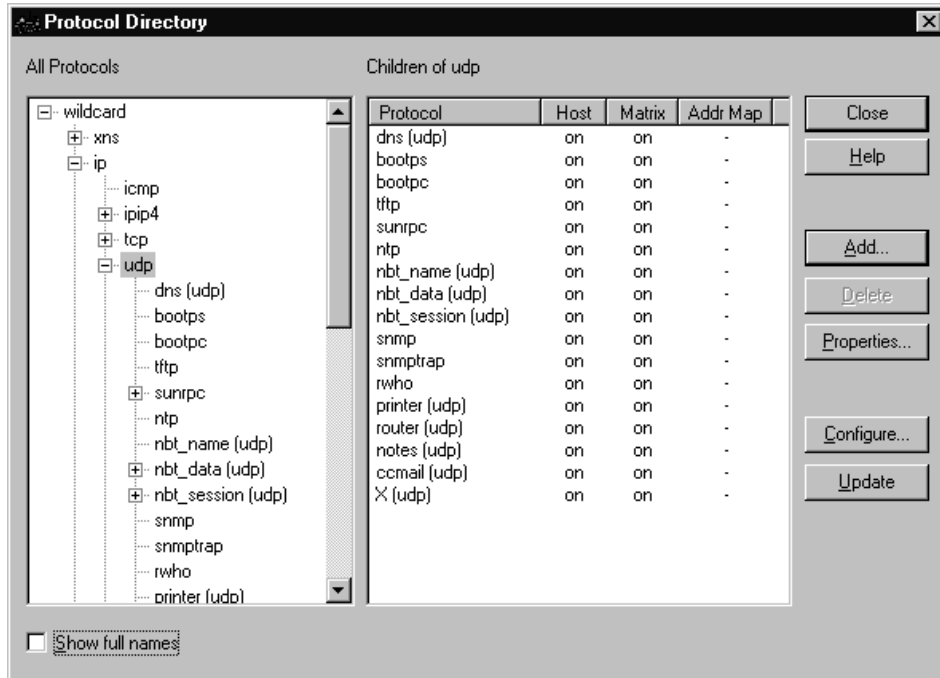


Figure 23. Protocol Directory Dialog Box

This dialog displays all the protocols for which the device is gathering statistics. Click **Show full names** to expand the protocol names to show the full encapsulation path. For example, *udp* would be displayed as **.ip.udp*.

Adding a Protocol

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

- Click **Add...** in the Protocol Directory dialog to open the User Defined Protocol dialog, shown in Figure 24 on page 51.

If a protocol cannot be extended, the Add... button is disabled.

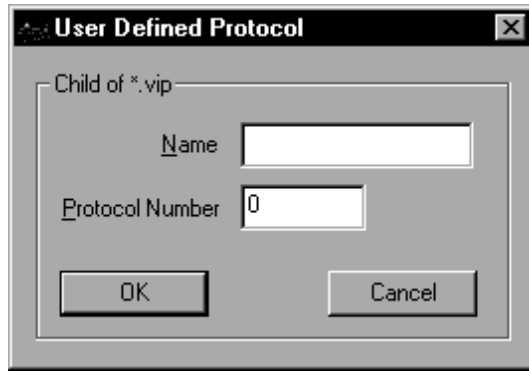


Figure 24. User-Defined Protocol Dialog

- 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.
 - You have tried to extend a protocol that cannot be extended-the *Add...* button is disabled.
 - The probe does not support user-defined protocols-the *Add...* button is disabled.
 - The probe has run out of memory. You must delete a protocol and warm-start the probe before adding another protocol.
- If you cold-start the probe, all user-defined protocol information is lost.
- Click **OK** to return to the Protocol Directory dialog.

Deleting a Protocol

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

1. Select the required protocol in the Protocol Directory dialog.
2. Click **Delete**.

Updating Protocol RMON2 Tables

Nways Remote Monitor allows you to update the RMON2 tables for a specific protocol or for a specific protocol entry and all its children protocols.

Select **Properties** to update the RMON2 tables for a specific protocol. This dialog displays the protocol's full name and if the protocol can be extended. Update the protocol using the following steps:

1. Select the protocol in the Protocol Directory dialog.
2. Click the **Properties** button.
3. Select the required RMON2 tables.

4. Select **OK** or **Cancel** to return to the Protocol Directory dialog.

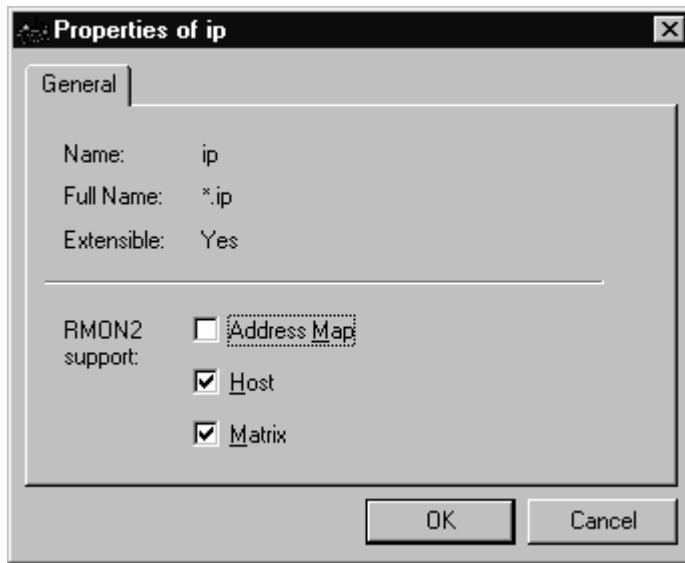


Figure 25. Example of a Protocol Properties Dialog.

Select **Configure** to update the RMON2 tables for a specific protocol and its children protocols. Update a protocol tree using the following steps:

1. Select the top level of the required protocol tree in the Protocol Directory dialog.
2. Click the **Configure** button.
3. Select the required RMON2 tables.
4. Select **OK** or **Cancel** to return to the Protocol Directory dialog.

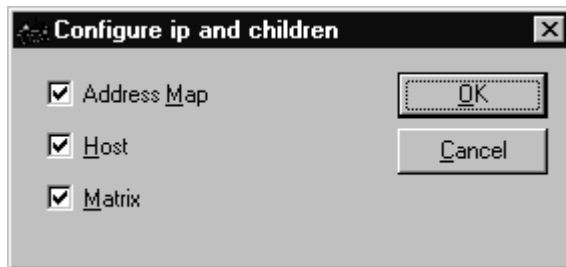


Figure 26. Example of a Protocol Configure Dialog.

Chapter 4. Setting Up Station Names

Information about the stations on your network can be added in two ways:

- Automatically collected from probes by Nways Remote Monitor Translator
With an RMON2 probe or the SmartAgent firmware downloaded to a probe, that probe will collect information about the stations on your network. This information can be gathered at regular intervals by the Nways Remote Monitor Translator application.
- Manually added via the Station List Editor
The level of station address that should be displayed within the Nways Remote Monitor applications can be set from both the Translator and the Configuration dialogs.

This chapter describes:

- Automatic detection of stations
- Launching the Translator
- Manual setup of stations
- Setting the Name Translation level
- Specifying vendor prefixes

Automatic Detection of Stations

A correctly configured probe automatically constructs a table that maps a MAC address to a network layer address for devices communicating on the network. An Nways Remote Monitor application called Translator combines the address tables from multiple probes into a single address translation table. This table provides station address information to all other Nways Remote Monitor applications.

The following two types of probes build an address table.

SmartAgent Probes

SmartAgent firmware is shipped with Nways Remote Monitor. With this SmartAgent firmware downloaded to a probe, the probe automatically constructs the address table. (See “Managing RMON2 (ECAM) SmartAgent Firmware” on page 46 for instructions on loading SmartAgent firmware to probes.)

RMON2 Probes

RMON2 probes must be configured to create the address table.

1. Launch the Device Configuration Dialog (See “Launching the Device Configuration Dialog” on page 21).
2. Select **RMON2 tables...** on the main dialog panel.
3. Check “Address mapping” in the “RMON2 Table Management” dialog.

4. Select **Apply** to have any changes applied to the probe.
5. Select **Close** to exit the dialog.

Note: Selecting **Close** without selecting **Apply** first will not make changes effective.

Launching the Translator

Translator can be launched from within Viewman, Nways Remote Monitor's main window, or from your system software.

1. From Viewman, click



or choose **Translator** from the applications window.

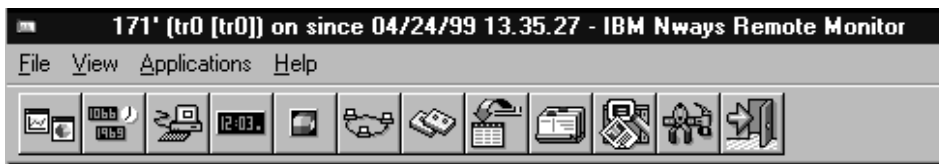


Figure 27. Nways Remote Monitor Menu and Toolbar

Start Menu

From the Start menu, select the *IBM Nways ReMon* Program group, then choose *Translator* from the Applications menu.

Translator Main Window

Translator's main window is divided into three areas:

- Menu bar
- Status log
- Status bar

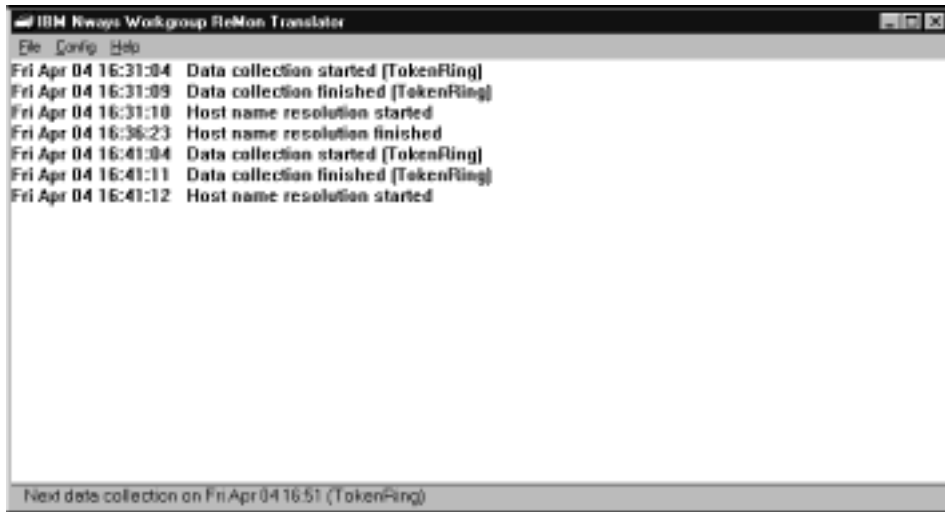


Figure 28. Translator Main Window

Menu Bar

The menu bar at the top of the window gives you access to the following functions:

File

Import	Loads station information from Nways LAN Remote Monitor for Windows.
Save Status Log	Saves the contents of the status log area in the main Window to an ASCII-format file.
Print Status Log	Prints the contents of the status log.
Exit	Quits the application.

Config

Data Collections	Launches the Data Collection Configurations dialog, from which you can add, modify, and delete data collections.
Translation Level	Lets you set the display level of station names to be used in all Nways Remote Monitor station-related views. This function is described in "Setting the Name Translation Level" on page 62.

Host Name Resolution

When selected, Translator will attempt to map a host name for any IP address found, using your PC's configured host name lookup process (for example, DNS).

RMON Devices

This gives access to the Device Configuration dialog (see "Launching the Device Configuration Dialog" on page 21). This configures the list of RMON-compliant devices available on the network.

Help**Contents**

Opens Nways Remote Monitor's on-line help system.

About Translator

Displays version and copyright information.

Status Log

The status log forms the largest area in the main window. While data collection is taking place, status messages will appear in this area. When the area becomes full of messages, you can scroll up and down through the log. The contents of the log can be saved to a file or printed from the **File** option in the menu bar.

Status Bar

The status bar, located at the bottom of the main window, is used to display the status of the current or next collection.

Importing Data

If you have upgraded from Nways LAN Remote Monitor for Windows, you can import the station information contained in the older version's Host.Map file into Translator. This means that you do not need to reenter station-specific information.

1. From the File menu, select **Import**. The Import Host Map File dialog will open.

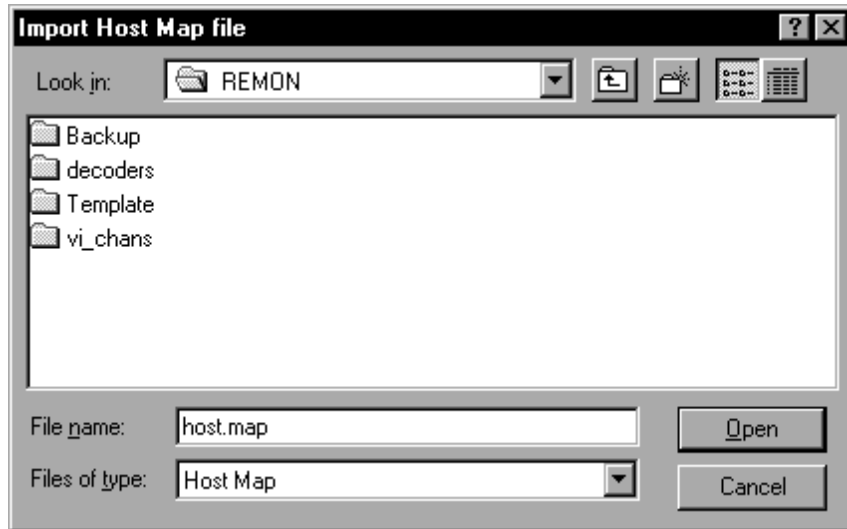


Figure 29. Import Host Map File Dialog

2. Locate the Host.Map file and click **Open** to import the contents of this file.
You will be returned to the main window and the status `Importing` will be displayed at the end of the status bar. When importing is complete, this status message will disappear.

Starting Data Collection

To start the collection of station information, you must set up a collection configuration specifying from which probes and interfaces data should be collected and what type of data should be collected.

1. In the Translator main window, select **Data Collections...** from the Config menu to open the Data Collection Configurations dialog.

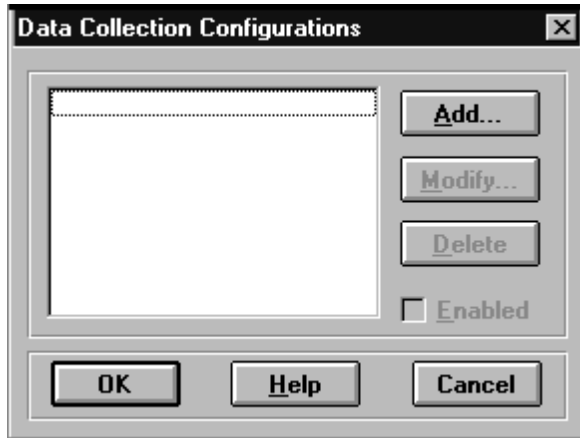


Figure 30. Data Collection Configurations Dialog

From this dialog you can create new collection configurations by adding a configuration or by modifying an existing configuration.

2. To add a configuration, click **Add...** to open the Data Collection Editor.

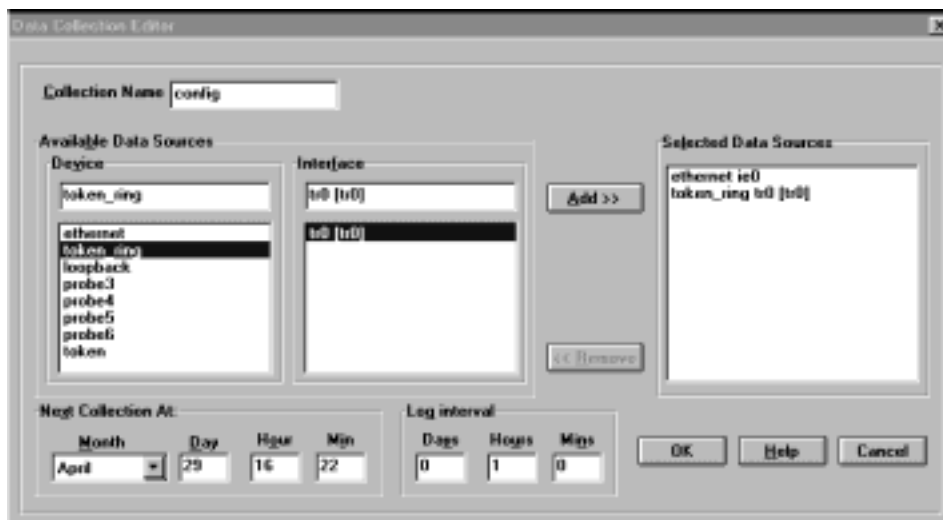


Figure 31. Data Collection Editor

3. Enter a unique name for this collection in the *Collection Name* field.
 - To select a probe and one interface, click the appropriate entries in the *Device* and *Interface* lists. Then click **Add>>**.
 - To select several probes:
 - a. Perform one of the following actions:

- Hold down **Ctrl** and click each probe in the *Device* list in turn.
 - Click the first probe and then drag it with the mouse to the last probe.
 - Click the first probe and, holding down the **Shift** key, click the last probe.
- b. Click **Add>>**. All interfaces on the selected probes will be added.

When more than one probe is selected, all available interfaces will be selected by default. If you are using an RMON2-compliant device, data is collected automatically from all interfaces on the device. If you are using an RMON device with RMON2 (ECAM) SmartAgent software loaded, you must select an interface from the Interface area.

- To deselect entries, click a single entry or use one of the selection procedures described in step 3 on page 58 to select multiple entries. Then click **<<Remove**.
 - Set the date and exact time at which collection should be started in the *Next Collection At* area.
 - Set the frequency at which subsequent collections should be made in the *Log Interval* area. By default this is set to every hour.
 - Click **OK** to create this collection configuration.
4. When a collection configuration is created, the *Enabled* toggle button in the Data Collection Configurations dialog will be selected automatically. To activate data collection for a new configuration, simply click **OK** in the Data Collection Configurations dialog to save your changes and return to the Translator main window.

The time of the next scheduled collection will be displayed in the status bar at the bottom of the main window. A log of data collections is maintained in the status log area in the main window.

Stopping Data Collection

To stop data collection for a configuration, you can either disable it or delete it.

1. In the Translator main window, select *Data Collections...* from the Config menu and the Data Collection Configurations dialog will open (Figure 30 on page 58).
2. To disable data collection for a configuration:
 - a. Select the configuration by clicking on it.
 - b. Click the **Enabled** toggle button to deselect it.
If you want to restart collection at any time, simply click again on the **Enabled** toggle button to select it.
3. To permanently delete a configuration:
 - a. Select the configuration that is to be deleted by clicking on it.
 - b. Click **Delete**.
4. To save your changes, click **OK**.

Deleting a Data Collection

To permanently delete a data configuration, follow these steps:

1. Select the configuration that is to be deleted.
2. Click **Delete**.
3. To save your changes, click **OK**. To abandon your changes, click **Cancel**.

Manual Setup of Stations

You can use the Station List Editor to add or modify entries in the Translator table, perhaps to set up a station in advance of its being added to the network, or to add a new name for an existing station.

1. The Station List Editor is launched from the Device Configuration dialog (see “Launching the Device Configuration Dialog” on page 21).
2. In the Device Configuration dialog, click **Stations....**

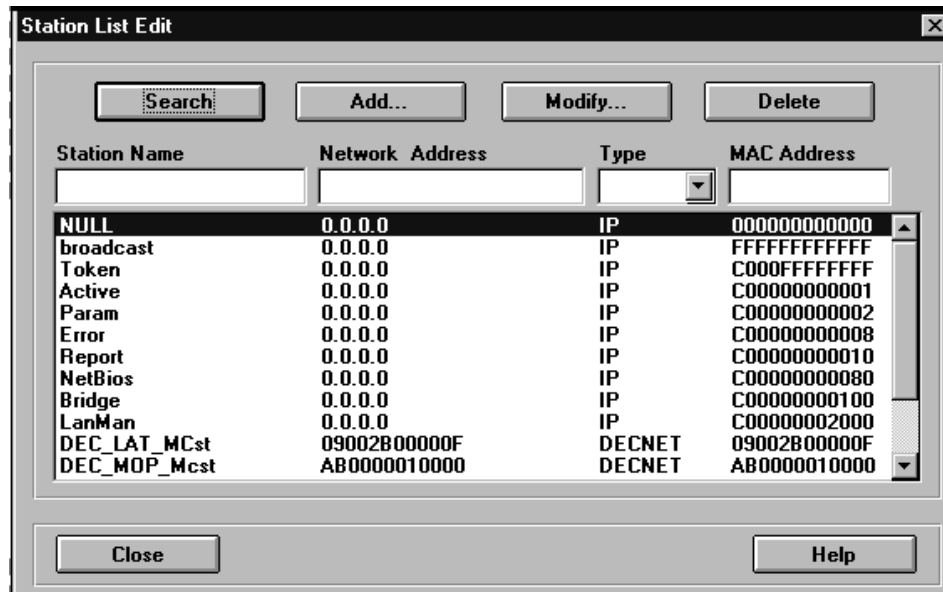


Figure 32. Station List Editor

The values displayed for each station are:

- Station Name** A user-defined name or a name discovered by the Translator using the host name lookup process configured on your PC.
- Network Address** The network address of this station.

Type Either IP, IPX, DECnet, SNA, AppleTalk, or VINES.

MAC Address The 12-digit MAC address of the station.

3. The Station List Editor dialog contains a search function to let you search for any string in any of the available fields.
 - a. To search for a specific string, enter a value in the *Station Name*, *Network Address*, or *MAC Address* fields or select a network type. Then click **Search** and any matching entries will be displayed in the station list.
 - b. Use an asterisk (*) as a wildcard character when entering a string and click *Search*. For example, entering **1127.40.*.*** in the *Network Address* field would result in every station whose Network Address begins with 127.40. being displayed in the station list.
 - c. To display all station entries, leave the *Station Name*, *Network Address*, and *MAC Address* fields and the network type blank and click **Search**. All entries will be displayed in the station list.
4. To add a new station, click **Add** to open the Add Station dialog.

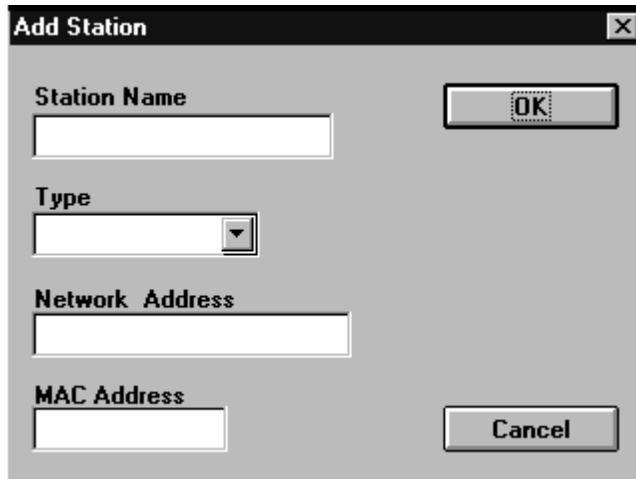


Figure 33. Add Station Dialog

- a. Enter new values in the *Station Name*, *Network Address*, and *MAC Address* fields.
 - b. Select a *Type* from the drop-down menu.
 - c. Click **OK** to create this new station and you will be returned to the Station List Editor.
5. To modify a station:
 - a. Click the entry in the station list and then click **Modify...** to open the Edit Station dialog.

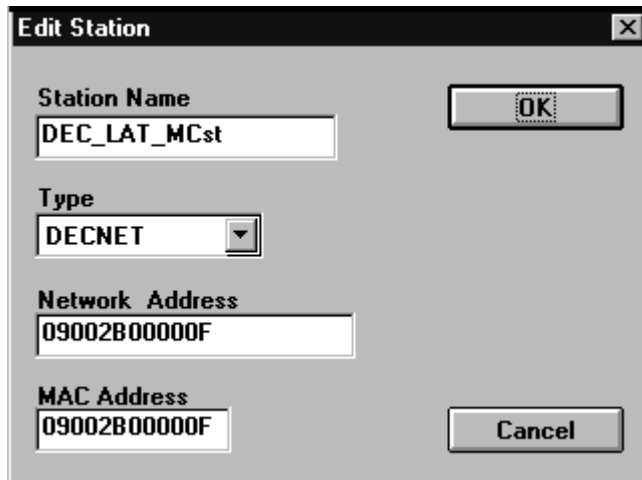


Figure 34. Edit Station Dialog

- b. Edit the values in any of the fields.
 - c. Click **OK** to confirm your changes.
6. To delete a station:
 - a. Click the entry in the station list.
 - b. Click **Delete**.
7. Click **Close** to return to the main window.

Setting the Name Translation Level

There are four name translation levels available in Nways Remote Monitor.

These levels are described in Table 8:

Table 8. Name 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.
Vendor ID	The first 6 characters of this name are taken from the vendor ID contained in the Vendor.Map file, followed by the remaining 6 digits of the MAC address (see "Specifying Vendor Prefixes" on page 63).
MAC Address	The 12-digit MAC address will be displayed.

Nways Remote Monitor will attempt to display a value for the selected level. If a value is unavailable, then the next level will be displayed, and so on. As a result, a mixture of different levels of names may be visible.

You can select which level of address Nways Remote Monitor should attempt to display in all station-related views via the Set Translation Level dialog. You can also set your preferred network protocol.

1. The Set Name Translation dialog can be accessed from within Remote Monitor Translator and also from the Device Configuration dialog.
 - In the Translator main window, select *Translation Level* from the Config drop-down menu.
 - In the Device Configuration dialog, click the **Translation...** button.

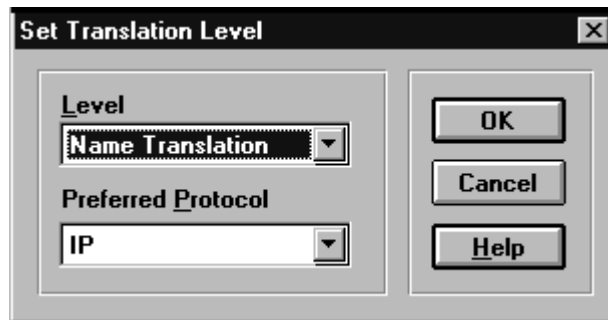


Figure 35. Set Translation Level Dialog

2. To set the level of address translation that Nways Remote Monitor should attempt to display, choose either *Name Translation*, *Protocol Address*, *Vendor ID*, or *MAC Address* from the Level drop-down menu.
3. To set the *Preferred Protocol*, choose either *IP*, *IPX*, *DECnet*, *AppleTalk*, *VINES*, or *SNA* from the drop-down menu. The preferred protocol indicates which protocol address or name should be displayed if a given MAC address has more than one network address.
4. Click **OK** to save the new setting.

The new level will appear in Viewman or in any station-specific application views at the next refresh or update point.

Specifying Vendor Prefixes

Every device—no matter where it is manufactured in the world—has its own unique MAC address. To make this possible, each vendor is allocated a block of addresses. The vendor then assigns a different address to every device it manufactures. For example, every address that begins with the string 0004AC is an IBM device. Nways Remote Monitor comes with most common vendor prefixes defined. To see them, open the Vendor.Map file in the installation directory. A typical entry in the Vendor.Map file is:

```
0004AC      IBM_
```

Every time Nways Remote Monitor sees an address such as 0004AC123456, it will display the address as IBM_123456. This makes identification of devices easier.

To add your own vendor names to the Vendor.Map file, simply edit the file using a text editor such as Notepad or Write.

Chapter 5. Viewman

Viewman's main window provides a simple check of a LAN segment, showing you key error and usage information. It also displays alarm locations and status messages.

By selecting a physical or virtual interface on a remote probe, you can view the performance and condition of the monitored network segment.

The graphs that appear in the main window will vary according to the media type of the selected interface. Click on parts of the displayed graphs to drill down for greater detail.

See "Chapter 2. Using the Nways Remote Monitor Interface" on page 7 for a guide to the Viewman window.

This chapter describes:

- Launching Viewman
- Configuring the main window
- Viewman graphs

Launching Viewman

To launch Viewman, select the **IBM Nways ReMon** Program Group from the Start menu and then choose **Viewman**.

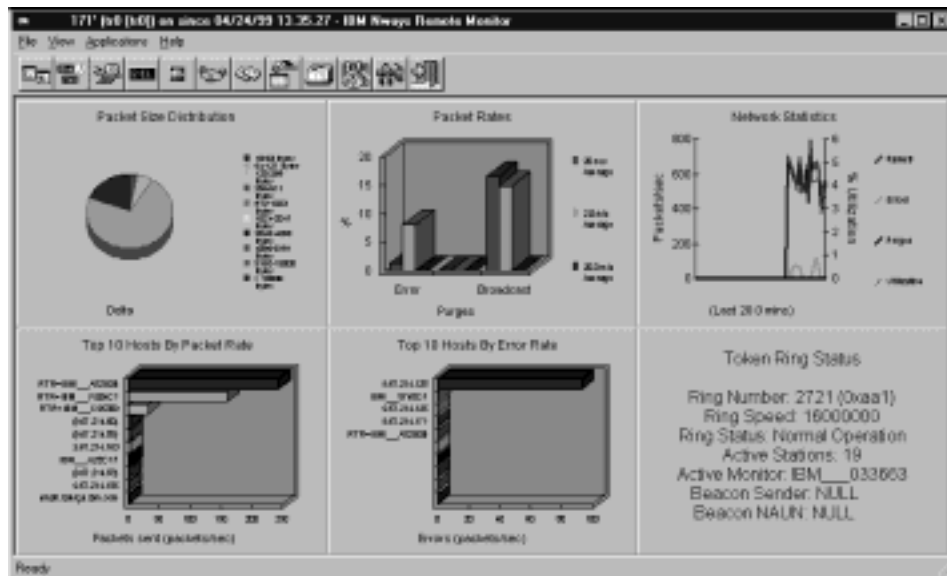


Figure 36. Viewman

Configuring the Main Window

All configuration of the main window is carried out from the View menu. The toolbar, status bar, and alarm bar window area may be displayed or not displayed.

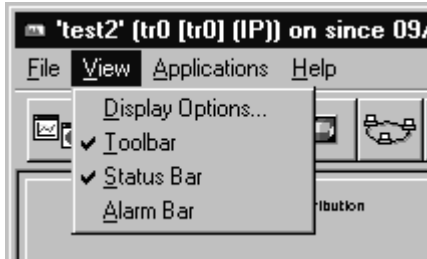


Figure 37. View Menu

The Viewman Display Options configures:

- LAN segment to be monitored
- Refresh rate for displayed data
- Graph display choices

1. Select *Display Options...* from the *View* menu to open the Display Options Dialog.

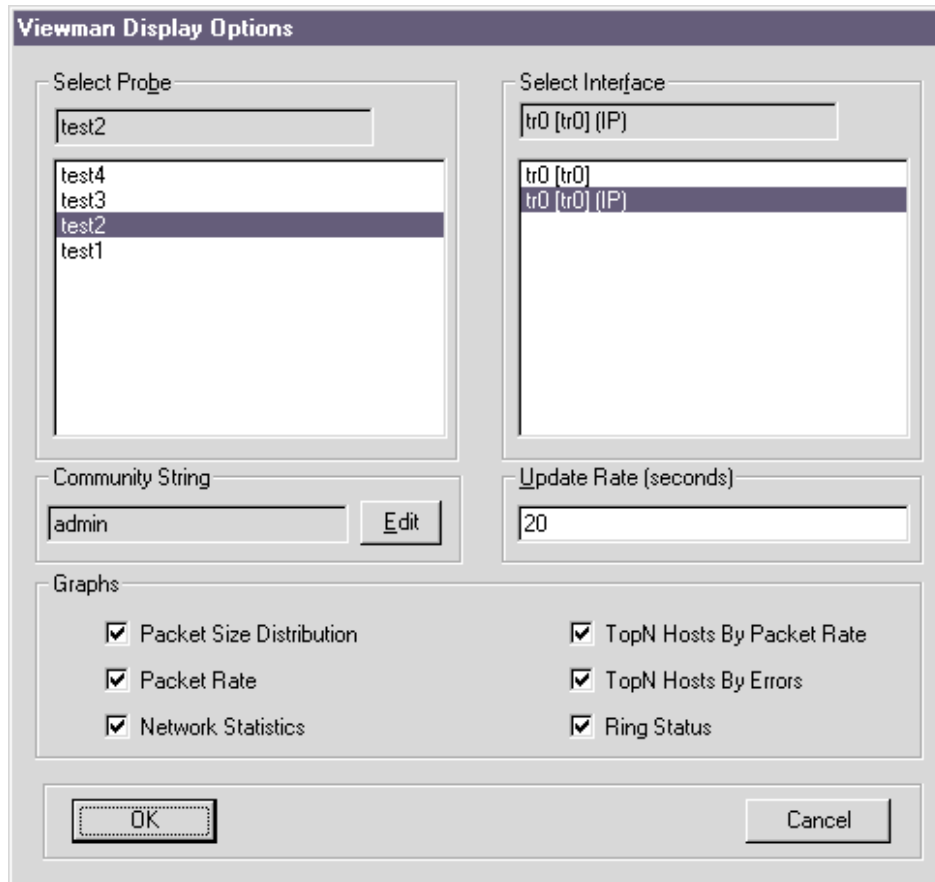


Figure 38. Display Options

2. Select the network segment to be monitored:
 - a. Click on a probe in the Select Probe list. If the probe is assessable, a list of available interfaces will be displayed in the Select Interface list.
 - b. Select a physical or virtual interface by clicking on it in the list. If you select a virtual interface, you will be monitoring the subset of data configured for that interface (see “Configuring Virtual Interfaces” on page 40).
3. The community string currently being used is displayed in the *Community String* field. To change the community string:
 - a. Click on **Edit** to open the Edit Community dialog.
 - b. Type the new community string.
 - c. Click on **OK** to save your changes and return to the Display Options dialog. The new community string will be used in subsequent communications with the probe. Click **Cancel** to discard your changes.

4. In the Update Rate field, set the refresh rate in seconds at which the graphs should be refreshed with new data.
5. Specify which graphs are displayed in the Viewman main window by selecting or deselecting the required graphs. By default, all graphs are displayed. For information on graph availability, see “Viewman Graphs”.
6. Click **OK** to confirm your selections, and Viewman will refresh to focus on the selected network segment.

Viewman Graphs

The list of graphs that are available to you will vary according to the media type of the selected probe or, in the case of multi-interface probes, of the selected interface.

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

Table 9. Available Graphs by Media Type

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

Packet Size Distribution

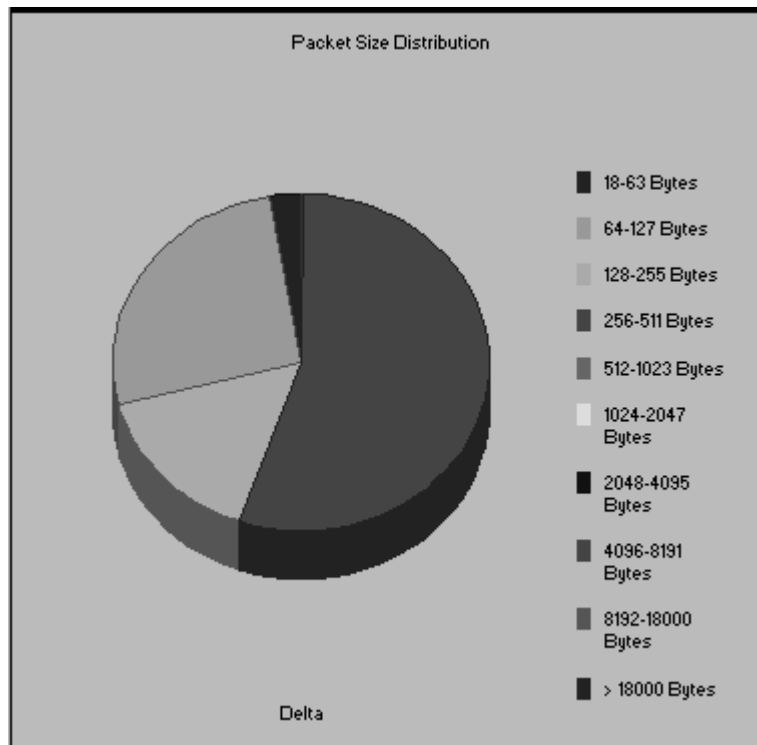


Figure 39. Packet Size Distribution Graph on Token Ring

The Packet Size Distribution graph provides an easy way to see just how the total traffic on your network is made up—typical packet size, how much of the traffic is made up of small versus large packets, and so on. It is displayed as the variation or *delta* over the last sample period.

Packet Rates

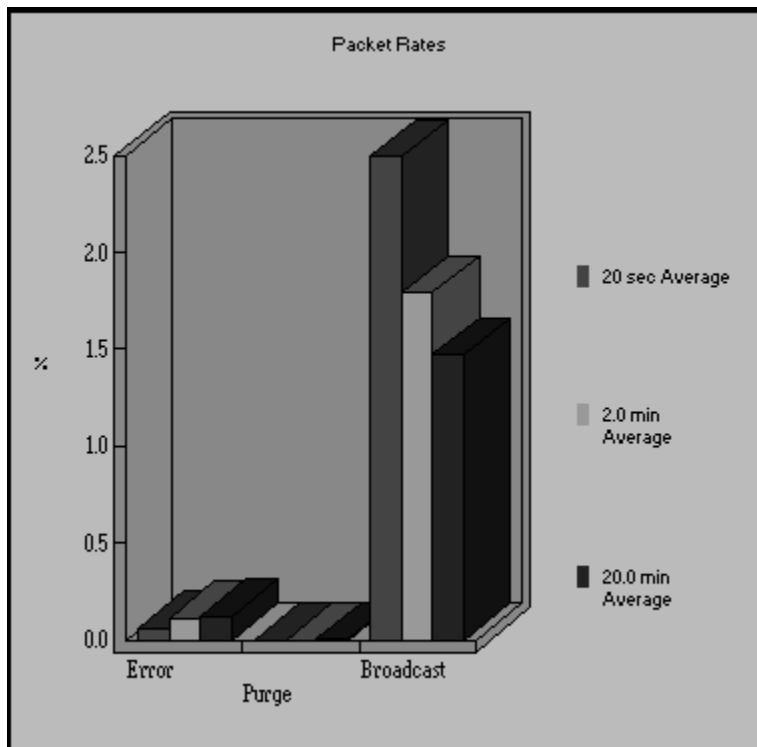


Figure 40. Packet Rates Graph on Token Ring

The Packet Rates graph shows you, at a glance, how many broadcast packets, errors, collisions, SMT frames, or purges have been detected on the network—a convenient way of making a rapid assessment of network performance. It lets you see what is happening right now and what happened over previous sample periods.

Table 10. Packet Rate Graph Variables by Media Type

Variables	Media Type		
	Ethernet	FDDI	Token Ring
Broadcasts	■	■	■
Collisions	■		
Errors	■	■	■
Purges			■
SMT Frames		■	

Network Statistics

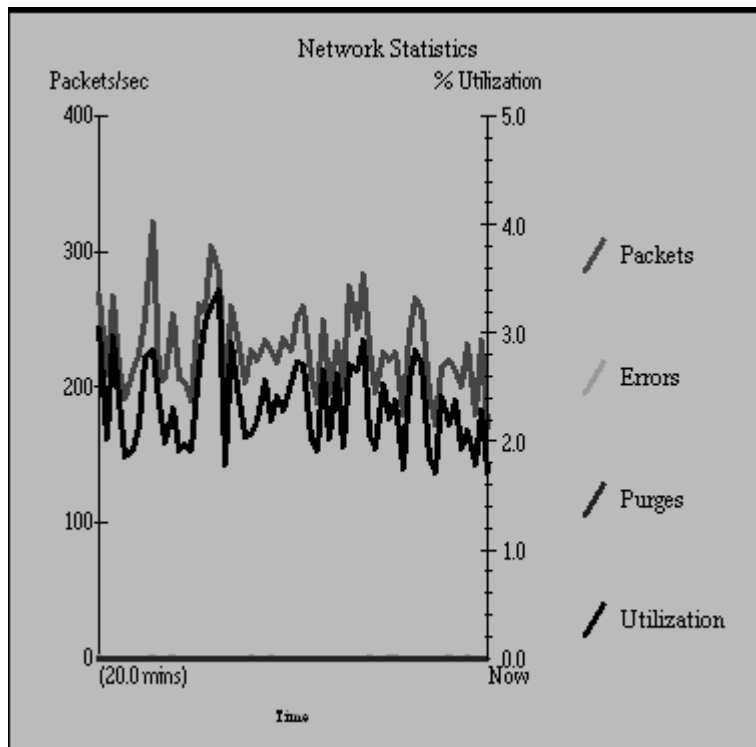


Figure 41. Network Statistics on Token Ring

The Network Statistics graph shows packets, errors, collisions, SMT frames, purges, and network utilization displayed graphically as a time-line chart. It compares spikes in traffic with spikes in errors, purges, or collisions for a rapid assessment of the condition of the network.

Table 11. Network Statistics Graph Variables by Media Type

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

Top 10 Hosts by Packet Rate

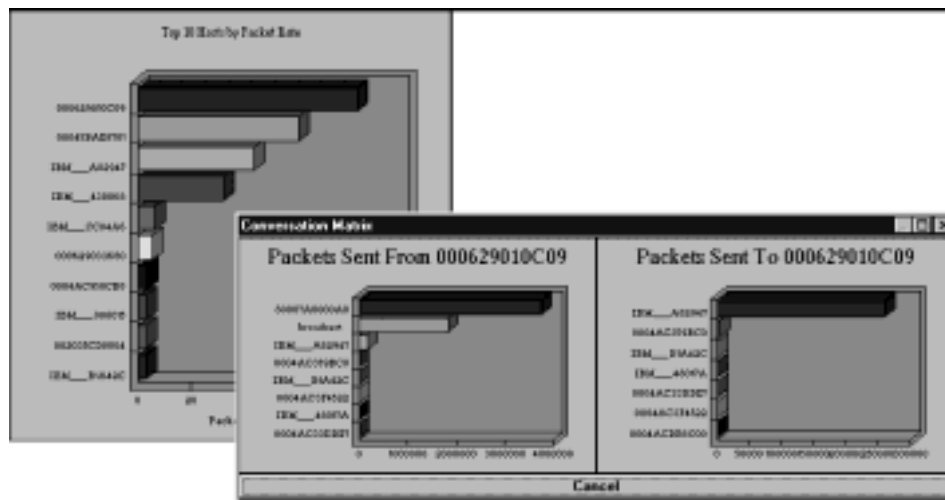


Figure 42. Top 10 Hosts by Packet Rate on Ethernet

Which hosts or stations on the network are generating the most traffic? For a breakdown on a particular station, or to find out whom it is talking to, simply click the appropriate bar on the histogram for a more detailed view.

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

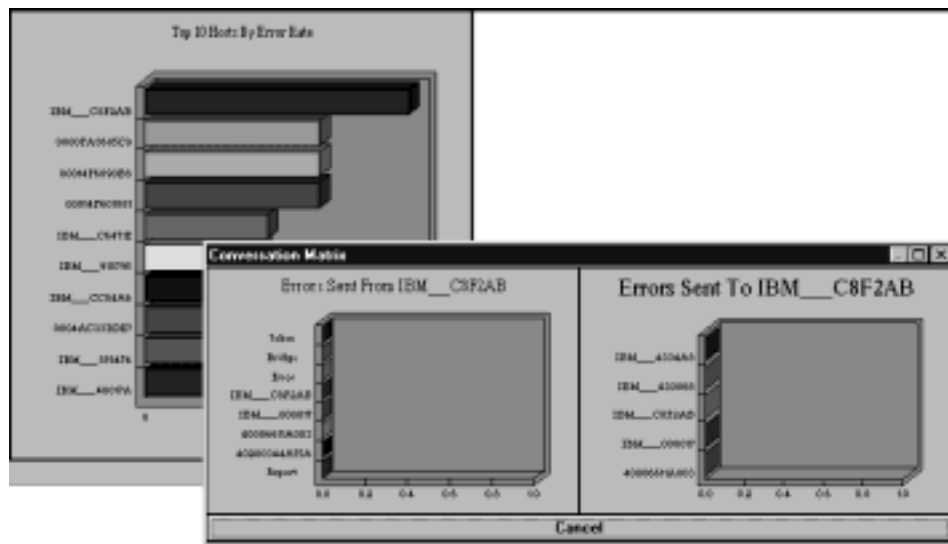


Figure 43. Top 10 Hosts by Error Rate on Ethernet

Available for Ethernet and token ring, this graph identifies:

- Where most error packets are coming from
- Which other stations these stations are talking to

Click the appropriate bar for a rapid report on the possible source of network problems.

Top 10 Receivers (FDDI)

The FDDI-specific panel replaces the Top 10 Hosts by Error Rate panel displayed for Ethernet and token-ring interfaces. At a glance, see the top 10 destination hosts or stations for traffic on the network. Click a bar on the histogram to see who is talking to these stations.

Event Distribution (Ethernet)

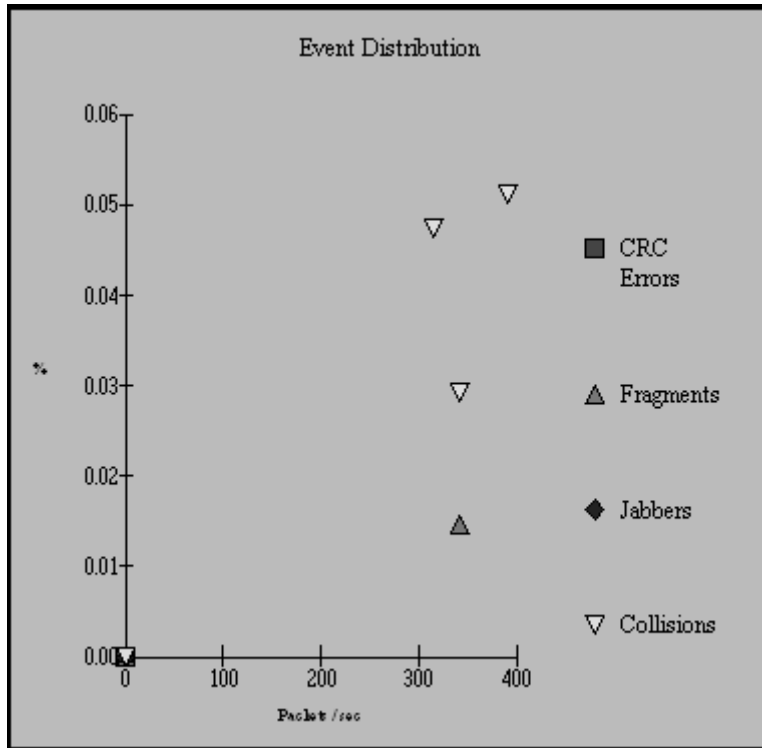


Figure 44. Event Distribution on Ethernet

Spot trends on Ethernet by looking for clusters. Do errors-for example, CRCs-increase as traffic gets above a certain level?

Ring Status (FDDI and Token Ring)

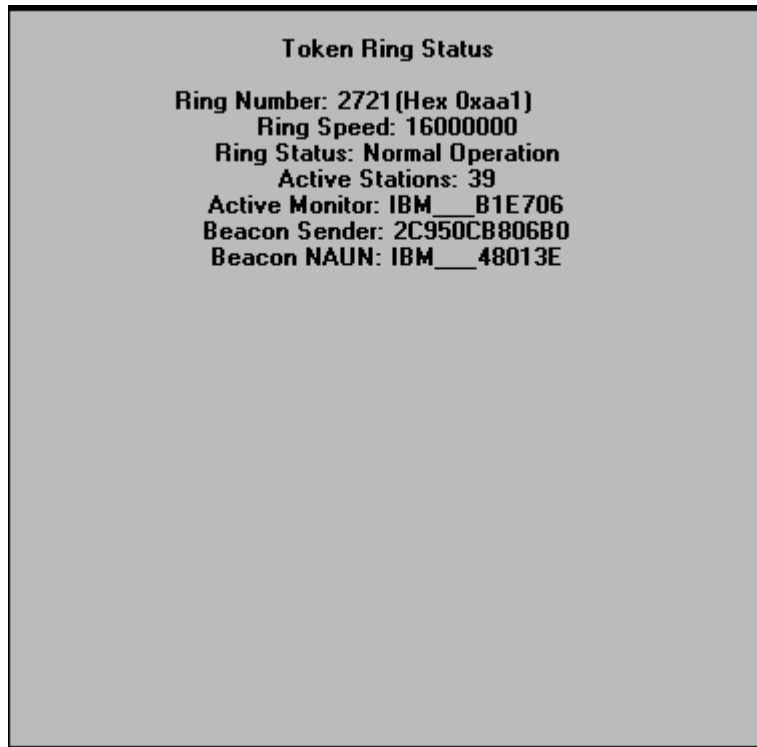


Figure 45. Ring Status

The ring status panel gives a constantly updated summary of ring information for either FDDI (Table 12) or token ring (Table 13).

Table 12. FDDI Ring Status Panel Variables

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.
Dir. Beacon Source	Address of the host that sent the last Directed Beacon.
Beacon Source	Address of the host that sent the last Beacon.

Table 12. FDDI Ring Status Panel Variables (continued)

Variable	Definition
Ring Status	Current operational status of the FDDI ring: <ol style="list-style-type: none">1. Ring Operational2. Non-Operational Claim3. Non-Operational Beacon4. Non-Operational Directed Beacon5. Unknown

Table 13. Token-Ring Status Panel Variables

Variable	Definition
Ring Number	The ring number of this ring segment.
Ring Status	The current overall status 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 to broadcast Beacon frames onto the ring.
Beacon NAUN	The last beaconing station's Nearest Active Upstream Neighbor.

Chapter 6. Rmonview and RMON Applications

Nways Remote Monitor's RMON applications are used to collect predefined or user-defined data about your network. The applications can be launched from within Viewman or separately from Rmonview. When an application is launched from Viewman, Rmonview is automatically launched and the application will be displayed within Rmonview's application display area.

This chapter contains the following sections:

- Launching Rmonview
- Launching RMON applications
 - from Rmonview
 - from Viewman
- Configuring RMON Applications
- Creating and Editing Views
 - Statistics view
 - History view
 - Host view
 - Matrix view
 - Token-ring view
 - Alarms View
- Address Translation View
- Using the protocol distribution application

A guide to Rmonview's main window is contained in "Chapter 2. Using the Nways Remote Monitor Interface" on page 7.

Launching Rmonview

To launch Rmonview, select the *IBM Nways ReMon* Program Group from the Start menu and then select *Rmonview*.

Launching RMON Applications

From within Rmonview or Viewman, an application can be launched. All applications, once launched, will be displayed within Rmonview's application display area.

Rmonview

To open an application from within Rmonview:

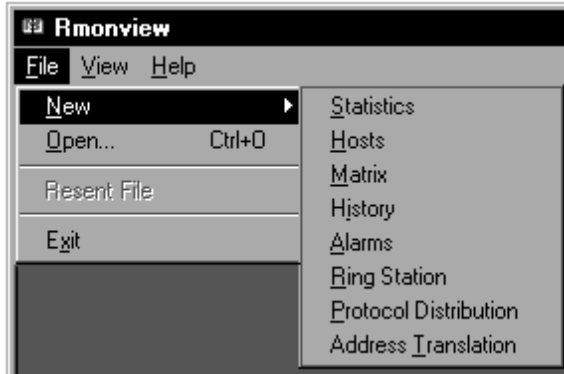


Figure 46. Opening an Application in Rmonview

1. Select **New** from the File menu.
2. Select the appropriate application. The application View dialog or Sample Point Selection dialog will open, from which you can configure the application.

Viewman

To open an RMON application from within Viewman either:

- Use the toolbar button (if one exists for the application you want for example, Statistics, Hosts, Matrix, History, Alarms, and Ring Station applications have buttons).

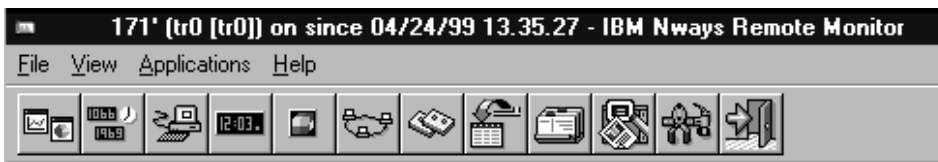
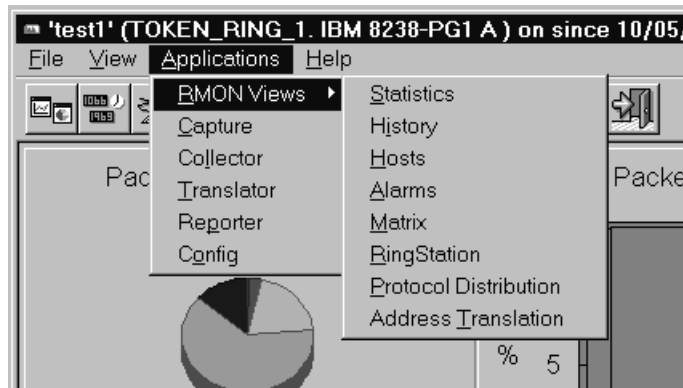


Figure 47. Viewman Menu Bar and Toolbar

- Select *RMON Views* from the Applications menu. Then select the appropriate application.



When Statistics, Hosts, Matrix, History, Alarms, or Ring Station applications are selected, the application View dialog will open.

When Protocol Distribution or Address Translation application is selected, the device displayed in Viewman is automatically selected as the sample point.

Note: This preselection of the sample point applies only when starting RMON2 (ECAM) applications from Viewman. Rmonview presents the Sample Point Selection dialog to select a device interface.

Configuring RMON Applications

This section contains the procedures for creating and editing views.

The statistics history, host, matrix, and token-ring view applications allow you to select from a number of predefined views, or to create your own views from a list of variables. The process for creating and editing views is the same for these applications and is described below.

Creating and Editing Views

To create a new view or edit an existing one:

1. Launch the appropriate application as described in “Launching RMON Applications” on page 77.

The View dialog for that application will open. A complete description of each application view follows this section.

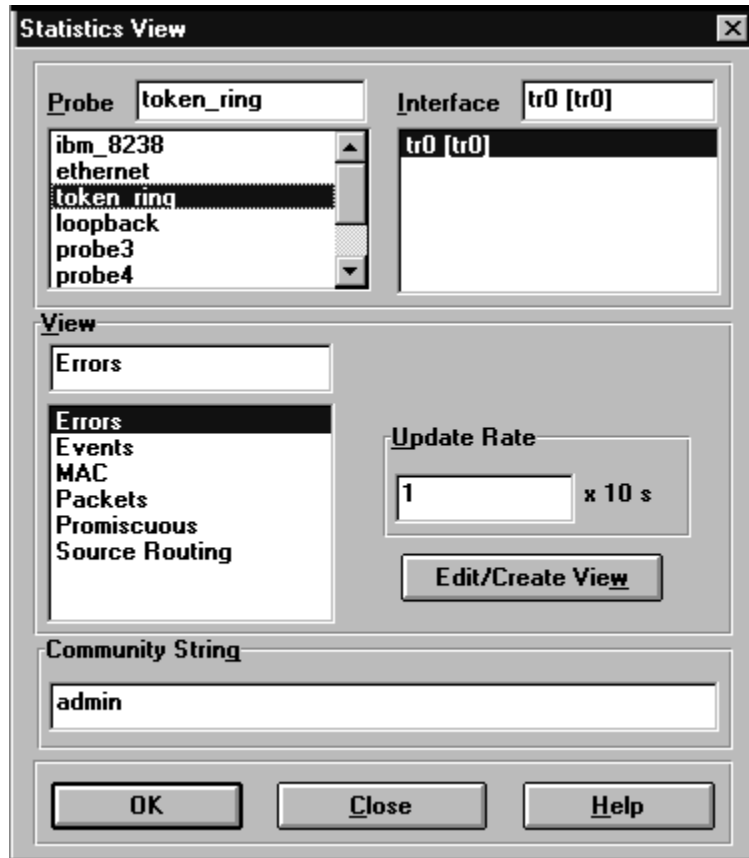


Figure 48. Application View Dialog

2. Select a probe and an interface.
3. Select a view in the View list. The list will vary according to the application and the media type of the selected interface.
4. Click **Edit/Create View** to open the Edit User View dialog.

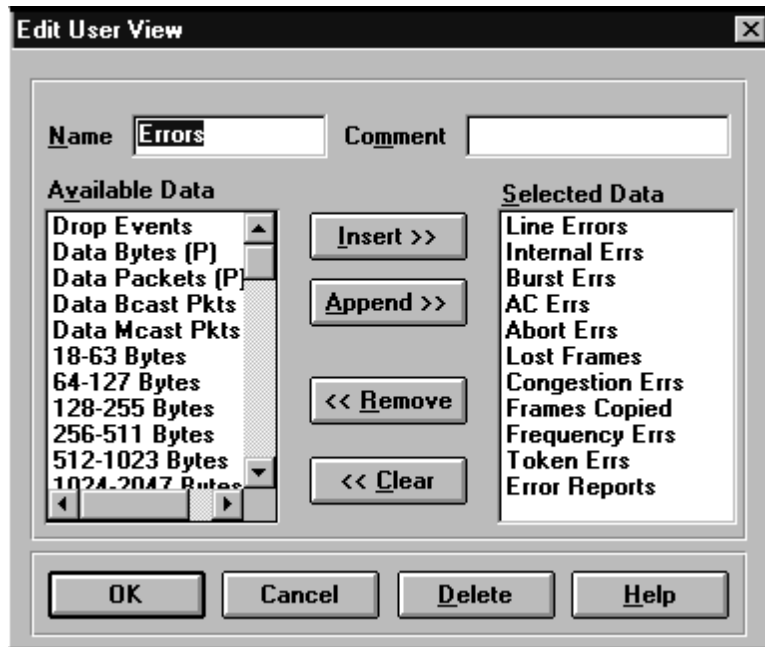


Figure 49. Edit User View Dialog

5. If required, change the existing name in the *Name* field. An additional comment can also be entered in the *Comment* field.
6. If required, click **<<Clear** to clear the existing set of variables from the Selected Data list.
7. Click a variable in the *Available Data* list to select or deselect it. The list of variables will vary according to the media type of the interface selected in the application View dialog.
8. Click **Insert>>** or **Append>>** to add these selections to the Selected Data list. This defines the order in which categories are displayed on screen.
 - a. *Insert>>* adds a new entry to the beginning of the list or before a selected entry in the list.
 - b. *Append>>* adds it to the end of the list or after a selected entry.
9. Click **OK** to save this view and return to the application View dialog.

Statistics View

All the time a probe is connected to a remote segment of your network-and is switched on-it is collecting statistics about all activity on that segment. These statistics include well-formed packets and error packets. Nways Remote Monitor graphs statistics as either a rate of change over the specified time interval or the absolute totals for each statistic since the probe was turned on.

To see which of these value types are to be graphed, select *Graphed Values* from the *Options* menu on the *RMON* main dialog.

Statistics are kept on a per-segment rather than a per-station basis. This is useful for taking a higher level view and highlighting spikes of activity on a segment.

Configuring Statistics View

1. Launch the Statistics View dialog as described in “Launching RMON Applications” on page 77.

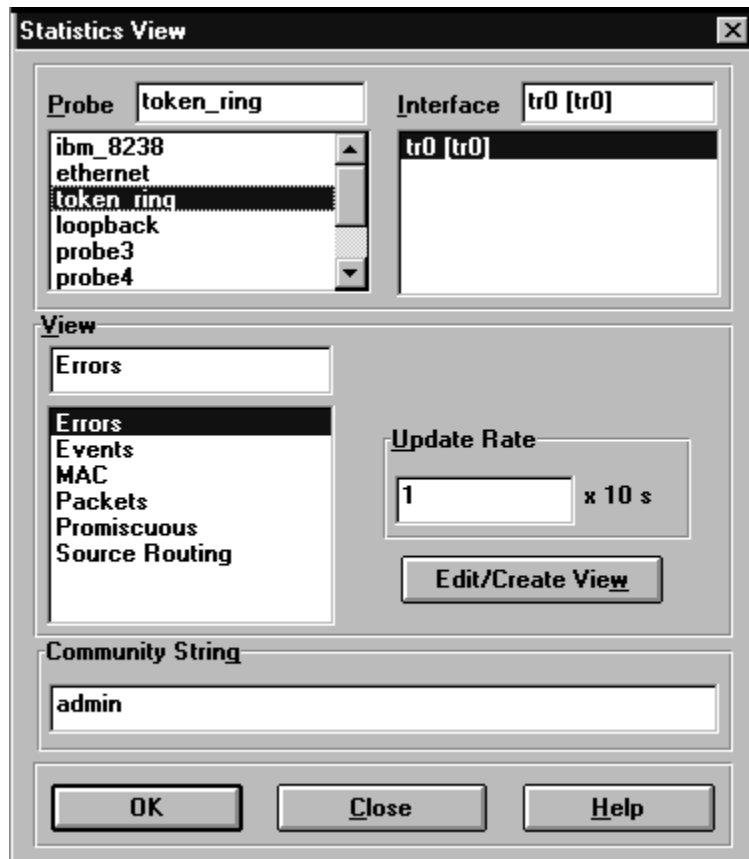


Figure 50. Application View Dialog

2. In the Probe list, click the probe whose statistics you want to analyze. If the probe is accessible, a list of interfaces on the probe will appear in the Interface list.
3. Click the name of an interface in the Interface list to access data on one of the LAN segments being monitored by the probe.
4. In the View area, choose one of the predefined views or one of your own customized views.

- a. The list of predefined views will change according to the media type of the selected interface. Table 14 describes the Statistics views available for Ethernet and FDDI.

Table 14. Predefined Statistics Views

View	Media Type	Description	Ethernet	FDDI
All	■	■		Contains all variables relevant to media type.
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.
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.
Source Routing			■	Ring number, frames in, out, and through, octets in, out, and through, all route and single-route broadcasts and octets, local LLC frames and hop frames.

- b. To create your own view, see “Creating and Editing Views” on page 79.

As an example, you could have a recurrent problem with short packets being generated on an Ethernet segment by file servers on the factory floor. Rather than set up the same view every time you want to examine this particular set of statistics, you can create a view. In the *View Name* field, enter the name: short stats. Then select the Short+CRC and Too Short variables. Finally, click **OK** to create and select this new view.

5. Enter an update rate in tens of seconds in the *Update Rate* field. This determines how often the display is refreshed with new data. If you type 1, this means 10 seconds, 2 means 20 seconds, and so on.
6. In the Community String area, Nways Remote Monitor displays the community string associated with the selected probe. This is described in detail in “Access Control Tables” on page 32.

7. Click **OK** to start the Statistics application.

History View

The History application complements the Statistics application. Using the History application, you can take a wider view of statistics to spot trends over hours, days, weeks, or even months. By specifying a sample period such as once every 30 seconds or once an hour, you can view network activity over longer periods.

If you spot an unusual spike or dip in network activity in the History display, simply click that part of the line graph to find out when that event occurred.

Configuring History View

1. Launch the History View dialog as described in “Launching RMON Applications” on page 77.

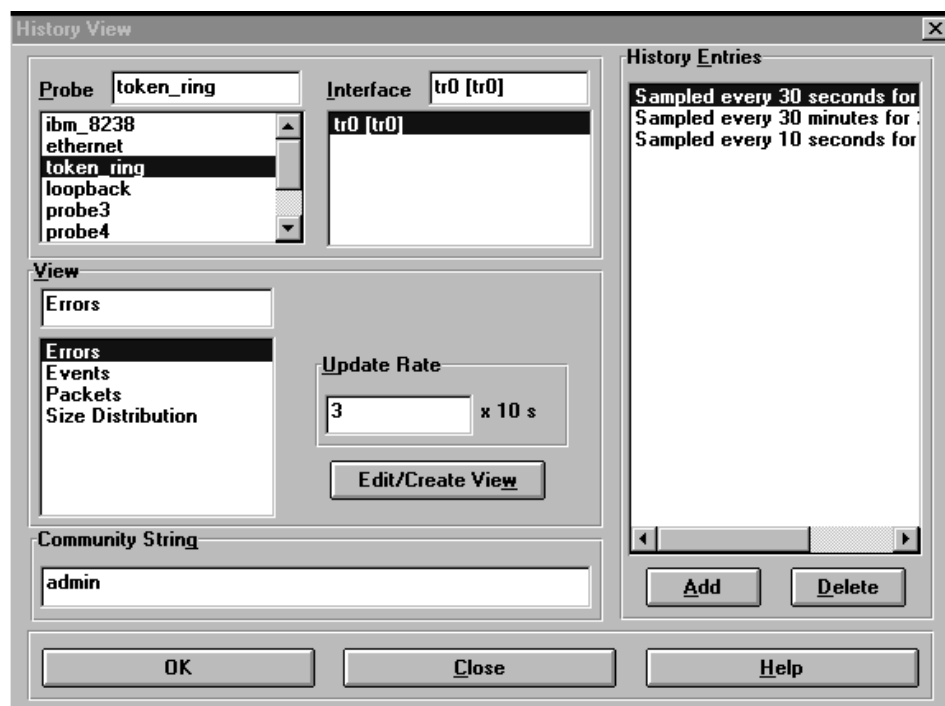


Figure 51. History View Dialog

2. In the *Probe* list, point and click the probe whose historical statistics you want to analyze. If the probe is accessible, a list of interfaces on the probe will appear in the *Interface* list.
3. Click the name of an interface in the *Interface* list to access data on one of the LAN segments being monitored by the probe.

4. In the *View* area, choose one of the predefined views or one of your own customized views.
 - a. The list of predefined views will change according to the media type of the selected interface. Table 15 describes the History views available for Ethernet and FDDI.

Table 15. Predefined History Views

View	Media Type	Description	Ethernet	FDDI
All	■	■		Contains all variables relevant to media type.
Bytes	■	■		The number of bytes making up these packets (in other words, the total number of bytes of traffic on that segment).
Errors	■	■	■	The number of errors detected on the segment.
Events			■	Purge events, beacon events, claim token events, and ring polls.
Load	■	■		The percentage network utilization at the time of this sample period.
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.
Size Distribution		■	■	Packets classified into specific size categories.

- b. To create your own view, see "Creating and Editing Views" on page 79.
5. In the *Update Rate* area, specify how often to update the displays. This determines how often the display is refreshed with new data. The default is set to the selected history sample interval.
6. Select the sample period you want from the *History Entries* list by pointing and clicking on it.
7. Click **Add** to create a new sample period, if the sample period you want does not already appear in the *History Entries* list. The History Entry Creation dialog will open.

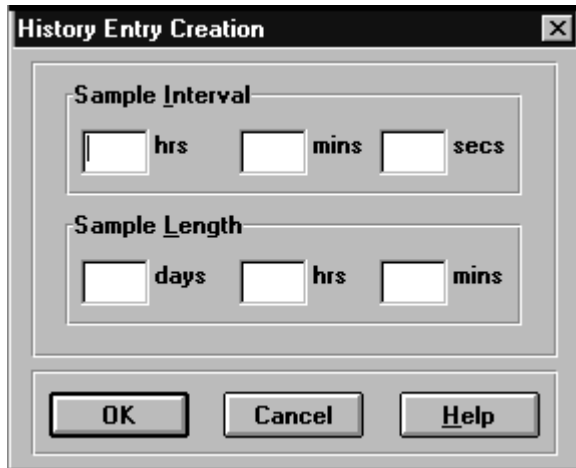


Figure 52. History Entry Creation Dialog

- a. In the *Sample Interval* fields, specify how often you would like to sample statistics on the segment.
If you select once an hour, every point on the graph reflects events at an hourly interval. So for any two contiguous events on the graph there is in fact a one-hour delay between them.
- b. In the *Sample Length* fields, specify the duration of the sample period.
- c. Click **OK** to create this new entry.

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

8. In the *Community String* area, Nways Remote Monitor displays the community string associated with the selected probe. This is described in detail in “Access Control Tables” on page 32.
9. Click **OK** to start the History application.

Host View

In network management and troubleshooting, much of a manager’s time can be taken up trying to determine the relationship between events. 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 application 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 Top N RMON groups.

Depending on your line of investigation, results can be sorted in different ways to help highlight the salient information:

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

If PACMIB has been enabled on the selected probe, you can also gather port and slot statistics. See “Enabling and Disabling PACMIB” on page 38.

Configuring Host View

1. Launch the Host View dialog as described in “Launching RMON Applications” on page 77.

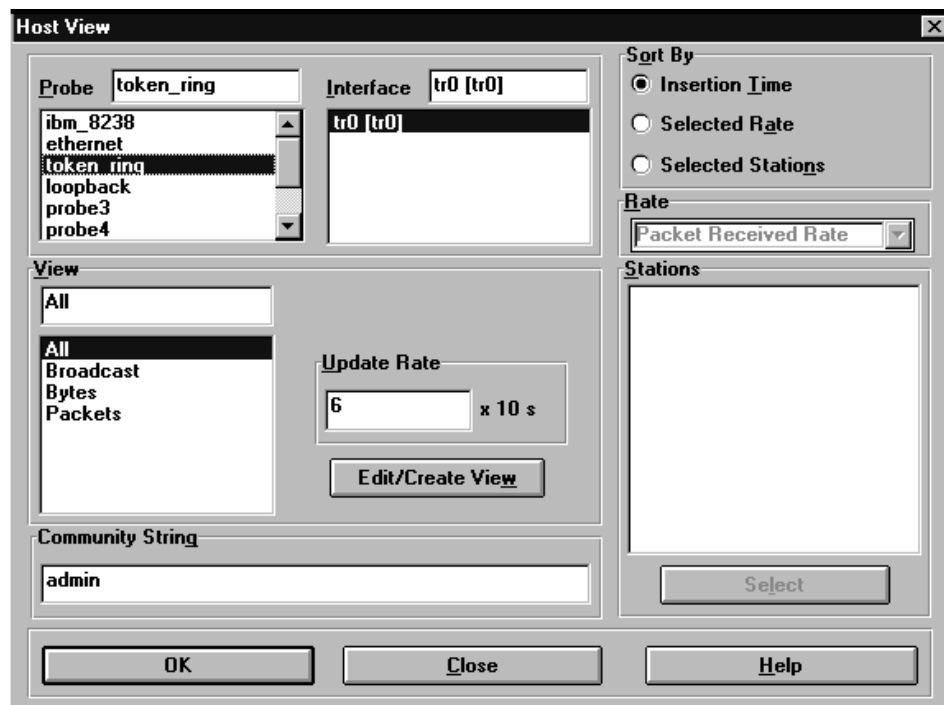


Figure 53. Host View Dialog

2. In the *Probe* list, point and click the probe whose statistics you want to analyze. If the probe is accessible, a list of interfaces on the probe will appear in the *Interface* list.
3. Click the name of an interface in the *Interface* list to access data on one of the LAN segments being monitored by the probe.
4. In the *View* area, choose one of the predefined views or one of your own customized views.

- a. The list of predefined views will change according to the media type of the selected interface. Table 16 describes the Host views available for Ethernet and FDDI.

Table 16. Predefined Host Views

View	Media Type	Description	Ethernet	FDDI
All	■	■	■	Contains all variables relevant to media type.
Broadcast			■	The number of broadcasts seen.
Bytes	■	■	■	The number of bytes making up these packets (in other words, the total number of bytes of traffic on that segment).
Errors	■	■		The number of errors detected on the segment.
Load	■	■		The percentage network utilization at the time of this sample period.
Packets	■	■	■	The total number of packets detected-including error packets-on the network segment.
Rate	■	■		The number of broadcasts and multicasts seen.

- b. To create your own view, see “Creating and Editing Views” on page 79.
- 5. In the *Update Rate* area, specify how often to update the displays. This determines how often the display is refreshed with new data.
- 6. Depending on your line of investigation-in other words, the theory you are trying to test out-you can choose to sort the host entries in a number of different ways:
 - a. To view them over time, point and click **Insertion Time**. This reflects the order in which the probe sees the stations on the network.
 - b. To view them by a selected rate, click **Selected Rate**—the *Packet Received Rate* list becomes active. This is in fact a default value only. Click the pull-down menu to select from: packet received rate, packet sent rate, bytes received rate, bytes sent rate, error packet rate, broadcast packet rate, and multicast packet rate.
 - c. To list by station, click **Selected Stations**. 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 on **Select** to open the Station Select dialog.

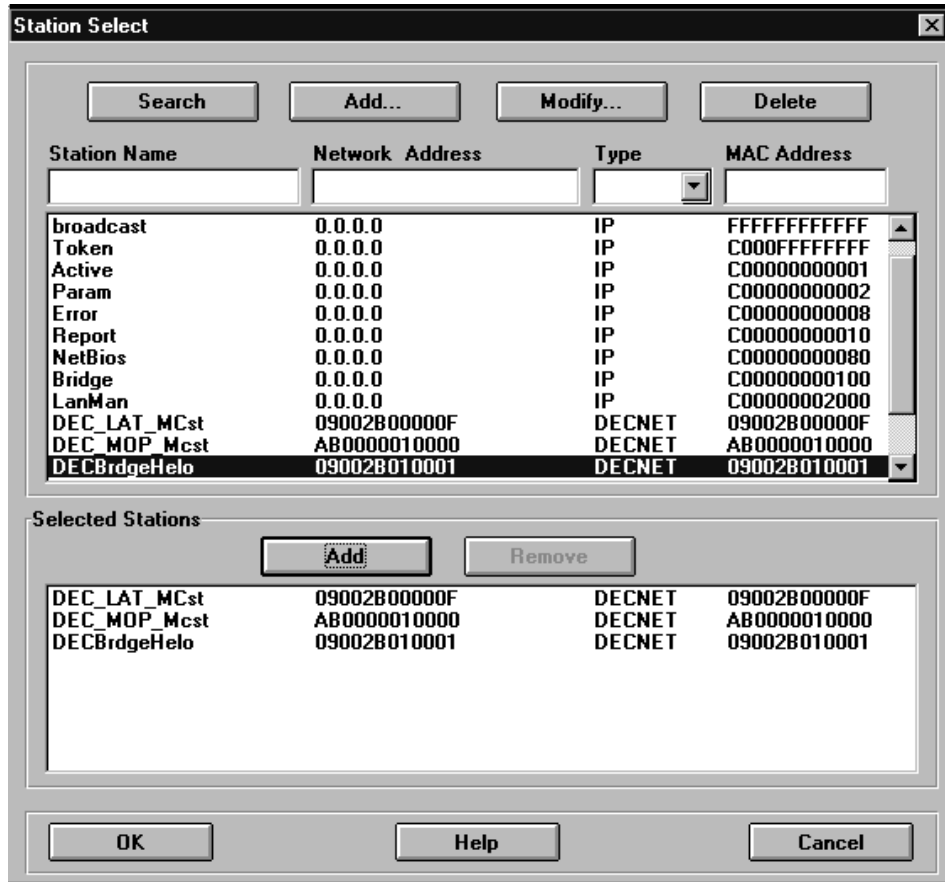


Figure 54. Station Select Dialog

The first part of the dialog operates in the same way as the Station List Editor. The search function defines the list of stations that will be displayed. You can also add, modify, and delete station entries. These functions are described in “Manual Setup of Stations” on page 60.

The second part of the dialog lets you select stations for inclusion in the Host View.

- Select single or multiple stations from the station list. Then click **Add...** and the stations will appear in the *Select Stations* list.
 - To remove stations from the *Select Stations* list, select single or multiple stations and then click **Delete**.
 - Click **OK** to return to the Host View dialog.
7. In the *Community String* area, Nways Remote Monitor displays the community string associated with the selected probe. This is described in detail in “Access Control Tables” on page 32.

8. Click **OK** to start the Host Table display.

Matrix View

As network managers start getting to the root of a particular problem, their investigations often lead to the requirement for a station-by-station analysis.

Using the Matrix application you can find out:

- Who is talking to whom on the network
- How much traffic is flowing between two stations
- What kind of traffic is flowing between them-whether good or bad

Typically, you would use this application to single out stations that might be responsible for generating problems on a given segment.

To analyze changing trends across stations on a Token Ring, use the Ring Station application.

Configuring Matrix View

1. Launch the Matrix View dialog as described in “Launching RMON Applications” on page 77.

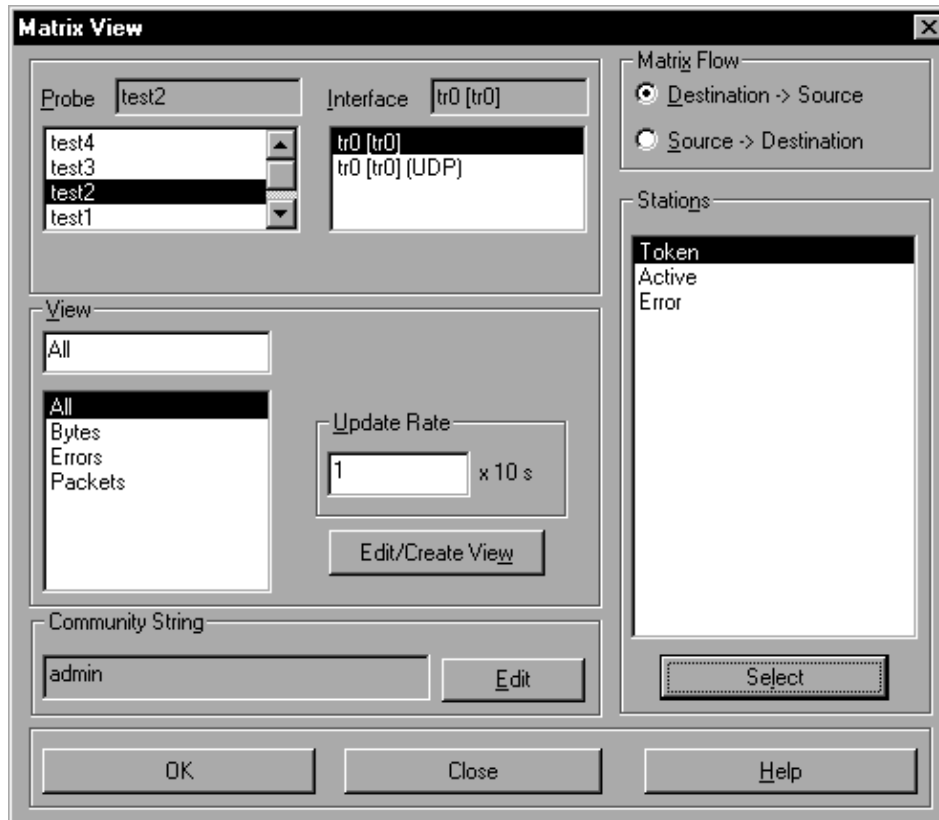


Figure 55. Matrix View

2. In the *Probe* list, click the probe whose statistics you want to analyze. If the probe is accessible, a list of interfaces on the probe will appear in the *Interface* list.
3. Click the name of an interface in the *Interface* list to access data on one of the LAN segments being monitored by the probe.
4. In the *View* area, choose one of the predefined views or one of your own customized views.
 - a. The list of predefined views will change according to the media type of the selected interface. Table 17 describes the Matrix views available for Ethernet and FDDI.

Table 17. Predefined Matrix Views

View	Media Type	Description	Ethernet	FDDI
All	■	■	■	All variables relevant to media type.
Bytes	■	■	■	The number of bytes making up these packets (that is, the total number of bytes of traffic on that segment).

Table 17. Predefined Matrix Views (continued)

View	Media Type	Description	Ethernet	FDDI
Errors	■	■	■	The number of errors detected on the segment.
Packets	■	■	■	The total number of packets detected-including error packets-on the network segment.

- b. To create your own view, see “Creating and Editing Views” on page 79.
5. In the *Update Rate* area, specify how often to update the displays. This determines how often the display is refreshed with new data.
6. In the *Stations* list, point and click the stations you want to focus on.
You can edit the stations that appear in the list by clicking on **Select** to open the Station Select dialog. This dialog is described in detail in “Host View” on page 86.
7. In the *Community String* area, Nways Remote Monitor displays the community string associated with the selected probe. This is described in detail in “Access Control Tables” on page 32.
8. Click **OK** to start the Matrix display.

Token Ring View

To manage a token ring effectively, a network manager has to be able to analyze the subtle relationships between seemingly separate events on the ring. Specific events on your own Token Ring can result in specific-and eventually recognizable-patterns of behavior among stations.

As a simple illustration, every time a station inserts onto the ring this causes a disruption. This in turn results in a ring purge event, and a new token is issued by the active monitor. You can use the Ring Station application to track who is doing this and find out who the active monitor issuing the new token is.

Using the Ring Station application you can:

- Learn to spot patterns on your own token ring
- Home in on isolating errors and non-isolating errors
- See who is currently active on the ring

Configuring Ring Station View

1. Launch the Ring Station View dialog as described in “Launching RMON Applications” on page 77.

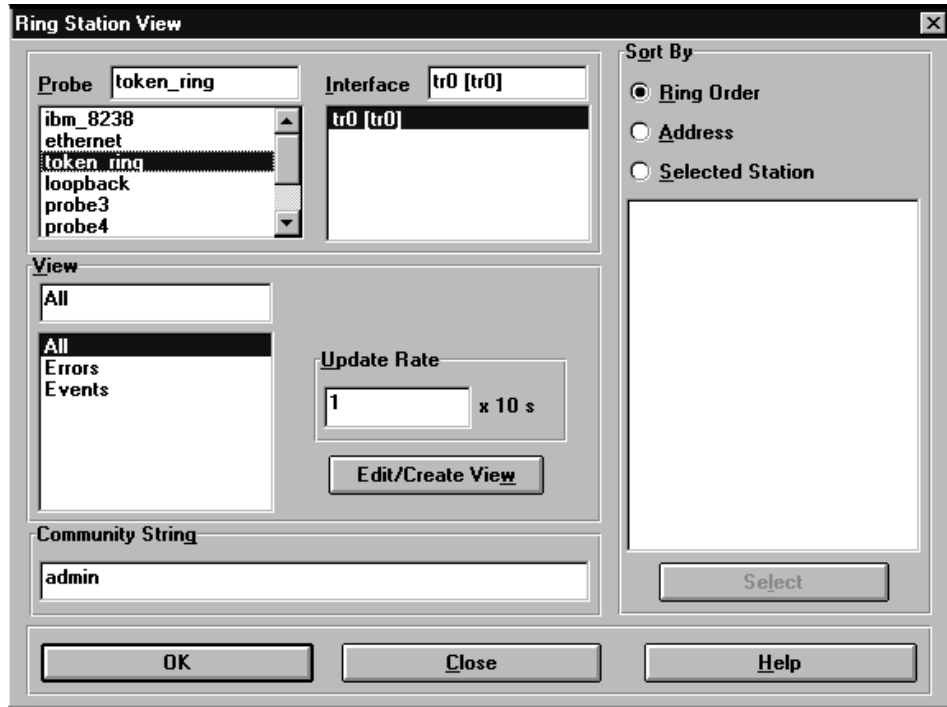


Figure 56. Ring Station View Dialog

2. In the *Probe* list, click a token-ring probe or a probe that supports a token-ring interface. If the probe is accessible, a list of interfaces on the probe will appear in the *Interface* list.
3. Click the name of an interface in the *Interface* list to access data on one of the LAN segments being monitored by the probe.
4. In the *View* area, choose one of the predefined views or one of your own customized views.
 - a. Table 18 describes the Ring Station views available.

Table 18. Predefined Ring Station Views

View	Description
All	Contains all variables.
Errors	The number of errors detected on the segment.
Events	Includes last NAUN, station status, last entered, and last exited.

- b. To create your own view, see “Creating and Editing Views” on page 79.
5. In the *Update Rate* area, specify how often to update the displays. This determines how often the table is refreshed with new data.
6. Depending on your line of inquiry, you can sort the ring station entries in a number of different ways.

- To view all stations by ring order, click *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.
- To view them by address, point and click **Address**.
- To sort by station name, click **Selected Station**. The *Select* button becomes active.

If a station you want does not already appear in this list, click on **Select** to open the Station Select dialog. This dialog is described in “Host View” on page 86.

7. In the *Community String* area, Nways Remote Monitor displays the community string associated with the selected probe. This is described in detail in “Access Control Tables” on page 32.
8. Click **OK** to start the Ring Station display.

Alarms View

Because so much of network management involves monitoring for specific events on a network, Nways Remote Monitor lets you specify these events in advance and then lets you know as soon as they occur. These events are called *alarms*.

Consider the following examples:

- The router on your network is capable of forwarding at 3000 packets per second (pps). Because 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 (Cyclic Redundancy Check) rate of more than 1% of network traffic is considered excessive, so 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 (see “Chapter 7. Packet Capture and Decode” on page 103). Taking the 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. Combining Alarms and Capture in this way lets you devise powerful management and troubleshooting applications.

Configuring Alarms View

1. Launch the Alarms View dialog as described in “Launching RMON Applications” on page 77.

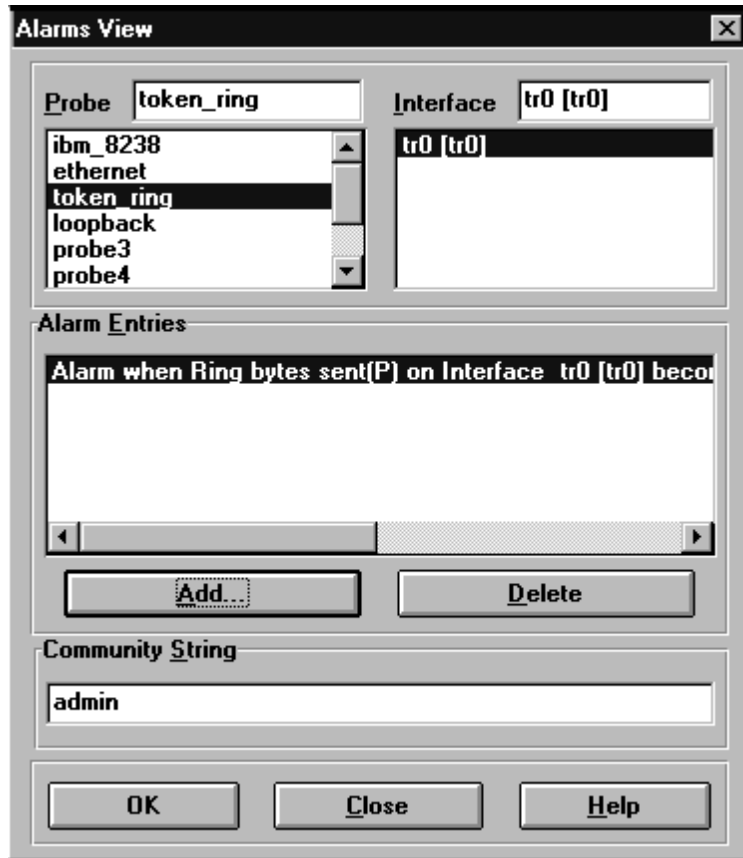


Figure 57. Alarms View Dialog

2. In the *Probe* list, click the probe whose statistics you want to analyze. If the probe is accessible, a list of interfaces on the probe will appear in the *Interface* list.
3. Click the name of an interface in the *Interface* list to access data on one of the LAN segments being monitored by the probe.
4. If this is the first time you have set alarms on this probe, or if you have deleted old ones, there will be no existing entries in the *Alarm Entries* list.
5. To add a new entry, click **Add...** to open the Alarm Creation dialog.

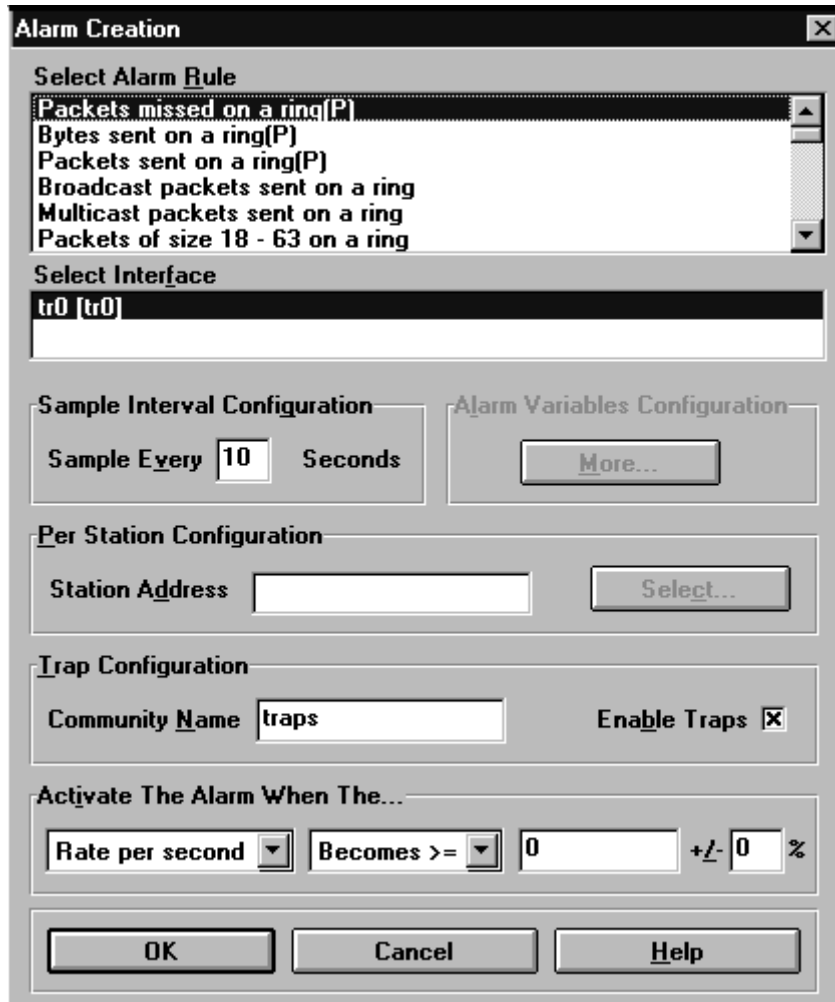


Figure 58. Alarm Creation Dialog

- a. In the *Select Alarm Rule* list, click the type of alarm you would like to set. The list of rules will vary according to the media type of the selected interface.
- b. In the *Sample Interval Configuration* area, specify how often you would like the application to check for this event.
- c. 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 required, click **More...** to open the Alarm Variables dialog and enter values for the variables in the appropriate fields.

- d. If you have selected a station-specific alarm type, the *Select* button will be active. Click this button to open the Station Select dialog. This dialog is described in “Host View” on page 86.
- e. If desired, change the *Trap Configuration Community* name. For more information on Trap Communities, see “Trap Communities” on page 34.
- f. Use the *Activate The Alarm When The...* 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.

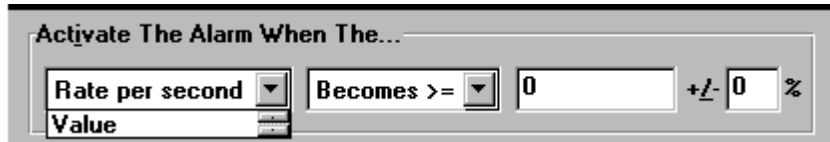


Figure 59. Specifying Alarm Activation

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

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 crosses below or above the set threshold. This will trigger only when the value or rate is crossed, not when the rate or value remains above or below the threshold.

To gain more control over the conditions to be met for the alarm, you can specify a hysteresis zone around the specified value. This gives you more flexibility over the triggering value by specifying a percentage barrier of plus or minus that value.

In Figure 60 on page 98 the horizontal line represents the alarm rate being monitored, and the shaded area represents the specified hysteresis zone.

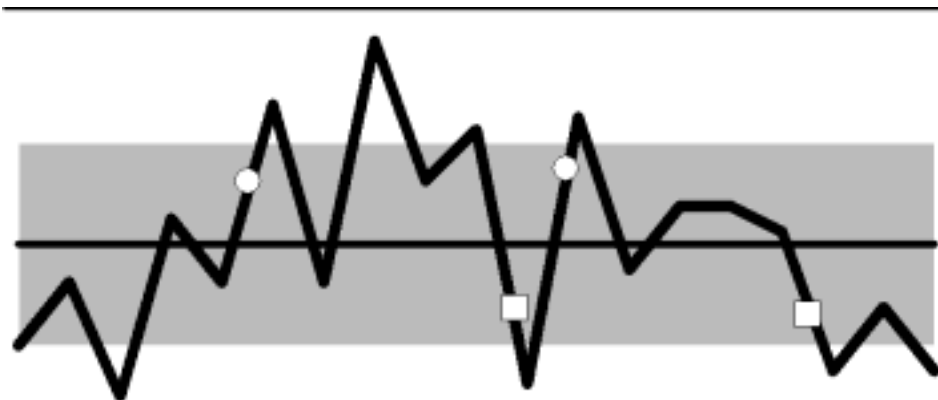


Figure 60. Hysteresis Zone

- 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* \geq , the circles in the diagram show when this event would trigger.
 - For an alarm specified as *Becomes* \leq , the squares in the diagram show when this event would trigger.
 - For an alarm specified as *Crosses*, both the circles and the squares in the diagram show when this event would trigger.
- Click **OK** to save this entry and return to the Alarms View.
6. Click **OK** in the Alarms View dialog to setup this alarm condition.

Address Translation View

The Address Translation application allows the probe to compile a table that maps MAC addresses to network layer addresses.

The probe can also check for any duplicate network layer addresses seen on the network. This could, for example, immediately highlight a networking problem if two devices have the same IP address.

The Address Translation application is displayed in the Rmonview window. You must be using one of the following devices to view this application:

- RMON2-compliant device
- RMON2 device with RMON2 (ECAM) SmartAgent software loaded

Address Translation Table Types

The table display varies slightly depending on whether you are using an RMON2-compliant device or an RMON device with RMON2 (ECAM) SmartAgent software loaded. These differences are outlined in Table 19.

Table 19. Address Translation Display

Display Feature	RMON2 device	SmartAgent software
Change Rate variable	no	yes
Last Changed variable	yes	no
Sorts by Duplicate Menu Option	no	yes

The Change Rate variable indicates which stations have multiple network layer 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.

The Last Changed variable indicates the last time the probe detected a change in the mapping between a network layer address and a MAC address. This value can be used to detect duplicate address problems. If addresses have been duplicated, this value will be updated frequently.

The Duplicate Addresses column lists stations where more than one MAC address has been assigned the same network layer address. This is usually regarded as an error which might arise from someone assigning the same protocol address to two machines. The symptoms can be hard to trace because they can be very unpredictable.

To view duplicate addresses, follow these steps:

- RMON2-compliant devices
Select *Sort By* from the View menu. Select *Last Changed*. The addresses that have changed most recently are likely to be duplicates.
- RMON device with RMON2 (ECAM) SmartAgent software
Select *Sort By* from the View menu. Select *Duplicates*. The duplicate addresses are marked *true*.

Viewing Address Translation Tables

You can launch the Address Translation application from the Viewman main window or from Rmonview.

From the Viewman Main Window

- From the *Applications* menu, select **RMON views...** and then select **Address Translation**. The current device whose interface is being displayed in Viewman is automatically selected as the sample point for the application (see "Launching RMON Applications" on page 77).

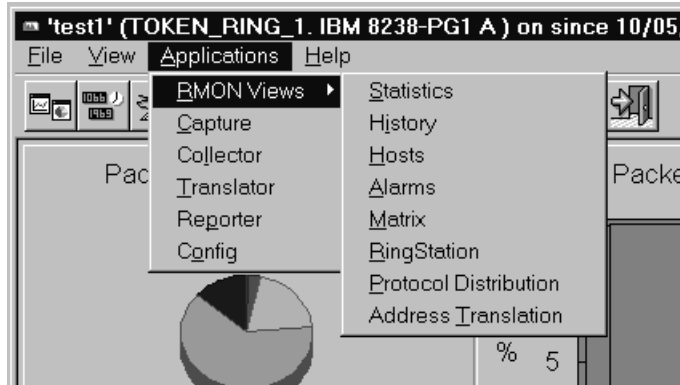


Figure 61. Current Device Shown in Viewman

From Rmonview

- Select **New** from the *File* menu in Rmonview and select **Address Translation**.
- Select a device and an interface on the sample point selection dialog.
- Select **OK** to have the data retrieved from the probe and displayed as a table in the Rmonview application display window. You can view multiple tables at the same time.

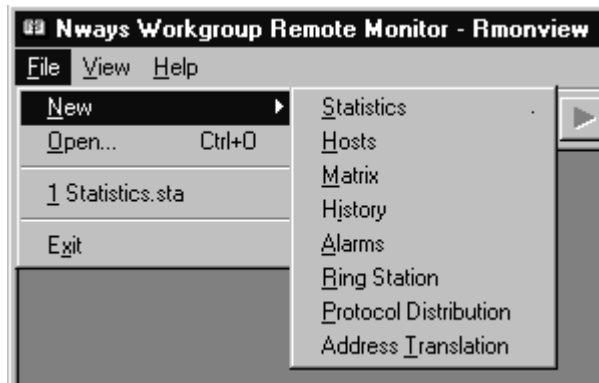


Figure 62. Rmonview Applications Menu

Using the Protocol Distribution Application

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

- Display Protocol Distribution data as a table, bar graph view, or pie chart.

- Export the contents of a Protocol Distribution Table to another application as an HTML table, Excel, or Tabbed Text formatted file.
- Print the contents of a Protocol Distribution graph view to file or direct to a printer.

The Protocol Distribution application is displayed in the Rmonview window. You must have one of the following devices to view this application:

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

Protocol Distribution View Types

The Protocol Distribution display varies slightly depending on whether you are using an RMON2-compliant device or an RMON device with RMON2 (ECAM) SmartAgent software loaded. These differences are outlined in Table 20.

Table 20. Protocol Distribution Display

Display Feature	RMON2 Device	SmartAgent Software
Set number of protocols for display	yes	no
Sort table display by packets/bytes	yes	no
Set Rmonview Update Rate	yes	no
Display different views simultaneously	yes	no

- To set the number of protocols for display (graphical displays only), select **TopN** from the *Edit* menu. The top 10 protocols are displayed by default.
- To sort a table display by packets or bytes, select **Sort by** from the *View* menu and then select the required view type. To view a graphical display in terms of packets or bytes, select **Packets** or **Bytes** from the *View* menu.
- To set the Rmonview Update Rate, select **Update Rate** from the *Edit* menu.
- To display different views simultaneously, select **New** from the *View* menu and then select **Table** or **Graph**.
- To export the data, select **Export** from the *File* menu. The export menu item is active only on the table display.

Viewing Protocol Distribution Tables

You can launch the Protocol Distribution application from the Viewman main window or from Rmonview.

From the Viewman Main Window

- From the *Applications* menu select **Rmon views...** and then select **Protocol Distribution**. The current device whose interface is being displayed in Viewman is automatically selected as the sample point for the application (“Launching RMON Applications” on page 77).

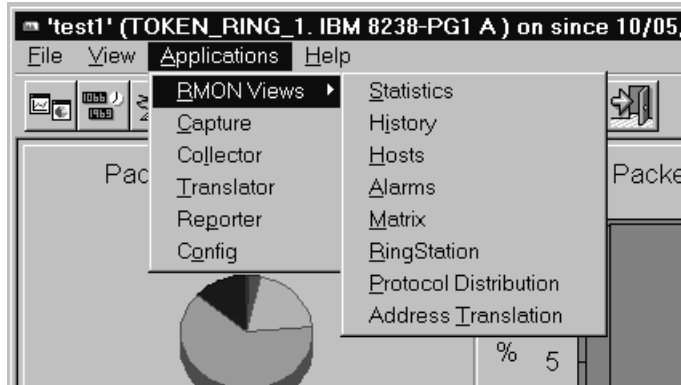


Figure 63. Current Device Shown in Viewman

From Rmonview

- Select **New** from the *File* menu in Rmonview and select **Protocol Distribution**.
- Select a device and an interface on the sample point selection dialog.

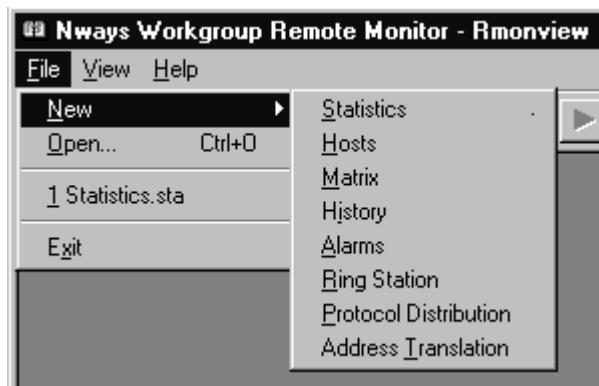


Figure 64. Rmonview Applications Menu

- Select **OK** to have the data retrieved from the probe and displayed as a graph in the Rmonview application display window. You can view multiple tables and graphs at the same time. To change the display to a table and to be able to export the data, select **New** from the *View* menu and then select *Table*.

Chapter 7. Packet Capture and Decode

Based on the principle of *filters*, the Capture application captures packets from the network using predefined patterns and start and stop conditions. The Decode application then 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 along with their transmission times. This is a quick and effective way to focus on delay and retransmit problems.

By saving configuration criteria to a file, you can create a library of commonly used configurations for use on one or more probes.

This chapter describes:

- Launching the Capture application
- Configuring Capture
- Working with buffers
- Creating new start and stop events
- Using the filter editor
- Launching the Decode application
- Reading captured packets
- Conversation trace and analysis
- Saving and loading captured packets

Launching the Capture Application

Capture can be launched from Viewman or independently from the Start Menu.

Viewman

To launch Capture from within Viewman, click



in the toolbar, or select capture on the application menu.



Figure 65. Viewman Menu Bar and Toolbar

Start Menu

From the Start Menu, select the **IBM Nways ReMon** Program Group and then choose **Capture**.

Configuring Capture

Configure the Capture application from the main dialog.

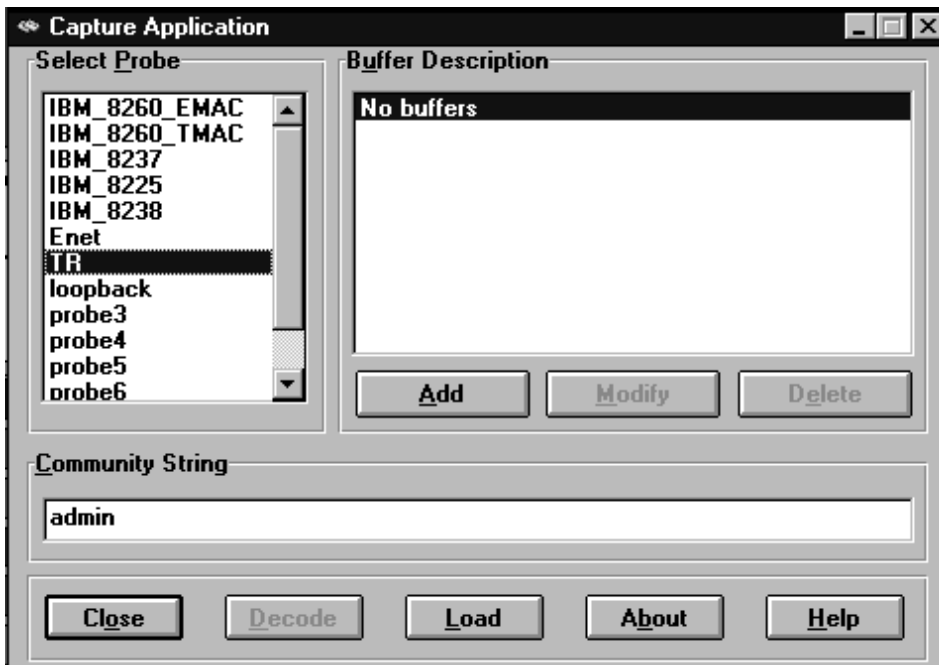


Figure 66. Packet Capture Application Main Dialog

1. Click the probe you want to use to capture packets in the Select Probe list.
2. Create, modify, and save capture buffers or load existing buffers from file. See "Working with Buffers" on page 105 for details.

3. Use the Packet Decode application to display captured packets and carry out trace analysis of packet contents.

Working with Buffers

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

Existing buffers for the selected probe are listed in the *Buffer Description* area of the main dialog. This area allows you to see the names of any predefined capture criteria running on the probe and who owns them.

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 Space** 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*).

The probe has only 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 choose to slice packets or assign maximum sizes to buffers as described in step 7 on page 109.

Creating New Capture Buffers

New capture buffers can be created from the Edit Packet Capture window.

1. Click *Add* in the main dialog to open the Edit Packet Capture window.

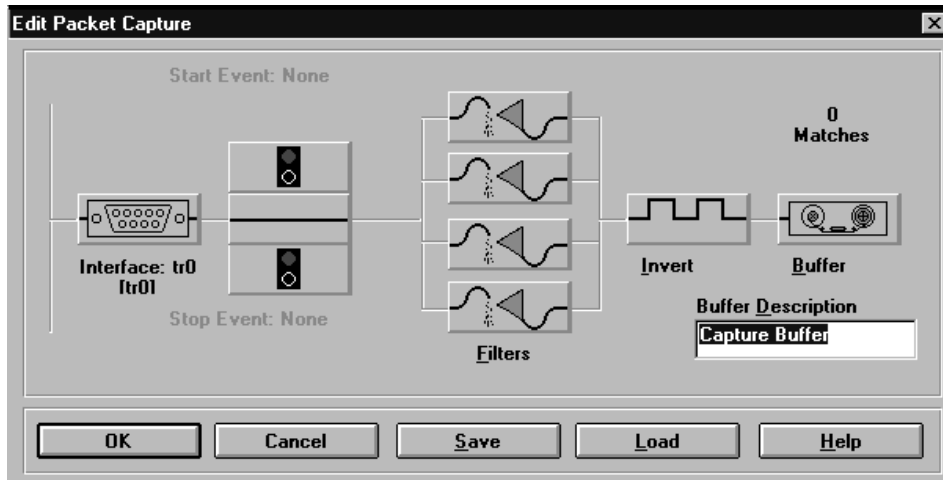


Figure 67. Edit Packet Capture Dialog

2. Click



to open the Configure Interface dialog. Use this dialog to select the interface to be used for packet capture.

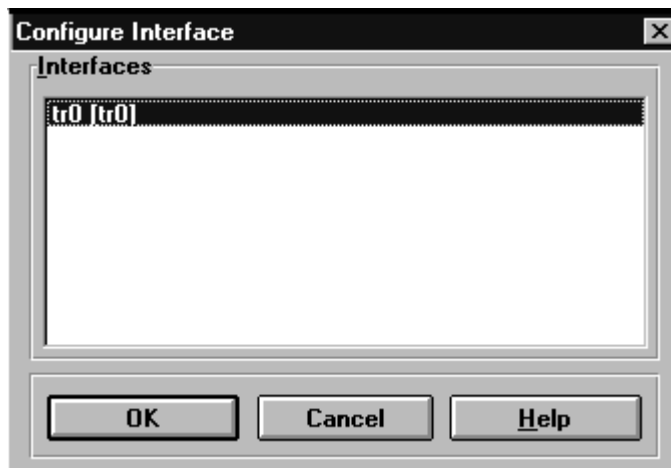


Figure 68. Configure Interface Dialog

- a. Click the interface to be used.
- b. Click **OK** to return to the Edit Packet Capture dialog.

3. You may want to start capturing packets automatically whenever a certain Alarm event occurs (see “Alarms View” on page 94 for more information), or whenever a set of packets matches a particular pattern. This is called the *trigger*.
 - a. Click the *Start Event* icon



to display the list of alarms and events available. The Start Events dialog will appear.

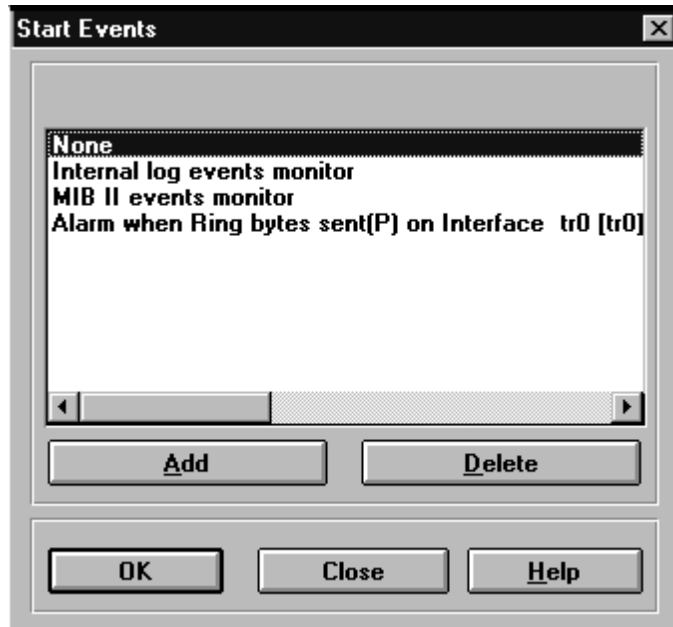
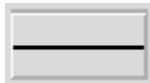


Figure 69. Start Events Dialog

- b. To use an Alarm or an existing event, simply click it to select it, then click **OK**.
- c. To add a new trigger, click **Add** and see “Creating New Start and Stop Events” on page 111.
- d. To make this start event active, click on the



activate switch. The switch changes to show that the start trigger is now active.

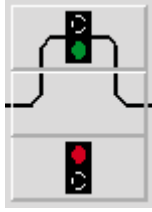


Figure 70. Start Event Active

4. Similarly, you may want to stop capturing packets when a certain condition occurs on your network. This allows you to see what was happening on your network before the event occurred.
 - a. Click the Stop Event icon



to display the list of alarms and events available. The Stop Events dialog will appear.

- b. Follow the instructions given in step 3 on page 107 to select an alarm or event, or to create a new stop event. Then click **OK** to return to the Edit Packet Capture dialog.
 - c. To make only this stop event active, click the



activate switch until only the stop event is active.

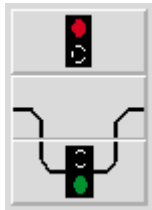
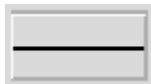


Figure 71. Stop Event Active

- d. To make both the start and stop events active, click the



activate switch until both events are now active.

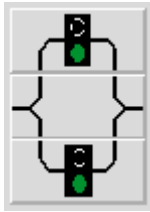


Figure 72. Start and Stop Events Active

- Click one of the





Filter buttons to specify what type of packet you are watching for. See “Using the Filter Editor” on page 113 for details.

- The *Invert* button



lets you invert the logic of the sample. For example, if you are capturing all TCP packets at the moment, simply click the button to start capturing everything except TCP packets.

Table 21. Invert Button

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

- Click



to specify how you would like the buffer to behave when storing packets. The Buffer Control dialog will open.

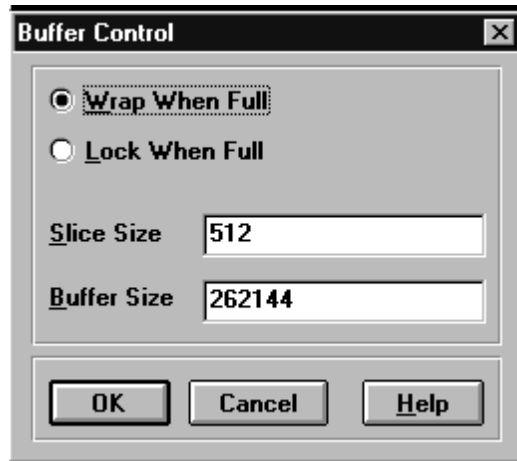


Figure 73. Buffer Control Dialog

Use the fields on the Buffer Control dialog to specify how to store packets on the probe.

- | | |
|--------------------|---|
| Wrap | Means capture packets continuously, throwing away old packets when the buffer is full. |
| Lock | Means stop 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. 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 want the probe to allocate as much memory as is available, set this value to -1 . This will show the buffer as being ON DEMAND in the Buffer Description list. |

8. Click **OK** to return to the Edit Packet Capture dialog.
9. Enter a name for your capture configuration in the Buffer Description field. If you have set it up to capture all TCP/IP packets, for example, you might call it **TCP Buffer**.
10. You can save capture buffers to file and then load them onto any other probe as required. Click **Save** to open the Save As dialog. Enter a file name, then click **Save** to save this capture buffer and return to the Edit Packet Capture dialog.
11. Click **OK** to add this new capture buffer to the Buffer Description list in the Capture main dialog.

Modifying Capture Buffers

You can edit existing capture buffers at any time as your requirements change.

To modify a capture buffer:

1. Click a buffer entry in the *Buffer Description* list to select it.
2. Click **Modify** in the *Buffer Description* area to open the Edit Packet Capture dialog.
3. Follow the same procedures used in “Creating New Capture Buffers” on page 105 to make changes to the existing capture configuration and to save the capture buffer as required.
4. Click **OK** in the Edit Packet Capture dialog to accept your changes.

Loading Capture Buffers from File

If you have previously saved a Capture buffer to file, you can load it onto any probe at a later date. You can also load virtual interface filters (see “Configuring Virtual Interfaces” on page 40). The selected interface on the destination probe must be of the same media type as the original interface on which the buffer or filter was created.

To load a Capture buffer or filter from file:

1. In the Capture main dialog, select a probe in the *Select Probe* list.
2. Click **Add** to open the Edit Packet Capture dialog.
3. Click **Load** and the Open dialog will appear.
4. Select the capture buffer file or the virtual interface filter that is to be loaded, and click **Open**. The selected buffer or filter must be based on the same media type as the selected interface on the destination probe.

*Predefined Virtual interface filters are stored in the *vi_chans* subdirectory, and the different media types are identified by the file extensions: *.eth* for the Ethernet and Fast Ethernet, *.fd* for FDDI, and *.tok* from the token ring.*

5. The selected capture buffer will be loaded and you will be returned to the Edit Packet Capture dialog. Follow the instructions in “Creating New Capture Buffers” on page 105 to change any of the capture buffer settings and to save changes to file.
6. Click **OK** to create this capture buffer on the selected probe and return to the Capture main dialog.

Creating New Start and Stop Events

You may want to start or stop capturing packets whenever a certain condition occurs on your network. Such an event is called the *trigger*.

To create a trigger event:

1. In the Edit Packet Capture dialog, click either the *Start Event*



or *Stop Event*



icons to display the list of Alarms and events available.

2. Click **Add** to bring up the Edit Start Event or Edit Stop Event dialog.

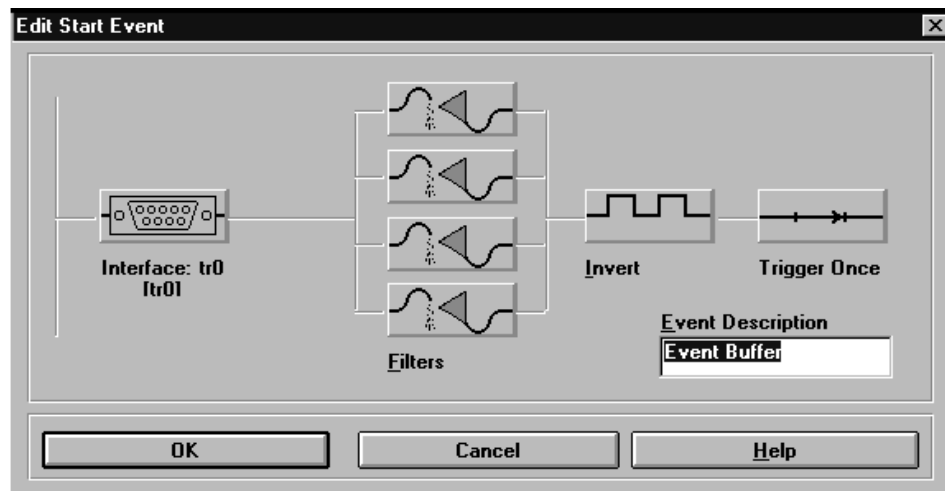


Figure 74. Edit Start Event Dialog

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

3. Click



to open the Configure Interface dialog (Figure 68 on page 106) and specify the interface on the probe 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.

- Click one of the



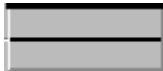
Filter buttons to specify what type of packet you are watching for. This is covered in “Using the Filter Editor” later in this chapter.

- If desired, click



to invert the logic of the original operation. See “Creating New Capture Buffers” on page 105 for details.

- The trigger button



is set to Trigger Once by default. To trigger every time a packet matches this set of criteria, click the button to put it into the Trigger Many



state.

- Enter a unique name for this event in the *Event Description* field.
- Click **OK** to save this new event. It now forms part of your own event library.

Using the Filter Editor

Nways Remote Monitor’s Capture application comes bundled with a number of protocol templates ready for use. Each of these templates is designed to let you rapidly specify the type of packets you want to filter off the network. A wide variety of protocol families are supported. Choose the template appropriate for the kind of packets you are trying to capture.

Using the Filter Editor you can capture-or monitor for-anything from a certain type of packet right down to a specific packet itself. And you can specify up to four filters to run in parallel.

Follow these steps to use the Filter Editor:

1. Click one of the



Filter buttons in the Edit Packet Capture dialog to open the Edit Filter dialog.

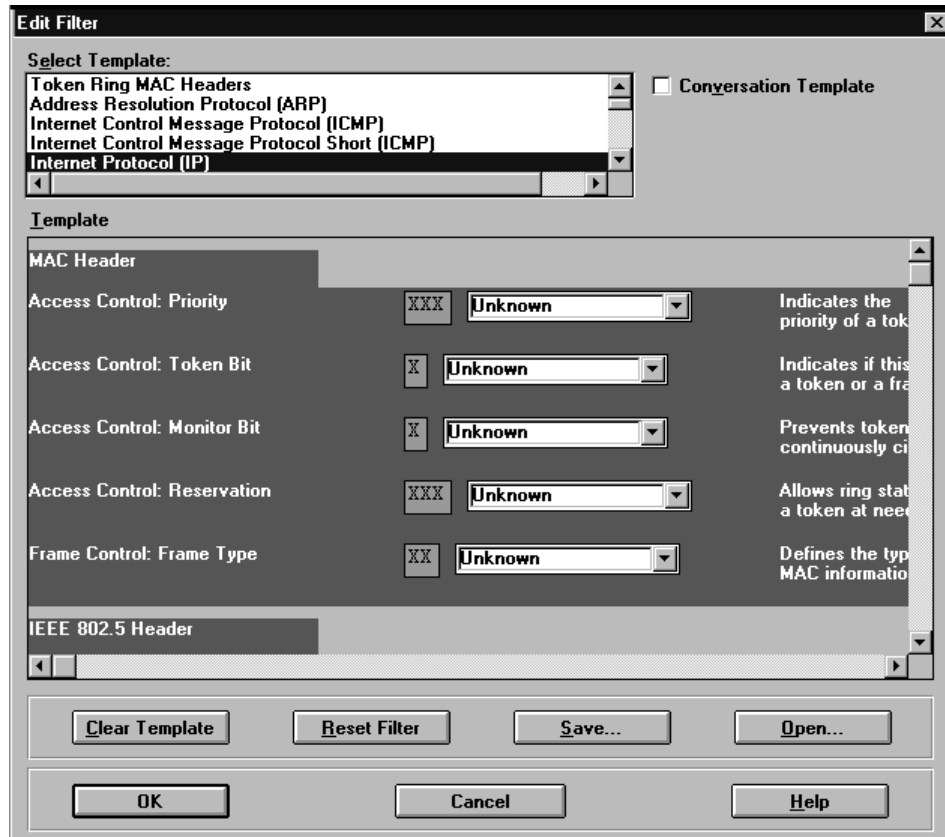


Figure 75. Edit Filter Dialog

The Edit Filter dialog offers a selection of protocol templates from which you can choose. The list of templates available will vary according to the media type of the selected interface.

You must fill in the fields for each of the header types. This ensures that Nways Remote Monitor filters the correct packet type. See “List of Filter Templates” on page 115.

2. Choose the template you would like to use from the *Select Template* list. See “List of Filter Templates” on page 115.

3. The templates provide source and destination fields to capture traffic from one address to another at network and device level. However, with the *Conversation Template* option in the top right corner of the dialog enabled, the application will capture traffic going in *both* directions between the specified points.
When activated, the conversation template will capture traffic going in both directions for any destination and source fields at any point in a template.
4. 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 Station Select dialog. Searching, adding, modifying, and selecting stations in this dialog is described in detail in "Manual Setup of Stations" on page 60. When you have selected a station, click **OK** to return to the Filter Editor.
5. Click the *Any Size* or *Any Packets* pop-ups 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.
6. Complete the rest of the dialog. The fields displayed vary from protocol to protocol and are color-coded. The colors relate to the type of value a field expects—either binary, decimal, or hexadecimal indicated by green, salmon, or purple, respectively. In some cases a field may have a pop-up menu for you to choose from—if so, simply point and click it to choose a value.
When you are filling in a template, 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.
7. Click **OK** to make this filter active.

List of Filter Templates

Table 22 contains a list of available filter templates by interface media type.

Table 22. Filter Templates by Interface Media Type

View	Media Type		
	Ethernet	FDDI	Token Ring
IEEE 802.3	■		
Ethernet LLC	■		
FDDI Header		■	
Token-Ring MAC Headers			■
Address Resolution Protocol (ARP)	■	■	■
Internet Control Message Protocol (ICMP)	■	■	■
Internet Control Message Protocol Short (ICMP)	■	■	■
Internet Protocol (IP)	■	■	■
Internet Protocol Short (IP)	■	■	■
Transport Control Protocol (TCP)	■	■	■

Table 22. Filter Templates by Interface Media Type (continued)

View	Media Type		
	Ethernet	FDDI	Token Ring
Transport Control Protocol Short (TCP)	■	■	■
User Datagram Protocol (UDP)	■	■	■
User Datagram Protocol Short (UDP)	■	■	■
Novell NetWare Internet Packet Exchange (IPX)	■	■	■
Novell NetWare Internet Packet Exchange 802.2 (IPX)	■	■	■
Novell NetWare Internet Packet Exchange SNAP (IPX)	■		
Novell NetWare Sequenced Packet Exchange (SPX)	■	■	■
Novell NetWare Sequenced Packet Exchange 802.2 (SPX)	■	■	■
Novell NetWare Sequenced Packet Exchange SNAP (SPX)	■		
Reverse Address Resolution Protocol (RARP)	■	■	■
Raw Data	■	■	■
Sub-Network Access Protocol (SNAP)	■	■	■
Xerox Routing Information Protocol (RIP)	■	■	■
Xerox Internet Datagram Protocol (IDP)	■	■	■
Xerox Error Protocol	■	■	■
Xerox Sequence Packet Protocol (SPP)	■	■	■
Banyan VINES Internet Protocol (IP)	■	■	■
Banyan VINES Routing Update Protocol (RTP)	■	■	■
Banyan VINES Address Resolution Protocol (ARP)	■	■	■
Banyan VINES Internet Control Protocol (ICP)	■	■	■
Banyan VINES Interprocess Communications Protocol Short (IPC)	■	■	■
Banyan VINES Interprocess Communications Protocol (ICP)	■	■	■
Banyan VINES Sequence Packet Protocol (SPP)	■	■	■
AppleTalk Address Resolution Protocol (AARP)	■	■	■
AppleTalk Short Datagram Delivery Protocol (DDP)	■	■	■
AppleTalk Long Datagram Delivery Protocol (DDP)	■	■	■

Table 22. Filter Templates by Interface Media Type (continued)

View	Media Type		
	Ethernet	FDDI	Token Ring
AppleTalk Transaction Protocol (ATP)	■	■	■
AppleTalk Sessions Protocol (ASP)	■	■	■
AppleTalk Filing Protocol (AFP)	■	■	■
DECnet Local Area Transport (LAT)	■	■	■
DECnet Network Services Protocol (NSP)	■	■	■
DECnet Maintenance Operations Protocol (MOP)	■	■	■
IBM Systems Network Architecture (SNA)	■	■	■
OSI End System to Intermediate System (ESIS)	■	■	■
OSI Intermediate System to Intermediate System (ISIS)	■	■	■
OSI Connectionless-Mode Network Service (CLNS)	■	■	■
OSI Transport Protocol (TP)	■	■	■

Launching the Decode Application

You can either launch the Decode application from the Capture application's main dialog or select the *IBM Nways Remote Monitor Program Group* from the Start menu and then choose **Decode**.

Capture

In the Capture main dialog, you can launch the Decode application either to view a capture buffer on a probe or to view the contents of a saved capture buffer.

Viewing a Capture Buffer on a Probe

1. Click a probe in the *Select Probe* list. A list of capture buffers on the selected probe will appear in the *Buffer Description* list.
2. Click a capture buffer to select it.
3. Click **Decode** to launch the Decode application, where the contents of the selected buffer will be displayed.

Viewing a Saved Capture Buffer

1. Click **Load** to launch the Decode application.
2. The Open dialog will appear automatically. Use this dialog to locate and select the saved capture buffer file that you want to view.
3. Click **Open** to open this file.

Reading Captured Packets

Any number of capture buffers can be displayed within the Packet Decode main window at a time. Figure 76 shows an example of a single capture buffer display.

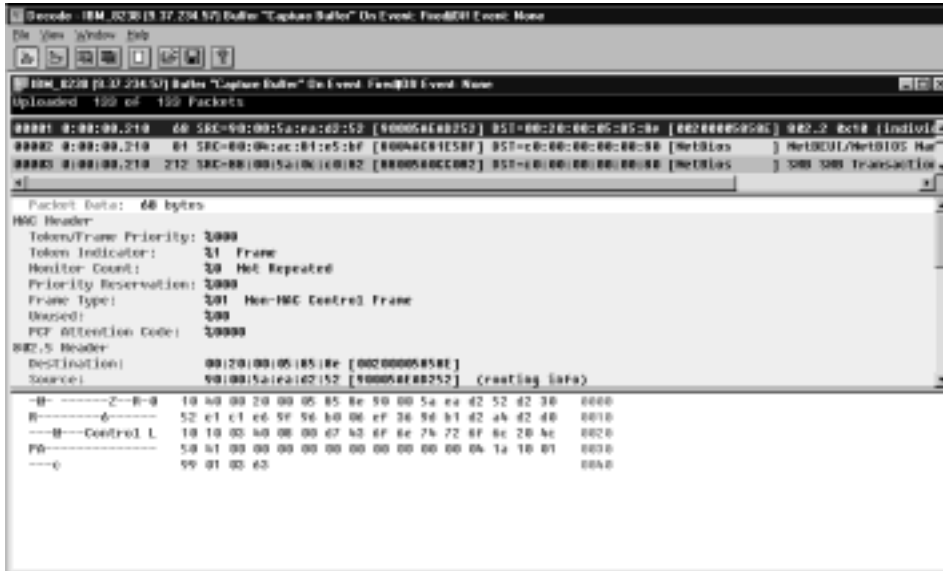


Figure 76. Packet Decode Display

The display is split into three views so that you can see as much information as you need about a given packet.

Use the top view to select the packet you would like to analyze further. Select the packet by clicking on it.

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

Each protocol is color-coded for quick and easy identification. (A complete list of supported decodes is given in "Appendix B. List of Protocol Decodes" on page 157.)

You can resize each of the views to suit your own requirements. Simply click and drag the bar at the bottom of each panel.

Clicking on



will clear the existing display.

Loading Probe Capture Buffer

To capture and upload packets from the capture buffer on a probe for display:

1. If required, click



to clear the existing display.

- 2.



controls the starting and stopping of capturing on the probe.

When you start the capture of packets, Nways Remote Monitor *clears* the existing buffer contents from the probe, resets any capture triggers, and starts capturing a completely fresh set of packets.

- 3.



controls the uploading of packets from the capture buffer on the probe.

When you start the upload of packets, Nways Remote Monitor will start *appending* packets from the capture buffer to the *existing* packets loaded in the Decode display. If you want to empty the display and start uploading a completely new display, click



first to empty the display and then click



The number of packets that have been uploaded and the total number of captured packets in the buffer are shown beneath the toolbar. As the application uploads more and more packets into the display, you will notice the slider bar in the top view shortening to reflect this.

Conversation Trace and Analysis

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

1. Click a packet in the top view in the Packet Decode display to select it.
2. Click either



for MAC Conversation Trace or



(highlighted in green) for IP Conversation Trace. The Trace functions allow you to view a time-stamped trace of the conversation, based on either the MAC addresses of the hosts in the selected packet or their IP addresses.

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 Remote Monitor then uses the packet selected in the Packet Decode view as the key to the conversation you want to watch. The packets involved in that conversation are filtered out and displayed in a conversation view.

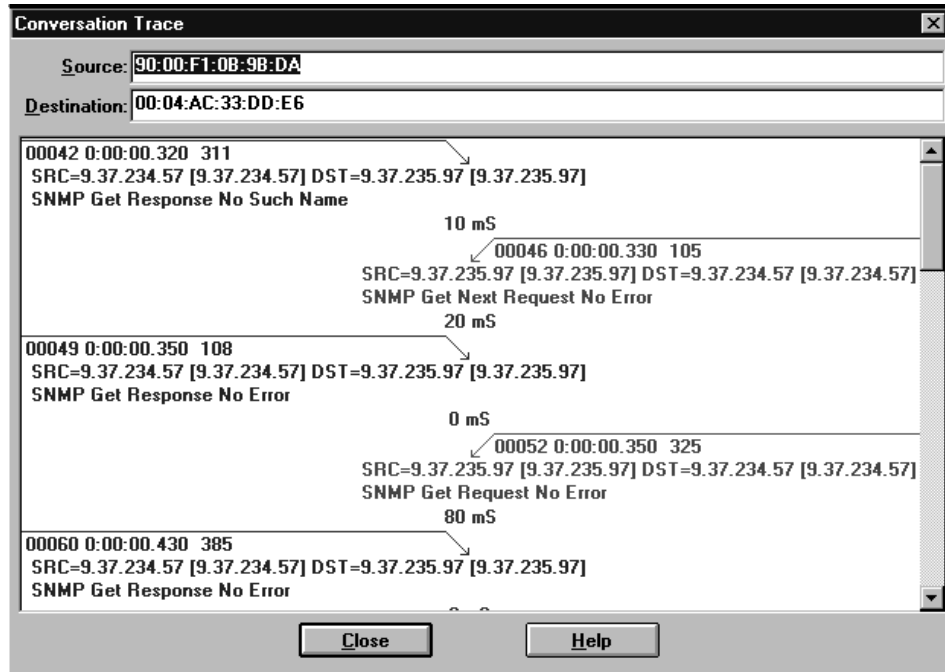


Figure 77. IP Conversation Trace View

This display highlights the relationship between packets in the conversation selected. It allows you to see the overall shape of the conversation.

Interesting points to look for are packets being sent by one side repeatedly before the other responds. This can point to congestion problems.

You can also easily see long delays where no packets are being sent. This may mean that one side is waiting for a response from the other that might have been lost.

Saving and Loading Captured Packets

The following sections describe saving and loading packet samples.

Saving Packets

Follow these instructions to save a packet sample:

1. To save the uploaded packets to file, click



to open the Save As dialog.

2. Specify a file name and location.
3. Choose the file format in which you want to save the packets (Table 23).

Table 23. Packet Decode File Formats

Format	For use with
IBM file (*.3co)	For use with the Packet Decode application.
Sniffer file (*.snf)	Network General Sniffer
Sniffer file (*.enc)	Network General Sniffer
Sniffer file (*.trc)	Network General Sniffer
DA30 Capture file (*.d30)	Wandel & Goltermann DA-30 Analyzer.
ASCII (*.asc)	Any text editor or printer.

4. Click **Save**.

Loading Packets

Follow these steps to load a saved packet sample. You can load Packet Decode application files in *IBM* format or files created with the Network General Sniffer or Wandel & Goltermann DA-30 Analyzer.

1. To load a saved packet sample, click



and the Open dialog will appear.

2. Locate and select the capture buffer file that is to be displayed.
3. Click **Open**.

Chapter 8. Collector

The Collector enables you to gather RMON History, Host, and Matrix data about the devices on your network and store that data in files, for the purpose of developing reports on this network activity.

You can specify exactly which probes and interfaces should be polled, choose which data should be logged, and then set when and how often the collection should take place. This set of information is called a *configuration*. Multiple configurations are supported. The collected data is stored in comma separated variables (CSV) format files to be imported into a database for use in reporting.

The Collector gathers History data from those RMON probes that have a History view configured. If there are no History views configured for a probe, no History data can be collected for that probe.

History views are configured in the History application, accessed from the Nways Remote Monitor main window.

In the Collector you set:

- Which interfaces on which probes to collect data from
- What data to collect
- How often to collect data
- At what time to collect data

The data is saved for import into the Reporter database.

This chapter discusses setting up data collections to gather RMON History, Host, and Matrix data from the devices on your network.

The steps involved in collecting data are:

- Launching the Collector
- Configuring data sources
- Setting the address translation level
- Setting up data collections
- Starting data collection
- Exiting the collector

Launching the Collector Application

Collector can be launched from Viewman or independently from the Start Menu.

Viewman

To open Collector from within Viewman, click



in the toolbar, or select capture on the application menu.



Figure 78. Viewman Menu Bar and Toolbar

Start Menu

Select the *IBM Nways ReMon* Program Group from the Start menu and then choose *Capture*.

The Collector main window will be displayed.



Figure 79. Collector Main Window

Configuring Data Sources

The first time the Collector is run, the PROBE.MAP file is used to generate a list of RMON-compliant devices on the network. The list consists of the device name and the name and physical number of each interface on that device. If required, you can add network devices from within the Collector.

From the Collector main window:

1. Choose *RMON Devices* from the *Config* menu to open the Device Configuration dialog (see "Launching the Device Configuration Dialog" on page 21).
The RMON devices that have been configured in Nways Remote Monitor are displayed in the *Select Probe* list.
2. See "Chapter 3. Setting Up Probes" on page 21 for further information on configuring RMON devices.

Setting the Address Translation Level

The level of address translation that is set will determine what device address information is displayed in the host tables and in reports generated in Reporter.

By default, the Collector attempts to discover the highest address translation level available to it. If you have previously run the Translator application (see Chapter 3. Setting Up Probes), the Collector will also be able to translate device addresses into network addresses or even station names.

When you select a translation level, the Collector will attempt to discover an address at that level first, then at each of the remaining levels in turn. For example, if you chose *Vendor ID*, the Collector would search for that level first and, if unsuccessful, would then search for the *MAC address*. It would not search for the *Name Translation* or *Protocol Address*.

This may lead to a mixture of names, vendor IDs, protocol addresses, and MAC addresses for the selected hosts when generating reports in the Reporter, as shown in Figure 80 below.

Top Ten Destinations (by total packets) from (08005ACC21F5)

Data gathered from logging point: 9.67.214.171 to 0 [to]

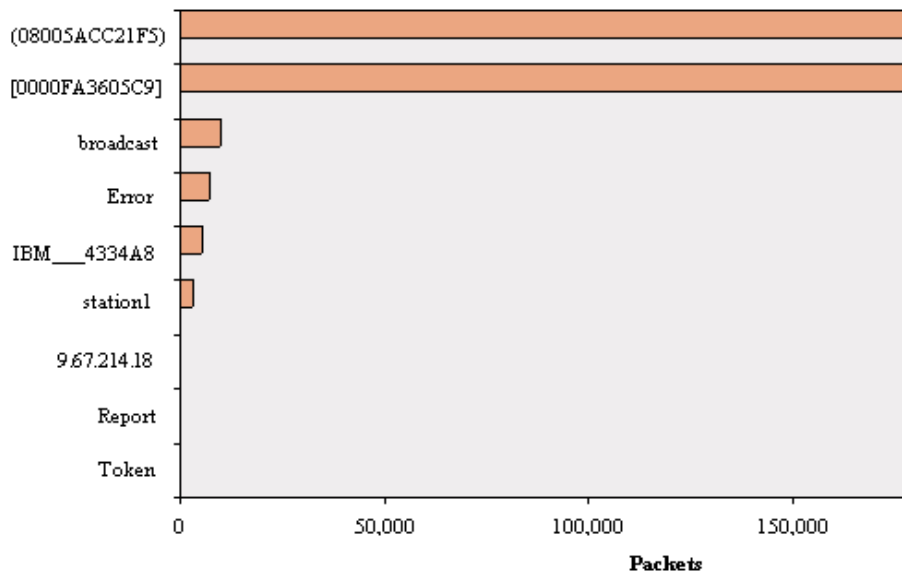


Figure 80. Mixed Address Translation Levels in the Reporter

1. From the *Device Configuration Dialog*, select *Translation* to open the Set Translation Level dialog.

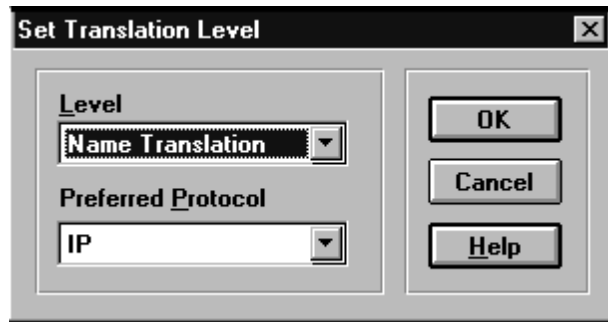


Figure 81. Set Translation Level Dialog

2. Select a level or protocol from the pull-down menus.
 - The levels available are: *Name Translation*, *Protocol Address*, *Vendor ID*, or *MAC Address*.
The *Name Translation* level is selected by default.
 - The preferred protocols available are: *IP*, *IPX*, *DECnet*, *AppleTalk*, *VINES*, or *SNA*.
IP is the default.
3. Click **OK** to confirm any changes.

Setting Up Data Collections

Data collections are set up from the Data Collection Configurations dialog. Data collections define what data is to be gathered from which RMON devices. For an example of the typical performance when processing the results of data collections, see Appendix D. Performance Guidelines.

To reach this dialog, choose *Data Collections* from the *Config* menu in the Collector main window.

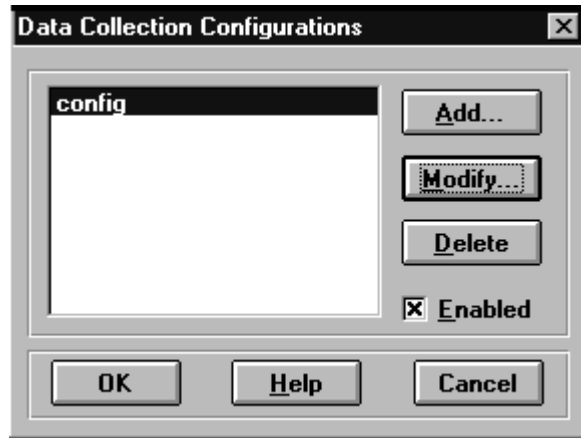


Figure 82. Data Collection Configurations Dialog

This dialog will be empty when you open it for the first time.

Adding a New Configuration

To add a new collection configuration:

1. In the Data Collection Configurations dialog, click **Add** to display the Data Collection Editor.

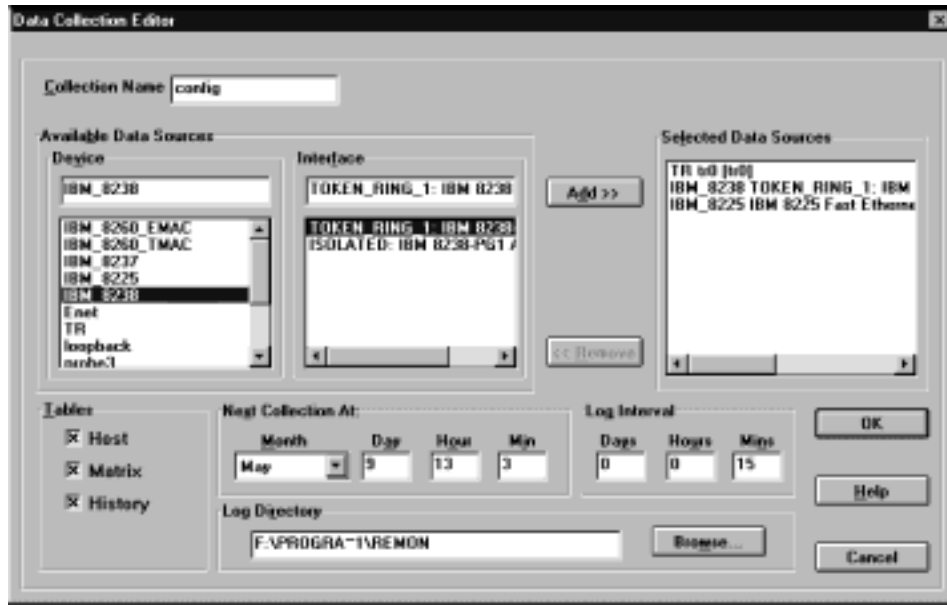


Figure 83. Data Collection Editor Dialog

2. Enter a unique name in the *Collection Name* field. By default this is set to *config*.
3. Select the devices and physical interfaces from which data will be collected:
 - a. To select a single device and physical interface, click the required entry in the *Device* and *Interface* lists.

When a single device and physical interface are selected, the selection is displayed in the fields above the *Device* and *Interface* lists.
 - b. To select multiple devices hold down **Ctrl** and click each required device. To select a number of consecutive devices, click the first device and, holding down **Shift**, click the last device.

When multiple devices are selected, the interface window is greyed out and *all* interfaces on those devices are chosen automatically. The fields above the *Device* and *Interface* lists are also greyed out.
 - c. Click **Add** and the interfaces will be displayed in the *Selected Data Sources* list.
4. To deselect entries in the *Selected Data Sources* list:
 - a. Select a single entry or multiple entries as described in the previous step.
 - b. Click **Remove**.
5. In the *Tables* area, all tables are selected by default. Select or deselect as required.

The selection you make will determine the reports you will be able to produce. If you deselect any of the *History*, *Host*, or *Matrix* tables, no data will be collected for that option. Therefore, you will not be able to produce some of the reports listed in the Reporter. (See Appendix F. Report Descriptions for a list of the reports that can be generated for each data type.)

History data will be collected from only those probes for which you have previously set up a History view in Nways Remote Monitor.

6. Set the date and time of the next collection in the *Next Collection At* area. The default is the current date and time.
7. To set the frequency of data collection, enter the number of days, hours and minutes in the *Log Interval* area. The default is one hour.
8. The *Log Directory* is the directory where the collected CSV files will be stored. By default, the log directory will be set to the installation directory. To select a new directory, click **Browse**....
For each collection, there will be one or more CSV files stored. You can separate the results of different collections by specifying a unique log directory for each collection.
9. To save this configuration, click **OK**. You will be returned to the Data Collection Configurations dialog, where the new configuration will be displayed and *Enabled* will be selected. Data collection will be started for this configuration only when you return to the main dialog.

Modifying Configurations

To modify a collection configuration:

1. Select a configuration in the Data Collection Configurations dialog.
2. Click **Modify** to open the Data Collection Configuration Editor.
3. Follow the instructions given in "Adding a New Configuration" on page 128 to modify any of the configuration details.
4. Click **OK** to save your changes and return to the Data Collection Configurations dialog. Click **Cancel** to abandon any changes.

If any old CSV files remain in the chosen directory, you will be asked whether the Collector should delete them. If they are not deleted, the modified data will be appended to them. Once CSV files have been imported into the Reporter, they can safely be deleted.

Stopping Data Collection

To stop data collection for a configuration, you can either disable it or delete it.

Disabling a Configuration

To disable data collection for a configuration:

1. Select the configuration for which collection is to be disabled.
2. Deselect *Enabled*.
3. Click **OK** to save your changes.

If you want to restart collection at any time, simply reselect **Enabled**.

Deleting a Configuration

Deletion of configurations should be carried out in the period between data collections.

To permanently delete a configuration:

1. Select the configuration you want to delete.
2. Click **Delete**.
3. Repeat as required.

If you have deleted a collection by mistake, immediately click **Cancel** to exit the Data Collection Configurations dialog without saving changes. When Config is selected again, the configuration will be displayed. However, any other changes you have made to the contents of the Data Collection Configurations dialog will also be lost.

4. Click **OK** to confirm any changes.

Starting Data Collection

After you click *OK* in the Data Collection Configurations dialog and return to the main window, data collection will start automatically at the next collection time and date set.

Collected Data Storage

Collected data is stored in CSV format files, in the directory defined in the Data Collection Configuration Editor (see “Adding a New Configuration” on page 128). As further data collections are made, new data is *appended* to the existing files. The files created for the different tables are listed in Table 24.

Table 24. CSV Format Files Created by the Collector

File Name	Description	Table Selected
hist.csv	Ethernet History Data	History
host.csv	Host Data	Host
matrix.csv	Matrix Data	Matrix
trml.csv	Token-Ring MAC-Layer History Data	History
trp.csv	Token-Ring Promiscuous History Data	History

The contents of the five CSV format files are described in “Selecting and Generating Reports” on page 139.

The size of the CSV files in the directory will depend upon the amount of data being collected. If you have set up frequent collections of large amounts of data from large numbers of devices on your network, the CSV files will grow in size quickly.

The CSV files can now be imported into the Reporter for the creation of reports (see “Selecting and Generating Reports” on page 139).

Once the data contained in these files has been imported to the database in the Reporter, it is no longer required by the Collector. Regular deletion of these files, after importing to the Reporter, is recommended. For additional safety, archive or back up the files before deletion.

Exiting the Collector

Generally, the Collector should be left running in the background. However, if you need to shut down the Collector, for example to restart your system, select *Exit* from the *File* menu. When you restart the Collector, data collection will also be restarted.

Chapter 9. Reporter

The Reporter enables you to generate historical reports from any time period contained in the reporting database.

The data collection files created in the Collector are imported into the Reporter, where they are stored in a reporting database. You can then specify multiple reports to be generated from this data, to be printed immediately or to be saved to file for printing at a later time. Reports can also be previewed before printing. The Data Management function allows you to consolidate or delete data contained within the database as it grows.

This release of the Reporter contains a run-time version of Microsoft Access for Windows® Version 8.0, a relational database application.

If you have a copy of Microsoft Access Version 8.0 and are an experienced user, you can customize the reports contained within the Reporter. Refer to the Microsoft Access User's Guide for instructions. You do not need to purchase Microsoft Access to use the Reporter application.

In the Reporter, you set:

- What data to import to the database.
- What reports to generate.

You can then print or save these reports.

The major features in Reporter include:

- Collects RMON History, Host, and Matrix data.
- Supports Ethernet, Fast Ethernet, and token-ring RMON devices.
- Flexibility of data collection, letting you specify:
 - Multiple devices
 - Groups of devices
 - Multiple interfaces on a single device.
- Easy-to-configure data collection.
- Passive collection of RMON data from devices.
- Supports historical trending of RMON data over longer periods of time.
- Reports can be created for:
 - RMON History, Host, and Matrix data
 - A single interface on a device or for all logging points seen during data collection
 - One or multiple hosts
 - A specific period of time.
- Data Management function lets you control the contents of the database as it grows.

This chapter describes how to create reporting databases from which multiple reports can be generated.

The steps involved are:

- Selecting a reporting database
- Importing data from CSV files created in Collector
- Viewing the contents of a database
- Selecting and generating reports
- Loading saved reports

Launching the Reporter Application

Reporter can be launched from Viewman or independently from the Start Menu.

Viewman

To launch Reporter from within Viewman, click



in the toolbar, or select reporter on the application menu.

Start Menu

Select the *IBM Nways ReMon* Program Group from the Start menu and then choose Reporter.

The Reporter main window will be displayed.



Figure 84. Reporter Main Window

Selecting a Reporting Database

Before you can import data from existing CSV files created by the Collector, you need to specify the database the Reporter will use.

- The first time you use the Reporter, you need to create a new database.
- When the Reporter is opened a subsequent time, the last database used will open automatically. Its name is displayed as the *Current Database* at the bottom left of the main window.

Creating a New Database

To create a new database:

1. Click **New** in the main window. This will launch the New Database dialog.

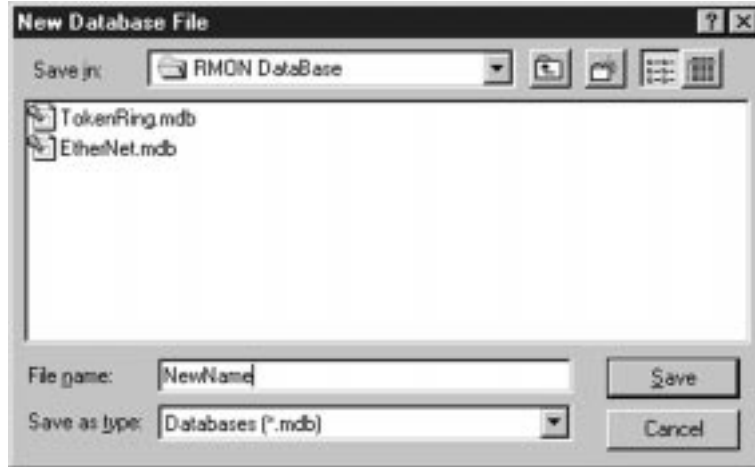


Figure 85. New Database Dialog

2. Enter the file name you want to use. The file type suffix .mdb will be added automatically.
3. Click **Save** to create this new database.

On returning to the main window, the new database name will be displayed as the *Current Database*.

Opening an Existing Database

To open an existing database:

1. Click **Open** in the main window. This will launch the Open Database dialog where all available .mdb files will be displayed.

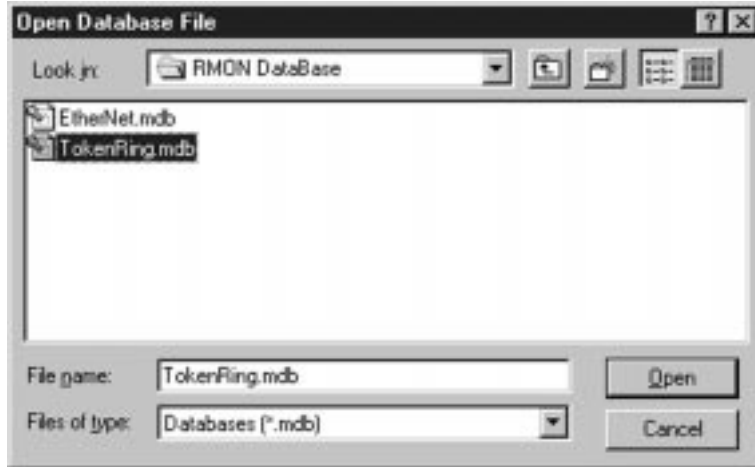


Figure 86. Open Database Dialog

2. Select the database you want to use.
3. Click **Open** to open this database.

On returning to the main window, the database name will be displayed as *Current Database*.

Importing Data

When you have selected the reporting database to be used, data can be imported to that database from CSV files created by the Collector. If an existing database has been selected, data is appended to the database.

For guidelines on maintaining an existing database, see "Appendix D. Performance Guidelines" on page 169.

To import data:

1. Click **Import** in the main window. This will launch the Import Files dialog.



Figure 87. Import Files Dialog

2. Locate the Collector directory that contains the .csv files created by the Collector.
3. Selecting any .csv file in the list will select *all* available .csv files.
4. Click **OK** to import the files or **Cancel** to abandon the import. If you click **Open**, all available .csv files will be added to the current database.

You can now view the contents of the database or start generating reports.

Viewing the Contents of a Database

You can view a summary of the contents of a Reporter database, showing:

- The time range covered in the database. The first and last dates for which data is held.
- The condition of the data. Whether data has been consolidated on a daily or weekly basis or remains unconsolidated (see “Compacting the Application Database” on page 153 and “Chapter 10. Data Management” on page 147 for a definition of consolidation).

To view a Data Summary:

1. Click **Data Summary** in the main window to open the Summary Data dialog.
2. The summary data for the database will be displayed.

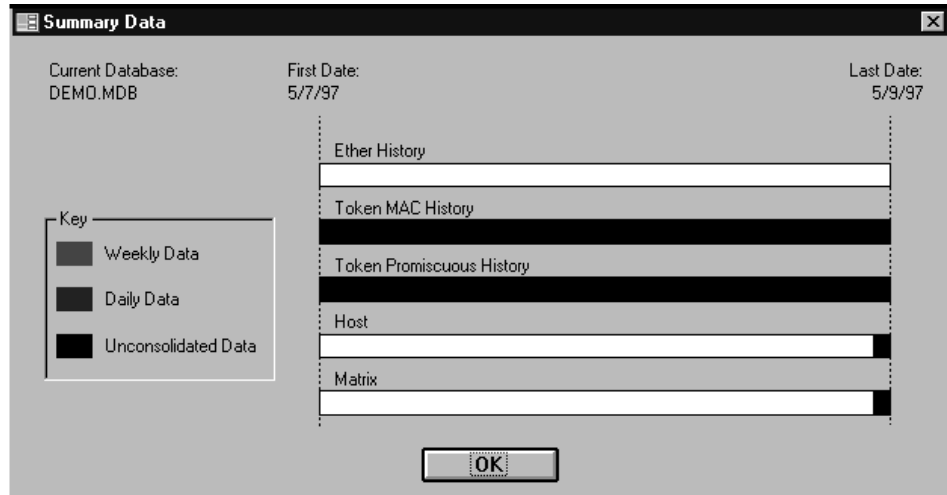


Figure 88. Summary Data Dialog

Figure 88 shows a sample database containing data collected and consolidated for all data types over a year.

The summary for a database may contain gaps in any of the data bars, as in the example above, perhaps as a result of changes to the collection configurations used or to the devices seen on the network.

3. Click **OK** to return to the main window.

Selecting and Generating Reports

Reports on the data contained in the Reporter database are generated from the Report Configuration dialog. To open this dialog, click Report in the Reporter main window.

From this dialog you can:

- Select which reports to generate for all, or specific logging points and hosts
- Select the time period for the reports
- Preview reports
- Print or save (or both) selected reports to file
- Save reports in HTML format

To set up reports, you need to select the report, the logging points, where the output will be placed, the time period, and, if appropriate, the hosts for which data should be displayed.

Once options have been set on all necessary tab pages, click **OK** to start report generation, save the set configuration options, and exit the dialog. Click **cancel** to abandon any changes made and exit the dialog.

Select Reports

1. Click the *Select Report* tab to display its page in the Report Configuration Dialog.
2. Click the *All* check box to select all reports or select one or more individual reports.
3. Click **None** to clear any selected reports.

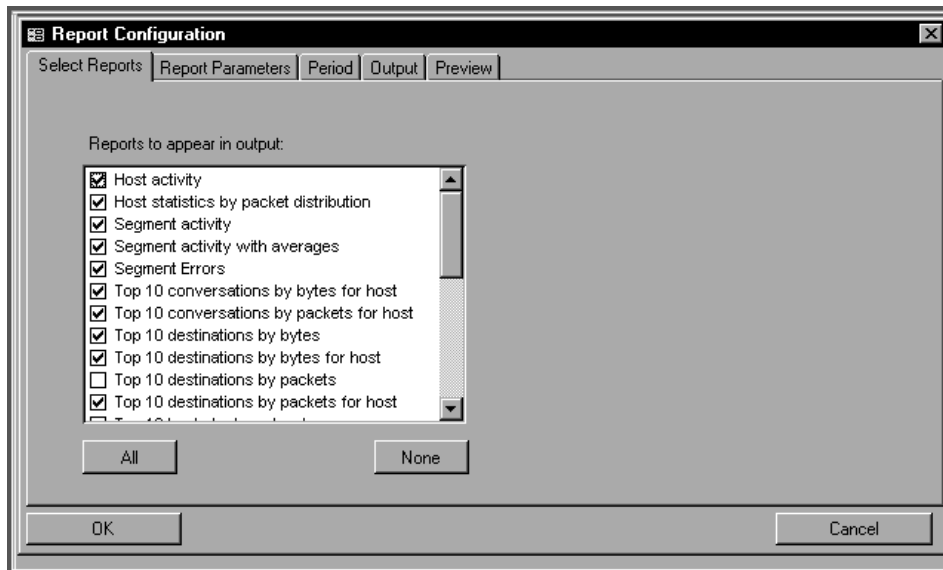


Figure 89. Report Period Configuration Dialog

Select Report Parameters

1. Click the *Report Parameters* tab to display the page in the Report Configuration dialog.
2. Click **Use same parameters for all reports** to have one set of options used for all the reports.
3. Complete the options for each of the reports that you selected on the “Select Reports” page that are now listed in the Per Segment Reports or Per Host Reports list boxes.
 - For the per-segment reports:
 - a. Select logging points from the list box in the per-segment report.
 - b. Enter the name of the Alarm Trigger in the Alarm Trigger box if applicable.
 - For the per-host reports:
 - a. Select either *Use all logging points* or *Use single logging point* in the per-host area of the page.

- b. Select the hosts for the report from the list box.

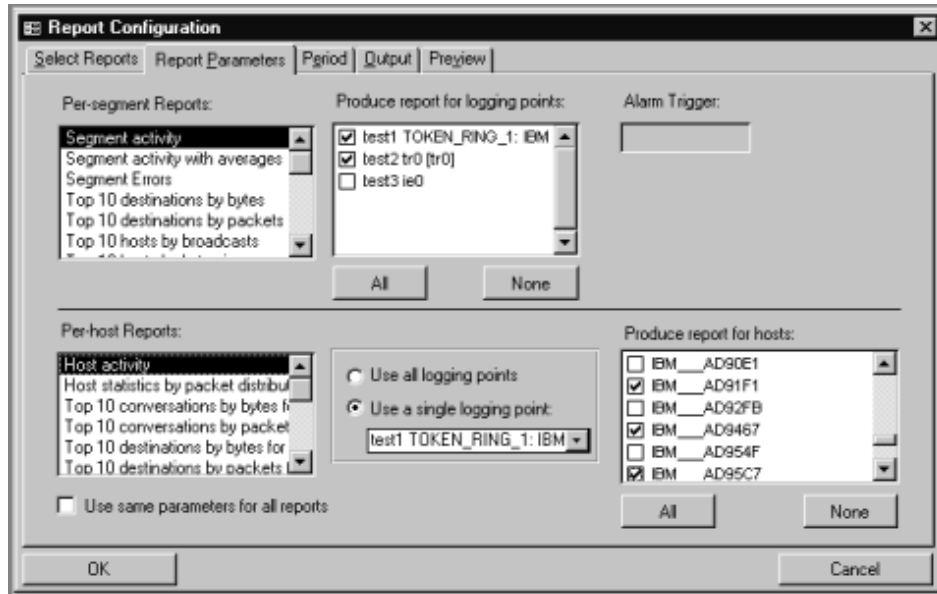


Figure 90. Report Configurations

Time period

Unless you modify the time period, the whole period of the database is used for the reports.

To specify the time period:

1. Click the *Period* tab to display the page in the Report Configuration dialog.

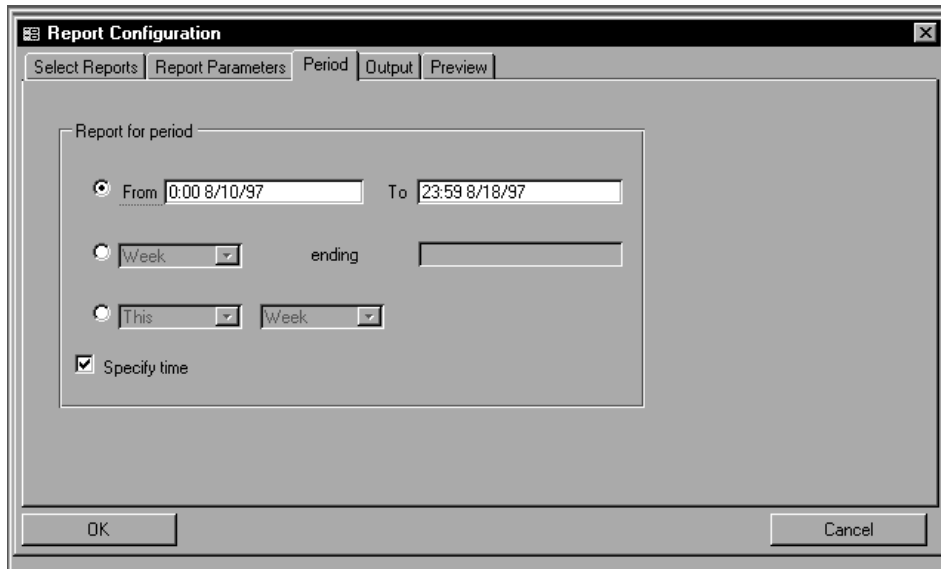


Figure 91. Report Configuration Dialog

2. Click a toggle button to select one of the following three options:
 - A specific start and end date
 - A period of a week, month, or year ending on a specific date
 - A general period, such as this week or last month

For the first two options, a specific time for the start and end dates can also be entered by first selecting Specify time check box.

3. Enter the required time period.

Selecting Report Output Options

To change output options, select the Output tab to display the page.

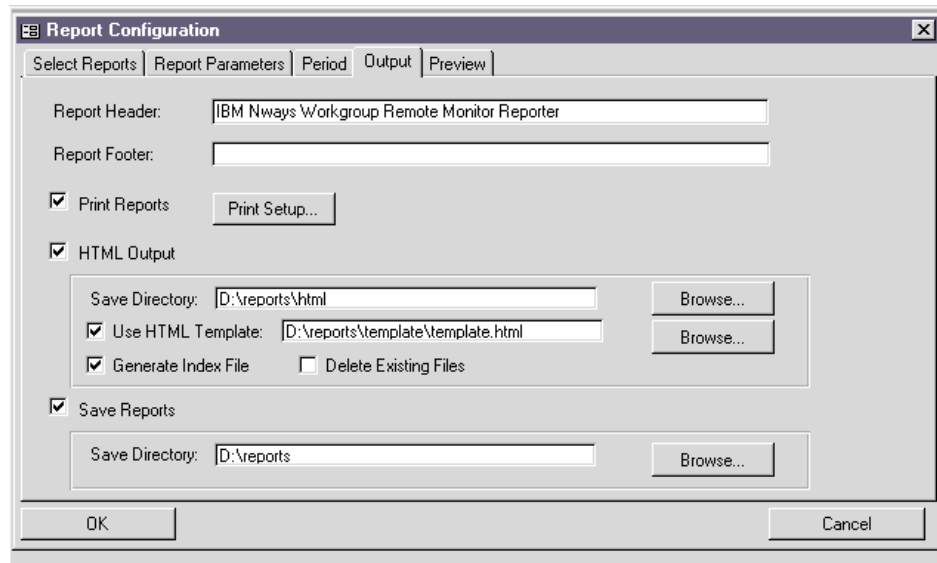


Figure 92. Selecting Report Output Options

Headings/Footers:

1. Enter text for the Report header and Report footer in the appropriate box.

Printing reports:

1. Select the *Print* check box to have the reports printed when generation completes.
2. Select *Print Setup* to start the System Printer Setup dialog.

Saving reports:

1. Select the *Save Reports* check box, then enter the directory location information for the saved report files. Use the *Browse* button to help locate a directory. The Reporter will automatically create the files and name them in this directory.

HTML reports:

1. Select the *HTML* check box to have the generated reports saved to HTML-formatted files.
2. Enter the directory location of the HTML saved reports. Use the *Browse* button to help locate a directory. The Reporter will automatically create the files and name them in this directory.
3. Select *Use HTML Template*: to use your template file for building the formatted files. Enter the name and directory location of that file. Use the *Browse* button to help locate a file. See “Appendix G. Customizing HTML Report Templates” on page 181 for more information.

Do not store your templates in the same directory as your HTML reports or they will be erased if you select the *Delete Existing Files* option.

4. Select *Generate Index File* to have an Index page built with HTML links that point to each of the different reports generated.
5. Select *Delete Existing Files* to replace any previously generated HTML reports.

Previewing

You have the option to preview reports before printing or saving them. Reports can then be printed or saved (or both) for printing later.

If you select OK in the Report Configuration dialog without amending print or save options, the previously set configuration will apply.

To preview:

1. Select the *Preview* tab to display a page in the Report Configuration Dialog.

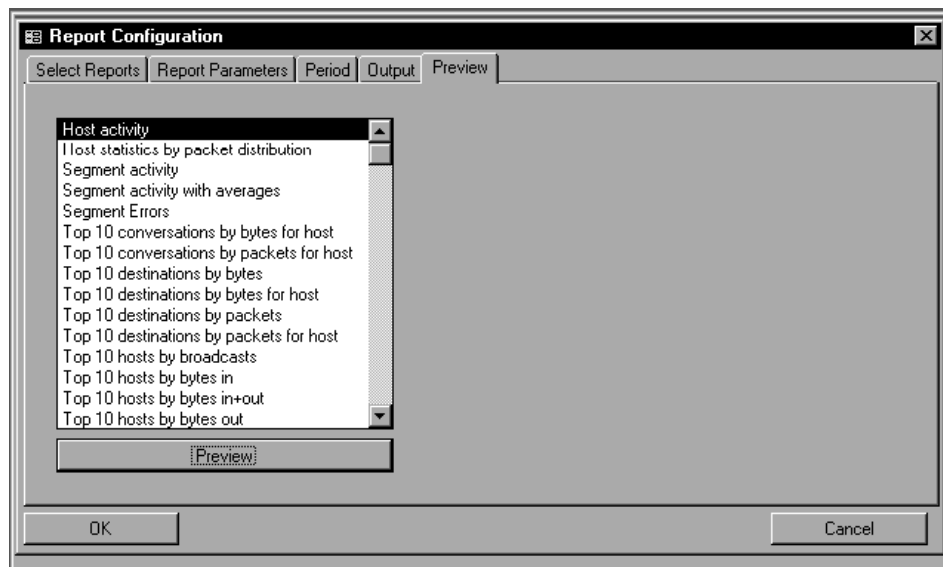


Figure 93. Preview Tab

2. Select a report from the displayed list that you previously selected on the Select Report page.
3. Click **Preview** to start report generation. The report will be displayed in the Preview Window.
4. When a report is in the Preview Window, you have the following options:
 - **Close**
Click the x in the upper-right corner of the window with the displayed report
 - **Print**
Select *File* from the Menu bar and then select *Print*. The Page Setup dialog will be displayed. Click **OK** to print or **Cancel** to abandon.

- **Print Setup**

Select *File* from the Menu bar, then select *Print Setup*. The Page Setup dialog will be displayed. You can use this to change page margins, orientation, and column layout. To change the print destination, click the *Page* tab, click **Use Specific Printer** and then click **Printer**. Click **OK** to save changes or **Cancel** to abandon.

Loading Saved Reports

Any saved report can be printed at a later date. To reload a saved report for viewing or printing:

1. Click **Load Report** in the main window to open the Load Report dialog.
2. Select the report that you want to print or view and click **Open**.

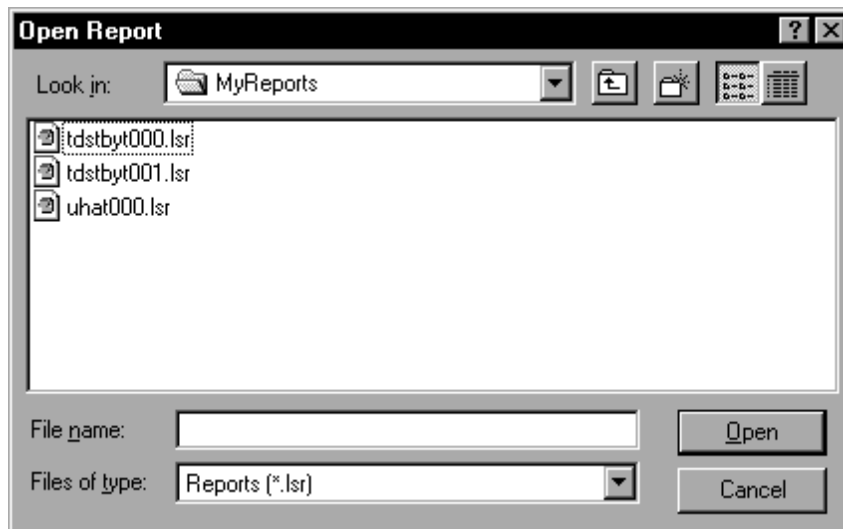


Figure 94. Loading Saved Reports

3. When a report is in the Preview Window, you have the following options:
 - **Close**
Click the **x** in the upper-right corner of the window with the displayed report.
 - **Print**
Select *File* from the Menu bar and then select *Print*. The Page Setup dialog will be displayed. Click **OK** to print or **Cancel** to abandon.
 - **Print Setup**
Select *File* from the Menu bar, then select *Print Setup*. The Page Setup dialog will be displayed. You can use this to change page margins, orientations, and

column layout. To change the print destination, click the *Page* tab, click **Use Specific Printer** and then click **Printer**. Click **OK** to save changes or **Cancel** to abandon.

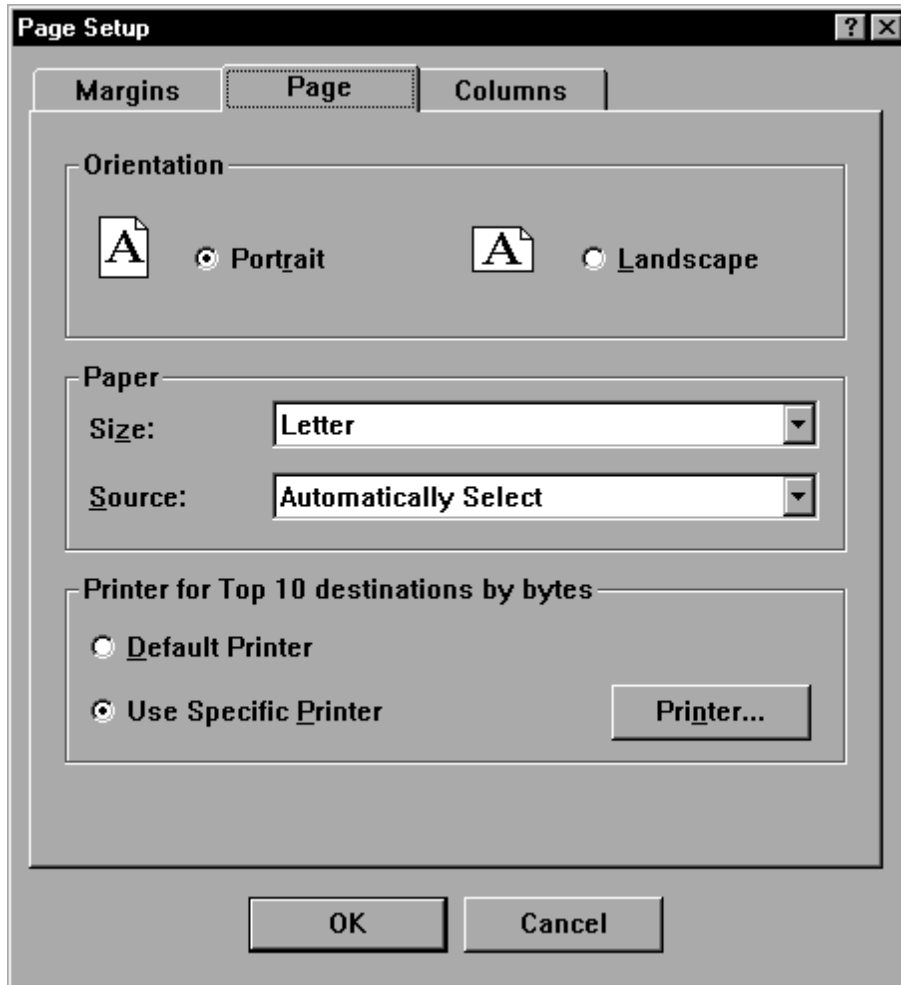


Figure 95. Page Setup

Chapter 10. Data Management

Making frequent collections of data from your network and gathering data consistently over a long period of time will have two consequences:

- Old data may become obsolete or may not be required in such detail.
- The Reporter database may become excessively large-increasing the time required by the Reporter to carry out its tasks.

Regular data management can overcome these problems.

The CSV files created in the Collector also need to be managed because they will quickly fill the hard disk. See “Appendix D. Performance Guidelines” on page 169.

This chapter describes:

- Managing data
- Consolidating data
- Deleting data
- Archiving data

Managing Data

As you store data collected over time, your database will use an increasing amount of disk space. The rate at which it grows depends on the granularity of the data you are collecting.

Fine granularity means frequent collections and therefore more disk space required for storage.

The Reporter can consolidate data by calculating daily or weekly averages from the original data. The original data is then *automatically deleted* from the database. In this way, you retain the essence of the original collections while using much less disk space.

Consolidation compresses multiple data records into a single data record, by averaging the data. The reduction in granularity means that consolidated data will be more appropriate for trending and baselining, which use average values, than for short-term troubleshooting, which requires more detail.

Data that has been consolidated into daily averages can then be consolidated into weekly averages, and so on.

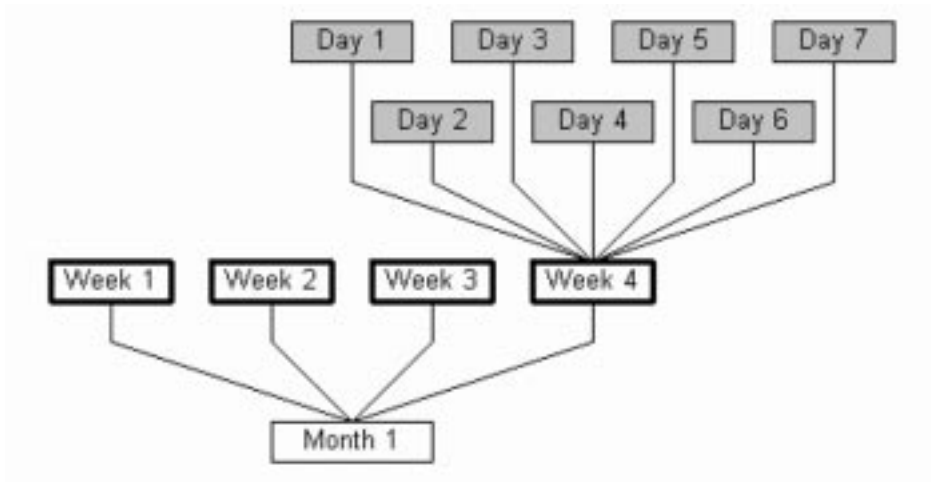


Figure 96. Consolidation of Multiple Data Records

Use the Data Summary function (described in “Viewing the Contents of a Database” on page 138) to see whether the data has been consolidated or remains unconsolidated.

Consolidation Examples

The following graphs show data over the same range of time, but when the data has reached different ages.

1. In its original form, there is much variation in the time line:

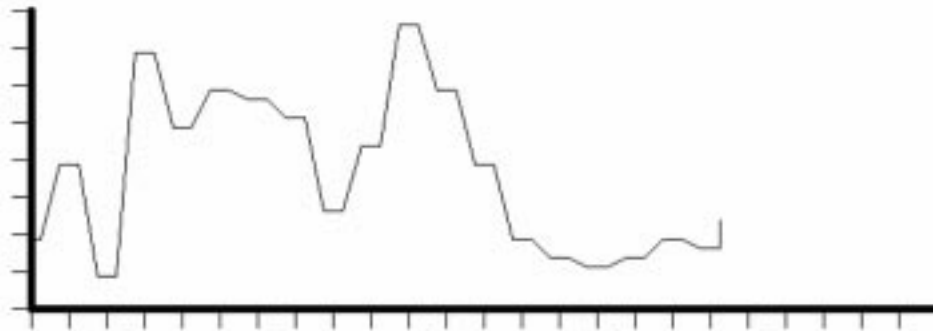


Figure 97. Original Data Collections

2. When the data becomes one week old, it is consolidated into daily records. The time line becomes smoother, though it still retains distinct peaks and troughs:

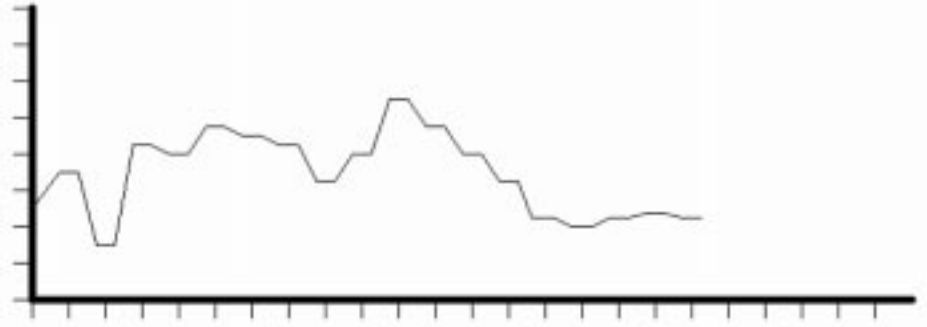


Figure 98. After First Consolidation

3. After one month, the daily records are consolidated further and the time line becomes even flatter:

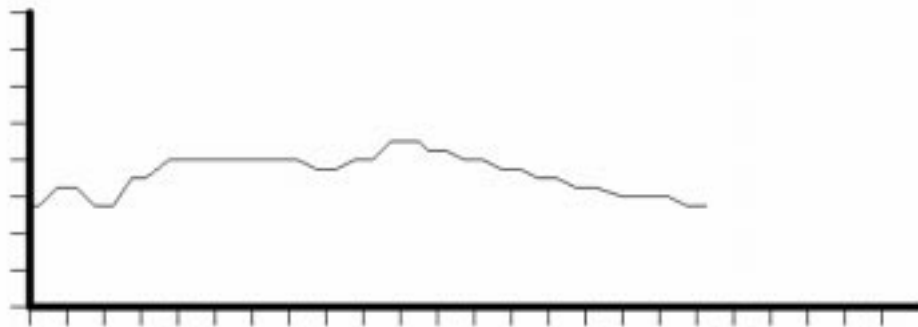


Figure 99. After Second Consolidation

If consolidation continues, the time line becomes progressively smoother. This would indicate the overall trend but would provide less information about periodic fluctuations.

Once data has been consolidated, this process cannot be reversed, so you may want to keep a copy of the database (see “Archiving Data” on page 151).

Consolidating Data

From the Reporter main window, click **Data Management** to open the Data Management dialog.

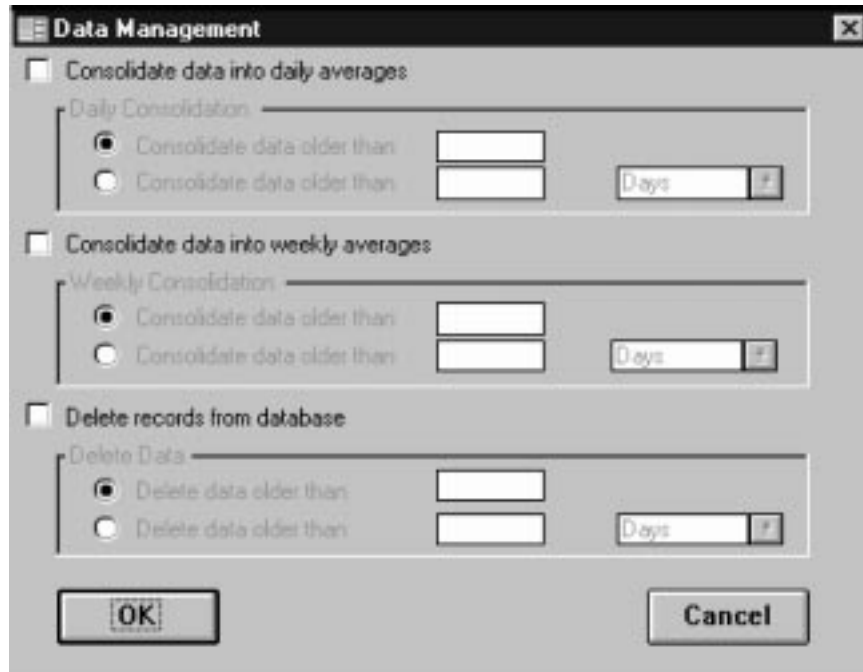


Figure 100. Data Management Dialog

To consolidate data in the Reporter database:

1. Select either **Consolidate data into daily averages** or **Consolidate data into weekly averages**.
2. For either option, to specify what data should be consolidated, do one of the following:
 - a. Click the first **Consolidate data older than** button and enter a specific date in the text field in the format dd:mm:yy.
 - b. Click the second **Consolidate data older than** button. Enter a specific number of days, weeks, or months in the text field and then select a time period from the pop-up menu.
3. Click **OK** to return to the main window, and Reporter will start consolidation. Click **Cancel** to abandon consolidation.

Deleting Data

You might need to delete data if, for example, you have reconfigured your network. Deleting data will permanently remove the data from the selected database. Be sure that you no longer require this data before you delete it.

Deleting data is not the same as consolidating data. When data is deleted from the database it is no longer available for future consolidation.

If in doubt, do one of the following:

- Make a backup copy of the database to a safe directory first, so that the data is not permanently lost. See “Archiving Data”.
- Use the Consolidate function instead-this will replace the original data with daily or weekly averages.

To delete data from the Reporter database:

1. From the Reporter main window, click *Data Management* to open the Data Management dialog (see Figure 100).
2. Select *Delete records from database*.
3. To specify the point at which deletion should take place, do one of the following:
 - a. Click the first **Delete data older than** button and enter a specific date in the text field in the format dd:mm:yy.
 - b. Click the second **Delete data older than** button. Enter a specific number of days, weeks, or months in the text field and then select a time period from the pop-up menu.
4. Click **OK** to return to the main window, and the Reporter will start the deletion of data. Click **Cancel** to abandon the deletion of data.

Archiving Data

After a period of time, you might want to archive the entire contents of a database and start importing collected data from the Collector into a new database.

To Archive Data

1. Stop importing data into the current database at an appropriate point, for instance, at the end of a week or month.
2. Save the database in a secure location.
3. Create a new database as described in “Creating a New Database” on page 135.
4. Import collected data from the Collector into the new database.

To reduce the amount of disk space used by archived databases, consolidate the data contained in the database, as described in “Consolidating Data” on page 149.

To Access Archived Data

1. Click **Open** in the Reporter main window to open the File dialog.
2. Select the old database.

You can now generate reports from this old data (see “Selecting and Generating Reports” on page 139).

Remember to close the archived database and select the new database before importing new data.

Chapter 11. Compacting and Repairing the Application Database

The Reporter uses two types of databases:

- A user-defined reporting database to contain imported data.
This is simply used for data storage-it holds the collected data that you have imported to the Reporter.
- An application database to hold the Reporter program.
This is called 1sr97.mdb. It contains the user interface and all the functionality for the Reporter application.

This chapter concentrates on the application database.

The application database will grow with use or might possibly become damaged. The Reporter application contains two additional programs to deal with these issues:

- Compacting the application database
- Repairing the application database

Compacting the Application Database

As you use the Reporter and delete data, the application database might become fragmented and use disk space inefficiently. Compacting makes a copy of the database, rearranging the way the database file is stored on disk. This should be carried out on a weekly basis.

Ensure that you have enough space on your disk for the original and temporary copy versions of the database. The compact operation will stop if there is not enough disk space available.

You must close the Reporter application before attempting to compact the application database.

To compact the application database:

1. Close the Reporter application.
2. Select the *IBM Nways ReMon* Program Group from the Start menu and then choose Compact Application Database.

The application database will compact automatically.

Repairing the Application Database

If the Reporter application database becomes damaged, for instance as a result of a power failure, the database can be repaired.

You must close the Reporter application before attempting to repair the database:

To repair the application database:

1. Close the Reporter application.
2. Select the *IBM Nways ReMon* Program Group from the Start menu and then choose *Repair Application Database*.

The database will be repaired automatically.

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

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

Pentium is registered trademark of Intel Corporation in the United States, or other countries, or both.

Sun is a registered trademark of Sun Microsystems, Inc. in the United States, other countries, or both.

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

Appendix B. List of Protocol Decodes

This appendix lists the protocol decodes supported for the RMON applications (Table 25) in this release.

Table 25. List of Supported Protocol Decodes by Protocol Family

Protocol Family	Protocols
AppleTalk Phase I & II	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 (Phase 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

Appendix C. Application Variables

This appendix contains definitions of the variables that can be selected in the following applications:

- Statistics
- History
- Host
- Matrix
- Ring Station

Statistics Variables

The Statistics application presents the following variables on Ethernet, FDDI, and token ring.

Variables Available on Ethernet

Table 26. Statistics Variables Available on Ethernet

Variable	Description
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.
Missed	The number of times the probe detected a lack of resources and so might 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.

Variables Available on FDDI

Table 27. Statistics Variables Available on FDDI

Variable	Description
Beacons	The number of beacons seen on the ring.

Table 27. Statistics Variables Available on FDDI (continued)

Variable	Description
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 might 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: <ol style="list-style-type: none"> 1. Ring Operational 2. Non-Operational 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, and so on	Packet sizes are inclusive and include FCS octets.

Variables Available on Token Ring

Table 28. Statistics 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 address copied (AC) 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.
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.

Table 28. Statistics Variables Available on Token Ring (continued)

Variable	Description
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—they include 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 <i>usually</i> a problem—see “Glossary” on page 195).
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 connecting 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.
Local LLC Frames	The total number of frames received which had no RIF field (or had a RIF field that included only the local ring’s number) and were not All Route Broadcast 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 did not see it again.
MAC Bytes	The total number of bytes making up all MAC packets detected on this segment.

Table 28. Statistics Variables Available on Token Ring (continued)

Variable	Description
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	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.
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 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.
Single Route Oct.	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 becomes corrupted.
1 Hop Frames, and so on	The total number of frames that will make 1, 2, 3, 4, 5, 6, 7, 8, or more than 8 "hops" (across bridges between ring segments) to reach their destination.
18 to 63 Bytes, and so on	Packet sizes are inclusive, and include FCS octets.

History Variables

The following tables list the variables available on Ethernet, FDDI, and token ring.

Variables Available on Ethernet

Table 29. 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.

Table 29. History Variables Available on Ethernet (continued)

Variable	Description
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 might have missed counting some packets.
Packets Sent	The total number of packets detected on this segment including error packets.
Short + CRC	Too short and CRC error.
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 30. 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 might 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.
TNEG	Negotiated token rotation time (TNEG). 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.
23 to 63, and so on.	Packet sizes are inclusive and include FCS octets.

Variables Available on Token Ring

Table 31. 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 address copied (AC) 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.
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-see "Glossary" on page 195).
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.

Table 31. History Variables Available on Token Ring (continued)

Variable	Description
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 to 63 and so on	Packet sizes are inclusive, and include FCS octets.
Utilization	Token-ring utilization calculations are based on using the <code>ifSpeed</code> variable from the interface table. If the value is 0, a 16-Mbps ring speed is assumed for the calculation.

Host Variables

The following list of variables is available for the Host application on Ethernet, FDDI, and token ring.

Table 32. Host Variables Available on Ethernet, FDDI, and token ring

Variable	Description
Packets In	The number of packets seen on the segment-including error packet-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 application on Token Ring.

Table 33. 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 at which this station entered the ring.
Last Exited	The time at which 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 from 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 from 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.
Inburst Errors	The total number of burst errors detected upstream from 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 from 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 reported in error reporting packets sent by the nearest 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 (not <i>usually</i> a problem-see "Glossary" on page 195).
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 has been corrupted.
In Beacon Errors	The total number of beacon frames detected upstream from this station-see "Glossary" on page 195.

Table 33. Ring Station Variables Available on token ring (continued)

Variable	Description
Out Beacon Errors	The total number of beacon frames detected downstream from this station (by the station naming this station as the NAUN)-see "Glossary" on page 195.
Insertions	The number of times the probe detected this station inserting into the ring.

Appendix D. Performance Guidelines

This appendix describes a typical data collection and importation of the data into a Reporter database from which the data is consolidated and reports are generated. Table 34 shows an example of how long each operation takes in order to give you a feel for how to set up your collecting and reporting schedules.

In general, the times for each operation will increase in proportion to the amount of data you gather. Performance is also significantly affected by the PC's processor and available memory. The example performance times were taken on a single Ethernet segment using a PC with a 120-MHz Pentium® processor and 16 MB of RAM.

Data collection was set up in the Collector to take place over 2 days, gathering all tables every hour from a single probe interface. The history entries were every 30 seconds and 30 minutes. There were 162 hosts and 1489 conversations on the segment. At the end of the collection phase, 6 150 050 bytes of data had been gathered and saved to disk in CSV format.

The files were then ready for import into a Reporter database. There are several discrete operations that can be performed on the data within the Reporter. These operations are shown in Table 34.

Table 34. Example of Operation Times in Reporter

Operation	Action	Time
Import	Import files into an empty database file.	9 mins 37 secs
Save Reports	Generate one report of each type and save to a file.	5 mins 37 secs
Print Reports	Generate one report of each type and print to printer.	11 mins 10 secs
Consolidate Daily	Consolidate all data in the database into daily averages.	12 mins 26 secs
Consolidate Weekly	Consolidate all data in the database into weekly averages.	10 mins 48 secs
Delete	Delete all records from the database.	8 mins 12 secs

Once the CSV files have been imported into a Reporter database, they are no longer required and should be deleted to avoid filling up hard-disk space.

Appendix E. CSV File Contents

The Collector creates the following CSV format files to contain collected data.

Table 35. CSV Format Files Created by the Collector

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

The contents of these files are given in the following sections. Take into consideration the following notes when interpreting the contents of these files.

1. There is a difference in the interpretation of TimeIndex between History and other tables. In History (hist.csv, trml.csv and trp.csv) tables, TimeIndex refers to the *start* of the interval-so the interval ends at (TimeIndex + dTimeIndex). In Host and Matrix tables, TimeIndex refers to the *end* of the interval-so the interval starts at (TimeIndex - dTimeIndex).
2. In the Host and Matrix tables, the absolute values are of little use because they keep incrementing. The delta values are likely to be much more useful.
3. The field name Probe actually refers to the data source (see "Configuring Data Sources" on page 125) and the interface number. Therefore, the Index field does not necessarily have to be used to distinguish between interfaces on a multi-interface probe.

History File Format

The contents of the CSV file created for History data by the Collector are shown in Table 36.

Table 36. History CSV Format File Contents

Field Name	Description
Probe	Name of logging point from which this entry was collected
TimeIndex	Date and time at which the interval corresponding to this collection started
HistoryIndex	Number that identifies which history study this entry is part of
Index	Interface from which data was collected
SampleIndex	Number that identifies this entry within a particular history study
IntervalStart	Time when interval started (in sysUpTime format)
DropEvents	Number of packets dropped by the probe in this interval
Octets	Number of bytes seen in this interval

Table 36. History CSV Format File Contents (continued)

Field Name	Description
Pkts	Number of packets seen in this interval
BroadcastPkts	Number of broadcast packets seen in this interval
MulticastPkts	Number of multicast packets seen in this interval
CRCAlignErrors	Number of CRC errors seen in this interval
UndersizePkts	Number of undersize packets (< 64 bytes) seen in this interval
OversizePkts	Number of oversize packets (> 1518 bytes) seen in this interval
Fragments	Number of fragments (packets < 64 bytes with CRC error) seen in this interval
Jabbers	Number of jabbers (packets > 1518 bytes with CRC error) seen in this interval
Collisions	Number of collisions seen in this interval
Utilization	Average Utilization of segment in this interval (on a scale of 0 to 10 000)
dTimeIndex	Length of this time interval (in seconds)

Host File Format

The contents of the CSV file created for Host data by the Collector are shown in Table 37.

Table 37. Host CSV Format File Contents

Field Name	Description
Probe	Name of logging point from which this entry was collected
TimeIndex	Date and time at which this entry was collected from probe
Address	Address of host to which this entry refers
CreationOrder	Creation order of host in RMON host table
Index	Interface from which the data was collected from
InPkts	Total number of packets received by host
OutPkts	Total number of packets sent by host
InOctets	Total number of bytes received by host
OutOctets	Total number of bytes sent by host
OutErrors	Total number of error packets sent by host
OutBroadcastPkts	Total number of broadcast packets sent by host
OutMulticastPkts	Total number of multicast packets sent by host
dInPkts	Number of packets received by host since previous collection
dOutPkts	Number of packets sent by host since previous collection
dInOctets	Number of bytes received by host since previous collection
dOutOctets	Number of bytes sent by host since previous collection

Table 37. Host CSV Format File Contents (continued)

Field Name	Description
dOutErrors	Number of error packets sent by host since previous collection
dOutBroadcastPkts	Number of broadcast packets sent by host since previous collection
dOutMulticastPkts	Number of multicast packets sent by host since previous collection
dTimeIndex	Time (in seconds) between this collection and previous collection

Matrix File Format

The contents of the CSV file created for Matrix data by the Collector are shown in Table 38.

Table 38. Matrix CSV Format File Contents

Field Name	Description
Probe	Name of logging point from which this entry was collected
TimeIndex	Date and time at which this entry was collected from probe
SourceAddress	Source Address of this conversation
DestAddress	Destination Address of this conversation
Index	Interface from which the data was collected
Pkts	Total number of packets in this conversation
Octets	Total number of bytes in this conversation
Errors	Total number of errors in this conversation
dPkts	Number of packets in this conversation since previous collection
dOctets	Number of bytes in this conversation since previous collection
dErrors	Number of errors in this conversation since previous collection
dTimeIndex	Time (in seconds) between this collection and previous collection

Token-Ring MAC-Layer Data

The contents of the CSV file created for token-ring MAC-layer data are shown in Table 39.

Table 39. Token-Ring MAC-Layer CSV Format File Contents

Field Name	Description
Probe	Name of logging point from which this entry was collected
TimeIndex	Date and time at which the interval corresponding to this collection started
HistoryIndex	Number that identifies which history study this entry is part of
Index	Interface from which the data was collected
SampleIndex	Number that identifies this entry within a particular history study

Table 39. Token-Ring MAC-Layer CSV Format File Contents (continued)

Field Name	Description
IntervalStart	Time that interval started (in sysUpTime format)
DropEvents	Number of packets dropped by the probe in this interval
MacOctets	Number of octets in MAC packets seen in this interval
MacPkts	Number of MAC packets seen in this interval
RingPurgeEvents	Number of times the ring enters the ring purge state from the normal state in this interval
RingPurgePkts	Number of ring purge MAC packets seen in this interval
BeaconEvents	Number of times the ring enters a beaconing state from a non-beaconing state in this interval
BeaconTime	The amount of time the ring has been in the beaconing state in this interval
BeaconPkts	The number of beacon MAC packets seen in this interval
MCEvents	The number of times the ring enters the claim token state in this interval
ClaimTokenPkts	The number of claim token MAC packets seen in this interval
NAUNChanges	The number of NAUN changes detected in this interval
LineErrors	The number of line errors reported during this interval
InternalErrors	The number of internal adapter errors reported during this interval
BurstErrors	The number of burst errors reported during this interval
ACErrors	The number of Address Copied errors during this interval
AbortErrors	The number of abort delimiters reported during this interval
LostFrameErrors	The number of lost frame errors reported during this interval
CongestionErrors	The number of congestion errors reported during this interval
FrameCopiedErrors	The number of frame copied errors reported during this interval
FrequencyErrors	The number of frequency errors reported during this interval
TokenErrors	The number of token errors reported during this interval
SoftErrorReports	The number of soft error reports during this interval
RingPollEvents	The number of ring poll events detected during this interval
ActiveStations	The maximum number of active stations detected by the probe during this interval
dTimeIndex	Length of this time interval (in seconds)

Token-Ring Promiscuous Data

The contents of the CSV file created for token-ring promiscuous data are shown in Table 40.

Table 40. Token-Ring Promiscuous CSV Format File Contents

Field Name	Description
Probe	Name of logging point from which this entry was collected
TimeIndex	Date and time at which the interval corresponding to this collection started
HistoryIndex	Number that identifies which history study this entry is part of
Index	Interface from which this data was collected
SampleIndex	Number that identifies this entry within a particular history study
IntervalStart	Time that interval started (in sysUpTime format)
DropEvents	Number of packets dropped by the probe in this interval
Octets	Number of bytes in non-MAC packets seen in this interval
Pkts	Number of non-MAC packets seen in this interval
DataBroadcastPkts	Number of non-MAC broadcast packets seen in this interval
DataMulticastPkts	Number of non-MAC multicast packets seen in this interval
Pkts18to63Octets	Number of non-MAC packets from 18 to 63 octets seen in this interval
Pkts128to255Octets	Number of non-MAC packets from 128 to 255 octets seen in this interval
Pkts256to511Octets	Number of non-MAC packets from 256 to 511 octets seen in this interval
Pkts512to1023Octets	Number of non-MAC packets from 512 to 1023 octets seen in this interval
Pkts1024to2047Octets	Number of non-MAC packets from 1024 to 2047 octets seen in this interval
Pkts2048to4095Octets	Number of non-MAC packets from 2048 to 4095 octets seen in this interval
Pkts4096to8191Octets	Number of non-MAC packets from 4096 to 8191 octets seen in this interval
Pkts8192to18000Octets	Number of non-MAC packets from 8192 to 18 000 octets seen in this interval
PktsGT18000Octets	Number of non-MAC packets greater than 18 000 octets seen in this interval
dTimeIndex	Length of this time interval (in seconds)

Appendix F. Report Descriptions

This appendix describes the reports available in the Reporter application, and gives examples of the different types of graphs generated by the application.

The Reporter contains the following reports for History, Host, and Matrix data. Report type L = Line graph and H = Histogram.

Table 41. History Reports

Report Title	Type	Description
Segment activity	L	Packet rate on the segment
Segment activity with averages	L	Packet rate on the segment with mean and standard deviations
Segment errors	L	Collisions and total errors for Ethernet Isolation errors and total errors for token ring
Utilization Summary with Broadcast Packets	L	1. Segment utilization
	L	2. Broadcast packets rate and all packets rate
Utilization Summary with Alarm Triggers	L	Utilization where utilization level exceeds the specified alarm trigger

Table 42. Host Reports

Report Title	Type	Description
Host Activity	L	Packet sent per second for each selected host
Host Statistics by Packet Distribution	H	1. Total packets sent and received, errors, broadcasts, and multicasts
	H	2. Top 10 hosts this station is talking to
Top 10 Hosts by Broadcasts	H	Top 10 senders of broadcast packets
Top 10 Hosts by Bytes In	H	Top 10 receivers of bytes
Top 10 Hosts by Bytes In + Out	H	Top 10 hosts sorted by total bytes sent and received
Top 10 Hosts by Bytes Out	H	Top 10 senders of bytes
Top 10 Hosts by Errors	H	Top 10 senders of error packets
Top 10 Hosts by Multicasts	H	Top 10 senders of multicast packets
Top 10 Hosts by Packets In	H	Top 10 receivers of packets
Top 10 Hosts by Packets In + Out	H	Top 10 hosts sorted by total packets sent and received
Top 10 Hosts by Packets Out	H	Top 10 senders of packets

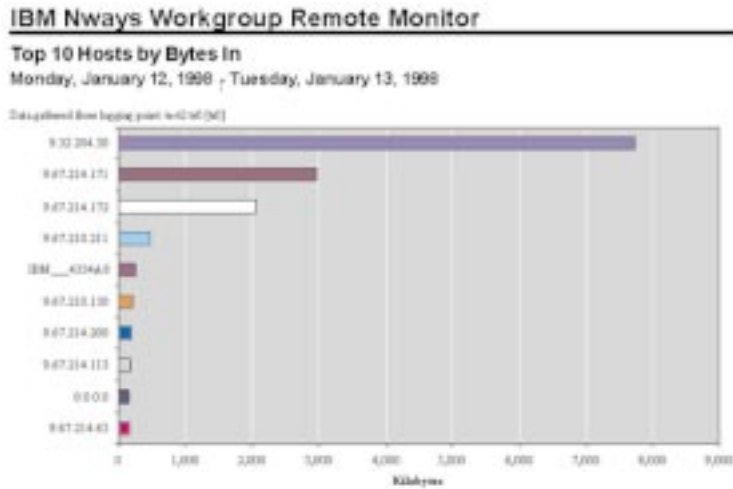
Table 43. Matrix Reports

Report Title	Type	Description
Top 10 Conversations by Bytes for Host	H	Top 10 stations talking to or being talked to by the selected host, measured in bytes

Table 43. Matrix Reports (continued)

Report Title	Type	Description
Top 10 Conversations by Packets for Host	H	Top 10 stations talking to or being talked to by the selected host, measured in packets
Top 10 Destinations by Bytes	H	Top 10 receivers of bytes
Top 10 Destinations by Bytes for Host	H	Top 10 receivers of bytes from the selected host
Top 10 Destinations by Packets	H	Top 10 receivers of packets
Top 10 Destinations by Packets for Host	H	Top 10 receivers of packets from the selected host
Top 10 Sources by Bytes	H	Top 10 senders of bytes
Top 10 Sources by Bytes for Host	H	Top 10 senders of bytes to the selected host
Top 10 Sources by Packets	H	Top 10 senders of packets
Top 10 Sources by Packets for Host	H	Top 10 senders of packets to the selected host

Example of Report with Histogram



Example of Report with Line Graph

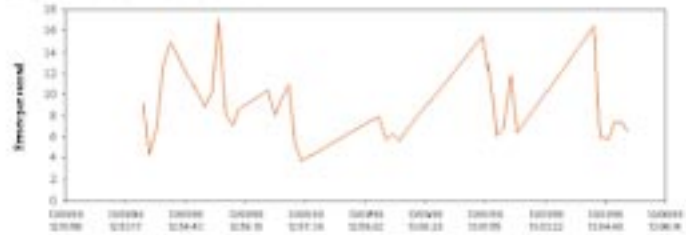
IBM Nways Workgroup Remote Monitor

Segment Errors

Monday, January 12, 1998 - Tuesday, January 13, 1998

test2 tr0 [tr0]

Logging start to 01:00:00, format 40 sampling every 10s between 01:00:00.00:00 and 01:00:00.00:00



Appendix G. Customizing HTML Report Templates

This appendix describes the following:

- Default HTML Template
- Customizing the Default Template

Customizing the Default Template

When the Reporter saves reports in HTML format, it uses a default HTML template, TEMPLATE.HTML. You can customize the default template to reflect your company identity or to add company-specific information. The noneditable areas of this template are marked by HTML comments, for example, `<!--AccessTemplate_Body-->`. These comments will be replaced in the final output with the information identified in Table 44.

Table 44. Noneditable HTML comments

HTML Comment	This area will contain.
<code><!--AccessTemplate_Title--></code>	The title of the report
<code><!--AccessTemplate_Body--></code>	The main body of the report itself.
<code><!--AccessTemplate_FirstPage--></code>	A link to the first page of the report
<code><!--AccessTemplate_PreviousPage--></code>	A link to the previous page of the report
<code><!--AccessTemplate_NextPage--></code>	A link to the next page of the report
<code><!--AccessTemplate_LastPage--></code>	A link to the last page of the report
<code><!--LSRTemplate_Index--></code>	A link to the index page (normally index.html)

As with all HTML documents, the reports may display differently depending on which browser you are using.

Formatting defaults are set by Microsoft Access. These are contained within `<!--AccessTemplate_Body-->` and cannot be edited.

Default HTML Template

The contents of this template are shown below:

```
<HTML>

<!--Set page title to report title-->
<TITLE><!--AccessTemplate_Title--></TITLE>

<!--Set the background colour to white-->
<BODY BGCOLOR="#FFFFFF">

<!--Insert the main report body here-->
<!--AccessTemplate_Body-->
```

```

<!--This rule ensures that the spacing is correct in all browsers-->
<HR noshade size=0 width=0>

<!--At the bottom of the page, place links to other pages in the report-->
<TABLE BORDER=0 WIDTH=718>
<TR >
<TD ALIGN=LEFT >
<FONT SIZE=2 FACE="Arial" COLOR=#000000>
<A HREF= >First</A>
<A HREF= >Previous</A>
<A HREF= >Next</A>
<A HREF= >Last</A>
</FONT>

<!--In the bottom right-hand corner, place a link to the Index page-->
<TD ALIGN=RIGHT >
<FONT SIZE=2 FACE="Arial" COLOR=#000000>
<A HREF= >Index</A>
</FONT>
</TR>
</TABLE>

</BODY>
</HTML>

```

Appendix H. RMON2 and ECAM Protocols

This appendix contains the following sections:

- ECAM Application Decodes
- RMON2 Protocols Overview
- RMON2 Predefined Protocols

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.

For clarity, each protocol appears only once.

Table 45. 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 (see note on page 186)
	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

Table 45. Protocols Associated with One Protocol Family (continued)

Protocol Family	Protocol	Description
DECnet	DEC	DECnet catch-all group (see note on page 186)
	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 (see note on page 186)
	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	Netware Core Protocol
	RIP	Routing Information Protocol
	SAP	Service Advertising Protocol
	SPX	Sequenced Packet Exchange

Table 45. 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 (see note on page 186)
	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

Note: 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.

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 user-defined 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 do not easily conform to the format of the other link-layer branches.
***** Denotes a wildcard protocol prefix that aggregates all link-layer protocols by their layer 2 encapsulated protocol. For example, if IPX is the layer 2 encapsulated protocol:
*.ipx = ether2.ipx + llc.ipx + snap.ipx + wgAssigned.ipx

RMON2 Predefined Protocols

This section shows an example of predefined protocols. 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 46. Statistics Variables Available on Ethernet

Protocols	Protocol Name
802.1-bridge	802.1D Bridge Spanning Tree Protocol

Table 46. Statistics Variables Available on Ethernet (continued)

Protocols	Protocol Name
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
cmail	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-3com	3Com 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

Table 46. Statistics Variables Available on Ethernet (continued)

Protocols	Protocol Name
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
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

Table 46. Statistics Variables Available on Ethernet (continued)

Protocols	Protocol Name
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 47. Predefined Protocols-MAC-Layer Protocol

Encapsulated Protocols	*	ether2.	llc.	snap.	vsnap_ether2.	wgAssigned.
802.1-bridge	✓		✓			
aarp	✓	✓		✓		
arp	✓	✓		✓		
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	✓	✓	✓	✓		

Table 47. Predefined Protocols-MAC-Layer Protocol (continued)

Encapsulated Protocols	*	ether2.	llc.	snap.	vsnap_ether2.	wgAssigned.
ip.icmp	✓	✓	✓	✓		
ip.igrp	✓	✓	✓	✓		
ip.ip	✓	✓	✓	✓		
ip.ip.icmp	✓	✓	✓	✓		
ip.ip.igrp	✓	✓	✓	✓		
ip.ip.opspf	✓	✓	✓	✓		
ip.ip.udp.ccm ail	✓	✓	✓	✓		
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	✓	✓	✓	✓		
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.ccm ail	✓	✓	✓	✓		
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	✓	✓	✓	✓		

Table 47. Predefined Protocols-MAC-Layer Protocol (continued)

Encapsulated Protocols	*	ether2.	llc.	snap.	vsnap_ether2.	wgAssigned.
ip.udp.snmp	✓	✓	✓	✓		
ip.udp.snmptrap	✓	✓	✓	✓		
ip.udp.sunrpc	✓	✓	✓	✓		
ip.udp.sunrpc.nfs	✓	✓	✓	✓		
ip.udp.tftp	✓	✓	✓	✓		
ipx	✓	✓	✓	✓		✓
ipx.nov-echo	✓	✓	✓	✓		✓
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.ccmil	✓	✓	✓	✓		
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	✓	✓	✓	✓		

Table 47. Predefined Protocols-MAC-Layer Protocol (continued)

Encapsulated Protocols	*	ether2.	llc.	snap.	vsnap_ether2.	wgAssigned.
ip.ip.tcp.notes	✓	✓	✓	✓		
ip.ip.tcp.pop3	✓	✓	✓	✓		
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	✓	✓	✓	✓		
ip.udp.ccmil	✓	✓	✓	✓		
ip.udp.dns	✓	✓	✓	✓		
ip.udp.nbt_data	✓	✓	✓	✓		

Table 47. Predefined Protocols-MAC-Layer Protocol (continued)

Encapsulated Protocols	*	ether2.	llc.	snap.	vsnap_ether2.	wgAssigned.
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-3com	✓	✓				
sna	✓	✓	✓*			
vecho	✓	✓	✓*	✓		
vip	✓	✓	✓*	✓		
vip.varp	✓	✓	✓*	✓		
vip.vicp	✓	✓	✓*	✓		
vip.vipc	✓	✓	✓*	✓		
vip.vipc.vipc-dgp	✓	✓	✓*	✓		
vip.vipc.vipc-rdp	✓	✓	✓*	✓		
vip.vrtp	✓	✓	✓*	✓		
vip.vspp	✓	✓	✓*	✓		

Glossary

AC. The Access Control field in a 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 *adapter* 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 adapter. The adapter 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.

beacon. If a problem arises on a token ring, a station might 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 can not 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.

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 might cross onto other networks.

burst error. More severe than a line error, a burst error is usually 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.

collision. The best estimate of the number of collisions on an Ethernet segment.

congestion. Reported by a station on a token ring when it receives a frame and does not have the buffer space to store it. Because we do not report who is flooding this adapter, 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.

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*.

FCS. Frame check sequence. A kind of checksum. An error means that the checksum does not match the contents of the frame.

fragment packet. An Ethernet packet fewer 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 a token ring, token frames are only 3 bytes long, whereas information frames can be over 18 000 bytes.

Frame copy error. Reported by a station on a token ring when it believes another station might 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 adapter on a token ring-from its NAUN-differs from its own internal clock by too much. Often caused by connecting more than 72 stations, and more prevalent in 16 Mb operations. Also known as a *jitter*. A *non-isolating error*.

hop. The process of crossing a bridge between token-rings-a count between 1 and 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*.

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 a 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 does not 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*).

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 might be directed to all bridges on a ring.

NAUN. Nearest active upstream neighbor on a token ring (see *beacon*).

Non-isolating error. A token ring error that *cannot* be pinpointed to a specific station or location on the ring (see also *isolating error*).

oversize packet. An Ethernet packet longer than 1518 octets (including FCS octets) but otherwise well-formed.

packets. The total number of packets detected-including error packets-on a segment.

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.

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.

REM. On a token ring, the Ring Error Monitor-the functional address that error reports are addressed to.

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*.

SD. Starting delimiter-a distinctive byte marking the start of a frame or a token.

short packet. See *undersize packet*.

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.

soft error. On a 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 file server, PC, workstation, printer, or probe.

token error. Reported by the Active Monitor when the token becomes corrupted. Similar to a line error, a token error is also a non-isolating error. A station that transmits many token errors is often not at fault-it is probably the active monitor.

token frame. A station wanting to transmit must first claim the token before doing so. When it has finished, it sends the token to its downstream neighbor, which in turn might hold it or simply pass it on. Token frames are 3 bytes long.

Undersize Packets. An Ethernet packet fewer than 64 octets long (excluding frame bits but including FCS octets) but otherwise well-formed.

Index

A

- Access
 - community access names 33
 - control tables 32
 - security levels 34
- Address Translation Tables 99
- Address Translation View 98
- Alarms View 94
- Application Variables
 - history 162
 - host 165
 - ring station 166
 - statistics 159

B

- Buffers
 - creating new capture 105
 - loading capture 111
 - modifying capture 111
 - working with 105

C

- Capture
 - buffers 105
 - configuring 104
 - launching 103
 - reading packets 118
 - start and stop events 111
- Captured Packet
 - saving and loading 121
- Captured Packets
 - buffers 105
 - configuring 104
 - launching 103
 - reading 118
 - saving and loading 121
 - start and stop events 111
- Cold Reset 30
- Collector
 - address translation level 126
 - configuring data sources 125
 - data collection, starting 131
 - data collection, stopping 130
 - data collections, setting up 127
 - exiting 132
 - interface 16
 - launching 123
 - overview 123
- Community Access Names 33
- Configuring Virtual Interfaces 40
- Conversation Trace and Analysis 120

CSV Files

- history format 171
- host format 172
- matrix format 173
- Token-Ring MAC-Layer data 173
- Token-Ring promiscuous data 175

D

- Data
 - archiving 151
 - collections, setting up 127
 - consolidating 149
 - deleting 150
 - managing 147
- Data Collection
 - date/time settings 27
 - deleting 60
 - importing 56
 - modifying configurations 130
 - starting 57, 131
 - stopping 59, 130
- Database
 - compacting 153
 - creating 135
 - importing 137
 - opening 136
 - repairing 154
 - reports 139
 - selecting 135
 - viewing 138
- Decode
 - conversation trace and analysis 120
 - ECAM application 183
 - launching 117
 - reading captured packets 118
- Default Gateway 29
- Dialog Format 9

E

- ECAM Application Decodes 183
- Events, start and stop 111

F

- Filter Editor
 - templates 115
 - using 113
- Firmware
 - downloading 27
 - versions 26

G

- Granularity 147

Graphs

- event distribution 74
- network statistics 71
- packet rates 70
- packet size distribution 69
- ring status 75
- top 10 hosts by error rate 73
- top 10 hosts by packet rate 72
- top 10 receivers 73

H

- Hardware, versions 26
- History View 84
- Host View 86
- HTML Report Templates 181
- Hysteresis Zone 98

I

Interfaces

- Collector 16
 - Reporter 17
 - Rmonview 9
 - Viewman 7
- IP Address 28

M

- Managing Data 147
- Matrix View 90
- Menu Bar
 - Rmonview 11, 16
 - translator 55
 - Viewman 8

N

- Name Translation Level 62
- Network Statistics 71
- Nways Remote Monitor
 - basics 3
 - overview 1
 - theory of operation 2
 - using 2
- Nways Remote Monitor interface 7

P

Packet

- rates 70
 - size distribution 69
- Packet Capture
- buffers 105
 - configuring 104
 - launching 103
 - reading 118
 - saving and loading 121
 - start and stop events 111
- Packet Capture and Decode 103
- Packet Decode
- conversation trace and analysis 120

Packet Decode (*continued*)

- launching 120
 - reading captured packets 118
- PACMIB, Enabling and Disabling 38
- Performance Guidelines 169

Probes

- access control tables 32
- default gateway 29
- device configuration 21
- IP address 28
- managing 24
- PACMIB 38
- resetting 29
- RMON2 53
- setting up 22
- SmartAgent 53
- static routes 37
- subnet mask 28
- trap communities 34
- user-defined protocols 49
- virtual interfaces 40

Protocol Decodes 157

Protocol Distribution

- launching view 101
- using 100
- viewing tables 101

Protocols

- adding 50
- decodes 157
- deleting 51
- directory 49
- RMON2 and ECAM 183
- updating RMON2 tables 51
- user-defined 49

R

Report Templates, HTML 181

Reporter

- compacting database 153
- generating reports 140
- importing data 137
- interface 17
- launching 134
- overview 133
- repairing database 154
- selecting a database 135
- viewing a database 138

Reports

- descriptions 177
- headers and footers 143
- HTML 143
- HTML templates 181
- loading saved 145
- parameters 140
- previewing 144

Reports *(continued)*
printing 177, 145
saving 143
selecting and generating 139
time period 141

Resetting a Probe 29

RMON

- address translation view 98
- alarms view 94
- configuring 79
- history views 84
- host view 86
- launching applications 77
- matrix view 90
- overview 2
- statistics view 81
- token ring view 92

RMON/RMON2 Tables 44

RMON2 and ECAM Protocols 183

RMON2 Mode, setting 39

RMON2 Protocols

- overview 186
- predefined 186
- updating tables 51

Rmonview

- application display area 14
- dialog format 9
- interface 9
- launching 77
- launching applications 77
- menu bar 11, 16
- toolbar 13

S

SmartAgent Firmware

- Auto-Boot Table 48
- disabling 48
- enabling 47
- maintenance dialog 46
- managing 46

Start and Stop Events 111

Static Routes, setting 37

Station Names, setting up 53

Stations

- automatic detection 53
- launching translator 54
- manual setup 60
- name translation level 62
- vendor prefixes 63

Statistics View 81

Subnet Mask 28

T

Token Ring View 92

Toolbar 13

Trademarks 156

Translator

- launching 54
- main window 54
- menu bar 55

Trap Communities

- control dialog 35
- destination IP addresses 36
- names 36

V

Variables

- history 162
- host 165
- ring station 166
- statistics 159

Vendor Prefixes 63

Viewman

- configuring 66
- graphs 68
- launching 65
- launching applications 78
- menu bar 8

Viewman Interface 7

Views

- address translation 98
- alarms 94
- creating 79
- editing 79
- history 84
- host 86
- matrix 90
- statistics 81
- token ring 92

Virtual Interfaces

- configuring 40
- creating 40
- deleting 44
- predefined channels 41, 42

W

Warm Reset 30



Part Number: 4301549



Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

Nways Management Web site:

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

SA27-4195-02



4301549

