

AIX NetView/6000 LAN Integration

Document Number GG24-4332-00

September 1994

International Technical Support Organization
Raleigh Center

Take Note!

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

First Edition (September 1994)

This edition applies to AIX NetView/6000 V2.1, Program Number (5765-077), which runs under the AIX operating system for RISC System/6000 Version 3 Release 2.5 (5756-030) or later.

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

An ITSO Technical Bulletin Evaluation Form for reader's feed back appears facing Chapter 1. If the form has been removed, comments may be addressed to:

IBM Corporation, International Technical Support Organization
Dept. 985 Building 657
P.O. Box 12195
Research Triangle Park, NC 27709-2195

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

© **Copyright International Business Machines Corporation 1994. All rights reserved.**

Note to U.S. Government Users — Documentation related to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

Abstract

This document describes the integration of AIX NetView/6000 LAN-related products. The perspective of this book is to use AIX NetView/6000 as the graphical user interface and focal point for problem determination and problem resolution. It provides systems programmers and network programmers with background on how to set up their network management environment.

This document was written for users who will be implementing LAN network management in an AIX environment. Some knowledge of LANs, AIX and AIX NetView/6000 is assumed.

(238 pages)

Contents

Abstract	iii
Special Notices	xvii
Preface	xix
How This Document is Organized	xix
Related Publications	xx
International Technical Support Organization Publications	xx
Acknowledgments	xx
Chapter 1. Product Integration Overview	1
1.1 Overview	1
1.1.1 AIX LMU/6000 Network View	4
1.1.2 IBM LAN Network Manager for AIX Network View	5
1.1.3 AIX NetView/6000 Network View	6
1.2 Integration	7
1.2.1 Map Integration	8
1.2.2 Status Propagation	19
1.2.3 Database Integration	21
1.3 Environment	23
1.4 RISC System/6000 TCP/IP Configuration	26
1.5 IBM TCP/IP for OS/2 and Database Manager 2/2 Installation and Configuration	30
1.5.1 TCP/IP Installation and Configuration	31
1.5.2 OS/2 Database Manager 2/2 Installation	38
1.5.3 RISC System/6000 Software Installation Procedures	40
Chapter 2. LAN NetView Management Utilities/6000	43
2.1 AIX LMU/6000 Overview	43
2.1.1 Prerequisites	44
2.1.2 Functionality	44
2.2 AIX LMU/6000 Installation	45
2.3 LMU/2 Installation	46
2.3.1 LMU/2 Installation for OS/2 Stations	46
2.3.2 LMU/2 Installation for DOS Stations	47
2.3.3 LMU/2 Installation for Windows Stations	47
2.3.4 LMU/2 Installation for NetWare Servers	47
2.4 AIX LMU/6000 Configuration	48
2.5 LMU/2 Configuration	49
2.5.1 LMU/2 Configuration for OS/2 Stations	49
2.5.2 LMU/2 Configuration for DOS Stations	54
2.5.3 LMU/2 Configuration for Windows Stations	55
2.5.4 LMU/2 Configuration for NetWare Servers	56
2.6 LMU/2 Startup	57
2.7 AIX LMU/6000 Operation	59
2.7.1 AIX LMU/6000 Submaps	59
2.7.2 Starting the AIX LMU/6000 Program	64
2.7.3 Using the AIX LMU/6000 Program	68
Chapter 3. IBM LAN Network Manager for AIX	75
3.1 Overview	75

3.2 LAN Network Manager Installation	76
3.2.1 LNM for AIX Installation	77
3.2.2 LNM OS/2 Proxy Agent Installation	77
3.3 LAN Network Manager Configuration	80
3.3.1 LNM for AIX Configuration	81
3.4 Starting LAN Network Manager	85
3.4.1 Starting LNM for AIX	86
3.4.2 Starting the OS/2 LNM Proxy Agent	89
3.5 LAN Network Manager Operations	89
Chapter 4. RMONitor for AIX	101
4.1 RMON Installation	102
4.1.1 RMONitor for AIX Installation	102
4.1.2 RMONitor Agent for OS/2 Installation	103
4.2 RMONitor Configuration	107
4.2.1 RMONitor for AIX Configurations	107
4.2.2 RMONitor Agent for OS/2 Configuration	111
4.2.3 Configuring Trap Information	113
4.2.4 Defining Policies	114
4.3 Starting RMONitor	122
4.3.1 Starting RMONitor for AIX	122
4.3.2 Starting RMONitor Agent for OS/2	124
4.3.3 RMONitor Operations	125
Chapter 5. IHMP/6000	139
5.1.1 Highlights of IHMP/6000	139
5.1.2 Description	140
5.2 Intelligent Hub Management Program/DOS Entry	140
5.2.1 Highlights of IHMP/DOS Entry	140
5.3 IHMP/6000 Installation	141
5.4 IHMP/6000 Configuration	142
5.5 IHMP/6000 Startup	144
5.6 IBM Hub Management Program Family for the IBM 8260	151
5.7 IHMP/6000 Version 2	151
Chapter 6. Router and Bridge Manager/6000	153
6.1 RABM/6000 Installation	153
6.2 Router and Bridge Manager/6000 Configuration	154
6.3 Starting Router and Bridge Manager/6000	156
Chapter 7. Trouble Ticket/6000	165
7.1 Capabilities	165
7.1.1 Prerequisites	166
7.1.2 Functionality	166
7.2 AIX Trouble Ticket/6000 Installation	167
7.2.1 AIX Trouble Ticket/6000 Code Installation and Configuration	168
7.2.2 Installing Additional AIX Trouble Ticket/6000 Clients	172
7.3 AIX Trouble Ticket/6000 Startup	174
7.3.1 Starting AIX Trouble Ticket/6000 from IBM Xstation	176
7.4 The Life Cycle of a Trouble Ticket	177
7.4.1 Populating the Inventory Tables	177
7.4.2 Generating Incident Reports from Traps	190
7.4.3 Receiving an Incident Report	193
7.4.4 Opening a Trouble Ticket	196
7.4.5 Assigning Actions	198

7.4.6 Solving the Problem and Closing the Trouble Ticket	201
Chapter 8. Integration Scenarios	205
8.1 A Critical Station on the Network Goes Down	205
8.2 An Unauthorized Adapter Enters the Network	213
8.3 Virus Detected on a DOS/Windows Workstation	222
8.4 Configuring the DOS/Windows Station	223
8.5 Configuring the Fault Manager Station	224
8.6 Preparing AIX NetView/6000 to Receive a Virus-Detected Trap	224
8.7 Automated Actions Against a Virus Detected-Trap	226
Appendix A. LMU-Related File	229
A.1 LMU.CTL File	229
A.2 USERVPD.CFG File	235
A.3 LMU.INI File	236
A.4 LMUBIND.CTL File	236
Index	237

Figures

1.	Complete Network Environment	4
2.	AIX LMU/6000 Network View	5
3.	IBM LAN Network Manager for AIX Network View	6
4.	AIX NetView/6000 Network View	7
5.	AIX NetView/6000 Root Map	9
6.	AIX NetView/6000 Navigation Tree	10
7.	AIX NetView/6000 IP 9.24.104 Submap	11
8.	AIX NetView/6000 LMU Managing System 00000009:40000003342 Submap	11
9.	AIX NetView/6000 LNM 5A980F53 CAU Submap	12
10.	AIX NetView/6000 Node Submap	13
11.	Integration Diagram	14
12.	AIX NetView/6000 Context Pull-Down Menu Options	15
13.	AIX NetView/6000 Protocols	16
14.	AIX LMU/6000 Event Card for Topology Change	17
15.	AIX LMU/6000 Submap	18
16.	AIX LMU/6000 Event Card for Adapter Insertion	18
17.	AIX LMU/6000 8230 Submap	19
18.	AIXAGENT1 Node Submap Protocol Status	20
19.	AIX NetView/6000 Navigation Tree Status Propagation	21
20.	AIX NetView/6000 Database Workstation Details	22
21.	AIX NetView/6000 Database Interface Details	23
22.	AIX NetView/6000 IP Topology	24
23.	RISC System/6000 TCP/IP Configuration Interfaces List	27
24.	RISC System/6000 TCP/IP tr1 Configuration	28
25.	AIX NetView/6000 SNMP Configuration	30
26.	LAPS Installation Initial Screen	31
27.	LAPS Configuration Option	32
28.	LAPS Adapter and Protocol Configuration	33
29.	LAPS Start Update	33
30.	TCP/IP Network Configuration	34
31.	TCP/IP SNMP MIB-II Information	35
32.	TCP/IP SNMP Configuration	36
33.	TCP/IP Hostname and Other Services Configuration	37
34.	TCP/IP Routing Configuration	37
35.	Database Manager 2/2 Installation Initial Screen	38
36.	Database Manager 2/2 Options Installation	39
37.	Database Manager 2/2 Configure Installation	39
38.	Database Manager 2/2 Installation Successful	40
39.	SMIT Initial Installation Screen	41
40.	SMIT Installation Screen	42
41.	Sample List from Input Device Prompt	42
42.	AIX LMU/6000 Management Environment	45
43.	/smit.log File Showing the AIX LMU/6000 Configuration During the Installation Process	46
44.	SMIT Screen for the lmuTopod Daemon Configuration	48
45.	IBM TCP/IP for OS/2 Configuration - REXEC Customization Panel	50
46.	IBM TCP/IP for OS/2 TCP/IP Configuration - Autostart Panel	51
47.	Remote Command Access Control Dialog Box	51
48.	LMUCUST Command Output	54
49.	LMU Managing Station Panel Showing Initial Messages	58

50.	LMU Proxy Agent and SNMPD Panels Showing Initial Messages	59
51.	Root Submap	60
52.	LAN Network Submap	61
53.	LAN Submap	62
54.	LMU/2 Graphical User Interface	63
55.	Node Submap	64
56.	Tool Palette Showing AIX LMU/6000 Icon	65
57.	AIX NetView/6000 Menu Showing AIX LMU/6000 Options	66
58.	AIX NetView/6000 Menu Showing LMU Subagent Test	67
59.	AIX NetView/6000 AIX LMU/6000 Related Events and Warnings	68
60.	AIX LMU/6000 Program Panel	69
61.	Attribute Retrieval Selection Dialog Box	70
62.	AIX LMU/6000 Data Retrieval Output	71
63.	Remote Command Dialog Box	72
64.	Remote Command Output Dialog Box	73
65.	LNM for AIX Install List	77
66.	Adding 802.2 Protocol to Adapter	78
67.	LNM 802.2 Modifications	78
68.	LNM Installation	79
69.	Signon to Local Database	80
70.	LNM Installation Complete	80
71.	LNM for AIX SMIT Options	81
72.	LNM for AIX SMIT Options	82
73.	LNM for AIX SMIT General Configuration	83
74.	LNM OS/2 Proxy Agent Configuration	83
75.	LNM OS/2 Proxy Agent Configuration	85
76.	LNM for AIX Startup	86
77.	LNM for AIX Started	87
78.	LNM for AIX Tasks Part 1 of 2	88
79.	LNM for AIX Tasks Part 2 of 2	89
80.	LNM for AIX Proxy Agent	90
81.	LNM for AIX Proxy Agent Information	92
82.	LNM DLC Startup Values Configuration	93
83.	LNM for AIX Defining a Bridge	94
84.	LNM for AIX Bridge List	94
85.	LNM for AIX Bridge Definitions	95
86.	LNM for AIX Network Map	96
87.	LNM for AIX Segment Details	97
88.	LNM for AIX CAU Details	98
89.	LNM for AIX Events	99
90.	RMONitor for AIX Install List	103
91.	RMONitor Agent for OS/2 Software Installer Screen	104
92.	RMONitor Agent for OS/2 Install Window	104
93.	RMONitor Agent for OS/2 Install Directories	105
94.	RMONitor Agent for OS/2 Disk Space	106
95.	RMONitor Agent for OS/2 Install Successful	106
96.	RMONitor for AIX SMIT Options	108
97.	RMONitor for AIX General Configuration	109
98.	RMONitor for AIX EUI Connection Configuration	110
99.	RMONitor for AIX Add RMONitor Agent for OS/2 IP Address	110
100.	RMONitor Agent for OS/2 Main Window	111
101.	RMONitor Agent for OS/2 SNMP Configuration	112
102.	RMONitor Agent for OS/2 Community Configuration	112
103.	RMONitor Agent for OS/2 Network Configuration	113
104.	RMONitor Agent for OS/2 Save Configuration	113

105.	RMONitor Agent for OS/2 Subscription Table	114
106.	AIX NetView/6000 Starting RMONitor Policy Editor	115
107.	RMONitor for AIX Policy Editor Main Screen	117
108.	RMONitor for AIX Agent Rules	118
109.	RMONitor for AIX All-Ethernet Threshold Rules	119
110.	RMONitor for AIX Some-TokenRing Threshold Rules	120
111.	RMONitor for AIX All_LONG Collection Rules	121
112.	RMONitor for AIX Processes Starting	123
113.	RMONitor for AIX Processes Running	124
114.	RMONitor Agent for OS/2 Network Statistics	125
115.	Starting RMONitor for AIX Network Monitor	126
116.	RMONitor for AIX Network Monitor	127
117.	RMONitor for AIX Active Monitor	128
118.	RMONitor for AIX Agent Profile	129
119.	RMONitor for AIX Ethernet Thruput Threshold Details	130
120.	RMONitor for AIX Token-Ring All Threshold Details	131
121.	RMONitor for AIX Segment Monitor	132
122.	RMONitor for AIX Token-Ring Base Stats Table	133
123.	RMONitor for AIX Host Monitor Window	133
124.	RMONitor for AIX Host Monitor Window	134
125.	RMONitor for AIX Host Monitor Graph	135
126.	RMONitor for AIX Quick Graph Setup	136
127.	RMONitor for AIX Token-Ring Thruput Category Quick Graph	137
128.	RMONitor for AIX All Categories Quick Graph	138
129.	IHMP/6000 Install List	141
130.	AIX NetView/6000 Selecting Administration Options	142
131.	8250 Hub Community Information	143
132.	AIX NetView/6000 Demand Poll	144
133.	8250 Hub Symbol	144
134.	AIX NetView/6000 Additional Menu Options	145
135.	IHMP/6000 Main Screen	145
136.	IHMP/6000 Daemons Status	146
137.	IHMP/6000 Agents Form Window - 8250 Hub Discovered	147
138.	IHMP/6000 8250 Hub Identified	147
139.	AIX NetView/6000 Selecting Modify Symbol Screen	148
140.	AIX NetView/6000 Changing Symbol to Executable	149
141.	AIX NetView/6000 Defining Target for IHMP/6000 Application	149
142.	AIX NetView/6000 Hub Icon as Executable	150
143.	IHMP/6000 Detailed 8250 Hub Display	150
144.	RABM/6000 Install List	154
145.	RABM/6000 Pull-Down Menu Options	154
146.	RABM/6000 Global Definitions	155
147.	RABM/6000 Polling List	157
148.	RABM/6000 Node Monitor	159
149.	RABM/6000 Context Menu	160
150.	RABM/6000 Error Analysis	160
151.	RABM/6000 Protocol Analysis	161
152.	RABM/6000 Graph	162
153.	RABM/6000 Detail Graph Information	163
154.	RABM/6000 Inheriting Read/Write Authority	163
155.	AIX Trouble Ticket/6000 Configuration Panel	168
156.	AIX Trouble Ticket/6000 Access from the AIX NetView/6000 Main Menu	169
157.	Tool Palette Showing AIX Trouble Ticket/6000 Options	170
158.	AIX Trouble Ticket/6000 Configuration Output	171
159.	AIX Trouble Ticket/6000 Client Installation Panel	173

160.	AIX Trouble Ticket/6000 Client Installation Output Messages	173
161.	AIX Trouble Ticket/6000 Control Panel	174
162.	AIX Trouble Ticket/6000 Daemons Status Output	175
163.	AIX Trouble Ticket/6000 Main Panel	176
164.	Example of a Minimum Contact Entry	179
165.	Contact List Dialog Box Updated with the New Entry	180
166.	Contact List Dialog Box with All the Fields Filled	181
167.	AIX Trouble Ticket/6000 Menu Selection to Import Network Resources from AIX NetView/6000	182
168.	Import/Verify Managed Elements Information Window	182
169.	Network Resource List Dialog Box after Importing the Elements	183
170.	Network Resource Detail Dialog Box with the Imported Information from AIX NetView/6000	184
171.	Example of an Organization Detail Dialog Box	185
172.	Organization List Dialog Box Showing the New Organization	185
173.	Example of a Site Detail Dialog Box	186
174.	Site List Dialog Box Showing the New Site	187
175.	Example of a Location Detail Dialog Box	188
176.	Location List Dialog Box Showing the New Location	188
177.	Example of a Vendor Detail Dialog Box	189
178.	Vendor List Dialog Box Showing the New Vendor	190
179.	Example of an Incident Filter Detail Dialog Box	191
180.	The New Incident Filter Rule Shown at the Bottom of the List	192
181.	Dialog Box to Select a Default Incident Reporter	192
182.	Event Card Showing the Trap that Is Going to Be Treated	193
183.	Incident Report List Dialog Box Showing the Trap that Matched the Incident Filter Rule	193
184.	Initial Incident Report Generated from a Trap	194
185.	E-mail Showing the Incident Report Creation	195
186.	Notification List Showing that the Incident Report Was Created	195
187.	Detailed View of the Notification of the Incident Report Creation	196
188.	A New Trouble Ticket with the Incident Report Attached	197
189.	Trouble Ticket List Dialog Box Showing the New Trouble Ticket	198
190.	Action Detail Dialog Box Showing a Hypothetical Situation	199
191.	Action List Dialog Box Showing the New Action	200
192.	Action Assignment Summary Panel	200
193.	Notification Dialog Box Showing that an Action Assignment Has to Be Acknowledged	201
194.	Completion of an Action	202
195.	Recording a Possible Cause of Failure	203
196.	Information Required before Closing a Trouble Ticket	203
197.	Final Status of the Notification Dialog Box	204
198.	LNM Proxy Agent Configuration Pull-Down Menu Options	206
199.	LNM Adapter Monitoring Parameters	207
200.	General Parameters	208
201.	LNM for AIX Station Profile Details	209
202.	LNM for AIX Station List	210
203.	LNM for AIX Environment	210
204.	AIX NetView/6000 trapd.log File	211
205.	AIX NetView/6000 Event Cards	212
206.	AIX NetView/6000 trapd.log File	212
207.	AIX NetView/6000 Event Cards	213
208.	LNM for AIX Access Control Configuration	215
209.	LNM for AIX Restart LNM Proxy Agent	216
210.	LNM for AIX Access Control Parameters	217

211.	LNМ for AIX Context Pull-Down Menu	218
212.	LNМ for AIX Context Pull-Down Menu	219
213.	LNМ for AIX Environment	220
214.	AIX NetView/6000 trapd.log File	221
215.	AIX NetView/6000 Unauthorized Access Event Card	222
216.	AIX NetView/6000 Adapter Removed Event Card	222
217.	Event Configuration Dialog Box Showing the Virus Trap Customized	225
218.	LNМ for AIX Environment	226
219.	LMU/2 GUI Showing the Virus Event Received	227
220.	LMUPOPUP Utility Warning about the Virus	227
221.	Excerpt from the trapd.log File Showing the Virus Trap	228
222.	Event Card Showing Additional Information about the Virus Trap	228

Tables

1. Agent Policies	116
2. Collection Policies	116
3. Reference Table Contents	178

Special Notices

This publication is intended to help AIX and LAN network systems programmers manage their environments from a single graphical interface. The information in this publication is not intended as the specification of any programming interfaces that are provided by AIX NetView/6000, LNM for AIX, LMU/6000, RMONitor for AIX or IHMP/6000. See the PUBLICATIONS section of the IBM Programming Announcement for AIX NetView/6000 V2.1, LNM for AIX, RMONitor, IHMP/6000 and RABM/6000 for more information about what publications are considered to be product documentation.

References in this publication to IBM products, programs or 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 intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent program that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

IBM may have patents or pending patent applications covering 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 the IBM Director of Licensing, IBM Corporation, 208 Harbor Drive, Stamford, CT 06904 USA.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The information about non-IBM (VENDOR) products in this manual has been supplied by the vendor and IBM assumes no responsibility for its accuracy or completeness. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Reference to PTF numbers that have not been released through the normal distribution process does not imply general availability. The purpose of including these reference numbers is to alert IBM customers to specific information relative to the implementation of the PTF when it becomes available to each customer according to the normal IBM PTF distribution process.

The following terms, which are denoted by an asterisk (*) in this publication, are trademarks of the International Business Machines Corporation in the United States and/or other countries:

AIX
NetView
OS/2
RS/6000

IBM
Operating System/2
RISC System/6000
Trouble Ticket

The following terms, which are denoted by a double asterisk (**) in this publication, are trademarks of other companies:

Novell, IPX, NetWare
Intel

Novell, Inc.
Intel Corporation

Other trademarks are trademarks of their respective companies.

Preface

This document is intended to assist individuals with the installation and tailoring of AIX LAN management products that work with AIX NetView/6000. It contains examples and details of product setup and configuration for different LAN management functions.

How This Document is Organized

The document is organized as follows:

- Chapter 1, "Product Integration Overview"

This chapter provides an overview of the AIX NetView/6000 family of products and the agents that run on OS/2 that communicate with the applications.

- Chapter 2, "LAN NetView Management Utilities/6000"

This chapter provides an overview of the LMU functions and how to install, configure and operate LMU/6000 and LMU/2. In addition, it will show how these functions are integrated into AIX NetView/6000.

- Chapter 3, "IBM LAN Network Manager for AIX"

This chapter describes how to use LNM for AIX, and the LNM proxy agent that runs on OS/2 to manage the LAN resources in your network.

- Chapter 4, "RMONitor for AIX"

This chapter describes how to install and configure RMONitor for AIX and RMONitor Agent for OS/2 to analyze the performance of your token-ring and Ethernet LANs. In addition, it shows how these functions are integrated into the AIX NetView/6000 graphical user interface.

- Chapter 5, "IHMP/6000"

This chapter describes the functions of IHMP/6000 and how it can be used with AIX NetView/6000 to manage 8250 and 8260 hubs. The graphical user interface helps with fault, configuration operations and change management.

- Chapter 6, "Router and Bridge Manager/6000"

This chapter describes how to tailor and use the Router and Bridge Manager/6000 program that is integrated into AIX NetView/6000.

- Chapter 7, "Trouble Ticket/6000"

This chapter describes AIX Trouble Ticket/6000 V2 functions and how to use them to help with problem management in an AIX NetView/6000 and LAN environment.

- Chapter 8, "Integration Scenarios"

This chapter describes how all the products mentioned in the previous chapters can be integrated to provide LAN network management solutions.

- Appendix A, "LMU-Related File"

This appendix describes the parameters necessary to set up LMU/6000 and LMU/2 environments.

Related Publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this document.

- *AIX LAN Management Utilities/6000 User's Guide*, SC31-7154
- *Getting Started with LAN Network Manager for AIX*, SC31-7109 (available by year-end 1994)
- *Using LAN Network Manager for AIX*, SC31-7110 (available by year-end 1994)
- *LAN Network Manager for AIX Reference*, SC31-7111 (available by year-end 1994)
- *Using RMONitor for AIX*, SC31-7115
- *Using RMONitor Agent for OS/2*, SC31-7116
- *NS Softcopy Collection Kit*, SK2T-6012
- *AIX Trouble Ticket/6000 User's Guide*, SC31-7160

International Technical Support Organization Publications

- *AIX Trouble Ticket/6000 Examples*, GG24-4014
- *System Management Reference for RISC/6000*, GG24-4115
- *LAN Reference*, GG24-4111

A complete list of International Technical Support Organization publications, with a brief description of each, may be found in:

Bibliography of International Technical Support Organization Technical Bulletins, GG24-3070.

To get a catalog of redbooks, VNET users may type:

```
TOOLS SENDTO WTSCPOK TOOLS REDBOOKS GET REDBOOKS CATALOG
```

How to Order Redbooks

IBM employees may order redbooks and CD-ROMs using PUBORDER. Customers in the USA may order by calling 1-800-879-2755 or by faxing 1-800-284-4721. Visa and Master Cards are accepted. Outside the USA, customers should contact their IBM branch office.

You may order individual books, CD-ROM collections, or customized sets, called GBOFs, which relate to specific functions of interest to you.

Acknowledgments

The advisor for this project was:

Barry Nusbaum
International Technical Support Organization, Raleigh Center

The authors of this document are:

Jerry Badalassi
IBM Australia

Roberto Shigueo Suzuki
IBM Brazil

This publication is the result of a residency conducted at the International Technical Support Organization, Raleigh Center.

Thanks to the following people for the invaluable advice and guidance provided in the production of this document:

Dave Shogren, Rob Macgregor
International Technical Support Organization, Raleigh Center

Martha Crisson and Judith Dietz
NetView/6000, Research Triangle Park, North Carolina

Dan Swango and Lucy Barnhill
LNM for AIX, Research Triangle Park, North Carolina

Joe Loewengruber, Arlindo Chiavegatto
LMU/6000, Research Triangle Park, North Carolina

Jeff Ferla, Bill Layne
RMONitor, Research Triangle Park, North Carolina

Jack Dunston
RABM/6000, Research Triangle Park, North Carolina

Ken Boggs
Trouble Ticket/6000, Research Triangle Park, North Carolina

Request for Feedback

Readers of this document are encouraged to feed back any information or comments regarding *any* of the material in this document. Please send your comments to:

Barry D. Nusbaum
ITSO-Raleigh
VNET: BARRY at WTSCPOK

or: IBM Corporation 585/B657/BB110
Attn: Barry D. Nusbaum
Building 657 Rm BB106
4912 Green Road
Raleigh NC 27604

INTERNET: bnusbaum@vnet.ibm.com

Chapter 1. Product Integration Overview

This chapter provides a brief overview of the IBM* AIX* NetView*/6000 family of products, and related Operating System/2* (OS/2*) products and agents, and describes how they can be integrated to provide a single management workstation console.

1.1 Overview

One benefit of integrating the various applications under a single management system such as AIX NetView/6000 is that these applications can use common functions familiar to AIX NetView/6000 users. Some of these functions are the GUI interface, common commands available to all AIX users, network topology mapping functions, event configuration, and event reporting. The AIX NetView/6000 family of products provide the ability to manage resources beyond the standard IP network, such as:

1. Novell** IPX** or NetBIOS Intel**-based systems by using the AIX LMU/6000 application
2. IBM 6611 Router by using the Router and Bridge Manager/6000 application
3. IBM Intelligent 8250 Hub by using the IBM Hub Management Program/6000 application
4. Token-ring segments, local and remote bridges and IBM 8230s by using the IBM LAN Network Manager for AIX application
5. Network performance by using the RMONitor for AIX application
6. Network problem Management with the AIX Trouble Ticket/6000* application

This provides AIX NetView/6000 users with an outstanding consolidated management console that fits into many mixed multi-vendor environments.

The various products available from IBM fall into two categories:

1. Products that utilize agents and proxy agents:

In these products a central application running on the RISC System/6000* communicates with either an agent or a proxy agent that is distributed throughout the network. The agents perform the routine tasks such as polling and collecting raw data. In addition, the agents perform any necessary processing of this data itself, sending the consolidated information to the central application on the RISC System/6000.

The benefits of this approach are:

- a. To offload the processing that needs to be performed by the central management system
- b. To limit the volume of traffic on a network

The products that we used which fall into this category are:

- IBM LAN Network Manager for AIX, which uses OS/2 as the platform for its LAN Network Manager proxy agent
- AIX LMU/6000, which uses OS/2 as the platform for its LAN NetView Management Utilities for OS/2 proxy agent

- RMONitor for AIX, which uses OS/2 as the platform for its RMONitor Agent for OS/2 agent

2. Products that do not utilize any kind of agent:

In these products a central application running on the RISC System/6000 communicates directly with the devices throughout the network. The device may perform some routine tasks such as polling and collecting raw data, but performs no processing of this data itself. The data is sent to the central application on the RISC System/6000 to perform all the processing.

The products that we used which fall into this category are:

- IBM Hub Management Program/6000, which manages and retrieves the information from the IBM 8250 hub.
- Router and Bridge Manager/6000, which collects the data from the IBM 6611 router.

AIX NetView/6000 distributes the management tasks to each of these products while maintaining a central point to consolidate the management information. All the above products employ the Simple Network Management Protocol (SNMP) to send the management information collected to AIX NetView/6000. SNMP has become the de-facto method for integrating management functions from a variety of devices. SNMP outlines a series of standards so that suppliers of network devices can send information to management systems. Each product however, uses a variety of different protocols to retrieve information from the network:

- AIX LMU/6000 uses either the IBM NetBIOS or the Novell IPX protocols to manage its devices.
- IBM LAN Network Manager for AIX uses the logical link control (LLC) layer of the token-ring architecture to manage the physical network.

This results in the various AIX NetView/6000 family of products providing different views of a complete network; however, you can still view the complete network when the information is consolidated under AIX NetView/6000.

As an example, we will look at the various submap views of this network that are produced by the individual products. The complete network is shown in Figure 1 on page 4. The individual views are described as follows:

- AIX NetView/6000 sees all devices having an IP address, as shown in Figure 4 on page 7. Devices are grouped into their appropriate IP network, which are then displayed on the graphical topology map.
- AIX LMU/6000 views the network as having LAN NetView Management Utilities for OS/2 proxy agents, which in turn manage a series of workstations or servers, as shown in Figure 2 on page 5. These workstations being DOS/Windows, OS/2 or Novell NetWare servers.
- IBM LAN Network Manager for AIX views the network as being token-ring devices including the token-ring bridges and the IBM Controlled Access Units (CAUs), as shown in Figure 3 on page 6. Ethernet segments are identified, but no management information can be retrieved from these segments.

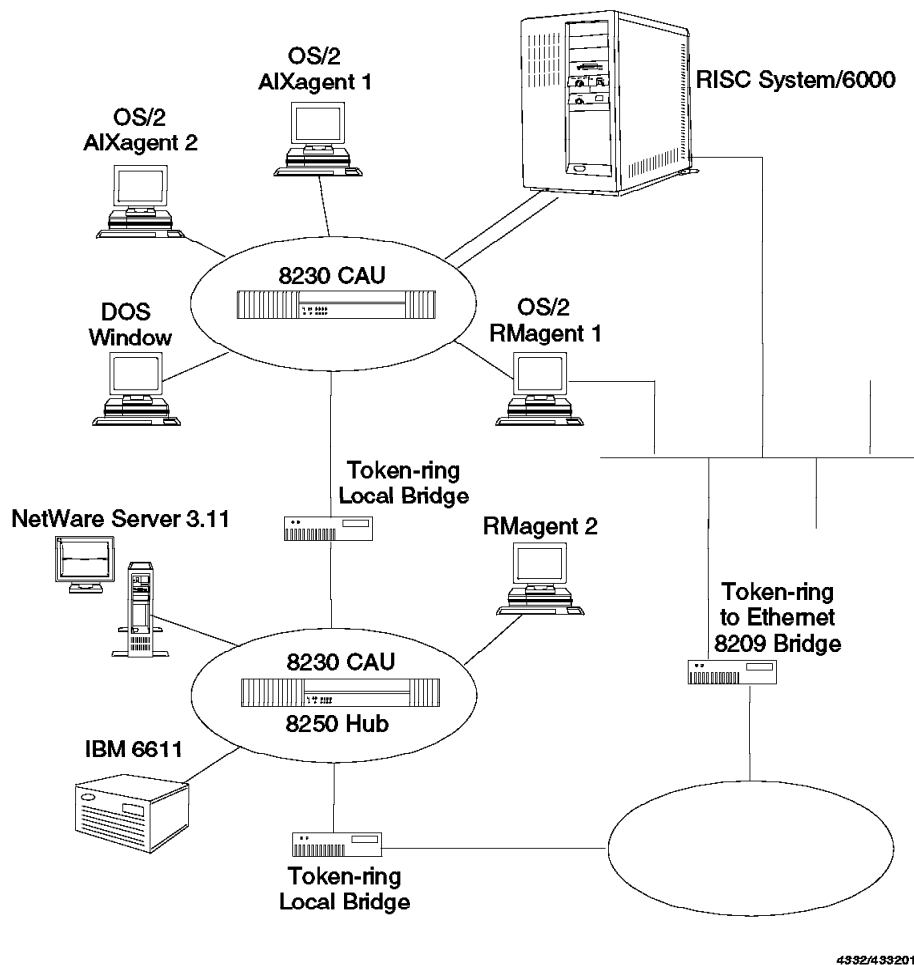
In addition to providing AIX NetView/6000 with the ability to manage beyond an IP network, additional management of certain devices and the network is provided by the following products:

- Performance of the IBM 6611 Router through the Router and Bridge Manager/6000 product
- Graphical configuration of the IBM Intelligent 8250 Hub through the IBM Hub Management Program/6000 product
- Performance monitoring of token-ring and Ethernet segments through the RMONitor product

This provides a thorough single management system with the above products integrated into the AIX NetView/6000 product. AIX NetView/6000 has many more products such as:

- Systems Monitor/6000 - for managing RISC System/6000s
- SNA Manager/6000 - for managing SNA networks
- Trouble Ticket/6000 - for problem management

All these products extend the network management capability of AIX NetView/6000 to manage more diverse networks.



4392/439201

Figure 1. Complete Network Environment

1.1.1 AIX LMU/6000 Network View

AIX LMU/6000's view of the network is based upon the LMU proxy agent and the devices managed by the proxy agent. AIX LMU/6000 manages workstations and servers, retrieves hardware and software inventory, issues commands and monitors the workstation and its applications. The devices that AIX LMU/6000 is able to view in the network are highlighted, as shown in Figure 2 on page 5. These devices are:

- The RISC System/6000 running AIX LMU/6000 (and AIX NetView/6000)
- The LMU proxy agent which is also the managing system

- The managed systems, which are:
 - Proxy agent on an OS/2 workstation
 - DOS/Windows workstation
 - OS/2 workstation
 - NetWare Server 3.11

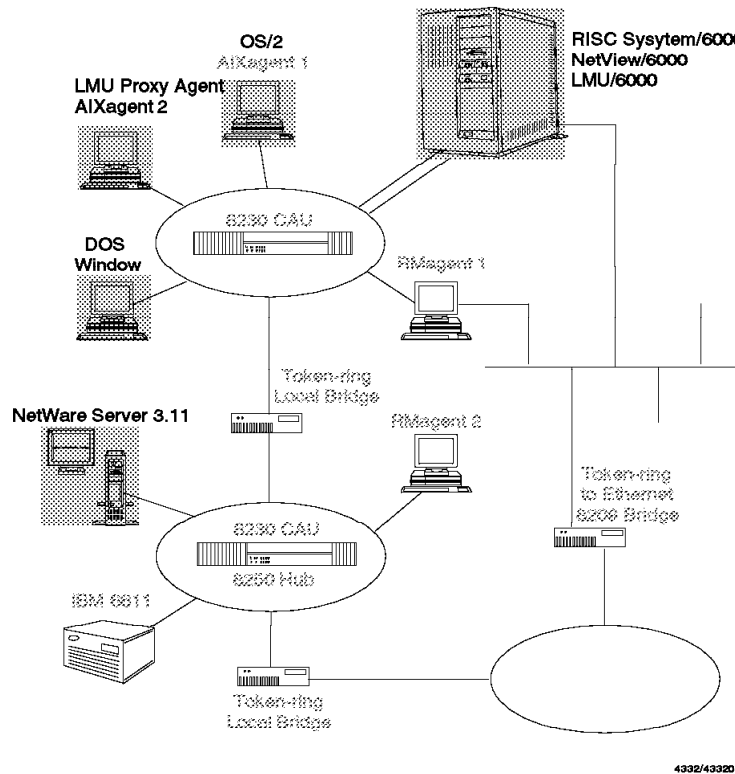


Figure 2. AIX LMU/6000 Network View

1.1.2 IBM LAN Network Manager for AIX Network View

IBM LAN Network Manager for AIX views the token-ring network, utilizing the LNM for OS/2 proxy agent, through the Logical Link Control (LLC) level. The devices that IBM LAN Network Manager for AIX is able to view are highlighted as shown in Figure 3 on page 6. These devices are:

- All token-ring adapters
- Token-ring bridges
- 8230 Controlled Access Units (CAUs)
- Ethernet segments

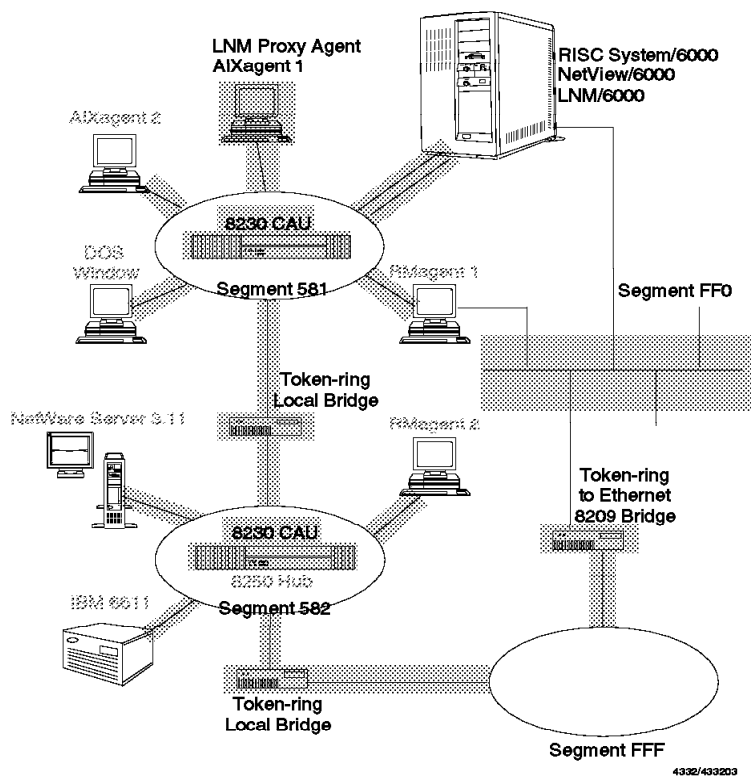


Figure 3. IBM LAN Network Manager for AIX Network View

1.1.3 AIX NetView/6000 Network View

The AIX NetView/6000 base view of the network is based upon the IP protocol. Each device having an IP address is identified and placed into the graphical topology database that AIX NetView/6000 maintains. If the SNMP standard is supported at the device the actual device type can be identified. The devices that AIX NetView/6000 is able to view are highlighted as shown in Figure 4 on page 7. These devices are:

- RISC System/6000 with a hostname of rs60005
- OS/2 workstations with hostnames of
 - aixagent1
 - aixagent2
 - rmagent1
 - rmagent2
- 8250 Hub with a hostname of trmb
- IBM 6611 Router with a hostname of 6611ral

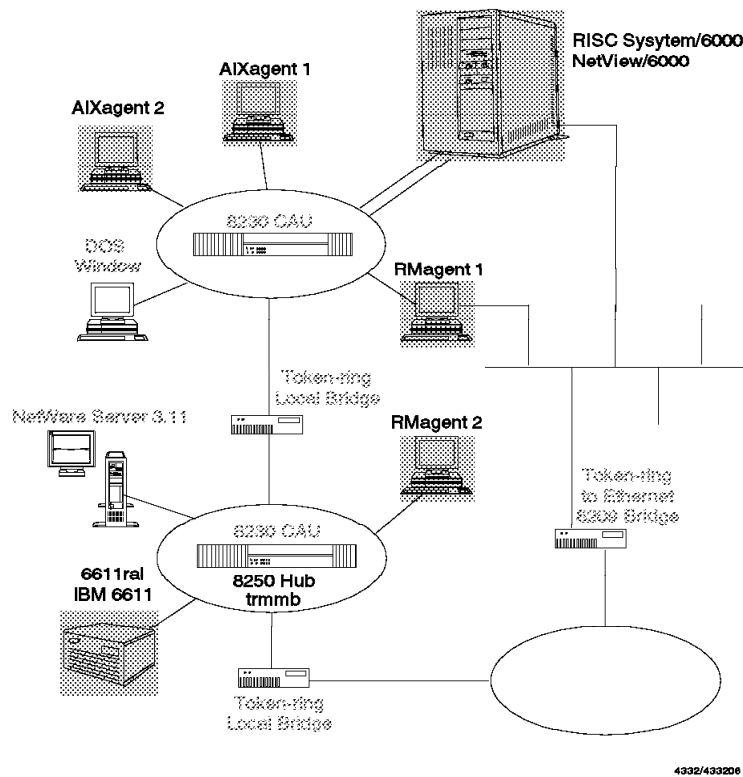


Figure 4. AIX NetView/6000 Network View

1.2 Integration

You can use base AIX NetView/6000 to manage IP nodes and SNMP devices and use the other products in the AIX NetView/6000 family to manage and integrate networks that use other protocols. AIX NetView/6000 provides APIs to allow you to integrate programs that manage resources from different protocols. By using AIX NetView/6000's open technology, this allows:

- Integration and correlation between protocols

A standard part of the open technology is the ability to identify situations where one object appears as a symbol in more than one network protocol, and provides a linkage between them.

If an object uses multiple protocols, as represented by several symbols in different submaps, then a process is triggered that links the symbols representing the different protocols back to the same object. This process also deletes obsolete objects.

- Protocol switching

You can select the list of protocols associated with the object, and then switch to the submap representing the required protocol. This allows you to display the object in the context of the protocol that you are managing.

- Integration with the control desk event cards

When there is an event card displayed, then the source of this event can be highlighted.

- Propagation of status between protocol

AIX NetView/6000's open technology allows for a status change in a protocol symbol to be automatically propagated to the object that is hosting the protocol.

The various components of the AIX NetView/6000 open topology that maintain the integration between the IP topology and the non-IP topology (open topology) are:

- **iptopmd/gtmd:** These two daemons generate and maintain the database that contains topology information: iptopmd for IP, and gtmd for open topology. Each creates its own database based on an abstract model of how a network is constructed.

iptopmd uses an internal IP-specific model, and builds its databases from this, based on information provided by netmon. gtmd uses the IBM open topology model to build its database using information from specifically formatted traps. Both daemons create and maintain entries in the object database, combining the information if the same object is being referenced.

- **ipmap/xxmap:** These two background processes are started whenever a user starts the AIX NetView/6000 GUI. They take information from the object database and the topology databases (ipmap for IP, xxmap for open topology) and convert it into submap and symbol definitions. They remain active, and are responsible for maintaining symbol status. xxmap additionally provides the symbol correlation and protocol switching function described above.

All that an application has to do to create a set of submaps depicting its own network topology, is send traps to gtmd. The format of these traps, and the MIB objects encoded within them, are all defined in the open topology MIB.

IBM LAN Network Manager for AIX and AIX LMU/6000 use this open technology to provide the integration of the protocols and environment that they manage into the AIX NetView/6000 application.

1.2.1 Map Integration

During the discovery process, AIX NetView/6000, AIX LMU/6000 and LNM for AIX each find the interface that is appropriate for their environment. In the case of of:

- AIX LMU/6000, AIX NetView/6000 starts the *ImuTopod* daemon to talk to the LMU SNMP proxy agent and discovers LMU clients using the IPX or NetBIOS protocol.
- IBM LAN Network Manager for AIX, AIX NetView/6000 starts the *Inm6kd* daemon to talk to the LNM SNMP proxy agent and discovers all token-ring adapters.
- AIX NetView/6000 uses the IP discovery process and identifies the IP address of the workstations.

This information is saved in the AIX NetView/6000 topology, providing the ability to navigate through each protocol to interrogate the workstation.

The root map contains the three topology views as shown in Figure 5, that is LMU/6000, IBM LAN Network Manager for AIX known as ITSCLAN and the AIX NetView/6000 IP internet.

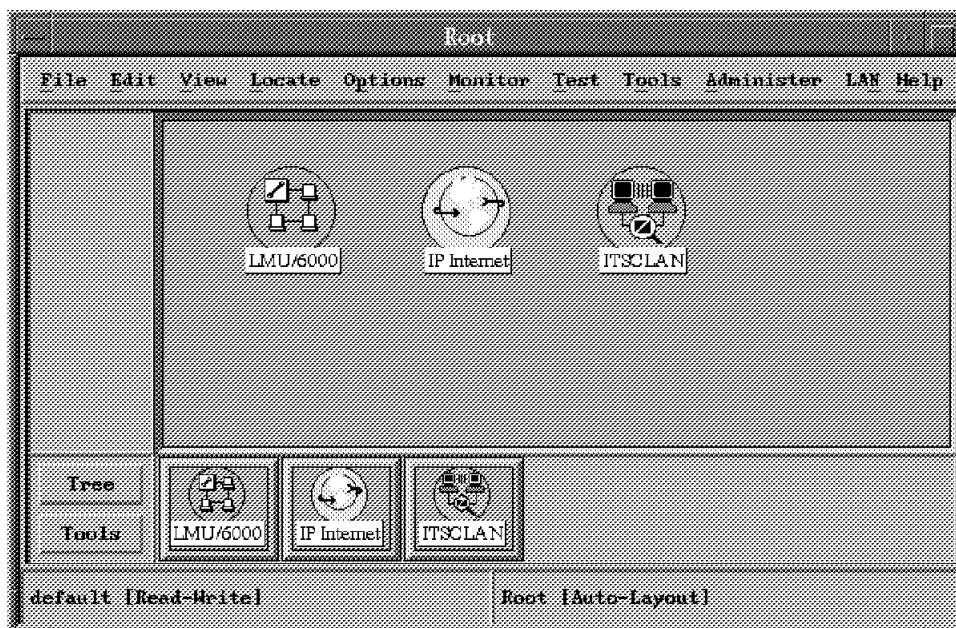


Figure 5. AIX NetView/6000 Root Map

Each of these views provides its own management and topology information. We will look at the workstation AIXAGENT1 which has all 3 protocols as follows:

- An IP address of 9.24.104.54, which belongs in the IP topology map as node aixagent1.
- The LMU client code installed, which belongs in the LMU topology as node 00000009:400000033322.
- A token-ring adapter installed, which is discovered by LNM for AIX and displayed in the LNM for AIX topology as node 400000033322.

The navigation tree screen shown in Figure 6 on page 10 shows the path to the various submaps that apply to this workstation. The various paths are:

1. IP

- IP Internet - displays all the IP networks and routers that AIX NetView/6000 has discovered.
- IP network 9.24.104 - displays an overview of this IP network identifying all the routers into this network.
- Segment1 - displays all devices belonging to this segment; AIXAGENT1 is displayed on this IP submap and identified as aixagent1.

2. LMU

- LMU/6000 - displays all the LMU proxy agents connected to this system.
- Managing System 00000009:400000033342 - displays all LMU clients connected to this LMU managing system. AIXAGENT1 is displayed in its submap, identified as node 00000009:400000033342.

3. LNM

- ITSCLAN - displays all the LNM proxy agents connected to this system.
- LABLAN - displays the LAN that this proxy agent is managing, which includes the token-ring and Ethernet segments and bridges.
- 581 - displays a detailed view of token-ring segment 581. This shows the IBM Controlled Access Units (CAUs) and workstations.
- 5A980F5E - displays the adapters attached to this CAU. AIXAGENT1 is displayed on this submap and is identified as node 400000033342.

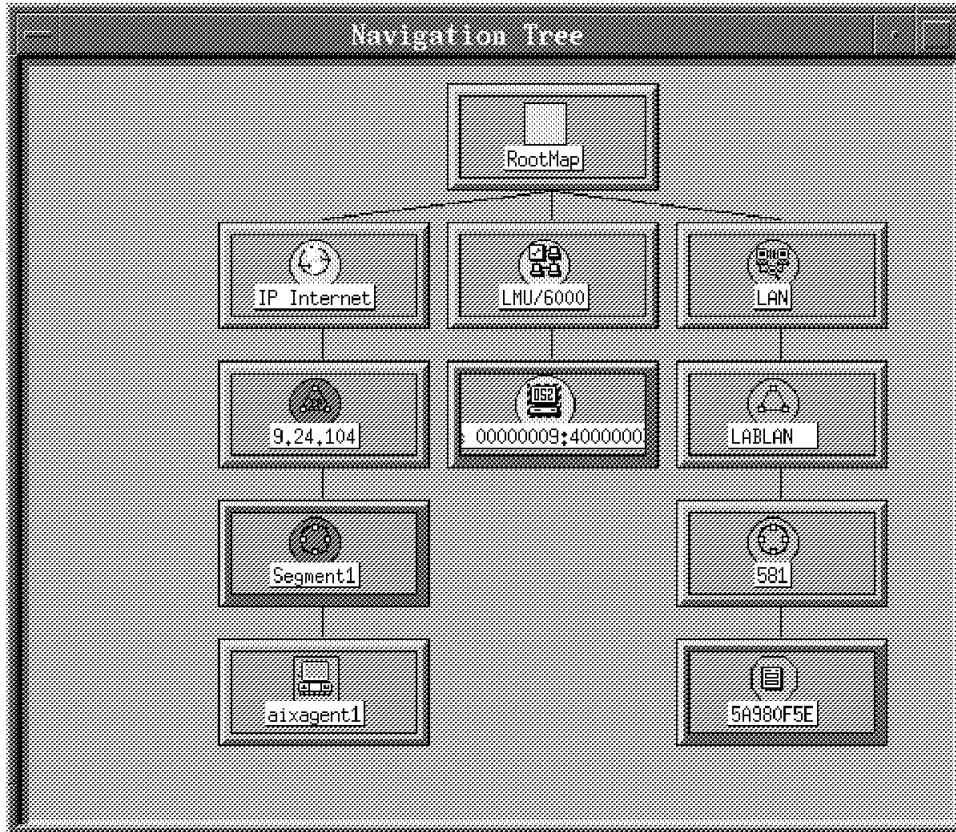


Figure 6. AIX NetView/6000 Navigation Tree

We will now look at the individual submaps that apply to the AIXAGENT1 workstations as described above.

AIXAGENT1 in the IP Topology: In Figure 7 on page 11 the AIXAGENT1 workstation is labeled as *aixagent1*, since this is the IP host name for that workstation.

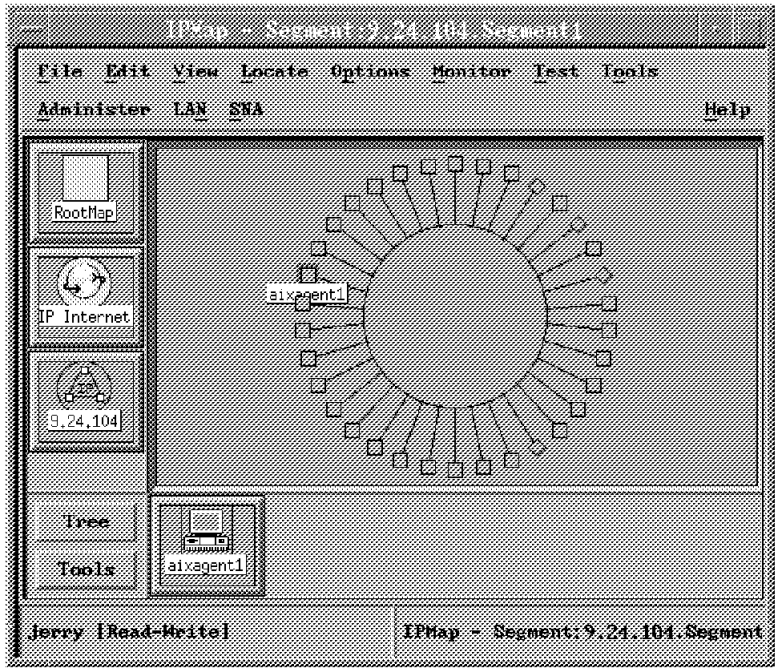


Figure 7. AIX NetView/6000 IP 9.24.104 Submap

AIXAGENT1 in the LMU Topology: In Figure 8 the AIXAGENT1 workstation is labeled 00000009:400000033322, since this is the Novell NetWare name for that device. In our environment the Novell IPX protocol was used.

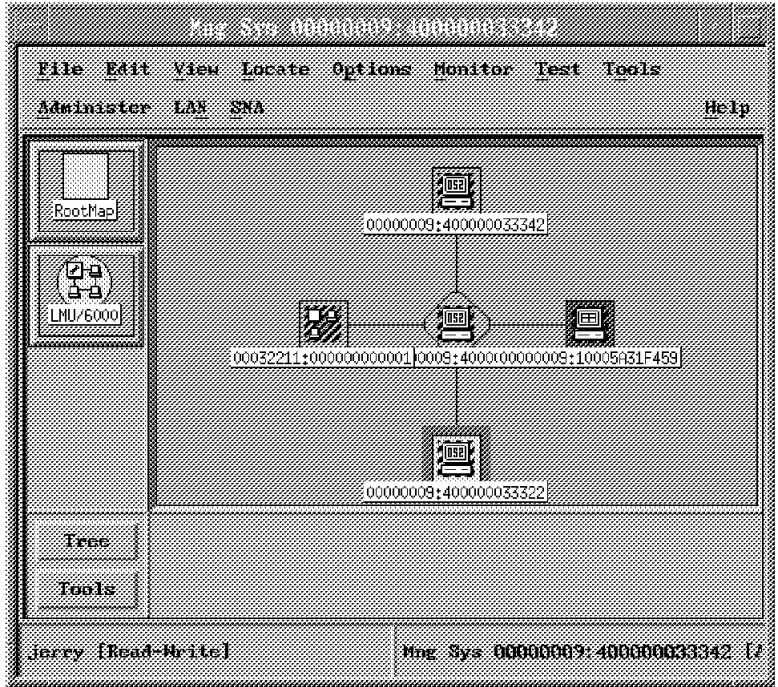


Figure 8. AIX NetView/6000 LMU Managing System 00000009:400000033342 Submap

AIXAGENT1 in the LNM Topology: In Figure 9 on page 12 the AIXAGENT1 workstation is labeled 400000033322. This is the MAC address (in our environment the Locally Administered Address - LAA) of the token-ring adapter in that workstation.

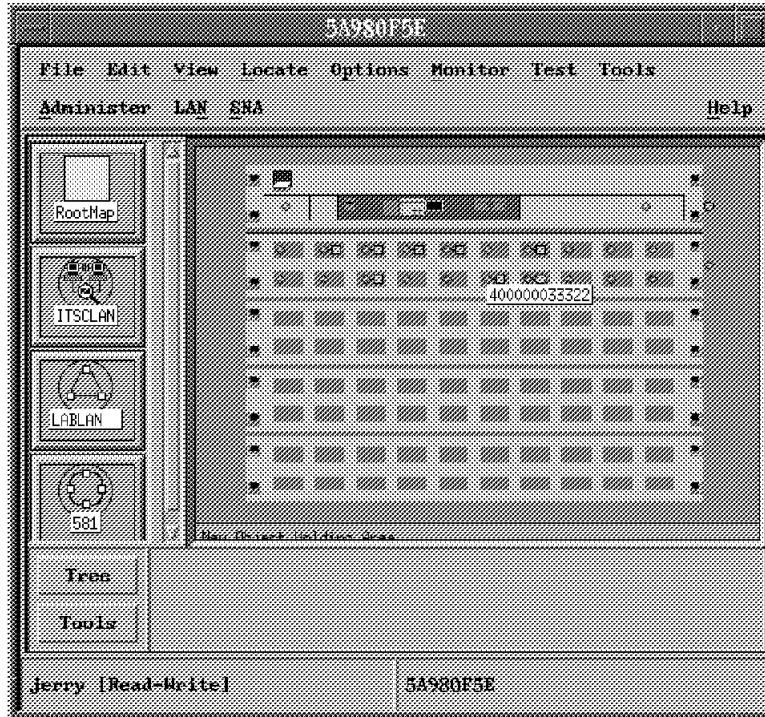


Figure 9. AIX NetView/6000 LNM 5A980F53 CAU Submap

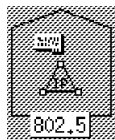
From any of the submaps shown in Figure 7 on page 11 through Figure 9, you can display the node submap of this workstation. An example of this is shown in Figure 10 on page 13. As can be seen in this node submap the three protocols that manage this workstation are combined, thus providing an integrated view of this workstation.

The submaps displayed on the left side of this screen indicate that the integration of the various protocols has been maintained in the IP node submap. The LMU and LNM Node submaps for this workstation have been deleted.



Figure 10. AIX NetView/6000 Node Submap

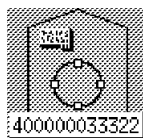
Each icon in the node submap represents:



AIX NetView/6000 IP Information - In this case an IP network using 802.5 (token-ring)



AIX LMU/6000 Name - In this case it is an OS/2 Novell requestor



IBM LAN Network Manager for AIX MAC Address - In this case in a token-ring network with a MAC address of 400000033322

The above environment is summarized in Figure 11 on page 14. At the root submap level all three management environments are displayed. By viewing

each of these environments the AIXAGENT1 workstation will be displayed in the appropriate submap for each protocol. The node submap for the workstation will display all three protocols combined into one submap, with the other two node submaps being deleted. If IP, LMU and LNM are used, the combination is then made using the IP node submap and deleting the LMU and LNM node submaps. The parent of this node submap can be found by going up the IP tree.

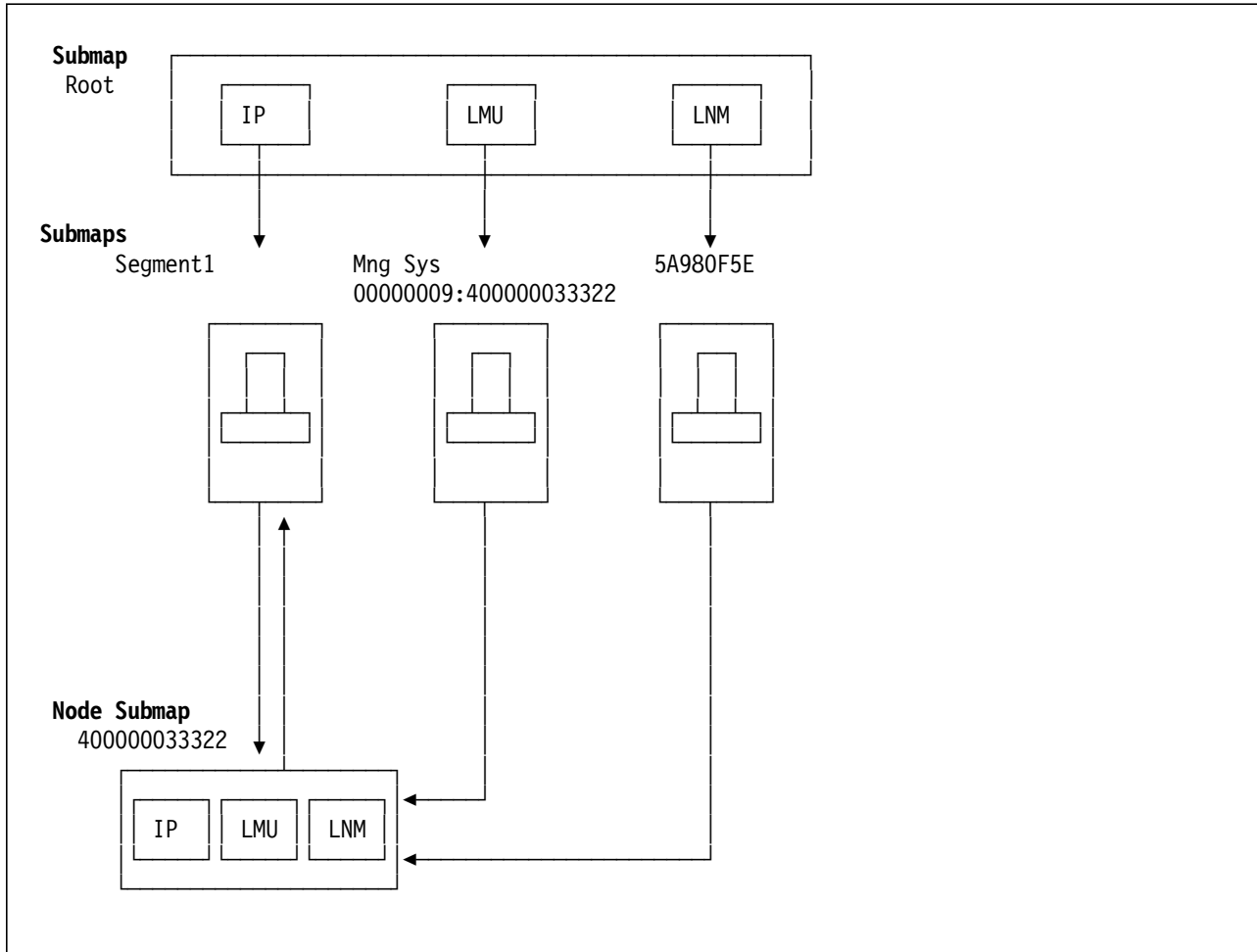


Figure 11. Integration Diagram

1.2.1.1 Context Menu Integration

Wherever this station appears on the AIX NetView/6000 topology the context menu is aware of all the protocols that this station supports. To display the context menu use the right button of the mouse and click on the individual node as shown in Figure 12 on page 15.

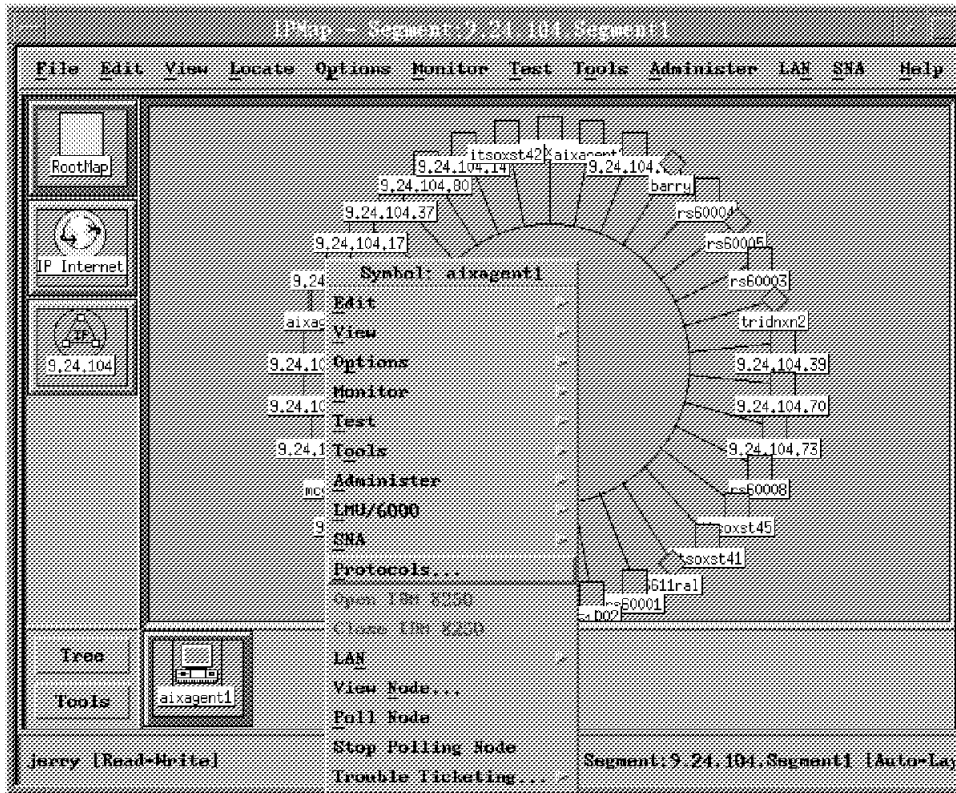
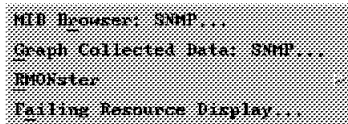
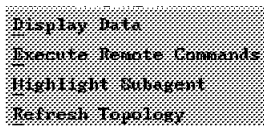


Figure 12. AIX NetView/6000 Context Pull-Down Menu Options

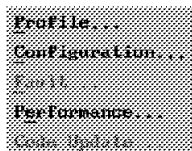
Since AIXAGENT1 has all three protocols, the following context menus are enabled:



Options specific to the AIX NetView/6000 IP environment such as MIB Browser, SNMP (as shown in this submenu) and Demand Poll, which is in the test submenu are available to this symbol.



Options specific to the AIX LMU/6000 environment such as Display Data, Remote Command Execution, Highlight Subagent and Refresh LMU Topology, are available for this symbol.



Options specific to the IBM LAN Network Manager for AIX environment such as Profile, Configuration, Fault, Performance and Code Update, are available to this symbol. Only certain options on this submenu are available depending on the type of node this workstation is defined as, such as a bridge, LAN segment or a node with a token-ring adapter.

This information is controlled by the registration files in the /usr/OV/registration/C directory. These files contain the rules that determine which options are enabled for each node using the context menus. For:

- AIX LMU/6000 the file is lmu6000.reg
- LNM for AIX the file is lnlnmemgr.reg

1.2.1.2 Protocol Integration

To display the protocols supported by this workstation, select the **Protocols** option from the context menu as shown in Figure 12 on page 15.

The Protocols screen displayed in Figure 13 shows all the protocols and submaps for this workstation. There are 2 entries for each of the three protocols visible at this workstation.

IP Identified with the IP entries in the protocol list with two entries having the values (addresses) 9.24.104.54 (IP address) and aixagent1 (hostname).

LMU/6000 Identified with the LMU6000_CLI entries in the protocol list with two entries having the same value 00000009:400000033322. This is the Novell network and MAC address of this workstation.

IBM LAN Network Manager for AIX Identified with the LANTR and IEEE 802.5 token-ring entries in the protocol list the value being 9.24.104.54-581-5A980FE-1-17-400000033322 (the LANTR entry has INTERFACE at the end of this value). This value is derived as follows:

- 9.24.104.54: IP address of the LNM proxy agent
- 581: LAN segment this workstation is on
- 5A980FE: IBM CAU this workstation is on
- 1-17: LAM and port number on the IBM CAU
- 400000033322: The MAC address of this workstation

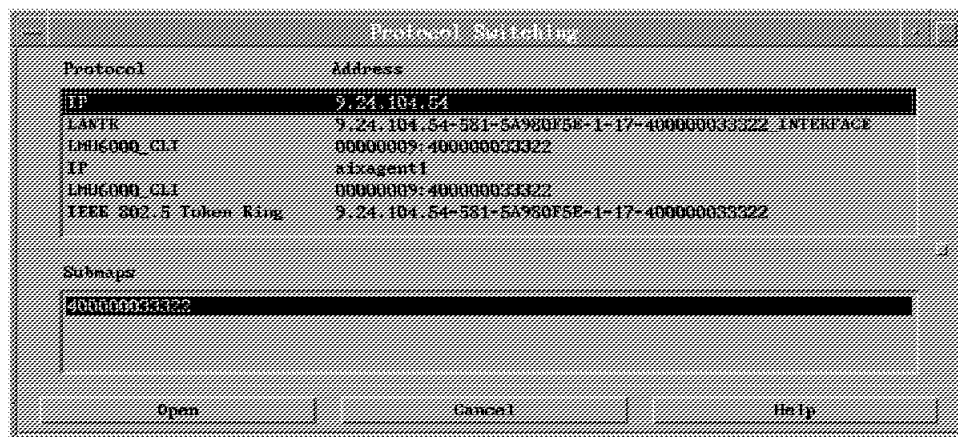


Figure 13. AIX NetView/6000 Protocols

The top three entries refer to the protocols available at the node. The submap these entries belong to is the node submap 400000033322, as shown in Figure 10 on page 13.

The bottom three entries refer to the submap for this workstation in the individual protocols, providing the ability to display the object in the context of that protocol as follows:

- The IP protocol displays this node in the Segment1 submap, as shown in Figure 7 on page 11
- The LMU6000_CLI protocol displays this node in the AIX LMU/6000 Managing System 00000009:40000033342 submap, as shown in Figure 8 on page 11
- The IEEE 802.5 token-ring protocol displays this node in the LNM for AIX CAU 5A980F5E submap, as shown in Figure 9 on page 12

1.2.1.3 Event Card Integration

Traps are displayed on the AIX NetView/6000 event cards for each of the applications integrated into AIX NetView/6000. We will show an event card from the AIX LMU/6000 and IBM LAN Network Manager for AIX applications and demonstrate the ability to display the device that generated the error in the appropriate submap.

Following is an event card displayed from AIX LMU/6000, as shown in Figure 14. In this instance an LMU topology change was identified.

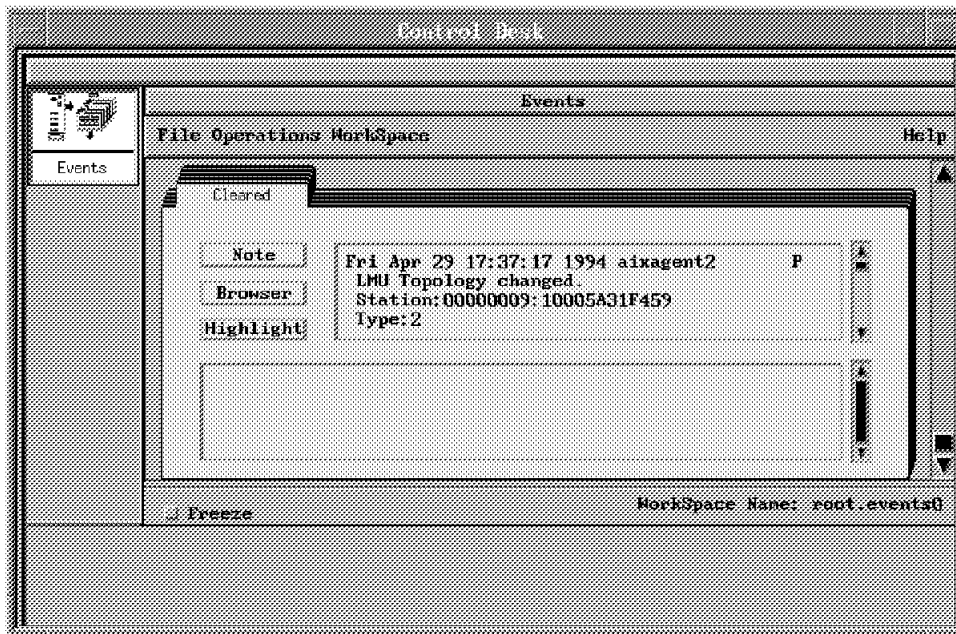


Figure 14. AIX LMU/6000 Event Card for Topology Change

By choosing the *Highlight* option on the event card the appropriate submap for this device is found and displayed, as shown in Figure 15 on page 18. Notice also that the device is highlighted on the submap to provide easier identification.

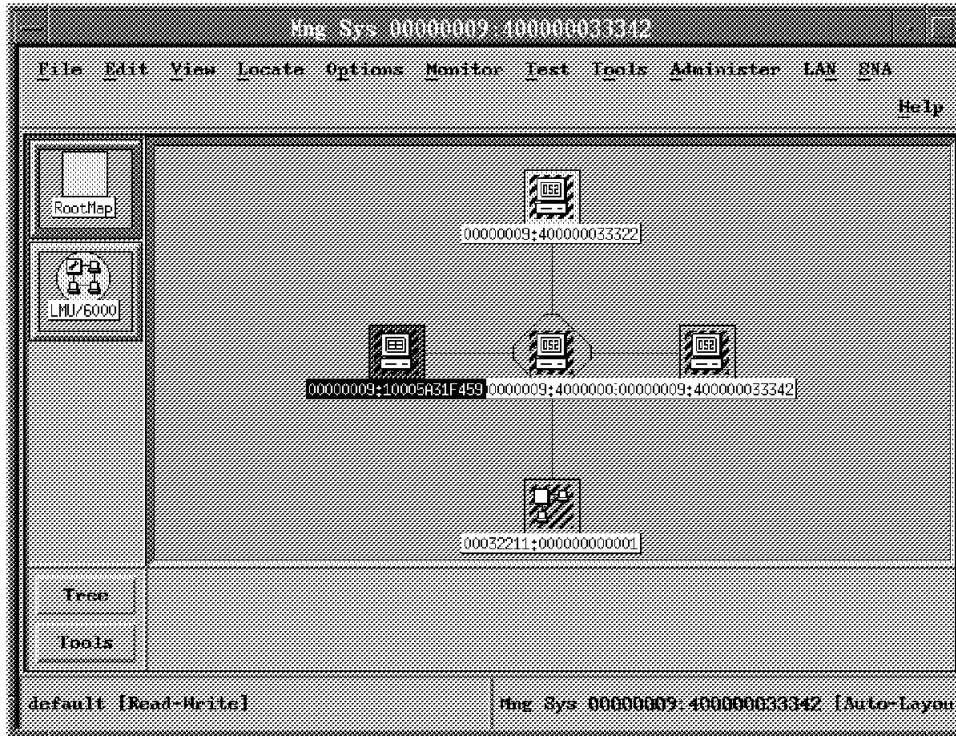


Figure 15. AIX LMU/6000 Submap

Following is an event card displayed from IBM LAN Network Manager for AIX, as shown in Figure 16. In this instance an adapter was inserted into LAN segment 582.

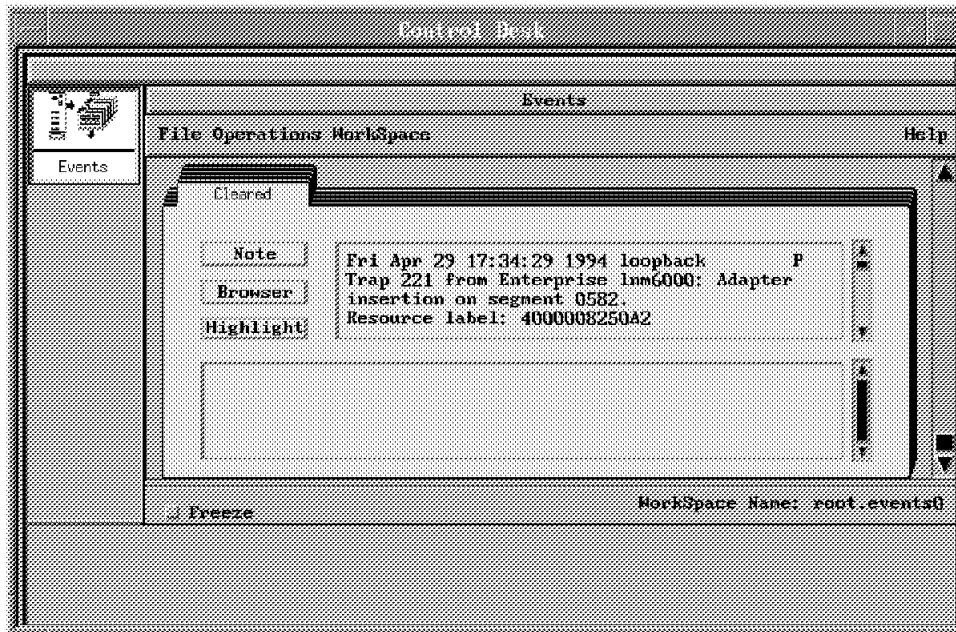


Figure 16. AIX LMU/6000 Event Card for Adapter Insertion

By choosing the *Highlight* option on the event card the appropriate submap for this device is found and displayed, as shown in Figure 17 on page 19. The device is highlighted on the port that it is attached to on the 8230.

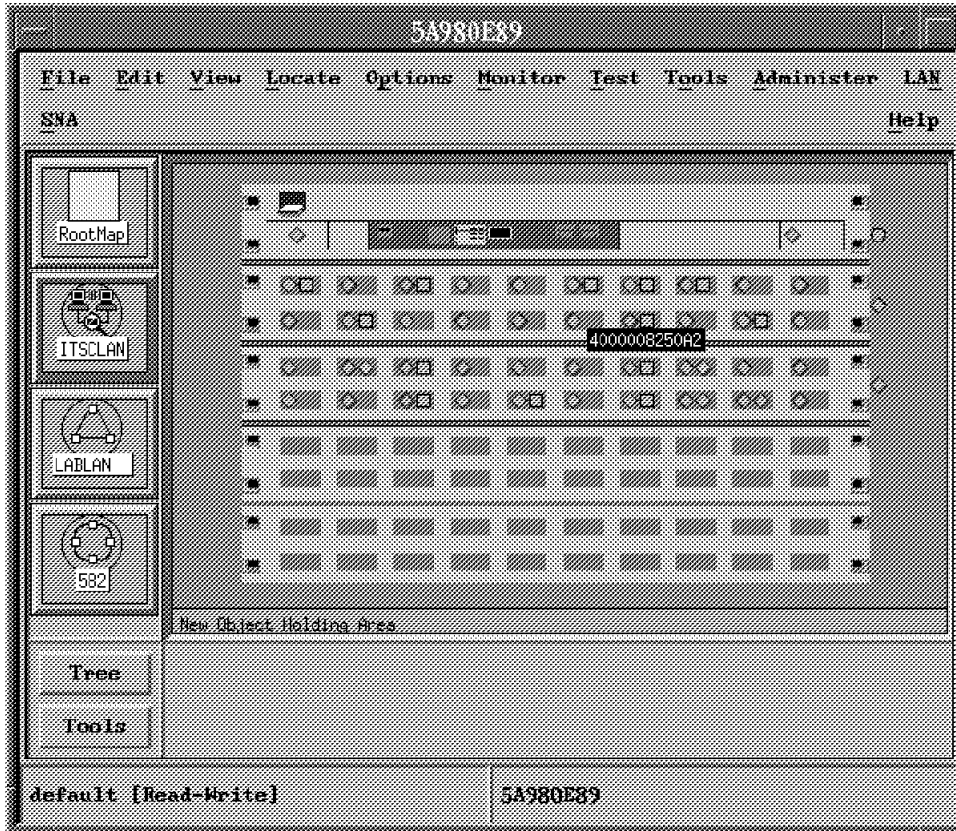


Figure 17. AIX LMU/6000 8230 Submap

1.2.2 Status Propagation

With one workstation being represented in three submaps and having the protocol symbols of each, the status of each protocol is automatically propagated to the parent submaps related to the protocol.

In our environment each protocol for symbol AIXAGENT1 is in the following state, as shown in Figure 18 on page 20:

Value	Status
802.5	Status is green
00000009:40000033342	Status is red
40000033322	Status is blue



Figure 18. AIXAGENT1 Node Submap Protocol Status

The respective submaps that aixagent belongs to are in the following states due to the propagation of the status for each protocol, as shown in Figure 19 on page 21:

Submap	Status
<i>Segment1 Submap</i>	Status is green. This is because all other devices within this IP segment are also green.
<i>Mng Sys 00000009:400000033342 Submap</i>	Status is yellow. Since all other devices in this submap are green and the AIXAGENT1 workstation is red, the aggregate submap becomes yellow.
<i>IBM LAN Network Manager for AIX - 5A980F5E CAU Submap</i>	Status is blue. Since the communication link with the proxy agent is disabled all other devices are also blue.

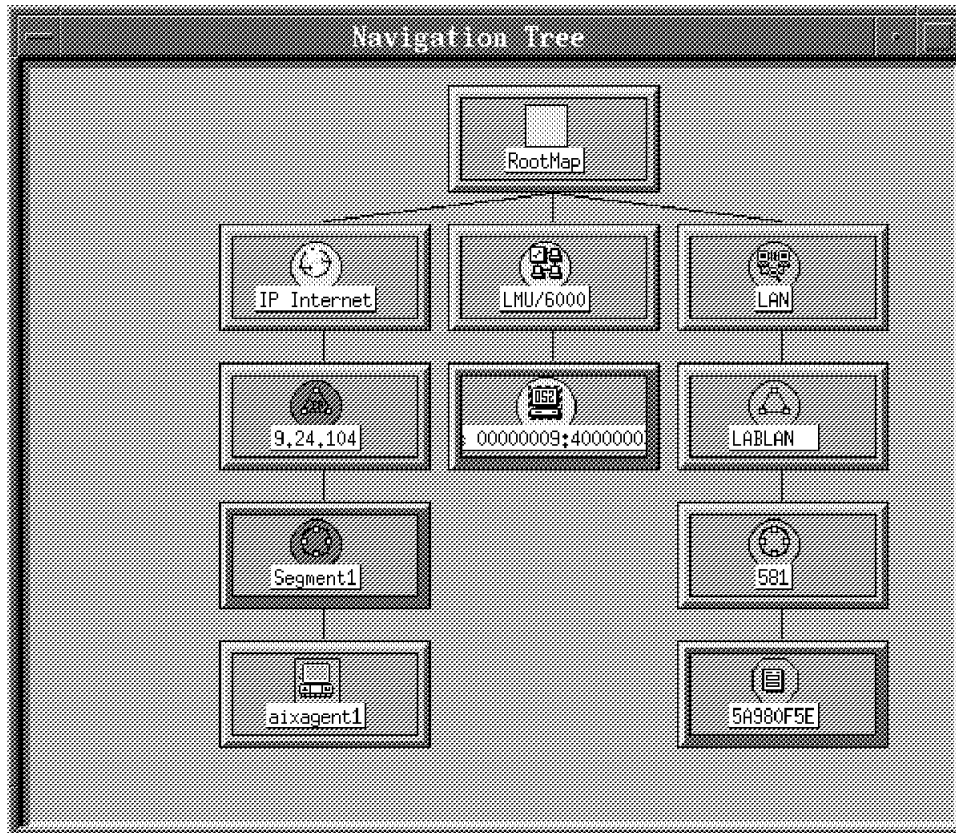


Figure 19. AIX NetView/6000 Navigation Tree Status Propagation

The status of the AIXAGENT1 workstation is determined by the last status change of any protocol within AIXAGENT1. This workstation is displayed in only one area, as a child submap to the IP submap as shown in the navigation tree in Figure 19. Its current status is blue since the IBM LAN Network Manager for AIX protocol was the last status change on the workstation.

1.2.3 Database Integration

The integration shown within the AIX NetView/6000, AIX LMU/6000 and LNM for AIX applications is made possible by the information entered into the AIX NetView/6000 database through the open technology MIB. The four components entered into the database about individual workstations are:

1. IP information - IP address and name
2. LMU information - LMU6000_CLI name
3. LNM information - LANTR and IEEE 802.5 token-ring address
4. Common information shared amongst all protocols

The following output shows the information added into the AIX NetView/6000 database for the AIXAGENT1 workstation. This workstation has two entries in the AIX NetView/6000 database.

1. The workstation details (selection name is aixagent1)

The definition of this workstation with information about the various protocols managing this workstation and the type of workstation

2. The interface details (selection name is 400000033322)

Since AIXAGENT1 has only one adapter interface into the network all three protocols use this interface. The information in the NetView/6000 database for this resource contains lots of details about the workstation.

The information relevant to each protocol is:

FIELD ID	FIELD NAME	FIELD VALUE
10	Selection Name	"aixagent1"
1	11 IP Hostname	"aixagent1"
14	OVW Maps Exists	1
15	OVW Maps Managed	1
19	IP Status	Normal(2)
22	isIPRouter	FALSE
32	isSNMPSupported	TRUE
1	34 SNMP sysDescr	"OS/2 SNMP AGENT version 1.2, with DPI version 1.1 06 (Oct 11, 1993)"
1	35 SNMP sysLocation	"IBM ITSC Raleigh Bld 657"
1	36 SNMP sysContact	"Jerry Badalassi"
1	37 SNMP sysObjectID	"1.3.6.1.4.1.2.2.1.2.2"
1	38 SNMPAgent	IBM TCPIP OS2(8)
42	vendor	IBM(1)
52	isNode	TRUE
54	isComputer	TRUE
55	isConnector	FALSE
56	isBridge	FALSE
57	isRouter	FALSE
58	isHub	FALSE
60	isPC	TRUE
61	isWorkstation	TRUE
75	isSoftware	TRUE
76	isIP	TRUE
80	TopM Interface Count	1
86	TopM Interface List	"802.5 Up 9.24.104.54.0 0x400000033322 ieee 802.5 tokenRing"
90	isXXMAP	TRUE
92	isBox	TRUE
95	isGraph	FALSE
97	XXMAP Protocol List	"IP" "LMU6000_CLI" "IEEE 802.5 Token Ring"
117	XXMAP Layout Algorithm	Row Column(7)
2	118 isLMU6000_CLI	TRUE
2	120 LMU6000_CLI Name	"00000009:400000033322"
2	121 LMU6000_CLI Management Address	"9.24.104.55"
3	126 isLNM	TRUE
3	169 isLNME	TRUE
1	526 IP Name	"aixagent1"
1	655 default IP Symbol List	82
2	669 LMU6000_CLI Management Extension	"1.3.6.1.4.1.2.6.14.1"
3	690 IEEE 802.5 Token Ring Name	"9.24.104.54-581-5A980F5E-1-17-400000033322"
3	692 isIEEE 802.5 Token Ring	TRUE
3	694 default LMU6000_CLI Symbol List	178
3	716 IEEE 802.5 Token Ring Management Address	"9.24.104.54- - -400000033322-581- - "
3	750 default IEEE 802.5 Token Ring Symbol List	424

Figure 20. AIX NetView/6000 Database Workstation Details

- **1** - IP specific information
- **2** - LMU specific information
- **3** - LNM specific information
- Where the entry is blank, this information is common to all protocols

FIELD ID	FIELD NAME	FIELD VALUE
10	Selection Name	"400000033322"
14	OVW Maps Exists	1
15	OVW Maps Managed	1
1 17	IP Address	"9.24.104.54"
1 18	IP Subnet Mask	"255.255.255.0"
1 19	IP Status	Normal(2)
1 39	SNMP ifType	IEEE 802.5 Token Ring(9)
1 40	SNMP ifPhysAddr	"0x400000033322"
1 41	SNMP ifDescr	"802.5"
61	isWorkstation	TRUE
67	isCard	TRUE
68	isInterface	TRUE
76	isIP	TRUE
82	TopM Network ID	522
83	TopM Segment ID	523
84	TopM Node ID	577
90	isXXMAP	TRUE
91	isVertex	TRUE
97	XXMAP Protocol List	"IP" "LANTR" "LMU6000_CLI"
98	XXMAP SAPs Used List	9 0 1
99	XXMAP Protocol Members	58 79
2 118	isLMU6000_CLI	TRUE
2 121	LMU6000_CLI Management Address	"9.24.104.55"
2 122	LMU6000_CLI Address	"00000009:400000033322"
3 126	isLNM	TRUE
3 169	isLNME	TRUE
1 655	default IP Symbol List	83
2 666	Other Address	"400000033322"
2 669	LMU6000_CLI Management Extension	"1.3.6.1.4.1.2.6.14.1.1"
2 671	LMU6000_CLI Operational State	Enabled(2)
2 672	LMU6000_CLI Unknown Status	FALSE
2 673	LMU6000_CLI Availability Status	0
2 674	LMU6000_CLI Alarm Status	1
2 675	LMU6000_CLI Status	Normal(2)
2 694	default LMU6000_CLI Symbol List	179
3 698	IEEE 802.5 Token Ring Address	"400000033322"
3 717	LANTR Address	9.24.104.54-581-5A980F5E-1-17-400000033322_INTERFA
3 719	isLANTR	TRUE
3 720	LANTR Management Address	"9.24.104.54- - -400000033322-581- -"
3 721	LANTR Operational State	Enabled(2)
3 722	LANTR Unknown Status	FALSE
3 723	LANTR Availability Status	0
3 724	LANTR Alarm Status	0
3 725	LANTR Status	Normal(2)
3 726	LANTR SAP Protocols Provided	List 9
3 752	default LANTR Symbol List	425

Figure 21. AIX NetView/6000 Database Interface Details

- **1** - IP specific information
- **2** - LMU specific information
- **3** - LNM specific information
- Where the entry is blank, this information is common to all protocols

1.3 Environment

Our IP network is represented in Figure 22 on page 24. The three main IP networks used and the devices on these networks were:

1. IP network 9.24.104, (subnet mask 255.255.255.0)
 - RISC System/6000 with IP address 9.24.104.25, known as rs60005
 - OS/2 system with IP address 9.24.104.54, known as aixagent1
 - OS/2 system with IP address 9.24.104.55, known as aixagent2
 - OS/2 system with IP address 9.24.104.72, known as rmagent2
2. IP network 9.67.46.128 (subnet mask 255.255.255.192)
 - RISC System/6000 with IP address 9.67.46.170, known as rs60005
 - 8250 Hub with IP address 9.67.46.138, known as trmmb

3. IP network 9.67.32 (subnet mask 255.255.255.0)

- RISC System/6000 with IP address 9.67.32.84, known as rs60005
- OS/2 system with IP address 9.67.32.87, known as rmagent1

The RISC System/6000 has three physical connections, two token-ring and one Ethernet, each to one of the IP networks listed above. The RISC System/6000 was also configured to act as a router as can be seen by the icon chosen to display the RISC System/6000 on the IP network diagram.

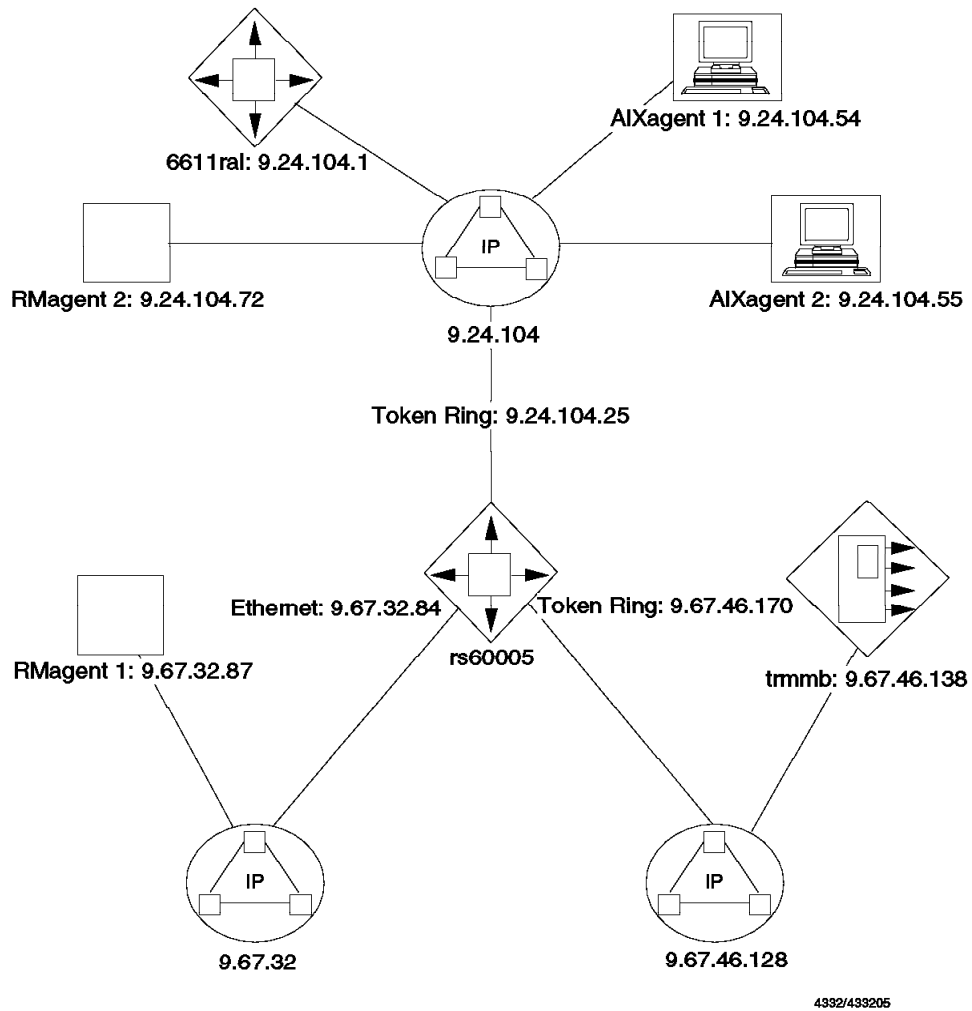


Figure 22. AIX NetView/6000 IP Topology

The hardware and software products that we used were:

1. On the RISC System/6000 rs60005:

- Hardware
 - Model 350
 - 64MB of memory
 - 2GB of disk space
 - 2 token-ring adapters
 - 1 Ethernet adapter
- Software
 - AIX V3.2.5
 - AIX NetView/6000 V2.1 with PTF U428927
 - IBM LAN Network Manager for AIX
 - AIX LMU/6000
 - RMONitor for AIX
 - IBM Hub Management Program/6000
 - Router and Bridge Manager/6000
 - AIX Trouble Ticket/6000 V2

2. On the OS/2 agents

- Hardware
 - Model 80 386 20MHz. We would recommend using a 486 processor
 - 16MB of memory
 - 200MB of disk space
- Software
 - IBM TCP/IP for OS/2 V2, plus CSDs
 - Database Manager 2/2, plus CSDs
 - LAN NetView Management Utilities for OS/2
 - LAN Network Manager
 - RMONitor Agent for OS/2
 - System Performance Monitor/2

A detailed description of the various components:

- RISC System/6000 Management System

This system has the AIX NetView/6000 and the AIX NetView/6000 family of products listed above.

- AIXAGENT1

This system is providing two functions in our network:

1. The OS/2 LNM proxy agent and has the following products installed:

- LAN Network Manager (plus Proxy Agent)
- IBM TCP/IP for OS/2
- Database Manager 2/2

2. An OS/2 LMU client with the following products installed:

- LAN NetView Management Utilities for OS/2 client
- OS/2 Novell NetWare requestor
- System Performance Monitor/2

- AIXAGENT2

This system provides the OS/2 LMU proxy agent and has the following products installed:

- LAN NetView Management Utilities for OS/2, providing the proxy agent and managing environment

- IBM TCP/IP for OS/2
- Database Manager 2/2
- OS/2 Novell NetWare requestor
- RMAGENT1

This system provides the RMONitor Agent for OS/2 for the Ethernet network with the following products installed:

 - 3com Ethernet adapter
 - RMONitor Agent for OS/2
- RMAGENT2

This system provides the RMONitor Agent for OS/2 for the token-ring network and has the following products installed:

 - IBM LAN Streamer adapter
 - RMONitor Agent for OS/2
- DOS/Windows providing a DOS/Windows LMU client with the following products installed:
 - IBM DOS 6.0
 - Windows 3.1
 - Novell NetWare requestor, with CSDs DOSUP9 and WINUP9
 - LMU client
- IBM Token-Ring bridges
- 8209 Token-Ring to Ethernet bridge
- IBM Intelligent 8250 Hub
- Several 8230 Controlled Access Units (CAUs)
- 6611 Router
- Novell NetWare Server 3.11

The SNMP community name was ITSC with the RISC System/6000 (rs60005) being defined as the destination for all SNMP traps.

1.4 RISC System/6000 TCP/IP Configuration

Following is the TCP/IP configurations used on the RISC System/6000. The configuration steps required are:

1. Configure each interface on the RISC System/6000. In our environment these were the two token-ring and the Ethernet interfaces.
2. Configure the */etc/hosts* file.
3. Configure the SNMP community names.

The configuration of each interface on the RISC System/6000 will be through the System Management Interface Tool (SMIT). This interface provides both an ASCII and a Motif interface, providing identical function. We will show the screens for the Motif interface. To start the configuration of TCP/IP either:

1. The *TCPIP* fastpath could be used, for example: SMIT TCPIP
or
2. From the SMIT main menu choose the following menu item:
 - Communications Applications and Services

- TCP/IP

Either approach will display the TCP/IP main configuration screen. Choose the **Minimum Configuration & Startup** option and you will get a display with a list of interfaces available for your system, as shown in Figure 23.

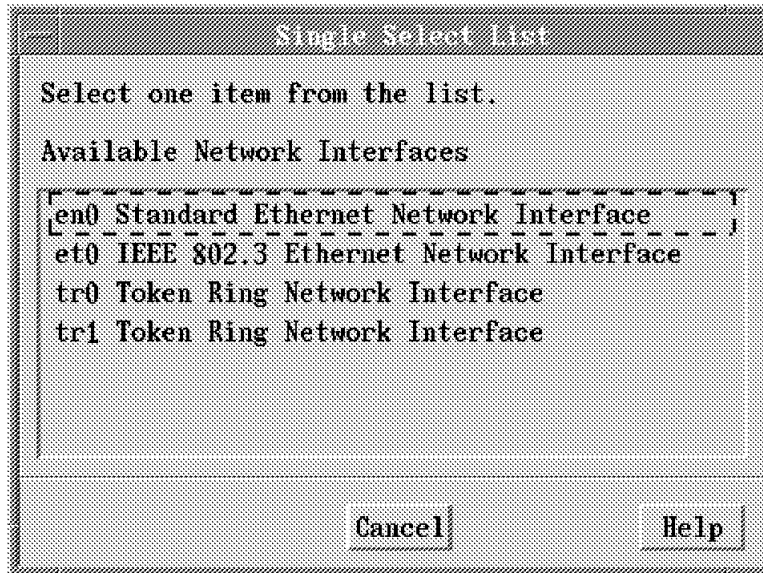


Figure 23. RISC System/6000 TCP/IP Configuration Interfaces List

From this screen choose the interface you want to configure for your TCP/IP environment. In our environment the TCP/IP configuration for the *tr1* interface was chosen and the following screen was displayed, as shown in Figure 24 on page 28.

The values entered were:

- **rs60005** for the hostname. This name will default in the configurations for the other interfaces.
- **9.24.104.25** for the Internet address.
- **255.255.255.0** for the subnet mask.
- A default gateway was entered, however, it is not essential
- Choose the **Do** button to update the configuration.

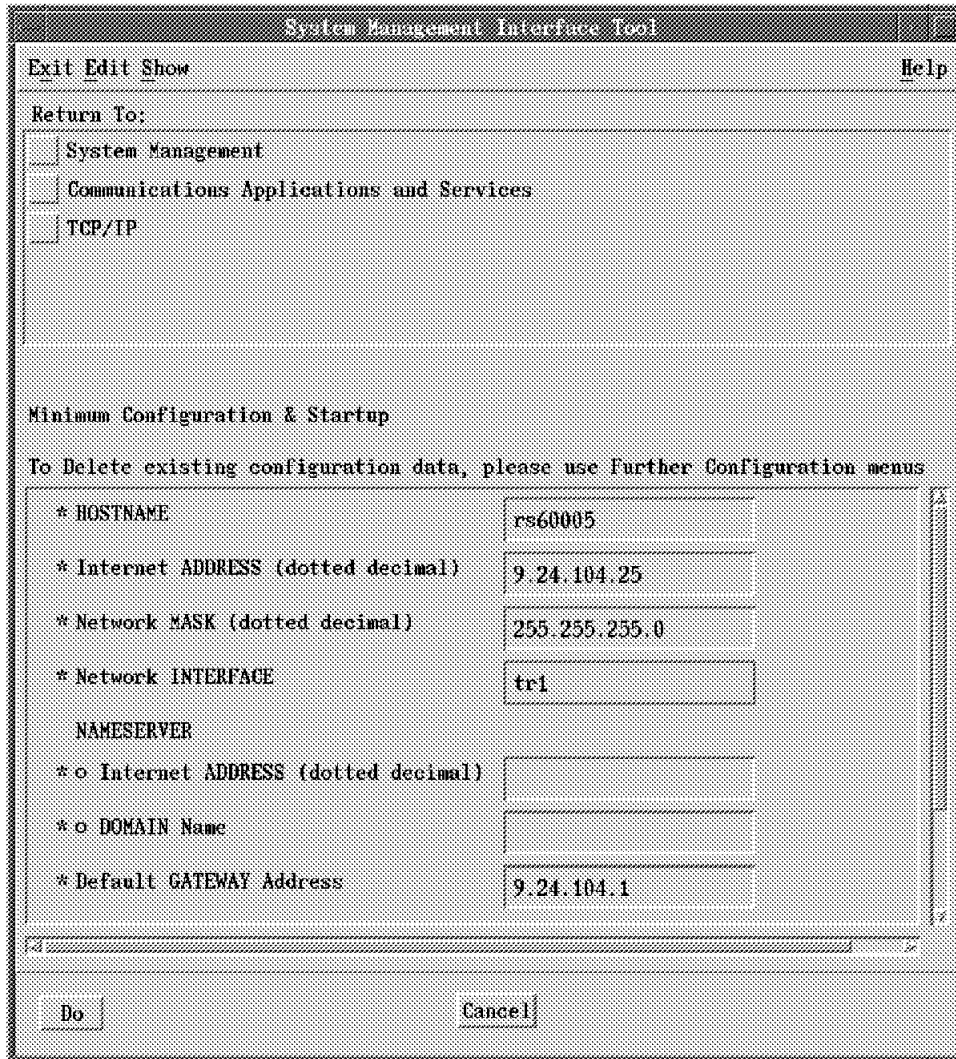


Figure 24. RISC System/6000 TCP/IP tr1 Configuration

For the other two interfaces defined in our environment the values were:

1. tr0

- **rs60005** for the hostname, which is the default value entered from the previous tr1 configuration.
- **9.67.46.170** for the Internet address.
- **255.255.255.192** for the subnet mask.
- A default gateway was entered, however, it is not essential.

2. en0

The en0 interface uses the Ethernet V2 standard whereas the et0 uses the IEEE 802.3 Ethernet standard. In order to communicate with the Ethernet RMONitor Agent for OS/2 only the en0 interface can be used.

- **rs60005** for the hostname, which is the default value entered from the previous configuration.
- **9.67.32.84** for the Internet address.
- **255.255.255.0** for the subnet mask.
- A default gateway was entered, however, it is not essential.

The /etc/hosts file information can be updated using the AIX vi editor. The following entries were added:

```
9.24.104.1      6611ral
9.24.104.25    rs600005
9.24.104.54    aixagent1
9.24.104.55    aixagent2
9.24.104.72    rmagent2
9.67.46.170    rs600005
9.67.46.138    trmmb
9.67.32.84     rs600005
9.67.32.87     rmagent1
```

The SNMP information used by AIX NetView/6000 can be configured by choosing **Options..SNMP Configuration** from the AIX NetView/6000 menu bar. You will get a display window with the SNMP Configuration screen as shown in Figure 25 on page 30. In this screen the default SNMP community name is *public*, as can be seen by the top entry.

In our environment we have set the default community name for the 9.24.104 network to ITSC. However, we set the default community name for individual nodes, the 6611ral (9.24.104.1) and rmagent2 (9.24.104.72), within this IP network to public.

To add these entries into the network and node community area do the following:

1. Network Community name

- Enter **9.24.104.*** in the target field.
- Enter **ITSC** in the community field.
- Enter a timeout, retry and polling values.
- Press **add** to add this entry.

2. Node Community name

- Enter **9.24.104.1** in the target field.
- Enter **public** in the community field.
- Enter a Timeout, Retry and Polling values.
- Press **Add** to add this entry into the node community information.

Add another community name for the 9.24.104.72 IP node.



Figure 25. AIX NetView/6000 SNMP Configuration

Once you have updated all the entries, press **OK** to apply the changes and close the SNMP Configuration window.

1.5 IBM TCP/IP for OS/2 and Database Manager 2/2 Installation and Configuration

Following are the TCP/IP and Database Manager 2/2 configurations that were used to demonstrate AIX NetView/6000's integration with the NetView/6000 family of products mentioned earlier. TCP/IP and Database Manager 2/2 are required on the LMU and LNM proxy agents. Following are the installation and configuration steps used in our environment.

1.5.1 TCP/IP Installation and Configuration

The installation and configuration steps required are:

1. Install IBM TCP/IP for OS/2 and apply the CSDs.
2. Install the TCP/IP drivers for the LAN adapter.
3. Configure the IBM TCP/IP for OS/2 information.

The information to be updated is:

- a. IP address
 - b. SNMP information - System contact and location, community name and trap destination
 - c. Host name
4. Configure RISC System/6000 TCP/IP information.

The installation of IBM TCP/IP for OS/2 is started by entering **A:TCPINST** in an OS/2 window with disk 1 in the A: drive. Once the TCP/IP product is installed the latest CSDs will need to be applied.

In addition to installing the TCP/IP product, the LAN adapter requires TCP/IP drivers. This is done using the LAN and Protocol Support (LAPS) diskette provided with the product. The following screens will step you through the installation of the TCP/IP drivers using LAPS.

To start the installation of LAPS enter **A:LAPS** from an OS/2 window with the LAPS diskette in drive A:. The following screen shown in Figure 26 will be displayed. Choose the **Install** button to start the installation.

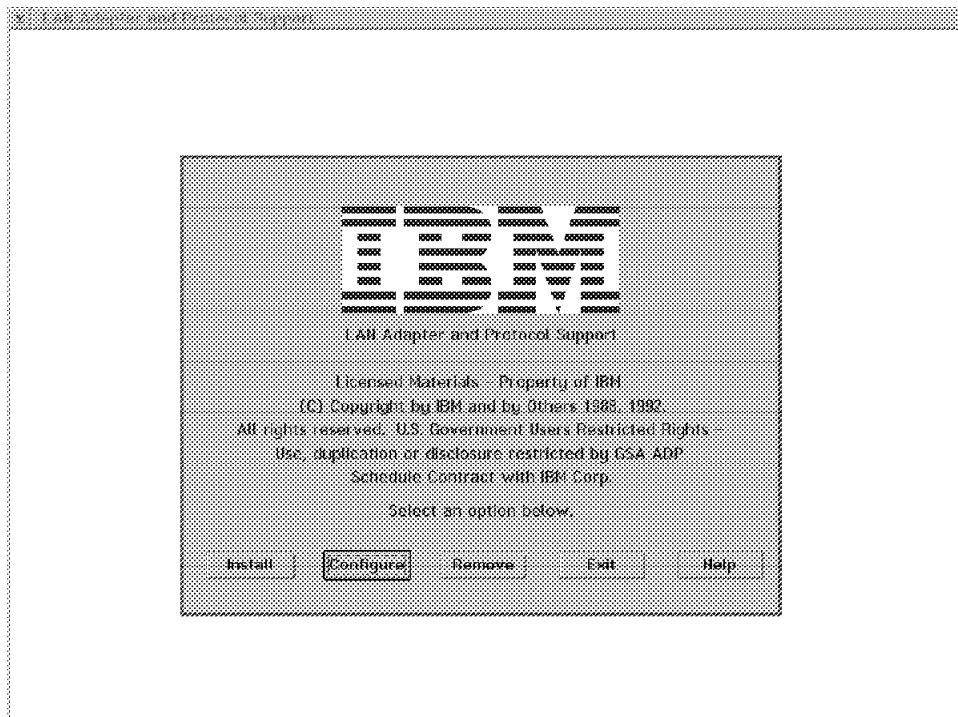


Figure 26. LAPS Installation Initial Screen

Choose to install the product on the C: drive. The progress of the installation will be shown.

Once LAPS is installed the initial screen will be displayed as shown in Figure 26. Choose the **Configure** button to then configure and install the adapter and driver information that you need.

After pressing the configure button, you will see the screen shown in Figure 27. Choose the **Continue** button, to configure LAPS.

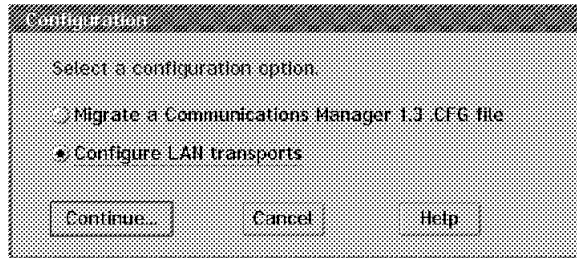


Figure 27. LAPS Configuration Option

Choose the appropriate information from the list boxes shown in Figure 28 on page 33. The following LAN configuration is required:

- *Network Adapter:* Choose the LAN adapter installed in your OS/2 workstation by selecting the adapter from the list and pressing the **Add** button.
- *Protocols:* Choose the TCP/IP protocol and the press the **Add** button to install the TCP/IP drivers onto the LAN adapter.

The *Current Configuration* list box shows what has been selected. We have shown both an IBM token-ring adapter and an IBM Ethernet adapter with the TCP/IP protocol installed on each. You need a minimum of one LAN adapter, but there will be times when you will use more than one. Select the **OK** button to update the LAPS configuration files with the new information. The files used by LAPS to store the information are:

- C:\CONFIG.SYS
- C:\IBMCOM\PROTOCOL.INI

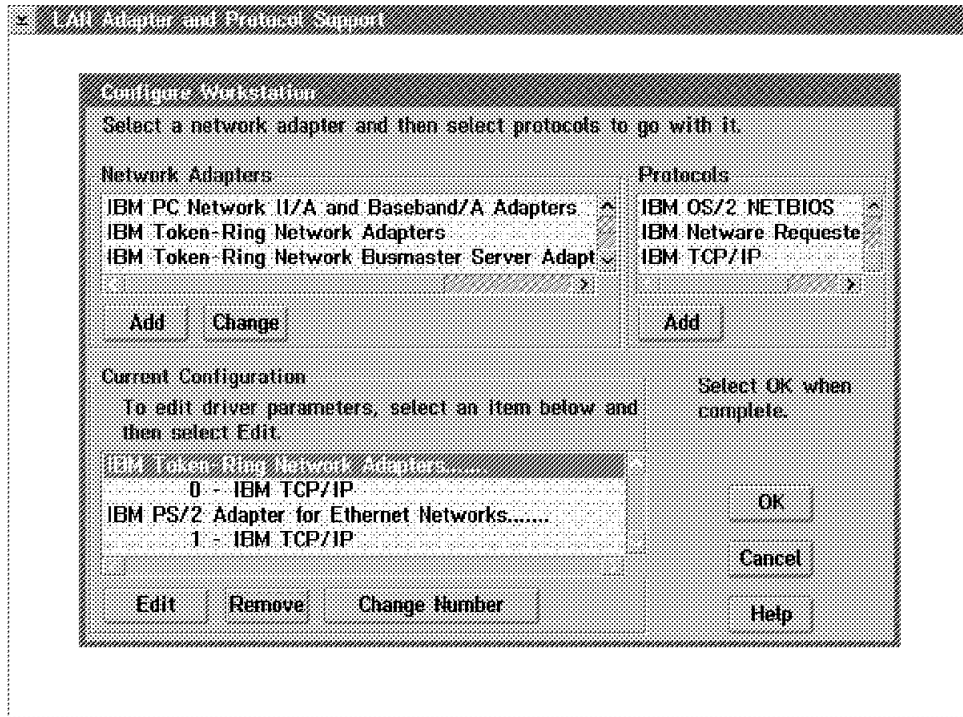


Figure 28. LAPS Adapter and Protocol Configuration

Choose **Continue** from the following screen in Figure 29 to update the CONFIG.SYS file on the C: drive.

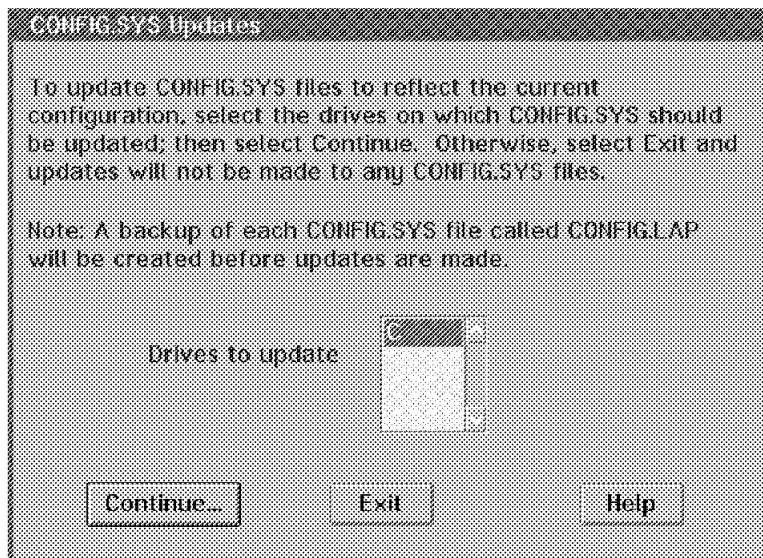


Figure 29. LAPS Start Update

The OS/2 system will need to be restarted for the new configuration to be activated.

The following TCP/IP configurations were done using the Notebook interface provided by OS/2 TCP/IP Version 2.0 configuration utility. The TCP/IP configuration is started by selecting the **TCP/IP Configuration** utility from the TCP/IP folder on the OS/2 desktop. The TCP/IP network used in this scenario had additional devices on the network, such as routers and domain name

servers. These are not required to enable the scenarios to operate; however, they were configured in our environment.

1.5.1.1 IP Address

The IP addresses of the two OS/2 workstations were as follows:

1. *AIXAGENT1* was defined as 9.24.104.54 with a subnet mask of 255.255.255.0.
2. *AIXAGENT2* was defined as 9.24.104.55 with a subnet mask of 255.255.255.0.

Click on the **Enable LAN Adapter 0** to configure the first adapter in this workstation for TCP/IP, as shown in Figure 30. In addition, the IP address and subnet mask information are entered.

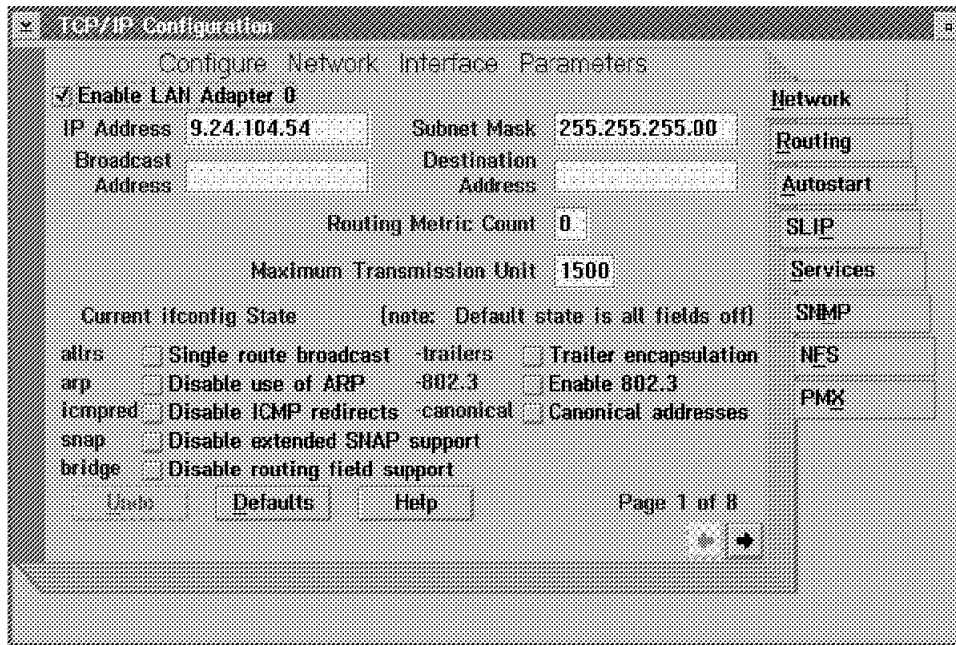


Figure 30. TCP/IP Network Configuration

1.5.1.2 SNMP Information

The management information flow between the RISC System/6000 and the OS/2 workstations is through the SNMP standard.

The SNMP information required is:

1. System contact and location

The information entered for these MIB-II variables SYSCONTACT and SYSLOCATION was:

- a. Jerry Badalassi and IBM ITSC Raleigh BLD 657
- b. Roberto Shigueo Suzuki and IBM ITSC Raleigh BLD 657

as shown in Figure 31 on page 35. This updates the C:\CONFIG.SYS file with the following two entries:

```
SET SYSCONTACT= Jerry Badalassi
SET SYSLOCATION=IBM ITSC Raleigh BLD 657
```

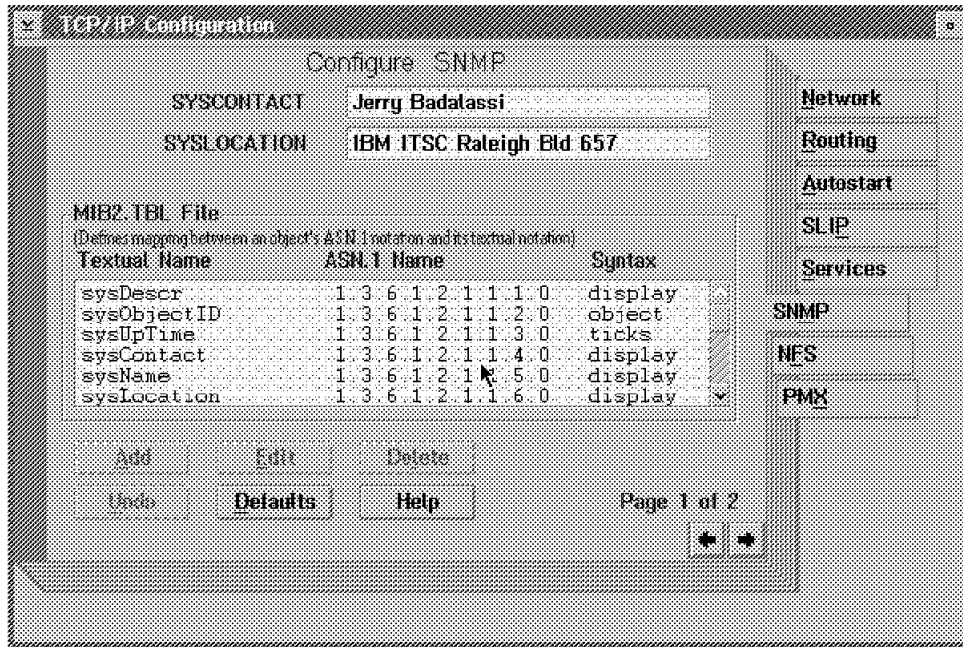



Figure 31. TCP/IP SNMP MIB-II Information

Click on the arrows to select the second page of the SNMP configuration tag as shown in Figure 32 on page 36.

2. SNMP trap destination

The IP address of the RISC System/6000 is needed to allow SNMP traps generated by the OS/2 workstations to be sent to the RS/6000, as shown in Figure 32 on page 36. The name of the RISC System/6000 can be entered if the D:\TCPIP\ETC\HOSTS file (or Domain Nameservers) has the mapping of the name (in our environment rs60005) to the actual IP address.

The following file D:\TCPIP\ETC\SNMPTRAP.DST is updated with this information:

```
9.24.104.25    UDP
```

3. SNMP community name

The community name is required and must match the community information on the RISC System/6000. This provides the authority for the RISC System/6000 to access the MIB information on the OS/2 workstations and receive the SNMP traps generated as shown in Figure 32 on page 36.

The following file D:\TCPIP\ETC\PW.SRC is updated with this information:

```
ITSC          9.24.104.0      255.255.255.0
```

The command *Make_PW* needs to be run against the PW.SRC file to compile the information. You need to make the ETC directory your current directory and then execute the command as shown:

- **CD \TCPIP\ETC**
- **Make_PW**

The following message will be returned if it compiled successfully:

```
I have written 1 entries into "snmp.pw"
```

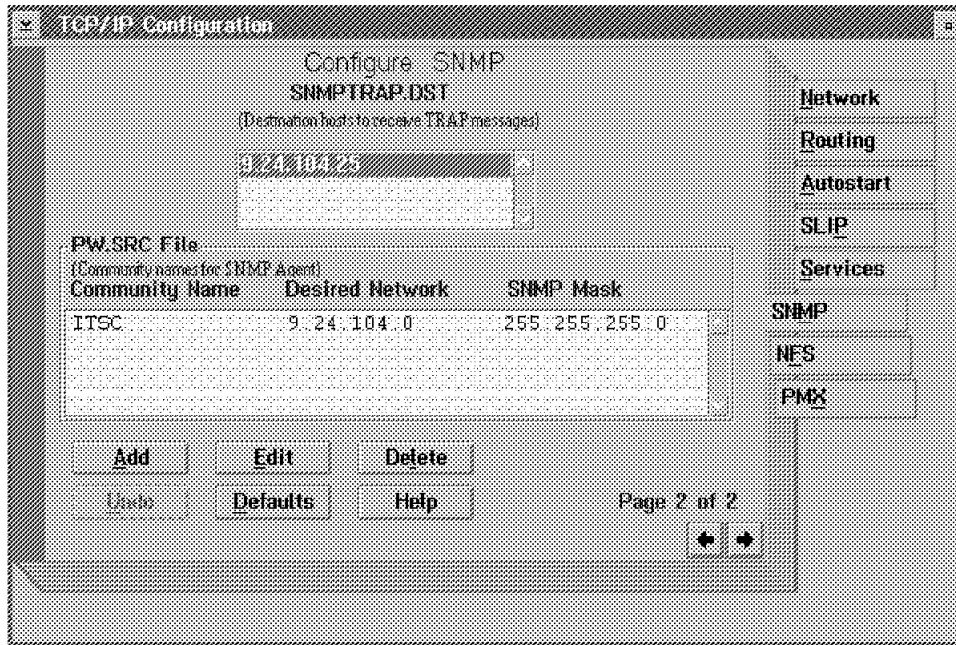


Figure 32. TCP/IP SNMP Configuration

4. Machine's hostname

Choose the **Services** tag on the TCP/IP configuration notebook to enter the machine hostnames as shown in Figure 33 on page 37. These are the names given to the OS/2 workstations, and in our environment the names were:

- AIXAGENT1
- AIXAGENT2

This updates the C:\CONFIG.SYS file with the following entry:

```
SET HOSTNAME=AIXAGENT1
```

1.5.1.3 Additional Information

Only the *This Machine's Hostname* entry is required. The remaining information is included, however, not essential to enable the OS/2 workstations to communicate with the RISC System/6000. The following screens show how to configure routers and domain nameservers if your network uses them.

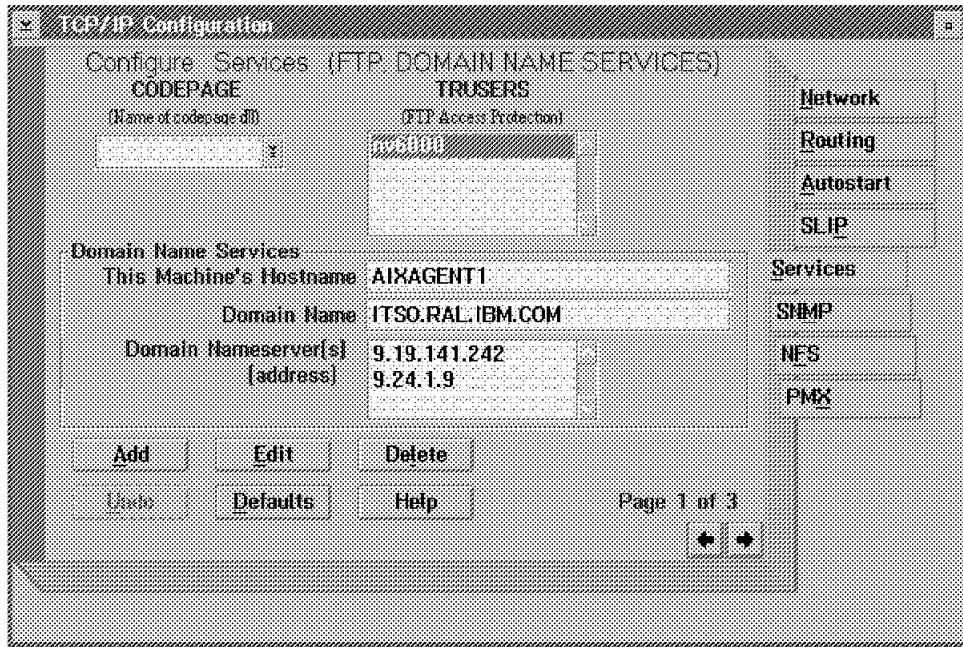


Figure 33. TCP/IP Hostname and Other Services Configuration

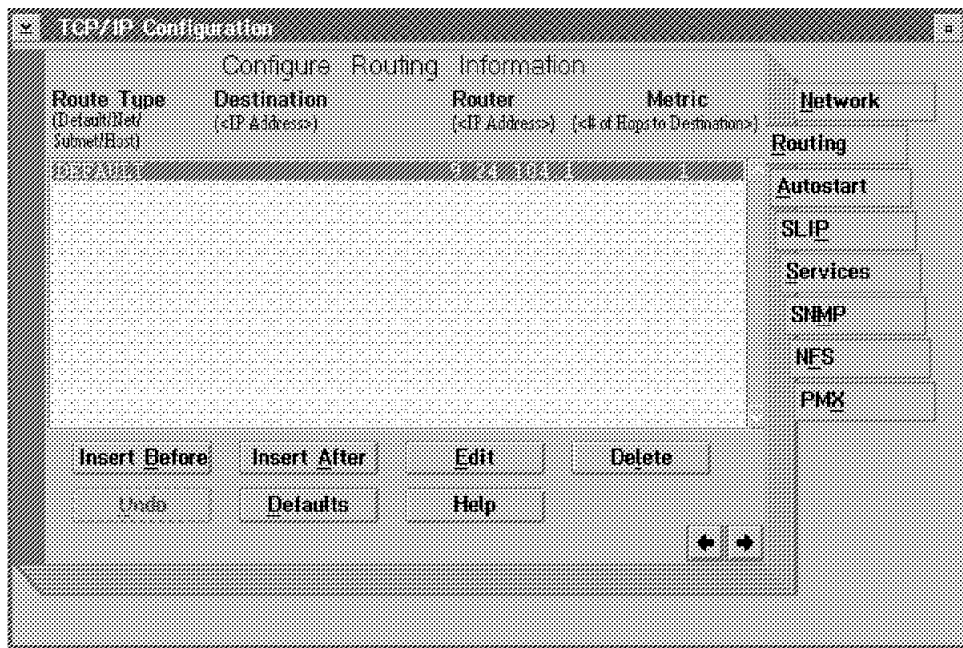


Figure 34. TCP/IP Routing Configuration

To ensure that TCP/IP is automatically started when OS/2 is started the OS/2 startup file, C:\STARTUP.COM, is displayed to show what is required to start the TCP/IP and SNMP daemons.

```

REM * OS/2 TCP/IP startup command file
REM *****
call tcpstart.cmd
REM * OS/2 TCP/IP SNMP daemon
start "SNMPD" /min snmpd.exe

```

The option to start TCP/IP through the OS/2 *startup folder* was not used, since the SNMP daemon requires that TCP/IP is started before it is loaded. There are other ways of doing this, but the easiest approach was to control the startup through the OS/2 startup file.

The OS/2 workstation needs to be restarted to complete the installation of the IBM TCP/IP for OS/2 product.

1.5.2 OS/2 Database Manager 2/2 Installation

IBM Database Manager 2/2 is required for the OS/2 workstations to store the information gathered from the network. The version of DB2/2 that we installed was Version 1.01.

The steps required to install DB2/2 are:

1. Configure the type of installation - Client with local databases
2. Configure workstation name - AIXAGNT1

To start the Database Manager 2/2 installation type **A:DBINST** from an OS/2 window. The following initial screen is displayed.

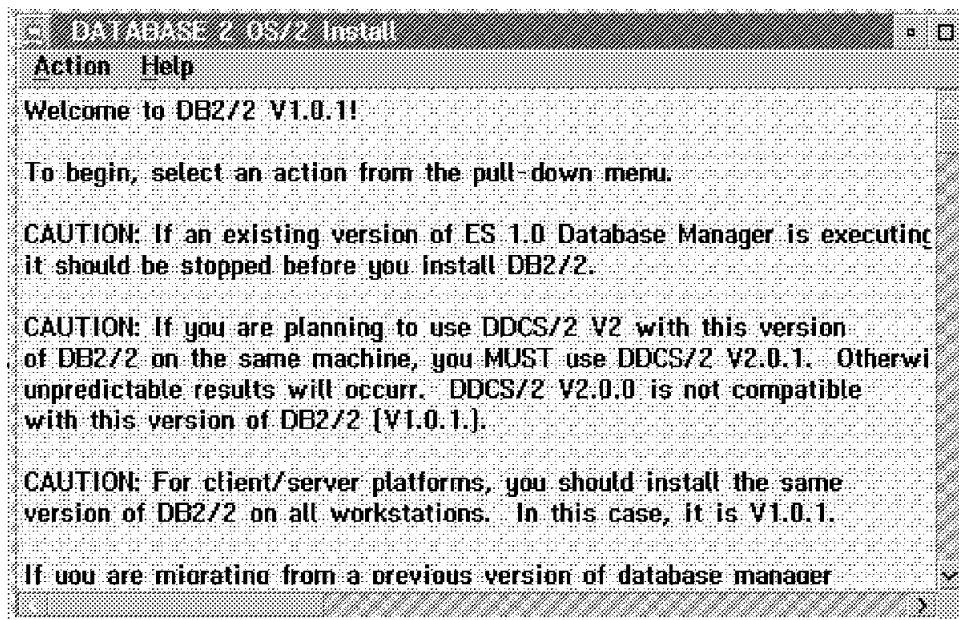


Figure 35. Database Manager 2/2 Installation Initial Screen

To start the installation choose **Action..Install** from the pull-down menu. The following screen as shown in Figure 36 on page 39 is displayed with the following options selected:

- Target Drive: Choose the drive location for the Database Manager 2/2 database code; in our environment drive **D** was selected. It is important to note that if drive **D:** is selected to install the database a requirement is to have approximately 3MB of free disk space on drive **C:** for temporary files.
- Type: Select **Client with local database**; this provides the ability for the workstations to be capable of creating local databases.
- Features: The other options such as *Query Manager*, *Database Tools* and *Documentation* where chosen; however, they are not required.

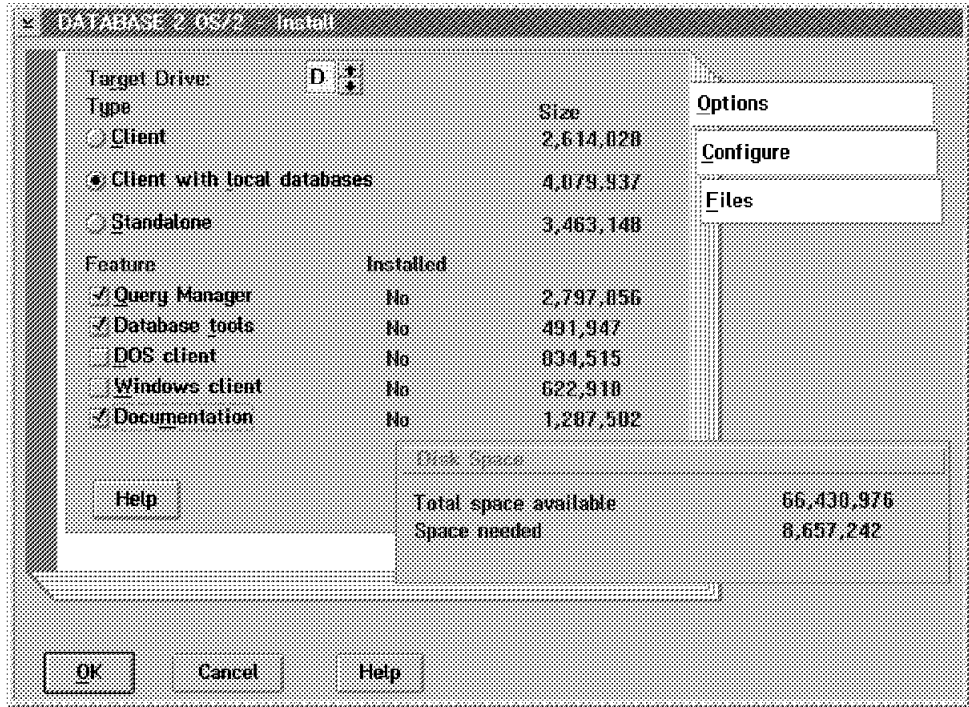


Figure 36. Database Manager 2/2 Options Installation

A workstation name is required, but this name is not checked in any of the other configurations.

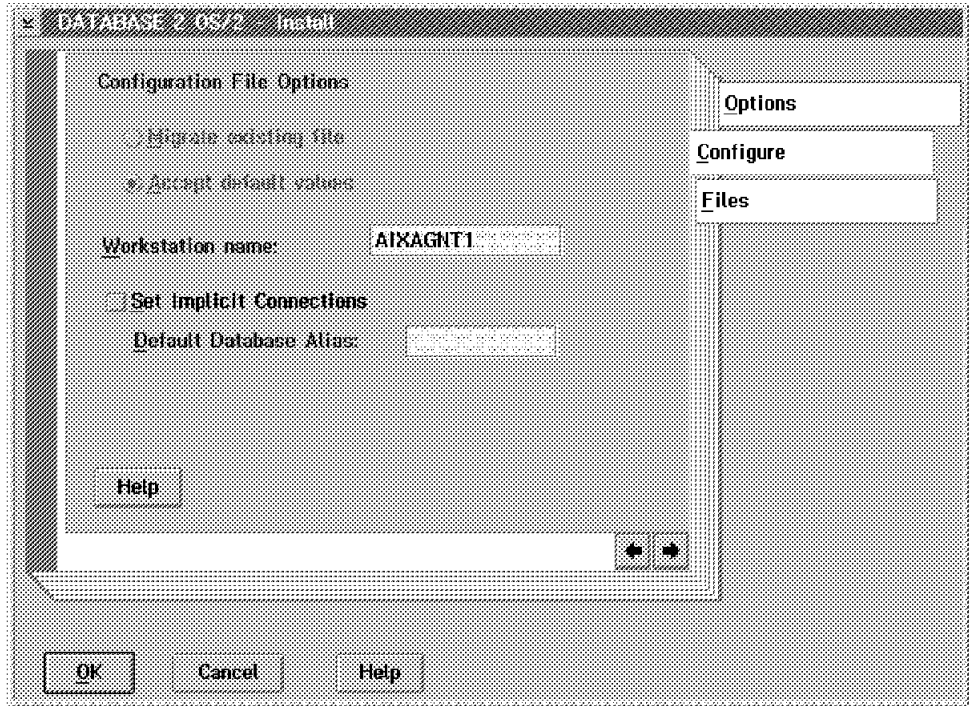


Figure 37. Database Manager 2/2 Configure Installation

Once you have entered the above information, select the **OK** button to start the installation. A screen is displayed showing the progress of the installation process. You will then be prompted for each additional diskette.

Once the installation has completed the following message, as shown in Figure 38 on page 40 is displayed.

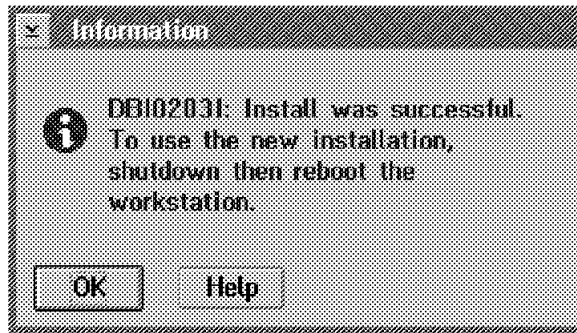


Figure 38. Database Manager 2/2 Installation Successful

The OS/2 workstation needs to be restarted to complete the installation of the Database Manager 2/2 product.

1.5.3 RISC System/6000 Software Installation Procedures

The installation of the various products for the RISC System/6000 is done using the System Management Interface Tool (SMIT). This interface provides both an ASCII and a Motif interface, providing identical function. We will show the screens for the Motif interface.

To start the installation of the software:

1. The *Install_Latest* fastpath could be used, for example: SMIT `Install_Latest`;
or
2. From the SMIT main menu choose the following menu items:
 - Software Installation and Maintenance
 - Install/Update Software
 - Install/Update Selectable Software (Custom Install)
 - Install Software Products at Latest Available Level

Either approach will display the following screen shown in Figure 39 on page 41. In this case we chose the second approach.

The initial installation screen requires you to specify the input device to install the software. By choosing the **List** button a list of the available devices is displayed, as shown in Figure 39 on page 41. Click on the installation device and then enter **Do**.

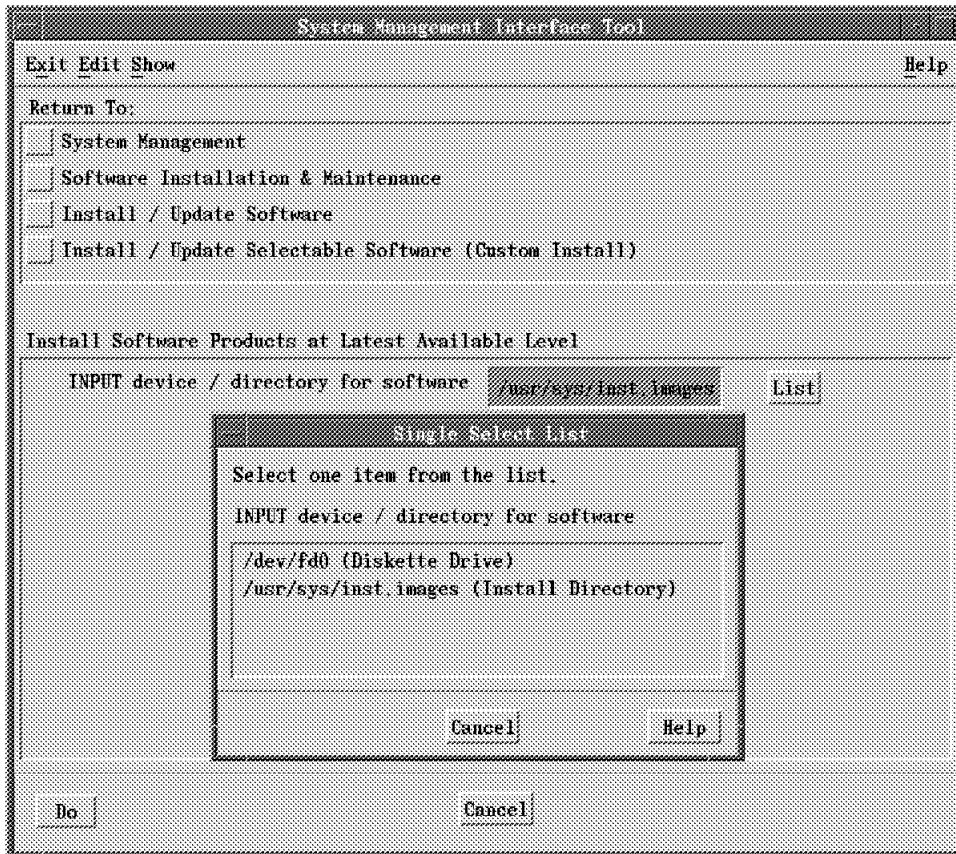


Figure 39. SMIT Initial Installation Screen

The options that we selected in the following screen for our installations are:

- Automatically install PREREQUISITE software was changed to **no**.
- COMMIT software was changed to **no**.
- SAVE replaced file was change to **yes**.

We used the default values for the remaining fields, as shown in Figure 40 on page 42.

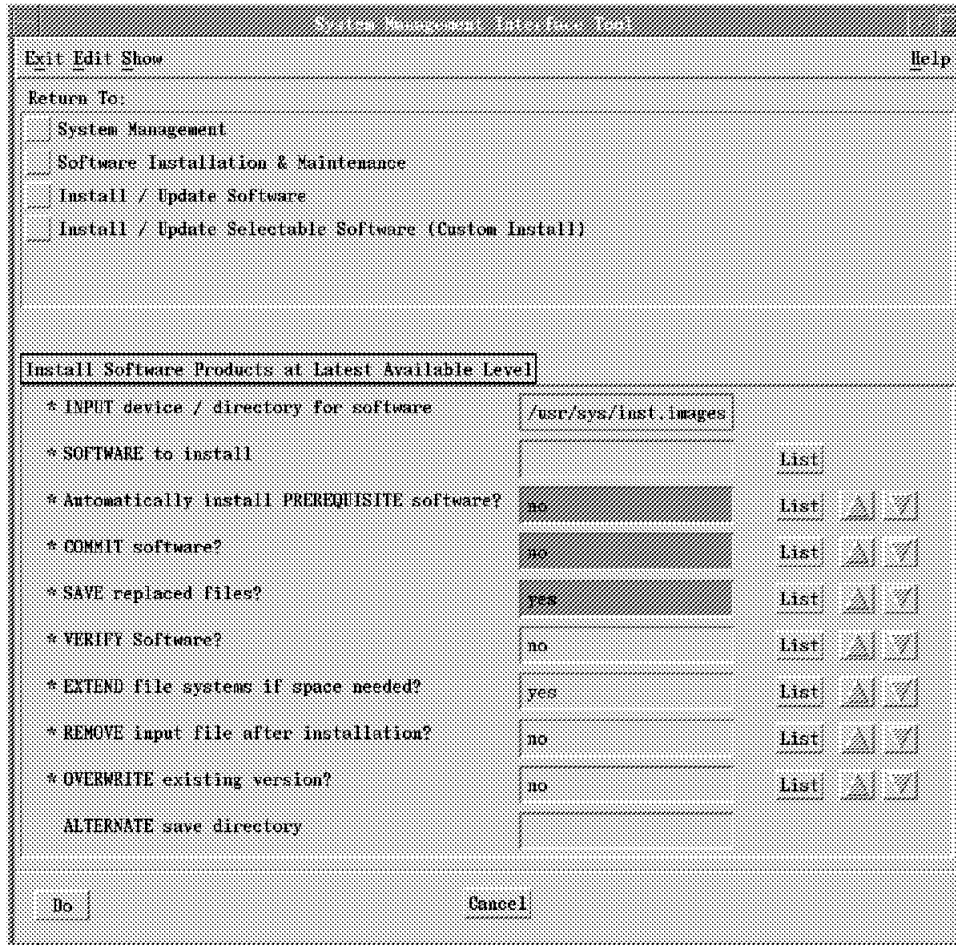


Figure 40. SMIT Installation Screen

You will need to fill in the field 'SOFTWARE to install' for each product. If you use the List function, it will search the directory that you have specified in the Input field. The system searches the input device and lists the products, similar to the screen shown in Figure 41.

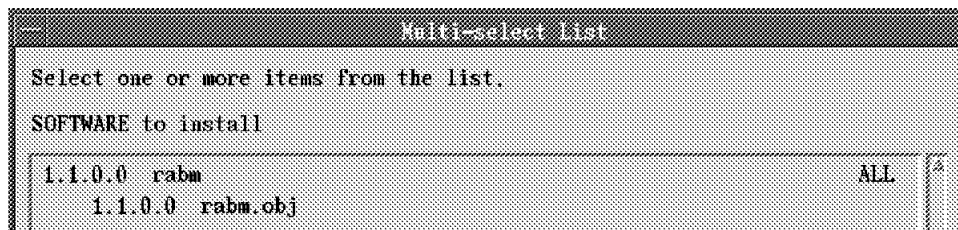


Figure 41. Sample List from Input Device Prompt

Select the software to install from the list shown. To start the installation select **Do**.

Chapter 2. LAN NetView Management Utilities/6000

This chapter gives a brief overview of the installation, configuration and operation of AIX LMU/6000 and LMU/2. It will not go into great technical depth on all the LMU/2 functions. Its purpose is to explain how to build a sample environment that will be used later in the scenarios shown in Chapter 8, "Integration Scenarios" on page 205.

For more detailed information, refer to the documents: *LAN NetView Management Utilities for OS/2 User's Guide* and *AIX LAN Management Utilities/6000 User's Guide*.

2.1 AIX LMU/6000 Overview

AIX LAN Management Utilities/6000, hereafter referred to as AIX LMU/6000, is an application that is integrated with AIX NetView/6000. It provides systems management services for LAN-attached servers and workstations which use IBM NetBIOS or Novell IPX protocols.

AIX LMU/6000 addresses four major disciplines:

- Operation management
 - OSF Motif-based graphical display
 - Remote command execution
- Configuration management
 - Retrieval of vital product data

This includes information like computer model, CPU speed, memory available, disk space available.
 - Access to data from a central OS/2 database
 - Generation of configuration change event

All the received traps indicating configuration changes are converted into event cards. These traps also update the submaps and topology database by adding new nodes or modifying the status of the existing ones.
- Performance management
 - OS/2 system performance
 - NetWare server performance
 - NetWare server volume information
 - Events generated on user-defined thresholds

It is possible to monitor critical files and applications, and generate warning events when they reach user-defined thresholds.
- Fault management
 - Generates virus events
 - Automated recovery from events received
 - Monitors event threshold and filtering

- Heartbeat monitoring of managed systems
- Monitor critical files and applications

2.1.1 Prerequisites

The minimum hardware components required are:

- RISC System/6000 POWERstation or POWERserver
- 48 megabytes of memory
- 10 megabytes of free disk space
- Color display supporting XWindow System
- IBM or compatible mouse
- Connection to your TCP/IP network
- Installation media (disk/tape)

The following software components must be installed, configured and operational:

- AIX Version 3 Release 2 or later
- AIX NetView/6000 Version 2
- AIXwindows Environment/6000 Version 11 Release 4 or 5
- OSF/Motif Version 1 Release 1.4
- TCP/IP
- LAN NetView Management Utilities for OS/2 (LMU) on your LAN

2.1.2 Functionality

Figure 42 on page 45 shows an example of the AIX LMU/6000 management environment.

Functionally, the AIX LMU/6000 program enables an AIX NetView/6000 operator to monitor LANs managed by the LMU/2 software. The management protocol between AIX LMU/6000 and LMU is SNMP and the transport protocol can be either NetBIOS, IPX, or both.

At the LMU manager station, an OS/2 machine, the `lmusnmpd` proxy agent executes and translates management operations on behalf of the managed nodes, by interacting with the `snmpd` process.

On the RISC System/6000 side, the `lmuTopod` daemon is responsible for continually retrieving and maintaining topology information about the managed nodes by communicating with the proxy agents.

The LMU/2 inventory data maintained by the OS/2 database is only refreshed on demand.

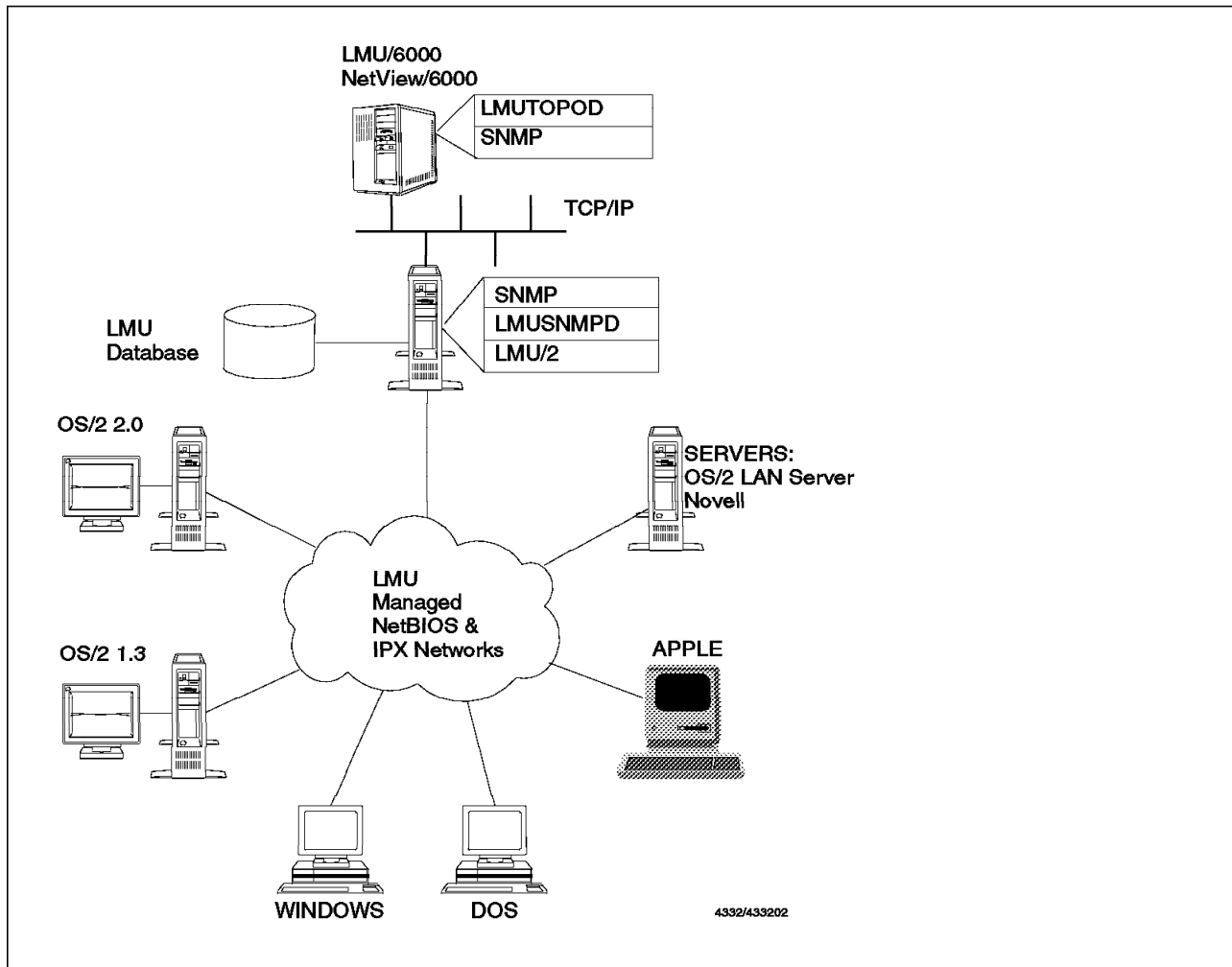


Figure 42. AIX LMU/6000 Management Environment

2.2 AIX LMU/6000 Installation

AIX LMU/6000 uses the standard SMIT installation process to install the product. After the software is physically installed, the installation process proceeds to the configuration of AIX LMU/6000 into AIX NetView/6000.

Figure 43 on page 46 is an excerpt of the /smit.log file that shows the configuration steps actually performed.

Notice that during this configuration the AIX NetView/6000 daemons are stopped and if the AIX NetView/6000 program is active it will also be stopped.

```
====> Initiating Configuration of LMU/6000 <====
-----
Updating /usr/OV subdirectories to include LMU/6000
updating configuration files...
Stopping NV/6000 daemons...
Running ovw to verify, configure, and load fields...
Registering lmuTopod daemon...
ovaddobj - Static Registration Utility
Successful Completion

Compiling and loading LMU proxy MIB...
Configuring LMU traps...
Trap has been added.
Trap has been added.
Trap has been added.
Trap has been added.
Trap has been added.
Trap has been added.
Trap has been added.
Trap has been added.
Trap has been added.
Trap has been added.
Trap has been added.
Trap has been added.
Trap has been added.
====> LMU/6000 Configuration completed. <====
```

Figure 43. /smit.log File Showing the AIX LMU/6000 Configuration During the Installation Process

2.3 LMU/2 Installation

The LMU/2 installation process is dependent on the platform that it will be executing on. In this session we will show the steps used to install the LMU/2 components for OS/2, DOS, Windows and for a NetWare server.

Remember that the last three components can only be managed stations and that the LMU/2 code needs to be installed in at least one OS/2 machine to act as the managing station. This terminology is better explained in 2.5, “LMU/2 Configuration” on page 49.

2.3.1 LMU/2 Installation for OS/2 Stations

The installation utility is called LMUINST, and it is located on the first LMU/2. If this utility is called with no parameters it will show the parameters available. We started the installation process with these options:

```
a:lmuinst all /Td
```

Where:

- all specifies that all the LMU/2 programs and files (for all platforms), the graphical user interface and the documentation are to be installed on the target disk d:.
- /Td specifies that the target drive is d, instead of the boot drive.

This target drive may be either a local or a network drive.

You must customize the LMU/2 software prior to using it. Refer to 2.5.1, "LMU/2 Configuration for OS/2 Stations" on page 49 for details on this customization.

2.3.2 LMU/2 Installation for DOS Stations

If the LMU/2 software was previously installed on a shared disk to which the DOS station has access, no additional action needs to be performed.

If that is not the case, then copy the following files from the LMU/2 diskette 4 to the DOS machine:

- DOSVIRGA.COM
- QDOSVPD.COM
- LMUDOSHB.COM
- AUEDOSAL.COM
- ADAPTERS.TBL
- CVT_VPD.EXE
- USERVPD.SMP
- ADAPTERS.SMP
- CRITFILE.SMP

The use of these files is explained in 2.5.2, "LMU/2 Configuration for DOS Stations" on page 54.

2.3.3 LMU/2 Installation for Windows Stations

To install the Windows portion of the LMU/2 code, use the LMUINSTW utility located on diskette 4:

```
a:\muinstw z:
```

where z: is the target drive.

This utility creates the LMU2 directory on the specified drive and copies the necessary files to it.

2.5.3, "LMU/2 Configuration for Windows Stations" on page 55 shows how to customize this environment.

2.3.4 LMU/2 Installation for NetWare Servers

If your NetWare server is going to maintain the LMU/2 code for both itself and its requesters, use the installation utility LMUINST in the LMU/2 diskette 1, as follows:

```
A:\muinst network /Tg
```

where /Tg is the target drive g. Make sure that you are specifying a shared drive that belongs to your NetWare server.

If you are going to install only the server code, copy the following files from the LMU/2 diskette 4 to a server's partition:

- All .NLM files (*.NLM)
- QDOSVPD.COM
- ADAPTERS.SMP
- CRITFILE.SMP
- LMUBIND.SMP
- USERVPD.SMP
- ADAPTERS.TBL

This is done at a NetWare requester and the server partition is one of the shared drives that was mapped at this station.

Also, copy the following files to the server's DOS partition:

- LMUDOSHB.COM
- CVT_VPD.EXE

To access the DOS partition, either do it before starting the NetWare server or after bringing it down.

The customization of the NetWare server is shown in 2.5.4, "LMU/2 Configuration for NetWare Servers" on page 56.

2.4 AIX LMU/6000 Configuration

The most important point while configuring the AIX LMU/6000 management environment is to correctly configure its partner, LMU, to exchange information. This configuration will be covered in the next section.

Be sure that the MIB values in the LMU proxy agent system can be accessed by the AIX LMU/6000 program using SNMP.

In addition to the SNMP agent configuration, options can be set for the ImuTopod daemon as shown in Figure 44. We have used the default configuration values in our machine.

The ImuTopod daemon is started along with the other AIX NetView/6000 daemons. Inside SMIT, choose the options **Communications Applications and Services...LAN Management Utilities/6000...Control the ImuTopod daemon** to start, stop or display the status of the daemon.

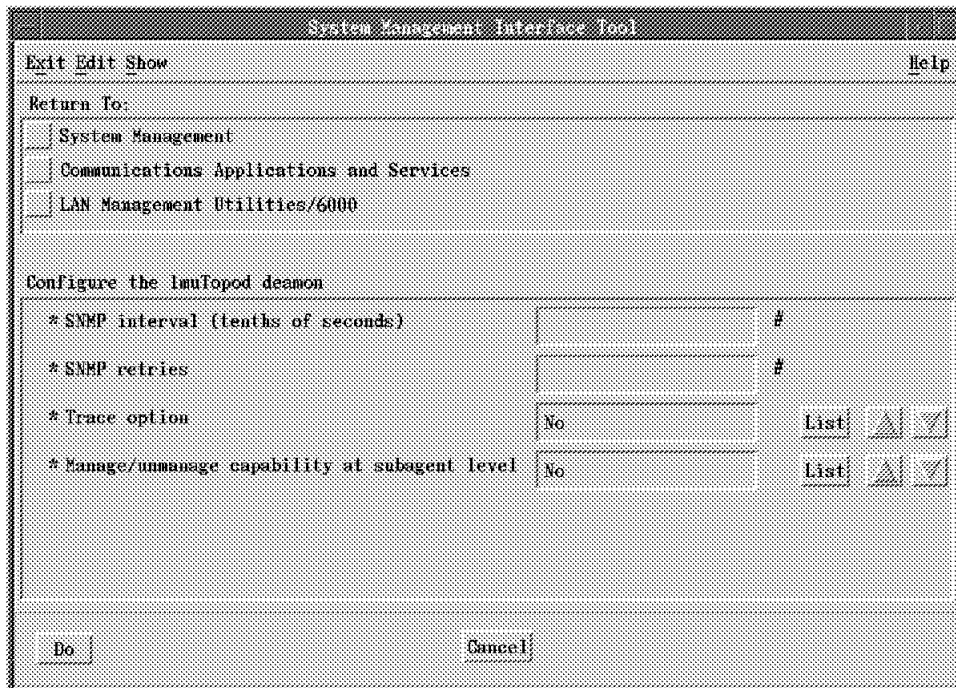


Figure 44. SMIT Screen for the ImuTopod Daemon Configuration

2.5 LMU/2 Configuration

When configuring LMU/2, one of the tasks is to decide which role each machine will play in the LMU/2 environment.

In general terms, a machine can be:

- A managing station: it is a NetWare requester and/or OS/2 LAN Server requester that receives configuration and performance information from the managed workstations and stores the data in an OS/2 database. It also directs alerts to the fault management system and monitors the heartbeat status of managed workstations.
- A managed station: it is a node in the NetWare and/or OS/2 LAN Server environment (server or requester) that:
 - Sends configuration information to a managing system for inclusion in an OS/2 database (any platform)
 - Directs alerts to the fault management system (any platform)
 - Executes remote commands received from an administrator workstation that do not require user response (OS/2, Windows, NetWare Server or Macintosh based)
 - Issues periodic heartbeat signals to the managing station to indicate that the station is alive (OS/2, Windows, NetWare Server or Macintosh based)
- Administrator workstation: it is a NetWare requester or OS/2 LAN Server requester, logged on as an administrator/supervisor, that has the ability to direct remote commands to a managed station.
- Fault manager: it is a requester (NetWare or OS/2 LAN Server) that receives alerts from managed stations, performs some action based upon the alert value, and forwards this alert to IBM NetView or IBM LAN Network Manager.
- Proxy agent station: it is a NetWare requester or OS/2 LAN Server requester that interacts with an SNMP agent and sends data to the AIX LMU/6000 program that, in turn, sends commands back. This station must have TCP/IP support. Examples of this interaction are shown in 2.7.3, “Using the AIX LMU/6000 Program” on page 68.

Notice that a single OS/2 workstation can perform more than one of these defined actions. For example, in our environment we have configured one machine to be a managed, managing, fault manager, proxy agent and administrator machine. In addition, it maintains the LMU database running DB2/2.

2.5.1 LMU/2 Configuration for OS/2 Stations

This section covers the configuration of the OS/2 station that has just been described. Bear in mind that modifications should be done according to your environment definitions. The key points are customization of the `lmu.ctl` file described in “General Customization File” on page 52 and the use of the LMUCUST utility, explained in more detail in 2.5.1.3, “Preparing the Environment” on page 53.

2.5.1.1 IBM TCP/IP for OS/2 Configuration

Refer to 1.5.1, "TCP/IP Installation and Configuration" on page 31 for a description of how to configure the base IBM TCP/IP for OS/2.

You have to update the MIB file to include the LMU/2 related MIB. To do that, type the following command:

```
copy tcpipetcmib2.tbl + lmu2lmumib.tbl = tcpipetcmib2.tbl
```

The administrator workstation has to be enabled to receive the remote commands that will be forwarded to the target managed stations and executed there. The configuration consists of defining a user ID and a password for the REXEC command, as shown in Figure 45. This is done through the TCP/IP Configuration application (tcpipcfg.exe) located inside the TCP/IP folder.

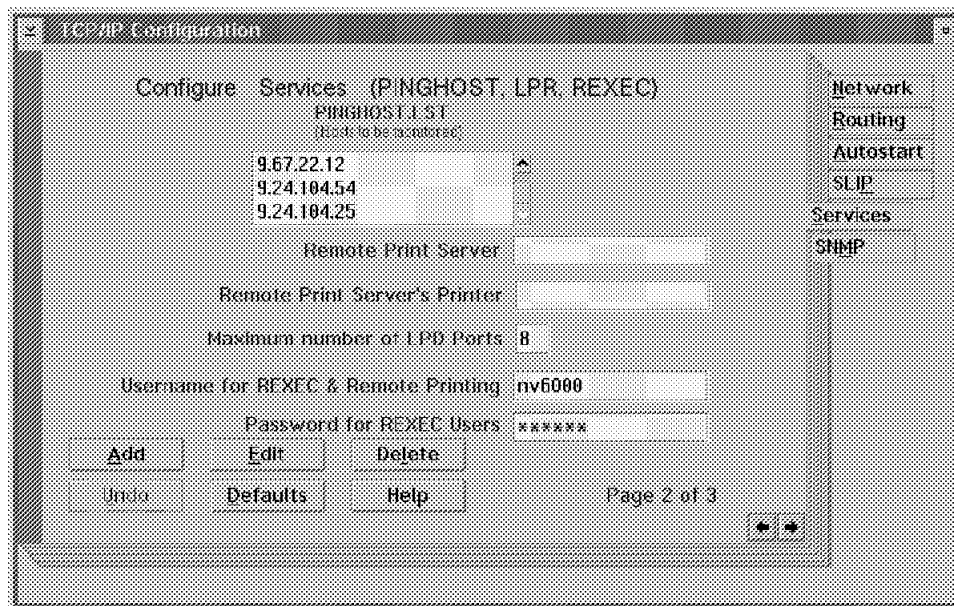


Figure 45. IBM TCP/IP for OS/2 Configuration - REXEC Customization Panel

Notice that the password is not shown for safety reasons. Actually, this configuration only inserts these lines in the CONFIG.SYS file:

```
SET USER=nv6000  
SET PASSWD=xxxxxx
```

Also, do not forget to specify that you want the rexec daemon to be started automatically. This is shown in Figure 46 on page 51.

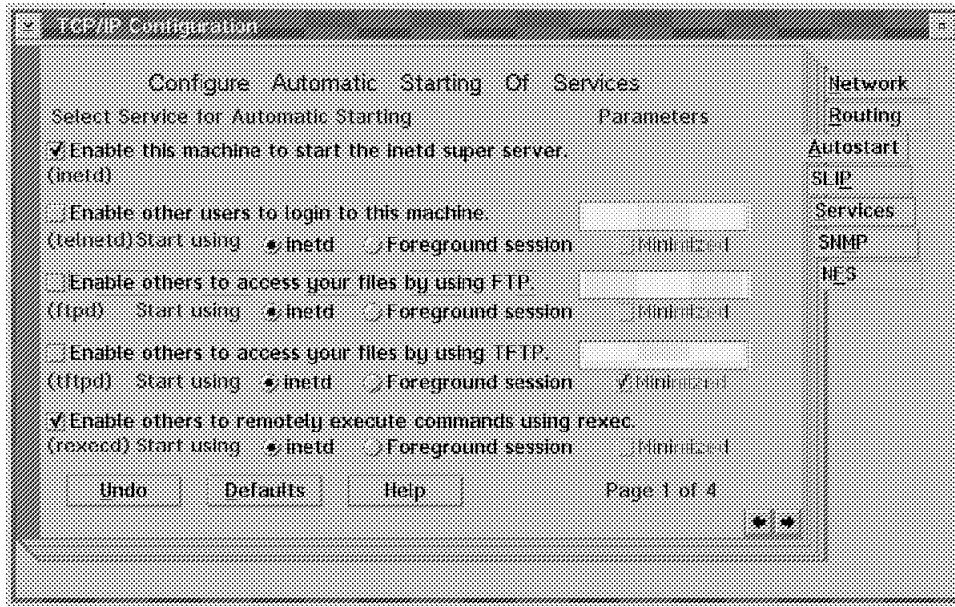


Figure 46. IBM TCP/IP for OS/2 TCP/IP Configuration - Autostart Panel

An optional configuration step would be to set up the RISC System/6000 that is running AIX LMU/6000 to automatically attach the user ID and password when communicating with the administrator station. Otherwise, operator intervention will be required to provide this information, as shown in Figure 47. This is done by inserting an entry in the netrc file located in the home directory of the user who is issuing the command. The entry we have used was:

```
machine aixagent2 login nv6000 password xxxxxx
```

Make sure that the permission bits for this file are:

```
rw-----
```

If not, use the command:

```
chmod 600 .netrc
```

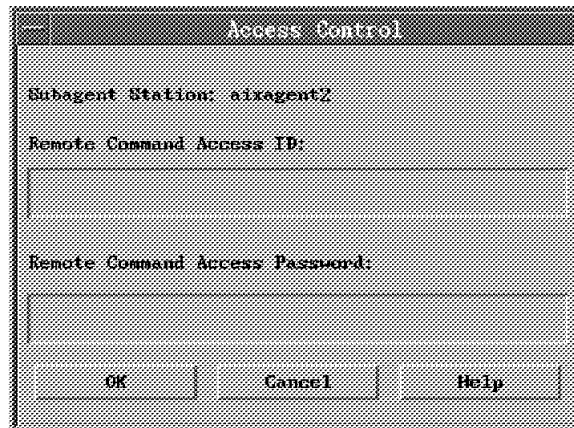


Figure 47. Remote Command Access Control Dialog Box

2.5.1.2 LMU/2 Control Files Configuration

There is a an OS/2 program called LMUCUST that automates most of the actions required to customize a workstation, but there are some changes that need to be done manually.

Note that all the configuration files are in the LMU2 directory.

General Customization File: The LMUCUST program reads the `lmu.ctl` file in order to perform the customization. There is a sample file called `lmuctl.smp` that might be used as a base to build the `lmu.ctl` file. This file specifies where to find the managing stations, the proxy agent, the fault manager and other components. It does not define the role of this machine. This definition is done when the LMUCUST program is executed.

The changes we made were:

- Substituted all *computername or internetwork address* references in the ASCIIZ entries to 00000009:400000033342. This number is the ID of our machine in the NetWare network and consists of the NetWare network number and the MAC address of the machine. If you are in a OS/2 LAN Server environment, you would change it to the value of the workstation field that is in the `ibmlan.ini` file located in the IBMLAN directory.

Of course, in your environment, you might have different machines performing the various roles that we have mentioned before. Therefore, make the changes to meet your specific case.

- Modified all the drive references from C: to D:, since we have installed the LMU/2 code on the D drive.

The only exception was the statement:

```
DEFINE_PROFILE INI_FILE(C:LMU.INI)
```

because this file needs to reside on the OS/2 boot drive and must have the name `LMU.INI`.

- When defining the proxy agent to be accessed, you also have to specify its name:

```
APP(LMU_UTILITY),  
KEY(SNMP_PROXY_AGENT),  
ASCIIZ(lmusnmpd,00000009:400000033342);
```

The sample file also has the characters `'...'` indicating that you may address more than one proxy agent. Whether you have one or many proxy agents, you need to remove these characters from the statements.

There is a copy of the `lmu.ctl` file that we have used in A.1, "LMU.CTL File" on page 229.

User-Provided Configuration File: Another file to customize is the `uservpd.dat`, that provides user-chosen information to the `QUERYVPD` program. This configuration data will be sent to the LMU database during the customization process.

There is a sample file named `uservpd.smp` that can be edited and used as a base file. Copy this file to `uservpd.cfg` and run the `CVT_VPD` utility against it to produce the `uservpd.dat` file, as follows:

```
cvt_vpd uservpd.cfg uservpd.dat
```

The uservpd.cfg file that we have used can be found in A.2, "USERVPD.CFG File" on page 235.

Fault Manager-Related File: There is a sample file called aueuser.smp that helps in the definition of the generic alert table that will be used with the fault manager. We copied it to the aueuser.tab file. A sample entry in this file is:

```
# Product/ Alert Alert
# App1 Id Type Desc Source Target Auto Notify Auto Notify
# ----- -----
5622153 11 C000 * * 0000Y 0000Y 0 0 -$B Alert from -$c is -$t
```

The sample table comes with the parameter -\$g in the command field. This value indicates that the alerts received by this machine will be sent to the LMU/2 graphical user interface. You might want to change this value to -\$b in all entries, so that it will send the alerts to both the LMU/2 GUI and the LMU/2 SNMP proxy agent.

You can run the AUEVERTB utility against this table to check for syntax errors. This utility needs the lmu.ini file because it sends its output to the log file defined there. You will only be able to do this checking after the first time you run the LMUCUST program.

As this table is read only at the startup of AUERECVR (the process that actually performs actions against the alerts received), whenever a change is made to this file, it has to be restarted. In order to do this, use these commands:

```
lmuquery /tf auerecvr
detach auerecvr
```

2.5.1.3 Preparing the Environment

After following the previous steps, we were able to use the LMUCUST program to customize LMU/2. The command we used was:

```
LMUCUST managing alerts fault_manager managed administrator proxy_db /Td
```

You will need to start this command from the lmu2 directory or specify the directory to be inserted in the OS/2 CONFIG.SYS file. The path entry will need to be updated.

The options that we used were:

- managing: the station will be a managing system, listening for heartbeats and maintaining the LMU database.
- alerts: the managing station will generate alerts.
- fault_manager: the station will handle alerts that originate from a workstation.
- managed: the station will receive controlling commands and send requested information to the managing system.
- administrator: the station will be able to issue controlling commands.
- proxy_db: the workstation will start the LMU proxy agent, which allows access to the LMU database.
- /Td: target drive will be redirected to drive d.

The output of this command is shown in Figure 48 on page 54.

If you want help on the LMUCUST options, enter LMUCUST ?.

If you are configuring a managed station only, you should run the LMUCUST program with the following parameters:

```
LMUCUST managed /Td
```

```
IBM LAN NetView Management Utilities
5622-153 (C) Copyright IBM Corp. 1991, 1993. All rights reserved.

IBM LAN NetView Management Utilities Maintenance Level LM00200

LMUCUST: If you have not already created a fault manager alerts table,
do so, based on AUEUSER.SMP.

LMUCUST: LMU.INI built from D:\LMU2\LMU.CTL.

LMUCUST: USERVPD.SMP is in your D:\LMU2 subdirectory.
See the IBM LMU/2 User's Guide for more information concerning
modifying USERVPD.SMP to make a USERVPD.DAT file.

LMUCUST: Cannot locate line in STARTUP.CMD that starts the
server or requester. You must manually add
'CALL D:\LMU2\LMUSTART.CMD' to your STARTUP.CMD.

LMUCUST: LMUCUST does not increase the number of NetBIOS resources available
to LMU. Modify the NetBIOS resources as needed.

LMUCUST: Customization complete, restart the computer to activate changes.
```

Figure 48. LMUCUST Command Output

Running the LMUCUST utility results in the CONFIG.SYS file being updated, the lmu.ini file is created and a LMU/2 folder is created for the administrator workstation. Since there is no entry in the startup.cmd file to start a requester, the lmustart.cmd command file will not be inserted. For the station that will maintain the LMU/2 database, this may be useful since there is a sequence that needs to be followed in the startup of the system. This sequence is covered in 2.6, "LMU/2 Startup" on page 57.

NOTE: If your proxy agent is not running in the station defined by the environment variable HOSTNAME or the community name to access the MIB variables in that machine is not *public*, you will have to specify these values in the proxy agent entry inside the lmustart.cmd file. 2.6, "LMU/2 Startup" on page 57 has an example of this entry. It is necessary to restart the OS/2 system to make these changes effective.

2.5.2 LMU/2 Configuration for DOS Stations

There is not much to customize in the DOS environment. The minimum function to configure is to issue a heartbeat when the machine is started. This is done by inserting the following line in the autoexec.bat file:

```
C:\lmu2\lmu2shb.com managing_system
```

The value managing_system can be either a computer name (if in the OS/2 LAN Server environment) or an internetwork address (if in a NetWare environment).

This line could also be included in the profile.bat file or in the NetWare login script.

Use the parameter ? to display the syntax for this command.

The DOSVIRGA.COM program sends an alert to a fault manager station warning that a virus is detected. It does not detect the virus. You will have to run a virus-detection program, check the return code from this program and, if the "virus detected" condition is satisfied, call DOSVIRGA. It will send an alert to the fault manager defined by the SET FAULT_MANAGER statement that will also have to be defined in the autoexec.bat file.

If you want to store specific information about your machine in the OS/2 database, customize the uservpd.smp file in the same way that it was done in "User-Provided Configuration File" on page 52. Use the QDOSVPD.COM program which is the equivalent of OS/2 QUERYVPD in the DOS environment to send this information to the database. To execute it, type:

```
qdosvpd /rdestination
```

Where *destination* is either the computer name or the internet network address.

The AUEDOSAL.COM program generates alerts and it is helpful if you are going to do your own alert generation.

2.5.3 LMU/2 Configuration for Windows Stations

Before proceeding to the actual configuration, make the LMU2 directory (or the one in which the Windows portion of the code was installed) the current directory.

We have used the following procedure to customize the Windows workstation:

- If you have already configured the lmu.ctl file as described in "General Customization File" on page 52, copy it to the LMU2 directory. The configuration utility will use this file to customize the lmu.ini file, that is used in the Windows environment to specify the LMU/2 related variables.

If not, copy the lmuiniw.smp file to lmuw.ini and fill in the appropriate information:

- MANAGING_SYSTEM: Station to receive the heartbeats
- MANAGING_SYSTEM_WITH_DATABASE: Station maintaining the LMU/2 database
- FAULT_MANAGER: Station to receive the alerts generated by the workstation
- PULSE_RATE: Frequency of the heartbeat. Zero means only initial and terminating heartbeat. The default value is 60 (one hour)
- MESSAGE_LOG: Path and name of the file to log messages related to LMU/2

- Run the customization utility:

```
LMUCUSTW NETWORK
```

If you are in an OS/2 LAN Server environment, change the parameter NETWORK to IBM.

This utility will:

- Update the PATH environment variable located in the autoexec.bat file.
- Update the windowwin.ini file to automatically execute the LMUCLIWR command (LMUCLIWB, if installing for OS/2 LAN Server), by placing this command in the RUN statement.
- Create the windowslmu.ini file (if it does not exist), retrieving the information from a source file searched in the following order:
 - LMUW.INI
 - LMUW.CTL
 - LMU.CTL

If you are going to modify an existing configuration, first remove the windowslmu.ini file.

The lmu.ini file that we have used is in A.3, "LMU.INI File" on page 236.

The station is now ready to be restarted.

2.5.4 LMU/2 Configuration for NetWare Servers

Follow these steps to configure your NetWare server:

- Copy the lmubind.smp file to lmubind.ctl. In this new file, you are going to set the values for:
 - MANAGING_SYSTEM: The internetwork address of the OS/2 machine that will monitor the heartbeat of this server.
 - M_WITH_DATABASE: The internetwork address of the OS/2 machine that will maintain the LMU/2 database. It can be the same station as defined in MANAGING_SYSTEM.
 - FAULT_MANAGER: The internetwork address of the OS/2 machine acting as the alert handler.
 - MESSAGE_LOG: The volume, path and file name of the LMU/2 message log on this server.
 - PULSE_RATE: The interval, in minutes, between the heartbeats. This value is specified in hexadecimal, four digits, 0000 meaning only initialization and termination heartbeats.

The lmubind.ctl file that we have used is in A.4, "LMUBIND.CTL File" on page 236.

- At the NetWare server console, run the following commands:
 - load <volume:path>LMUBNDCS.NLM
This module will update the bindery (NetWare internal database) with the LMU/2 control variables provided by the lmubind.ctl file.
 - load <volume:path>LMUNLMCS.NLM
This module updates the bindery with the location of the autoexec.bat file and inserts the following line in this file:
c:\qdosvdp.com +kc: +Q
This command stores the user-provided data in the C drive, in quiet mode. This data will be used afterwards by the QUERYVPD.NLM.
 - load <volume:path>LMUNCFCS.NLM

The autoexec.ncf file (one of the files used in the server startup) is appended with these lines:

```
SEARCH ADD SYS:LMU2
LOAD QUERYVPD /R
LOAD LMUCLI
```

This will add the LMU2 subdirectory to the search path, send the user-provided data to the managing system maintaining the database and load the LMU/2 client code to receive remote commands and send heartbeats to the managing system.

- load <volume:path>LMUVPDCS.NLM

Copies the qdosvpd.com and the adapters.tbl files to the DOS partition in the same path as the autoexec.bat file.

- Restart the machine.

After this customization, a utility called LMULOAD will be available at the server's console that enables you to view and modify the parameters defined in the lmubind.ctl file (and others) in interactive mode. Be careful while using this utility because it considers a space as a valid entry. If you accidentally press the space bar, it will overwrite the previous information and store a space in its place.

2.6 LMU/2 Startup

Because there is a determined sequence for the software components to be started in order to have the LMU environment available, it is advisable to check the behavior of your system.

As you will see, there are some phases that need the user's intervention and you might want to disable the automatic startup procedure. These procedures are located in the startup.cmd file and in the startup folder under the OS/2 System icon.

Be aware that there are also some procedures that are automatically performed by the OS/2 system to reproduce the condition that you had when the machine was last stopped, regardless of whether you request it or not.

The sequence we found to be most effective in our environment (administrator, managing, managed and proxy agent station maintaining the LMU/2 database) was:

- Start TCP/IP

From an OS/2 command prompt type:

```
'Call tcpstart'
```

- Start SNMPD daemon:

If the SNMPD daemon is not being automatically started, use the command:

```
start "SNMPD" /min d:tcpiplibsnmpd.exe
```

Note: Make sure that you are using the correct path.

Do not insert this command in the tcpstart.cmd file because every time a configuration change is made, the TCP/IP Configuration program overwrites the existing file with a new one and all the manually inserted entries are lost. Insert it into the tcpexit.cmd file instead.

- Login to your LAN
Login on your LAN environment as you would normally do. For example:
login supervisor
- Login on the local environment
For example:
login USERID /p:PASSWORD
This login is necessary to have access to the DB2/2 database. From the USER PROFILE MANAGEMENT SERVICES folder, double click on the LOGON icon and logon as the administrator user who has created the LMU/2 database.
- Start LMU/2:
From an OS/2 prompt, type:
lmustart

If you are starting the LMU/2 server for the first time, it will build the LMU/2 database. This operation takes a few minutes and you should receive the messages shown in Figure 49, as for the first time startup. On subsequent occasions, the line *Creating database LMU2* will not show up.

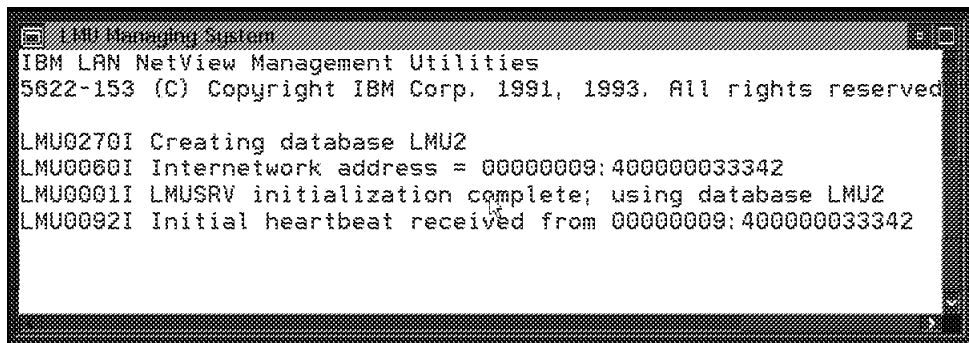


Figure 49. LMU Managing Station Panel Showing Initial Messages

While the database is being created, you may have problems starting the proxy agent with database access (LMUCUST with proxy_db parameter specified), as it will try to access a database that is still being built. In this case, the proxy agent fails. To restart it type the following command:

```
start "LMU SNMP proxy agent" /C d:\mu2\musnmpd.exe /d aixagent2 ITSC
```

Note: Do not forget to change the parameters *aixagent2* and *ITSC* to match your SNMP agent station and community name, respectively.

If the proxy agent starts correctly you will receive the messages shown in Figure 50 on page 59, in the proxy agent window and the SNMPD window.

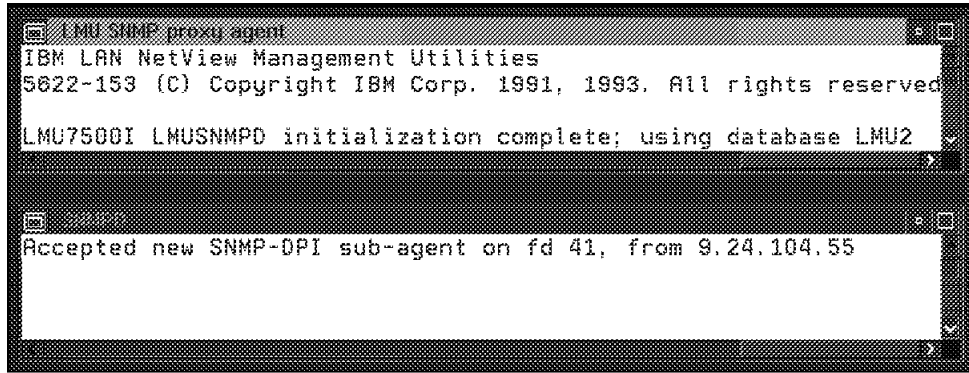


Figure 50. LMU Proxy Agent and SNMPD Panels Showing Initial Messages

When the environment is up and running, you can populate the LMU/2 database with the information you have provided in the `uservpd.dat` file for the OS/2 managed system, by using the command:

```
queryvpd /r
```

You can request that the other managed stations that you have configured (DOS, Windows, NetWare Server) send their `uservpd.dat` data as well. Refer to each configuration section to learn how to do that manually.

2.7 AIX LMU/6000 Operation

After AIX LMU/6000 is installed, an AIX LMU/6000 icon will appear in the root submap when the AIX NetView/6000 program is restarted, as shown in Figure 51 on page 60. This icon will show up blue indicating unknown status, but as soon as `lmuTopod` starts communicating with the proxy agents it should change to a known state, that can be green, yellow or red, following the same rules that apply to an IP icon.

If you have more than one agent, the status that will be displayed will be the aggregate status. If you double-click to go down to a lower-level resource, you will see the status of the individual agents.

2.7.1 AIX LMU/6000 Submaps

There are four levels of hierarchy while navigating through AIX LMU/6000 that can be seen in Figure 51 on page 60 through Figure 55 on page 64.

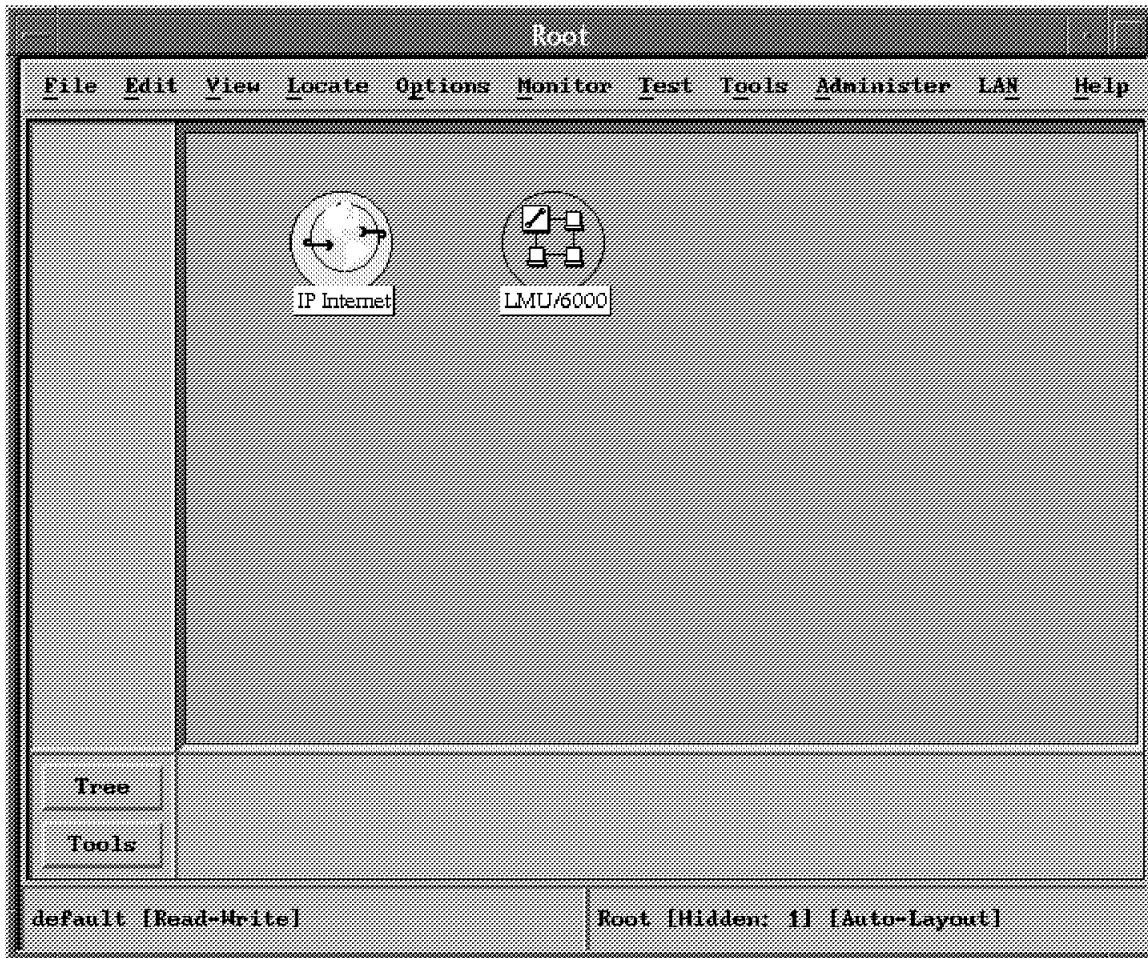


Figure 51. Root Submap

- Root submap, the highest level, shown in Figure 51.

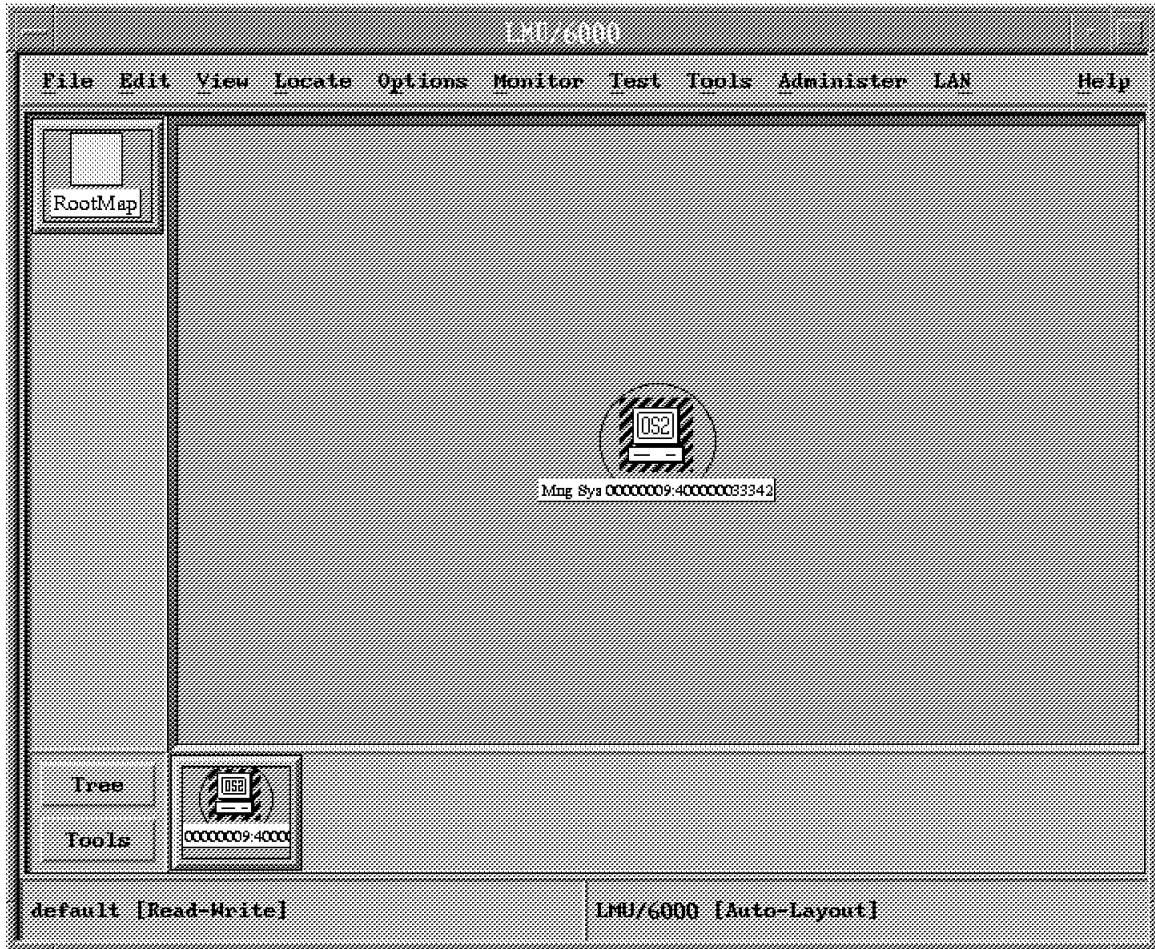


Figure 52. LAN Network Submap

- LAN network submap, that displays the LMU/2 managing system domains, where each icon represents a managing system and its managed stations. An example of this submap is shown in Figure 52.

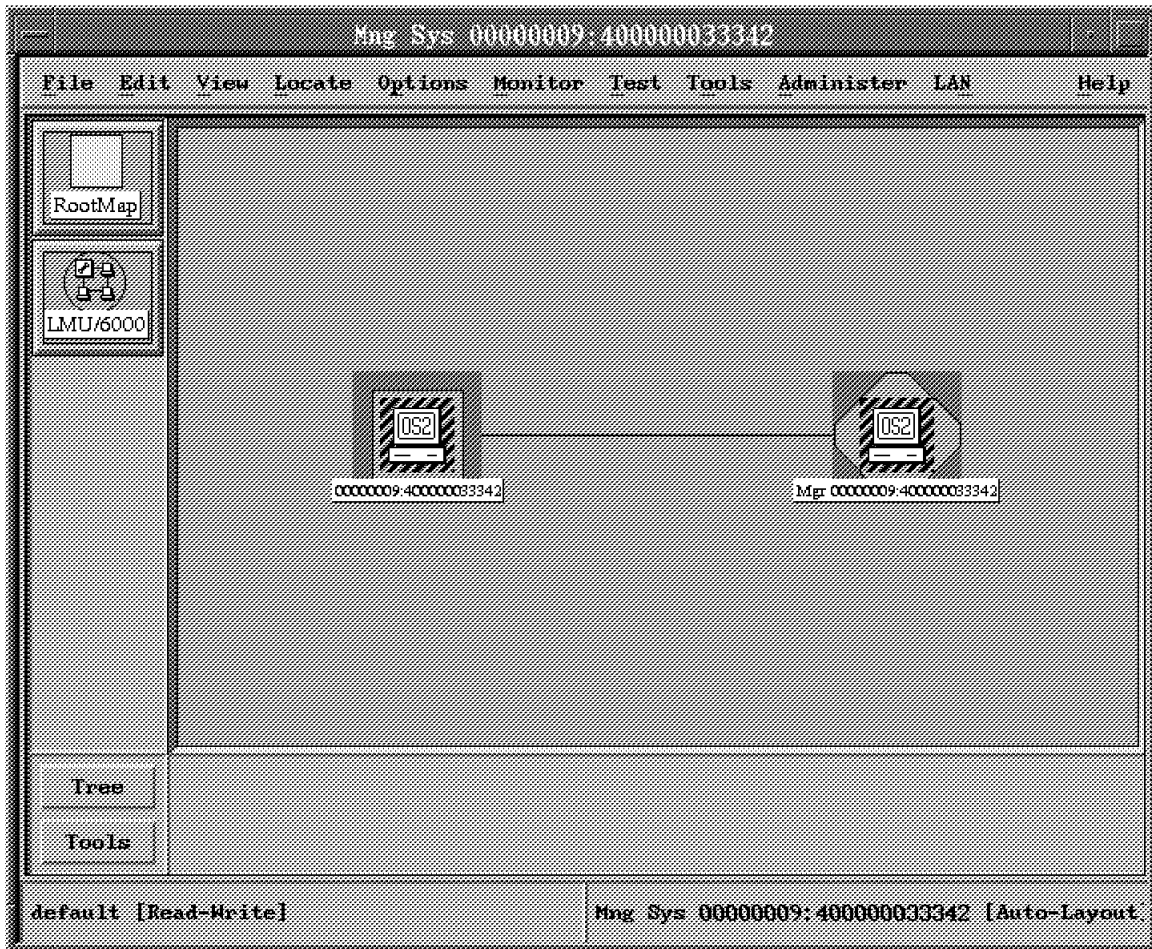


Figure 53. LAN Submap

- LAN submap, that provides a detailed view of a particular LAN network, each icon representing a node. Figure 53 shows a LAN submap, while Figure 54 on page 63 shows the equivalent view using the LMU/2 Graphical User Interface.

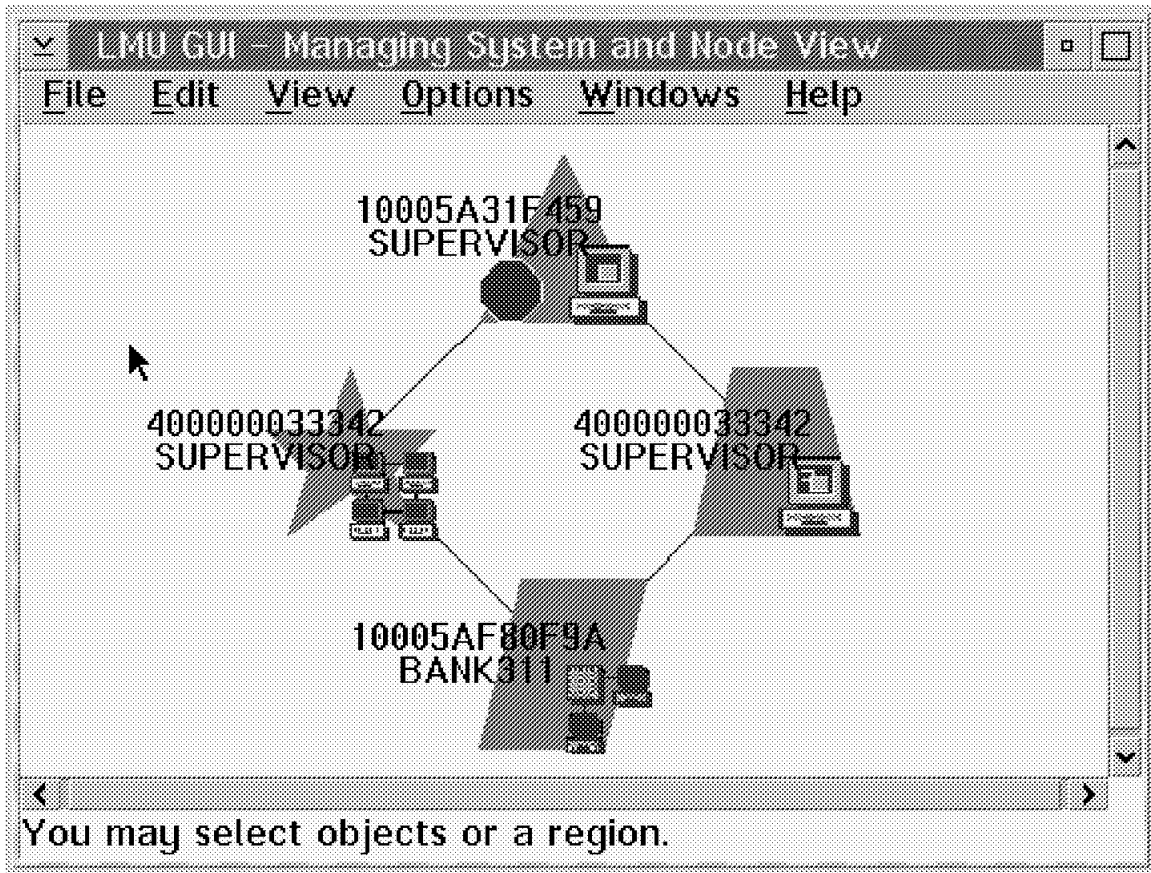


Figure 54. LMU/2 Graphical User Interface

Note that this Graphical User Interface is not automatically started by LMUSTART and it is available under the LMU folder. You start the GUI on OS/2 with the command: start lmugui.

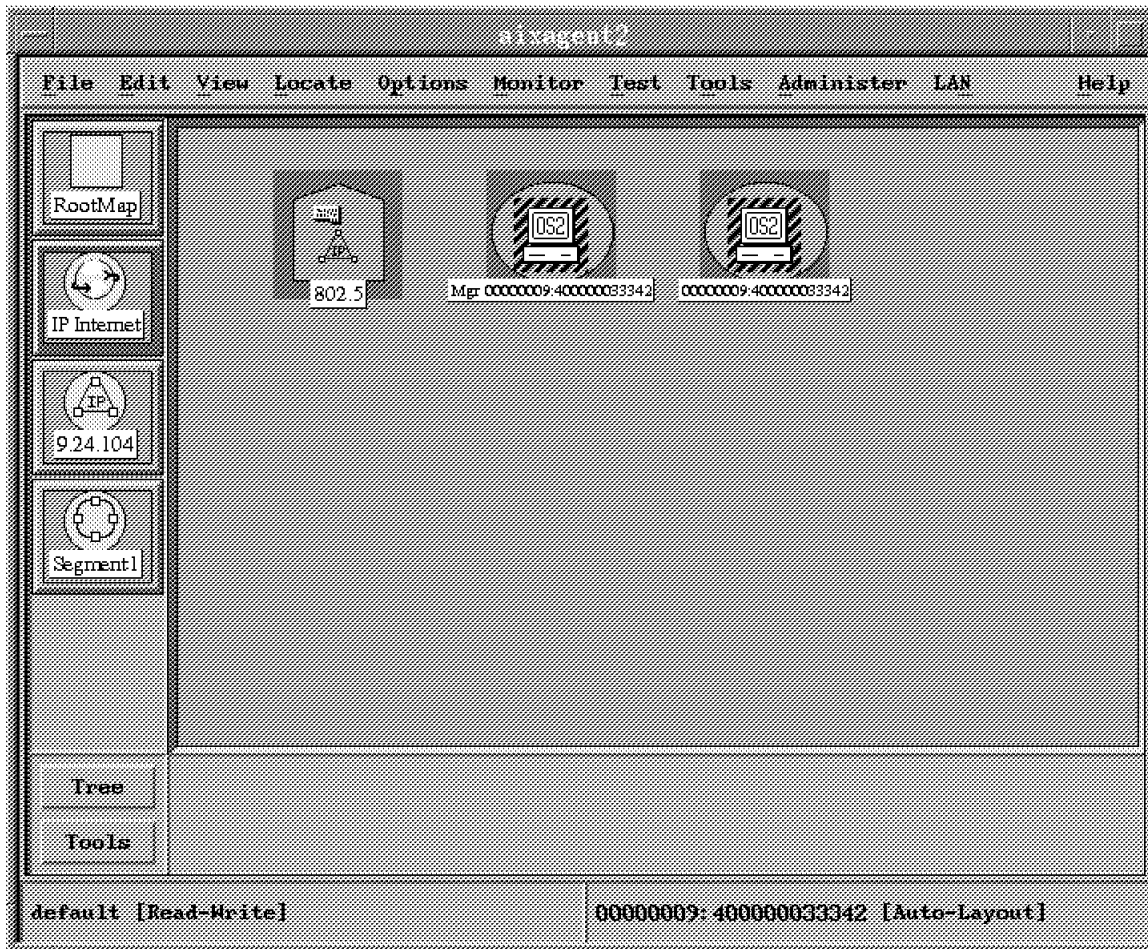


Figure 55. Node Submap

- Node submap, that displays the interfaces present in a node, as shown in Figure 55. As you can see, this node level is shared with other protocols that may be running in the specified machine. If you try to go backwards in the hierarchy you will go to the IP network tree.

2.7.2 Starting the AIX LMU/6000 Program

The AIX LMU/6000 program can be started in three different ways:

1. From the command line, type:

```
lmucmd [node] &
```

To start the Display Data dialog box:

```
lmucmd -rmtcmd [node] &
```

2. Select a proxy agent node from a LAN submap and drag and drop the AIX LMU/6000 icon, as shown in Figure 56 on page 65, to anywhere on the screen. Notice that the AIX LMU/6000 application will not run within the Control Desk.

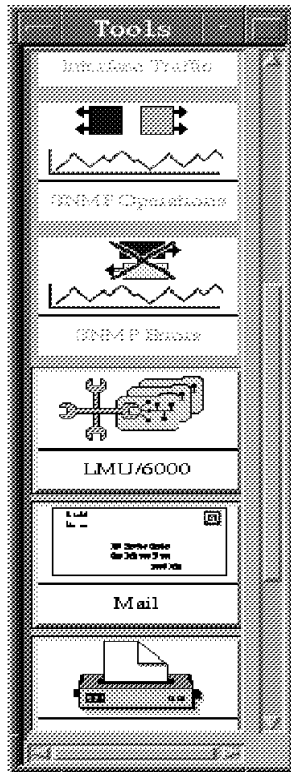


Figure 56. Tool Palette Showing AIX LMU/6000 Icon

3. Select a proxy agent node from a LAN submap and select **Tools...LMU/6000...Display Data**, as shown in Figure 57 on page 66.

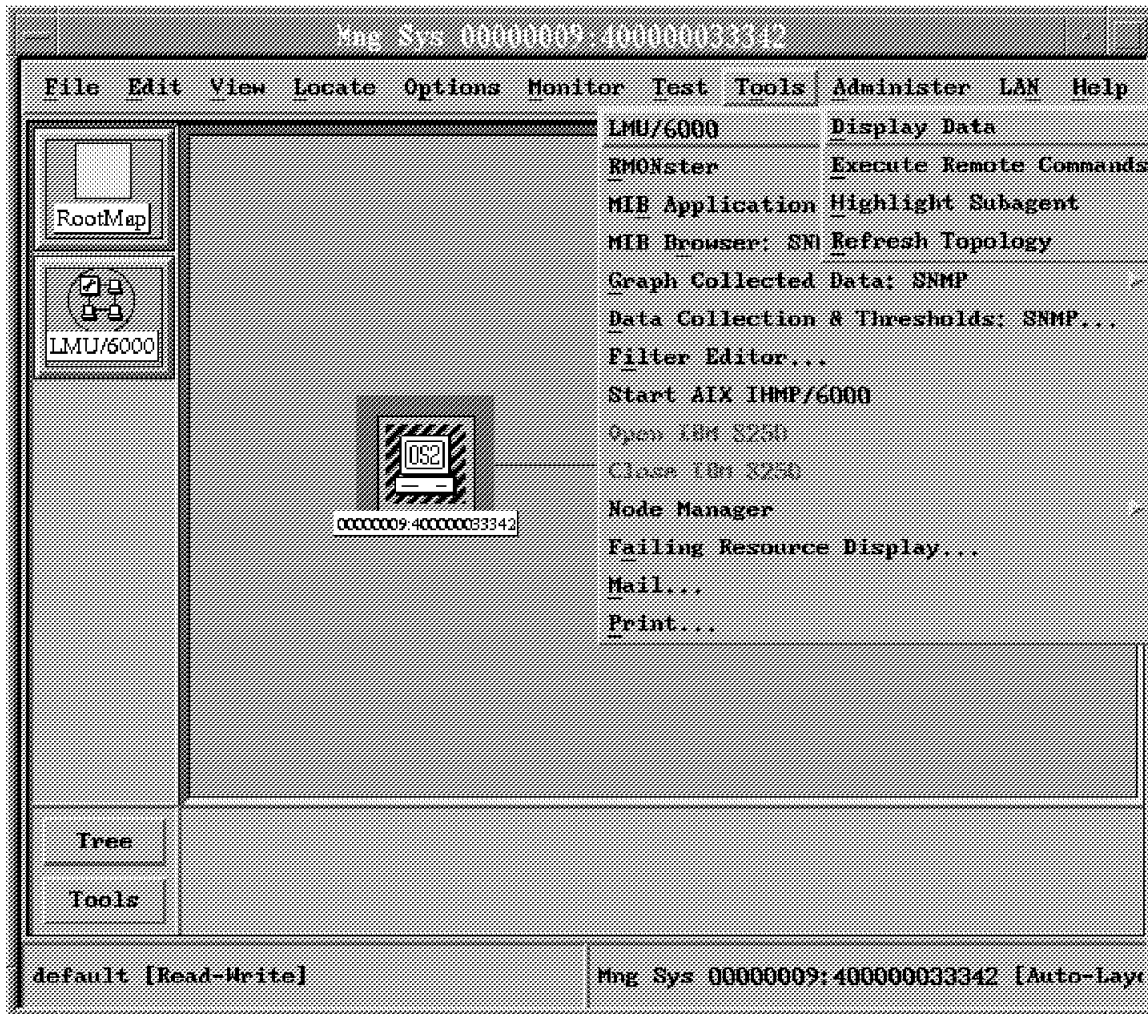


Figure 57. AIX NetView/6000 Menu Showing AIX LMU/6000 Options

Before proceeding to the operation itself, test the activity of the LMU/2 subagent by selecting **Test...LMU Subagent** from the AIX NetView/6000 main menu.

The expected output is shown in Figure 58 on page 67. If you receive all the output values filled with **<NO VALUES>** messages, recheck your LMU/2 system as it indicates that the ImuTopod is not able to communicate with the proxy agent. On the other hand, if you receive values but the Database Support field is not 1, this denotes that you are not able to retrieve information from the LMU database.

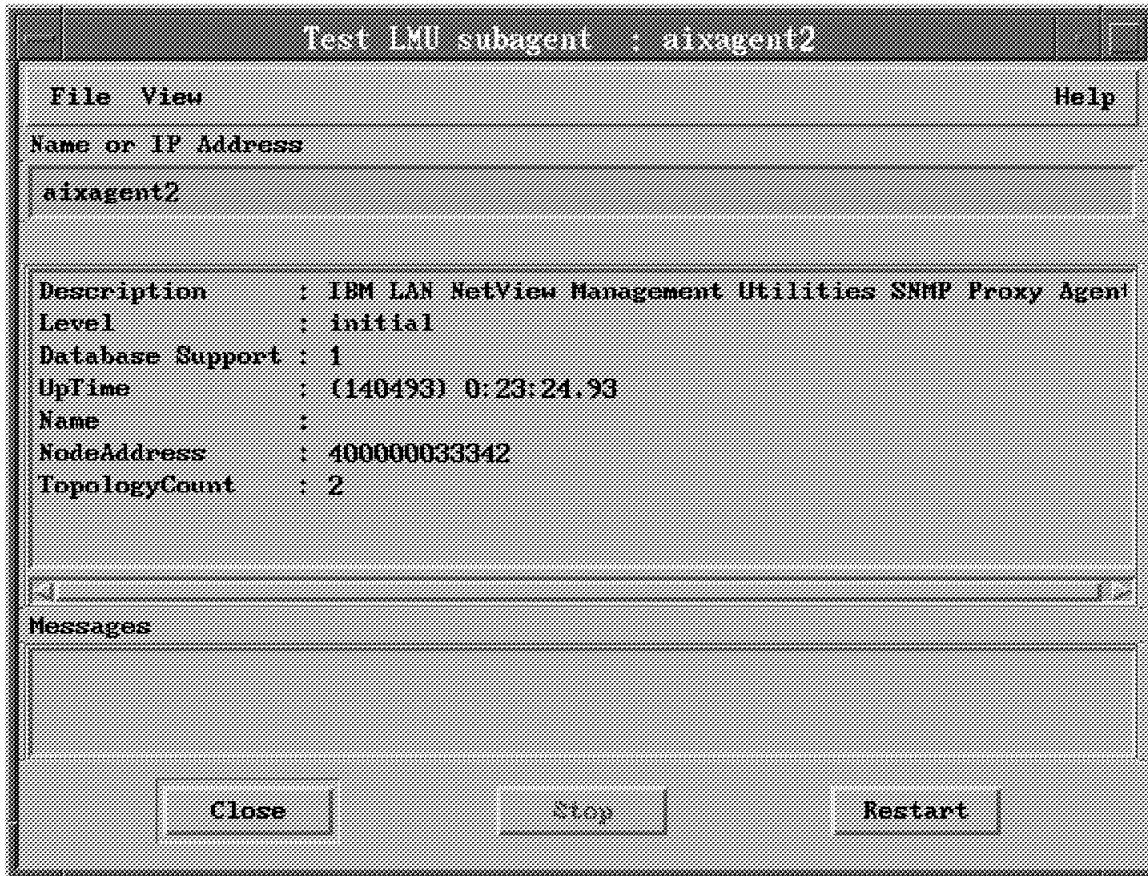


Figure 58. AIX NetView/6000 Menu Showing LMU Subagent Test

By this time, event cards indicating LMU/2 proxy agent activity should be appearing at the AIX NetView/6000 current event application window.

To make sure that the most recent topology is shown, select **Refresh Topology** from the AIX LMU/6000 menu, as was shown in Figure 57 on page 66. Temporarily, the objects will change to the unknown color state but their status will get updated with the current status shortly.

The AIX NetView/6000 event window containing the AIX LMU/6000 related events along with the topology refresh warning is shown in Figure 59 on page 68.

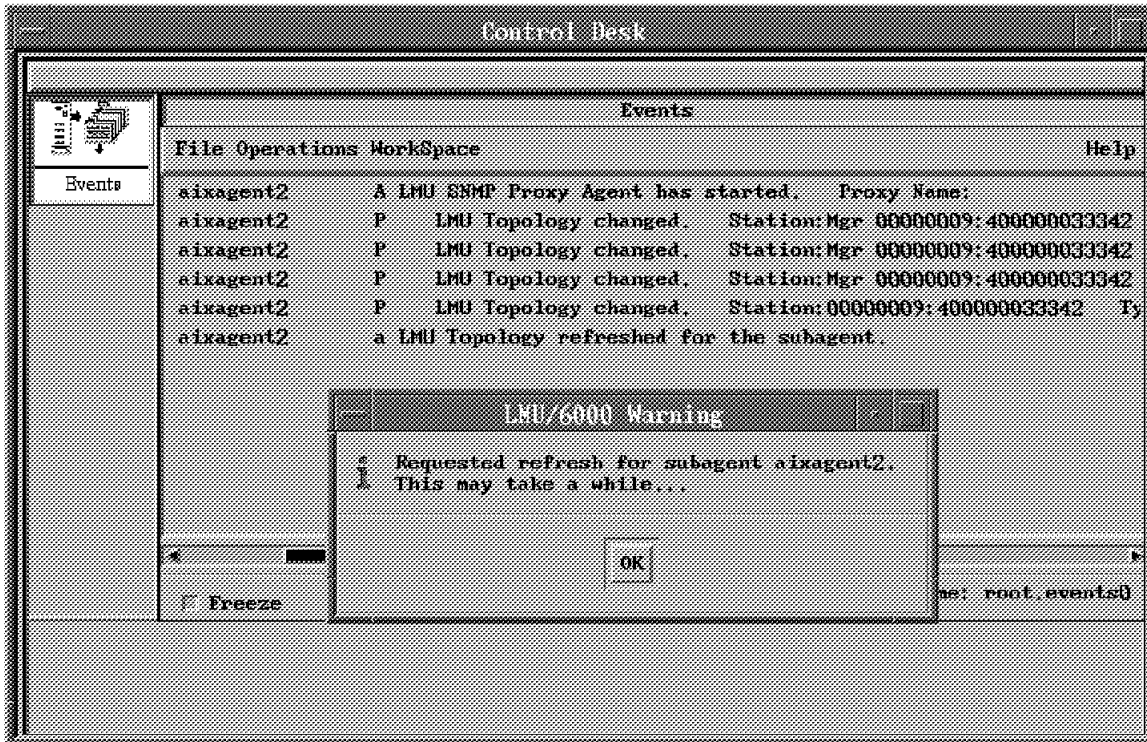


Figure 59. AIX NetView/6000 AIX LMU/6000 Related Events and Warnings

2.7.3 Using the AIX LMU/6000 Program

After starting the AIX LMU/6000 program using one of the methods described in 2.7.2, "Starting the AIX LMU/6000 Program" on page 64, the panel shown in Figure 60 on page 69 will be displayed.

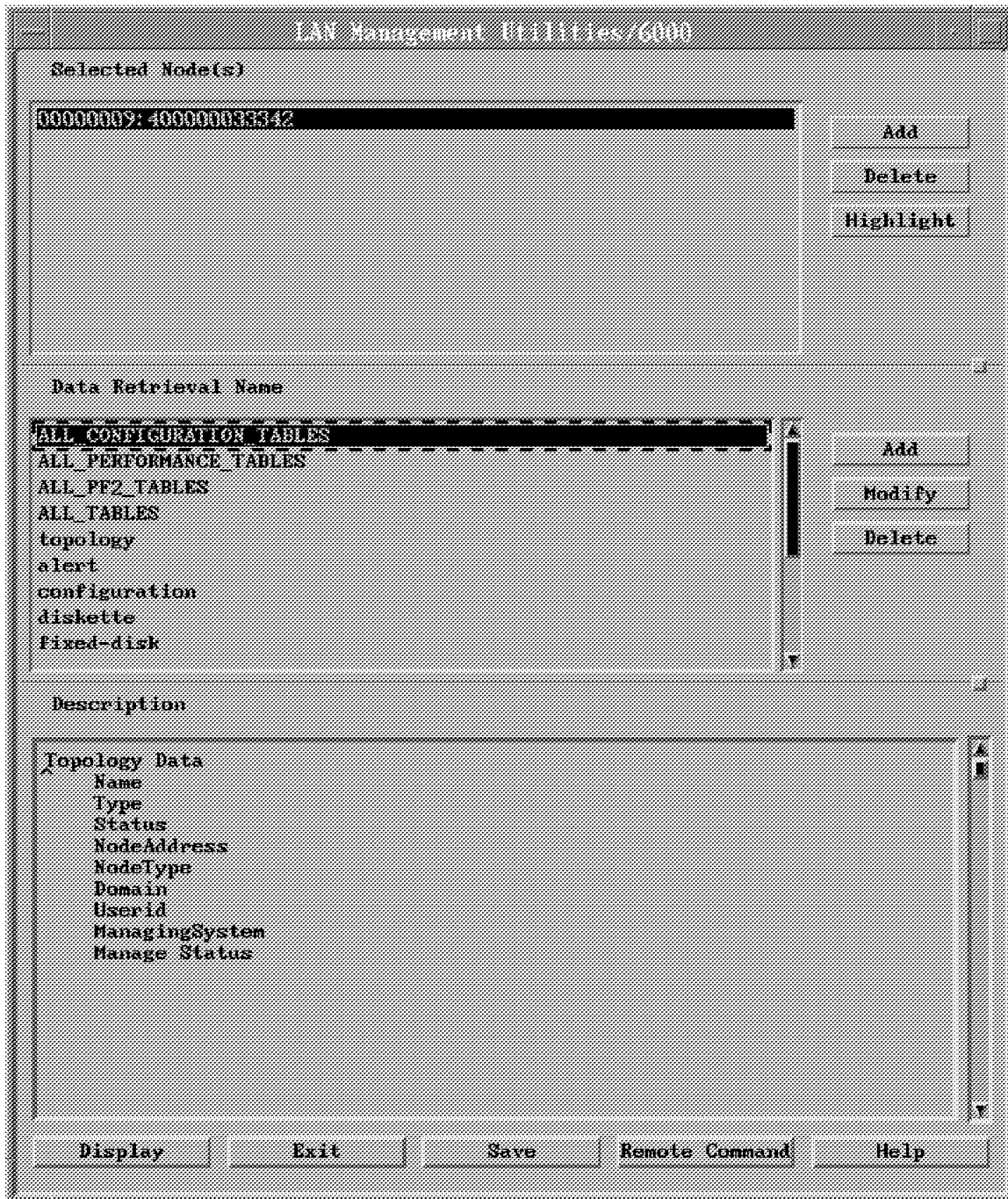


Figure 60. AIX LMU/6000 Program Panel

In order to create your own data retrieval, follow this sequence:

- Click on the **Add** button next to the Data Retrieval Name section. The Attribute Retrieval Selection window will appear with the available data, as shown in Figure 61 on page 70.

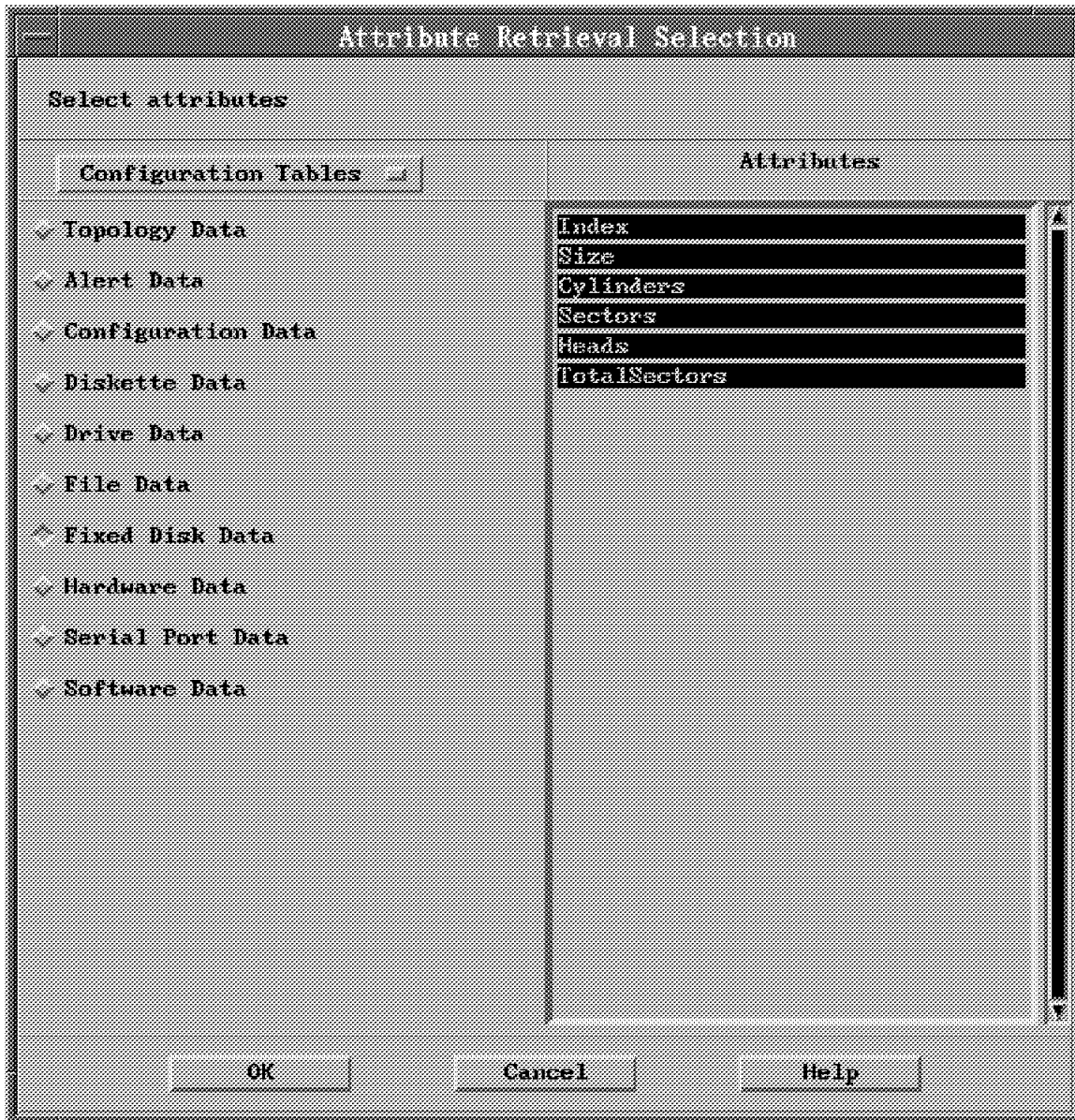


Figure 61. Attribute Retrieval Selection Dialog Box

- Select **Fixed Disk Data** from the Configuration Tables selection list.
- Click on **OK**.
- Enter **mydisk** as the retrieval name.
- Click on **OK**.
- Select a node (if not already selected) under the Selected Nodes list.
- Select **mydisk** from the Data Retrieval Name selection list.
- Click on **Display**.

The Output window will be displayed and, after the LMU database is accessed, it should produce an output similar to the one shown in Figure 62 on page 71.

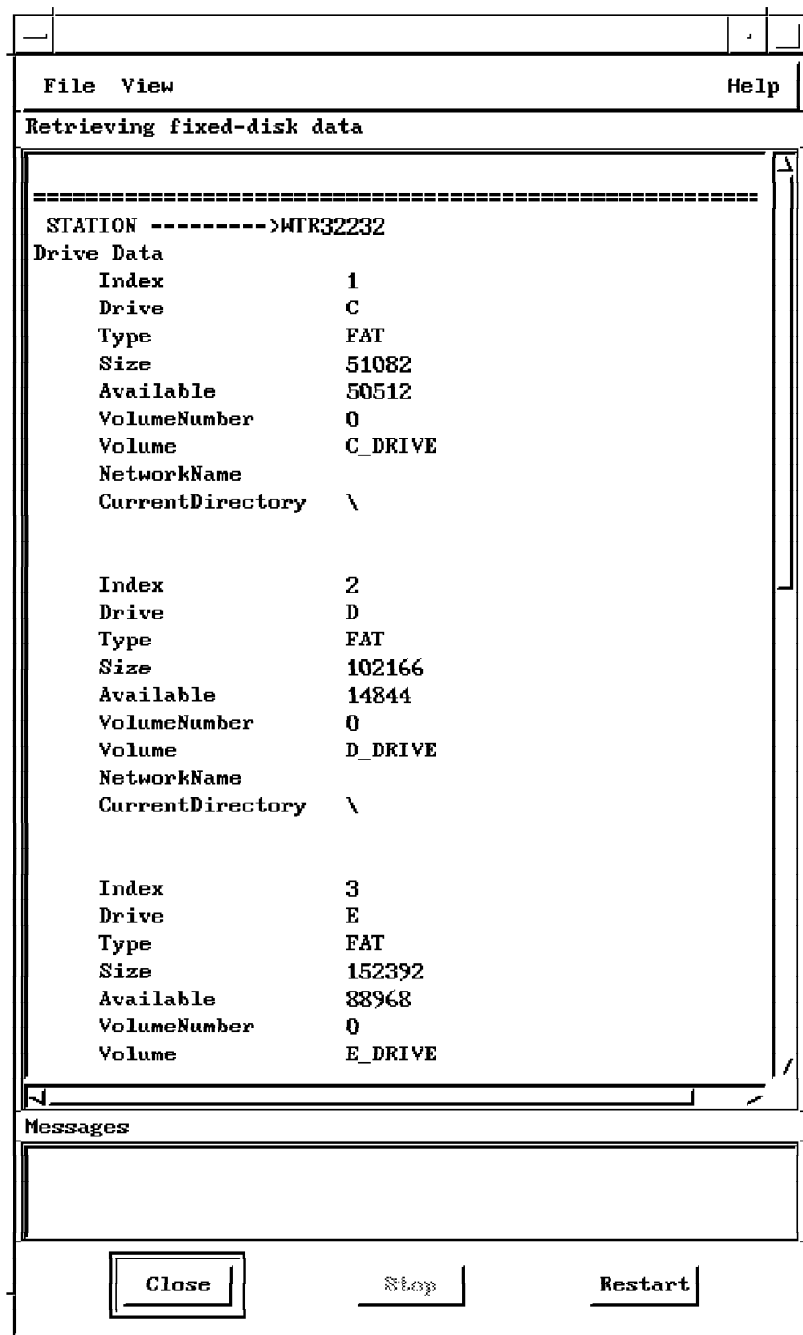


Figure 62. AIX LMU/6000 Data Retrieval Output

It is also possible to issue a remote command to a managed station from the AIX LMU/6000 program. Refer to 2.5.1.1, "IBM TCP/IP for OS/2 Configuration" on page 50 on how to customize LMU proxy agent.

- Click on **Remote Command** in the main AIX LMU/6000 panel.

This will bring up the Remote Command dialog box as shown in Figure 63 on page 72.

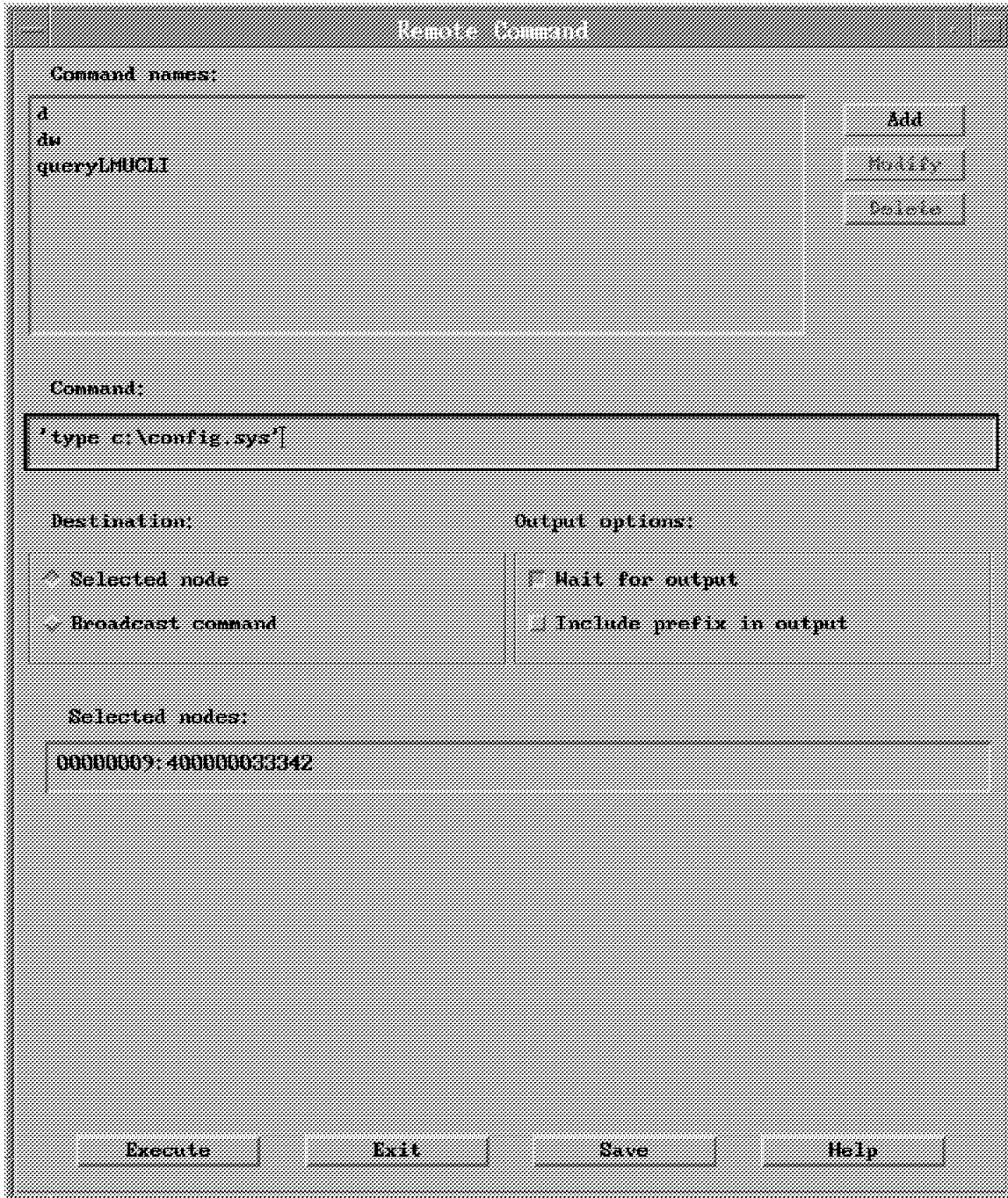


Figure 63. Remote Command Dialog Box

- Type a command in the command section. For example:
`'type c:\config.sys'`

The single quotes are needed to state that the command is to be forwarded as is to the proxy agent without being interpreted by the AIX shell.

- Click on **Execute**.

The remote command output box will be displayed as shown in Figure 64 on page 73. Actually, the command is sent via an REXEC command to the proxy

agent. This command is passed to the administrator station, which in turn requests the managed station to execute the command.



Figure 64. Remote Command Output Dialog Box

Note: A pure DOS machine cannot execute remote commands. NetWare servers can execute remote commands but the output cannot be sent to the AIX LMU/6000 panel, not even to the LMU/2 remote execution output window.

Chapter 3. IBM LAN Network Manager for AIX

This chapter describes how you can use IBM LAN Network Manager for AIX to effectively manage the LAN resources of your network. Topics include:

- Installation
- Configuration
- Operation

3.1 Overview

The IBM LAN Network Manager for AIX (LNM for AIX) program works with the AIX NetView/6000 program to enable you to effectively manage the LAN resources of your network. The functions of LNM for AIX are integrated into the AIX NetView/6000 interface, enabling you to manage the physical resources in your multiprotocol network from a single workstation. You can monitor and manage IP-addressable devices with AIX NetView/6000 and expand your scope of management to token-ring, FDDI and Ethernet environments with LNM for AIX.

The LNM for AIX program provides views of a logical topology of the LAN, which allows you to correlate different protocol views with the underlying physical topology. The LNM for AIX program also provides configuration, fault and performance information for your LAN resources.

The LNM for AIX program manages the different types of networks and resources in your LAN environment by communicating with agent programs, known as LNM OS/2 proxy agents. The proxy agent reports information, such as topology updates or status changes, to LNM for AIX and also responds to management instructions from LNM for AIX. The LAN hardware that is managed by the logical link control (LLC) protocol can be integrated into the SNMP managed environment of AIX NetView/6000 through LNM for AIX and managed along with the SNMP-addressable resources. The LNM proxy agent communicates with LNM for AIX through SNMP that is built into the LAN Network Manager for OS/2 program. The LNM proxy agent also converts event notifications that are generated in the token-ring network to SNMP traps and forwards these traps to LNM for AIX.

Specifically, the IBM LAN Network Manager for AIX program provides:

- A graphical user interface

LNM for AIX integrates topological changes and status updates with AIX NetView/6000. You can access current information about your IP-addressable resources and your LAN resources from a common interface.

- AIX NetView/6000 integration

LNM for AIX sends events for the resources it is managing to AIX NetView/6000, and these are logged and displayed with those from other AIX NetView/6000 applications, such as AIX LMU/6000 and IBM Hub Management Program/6000.

- Token-ring segment management

LNM for AIX enables you to manage both link level control (LLC) and SNMP-based token-ring segments. LNM for AIX utilizes an OS/2 proxy agent running LAN Network Manager for OS/2 to manage the token-ring segment.

The LNM proxy agent converts events that are received from the token-ring environment into SNMP traps before passing them on to the LNM for AIX program. The LNM for AIX program manages the LLC networks based on solicited and unsolicited requests from LNM to LNM for AIX. You can:

- Manage stations, bridges and IBM 8230 Controlled Access Units (CAUs).
 - Collect and graph historical data.
 - Manage access control for adapters and concentrators.
 - Monitor critical resources.
- FDDI segment management

In our environment we did not use an FDDI proxy agent.

- SNMP token-ring management

In our environment we did not use an SNMP token-ring proxy agent

- Integration with hub management applications
- Integration with remote monitor (RMON) applications
- Resource monitoring

LNM for AIX enables your network resources to be easily monitored; different colors are used on the graphical topological display to represent the status of resources displayed in submaps.

- Configuration information

LNM for AIX provides configuration information for all of the LAN resources that it can manage. Some of the information that can be retrieved is:

- LNM proxy agent configuration details
- Bridge configuration and performance

- Fault information

The LNM for AIX program provides a complete set of messages, traps and event notifications. This information is integrated into the AIX NetView/6000 logging capacity and event card display.

- Performance information

3.2 LAN Network Manager Installation

The installation of the LNM for AIX environments involved:

1. Installing LNM for AIX on the RISC System/6000
2. Installing the LNM proxy agents on the OS/2 system
3. Updating and modifying C:\CONFIG.SYS on the LNM OS/2 proxy agent
 - Adding LNM port number
 - Adding community name information
4. Updating and modifying LAPS on the LNM OS/2 proxy agent
 - Adding 802.2 protocol
 - Modifying 802.2 values, SAPS and user IDs
5. Installing IBM TCP/IP for OS/2 and Database Manager 2/2 as shown in 1.5, "IBM TCP/IP for OS/2 and Database Manager 2/2 Installation and Configuration" on page 30

3.2.1 LNM for AIX Installation

To install the LNM for AIX code use SMIT and the values defined in 1.5.3, "RISC System/6000 Software Installation Procedures" on page 40. The list shown when you prompt for the *SOFTWARE to install* field for IBM LAN Network Manager for AIX is shown in Figure 65. Select the top item *1.1.0.0 lnm6000 ALL*.

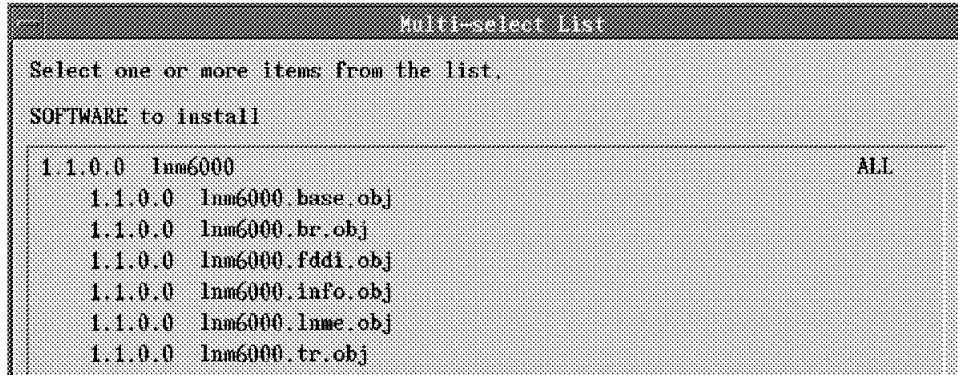


Figure 65. LNM for AIX Install List

The installation requires no further interaction.

3.2.2 LNM OS/2 Proxy Agent Installation

In the OS/2 proxy agent the installation steps were:

1. Added the 802.2 protocol for the LAN adapter
2. Increased the SAPS and user IDs to access bridges and IBM 8230s
3. Updated CONFIG.SYS with the LNM proxy agent requirements
4. Installed the LNM proxy agent code

To add the 802.2 protocol for the LAN adapter we used LAPS as was shown in Chapter 2. To start LAPS key the following in an OS/2 window:

```
cd \ibmcom
laps
```

To start the configuration choose the **Configure** button on the main screen. On the next screen choose the **Configure LAN transports**, then the **Continue** button.

To add the 802.2 protocol to the token-ring adapter that the LNM proxy agent is using do the following:

- Select the **IBM Token-Ring adapter...** from the *Current Configuration* area.
- Select **IBM IEEE 802.2** from the *Protocols* area.
- Click on **Add** to then add this protocol to the token-ring adapter, as shown in Figure 66 on page 78.

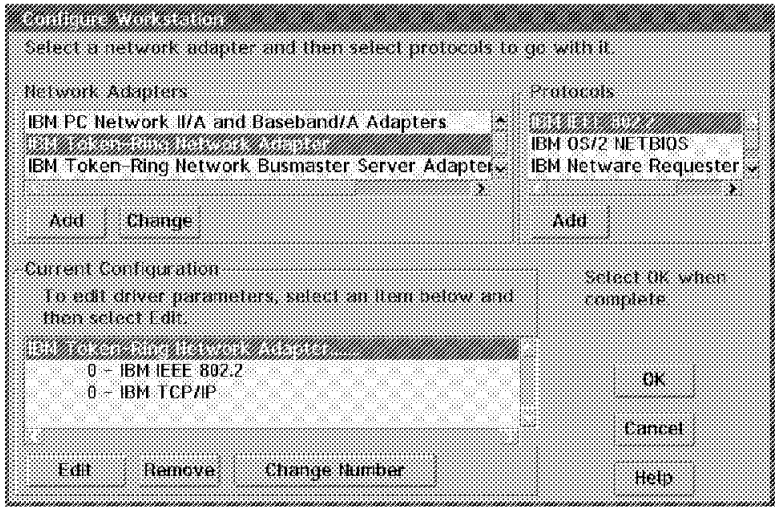


Figure 66. Adding 802.2 Protocol to Adapter

To edit the 802.2 protocol values, **double click** on the 802.2 protocol in the *Current Configuration* list box. Change the values of the following items:

- Maximum SAPs: default is 3. We changed this value to **20**.
- Maximum number of users: default is 3. We changed this value to **10**.

This is shown in Figure 67.

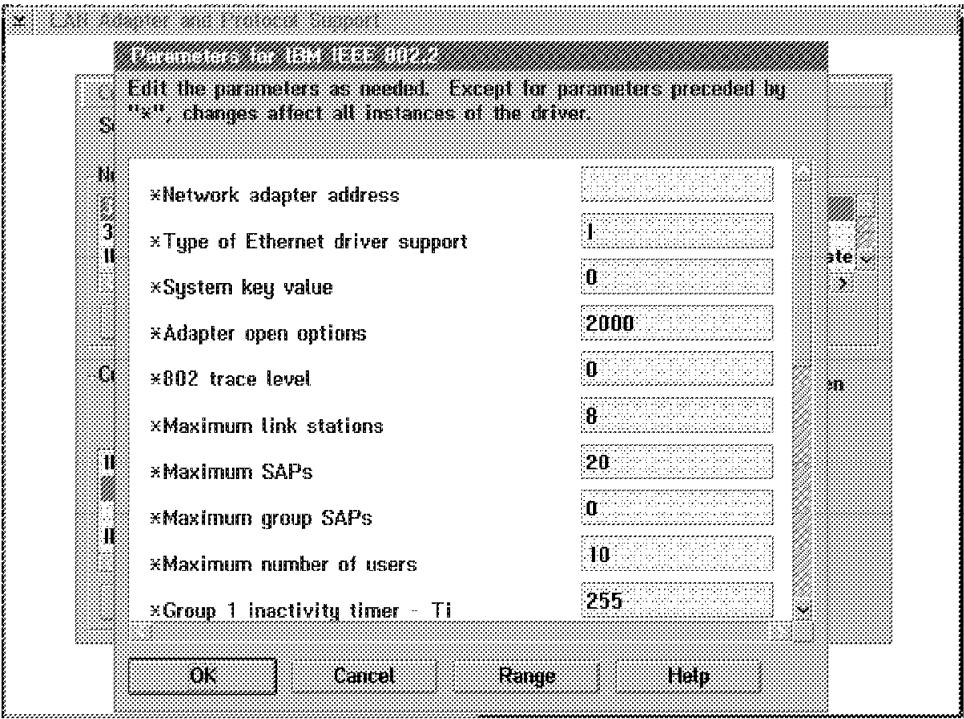


Figure 67. LNM 802.2 Modifications

Choose **OK** to update the configuration and choose the option to update C:\CONFIG.SYS.

Additional items need to be entered into CONFIG.SYS. Use the OS/2 editor to change the CONFIG.SYS file.

The updates to C:\CONFIG.SYS that are required are:

```
SET LNM_PORT=6005
SET COMMUNITYNAME=ITSC
```

In our environment the port number of 6005 and the community name of ITSC were used. These values much match the values that were customized for IBM LAN Network Manager for AIX.

The port number is the TCP/IP socket number that will be used between the OS/2 LNM proxy agent and LNM for AIX; therefore this number must match the port number configured for this proxy agent in LNM for AIX.

Note: If the LNM proxy agent code is installed prior to updating LAPS, (or possibly the installation of other OS/2 products) ensure that the LNM device driver statement

```
DEVICE= D:\LNMEP\EVYDD.SYS
```

is the last line in the C:\CONFIG.SYS file. If it is not then during OS/2 startup a message will be displayed indicating that the device driver was not installed.

Ensure that the IBM TCP/IP for OS/2 and Database Manager 2/2 are installed as shown in 1.5, "IBM TCP/IP for OS/2 and Database Manager 2/2 Installation and Configuration" on page 30.

The installation of the LNM OS/2 proxy agent code is started by keying **A:INSTALL** from an OS/2 window with Disk 1 of 4 in drive A:. This will result in a screen like Figure 68. Choose the drive locations for the LNM code and database and select **Install**. Informational messages are displayed indicating the status of the install process.

Note: If you have already signed onto the local OS/2 database ensure that the user ID that you have used has administrator authority; otherwise the LNM installation will not be able to create the necessary database. If you are unsure then enter **LOGOFF** from an OS/2 window and the LNM installation procedure will then prompt you for the user ID.

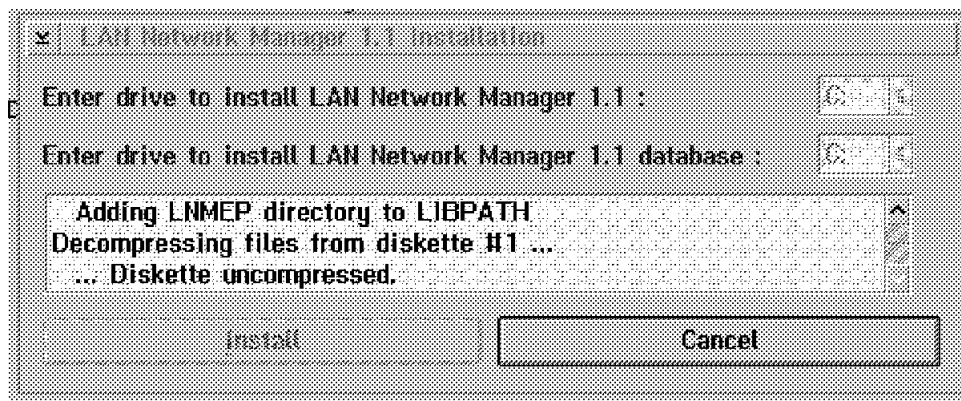


Figure 68. LNM Installation

You will be prompted when additional diskettes are needed.

The LNM proxy agent creates the LNM database during the installation. You may be prompted to sign onto the local database as shown in Figure 69 on page 80. As part of the installation of DB2/2 the default values for the administrator were:

1. User ID: **USERID**
2. Password: **PASSWORD**

A message will be displayed indicating if the above values were entered correctly.



Figure 69. Signon to Local Database

Once the installation has completed the OS/2 system will need to be restarted.

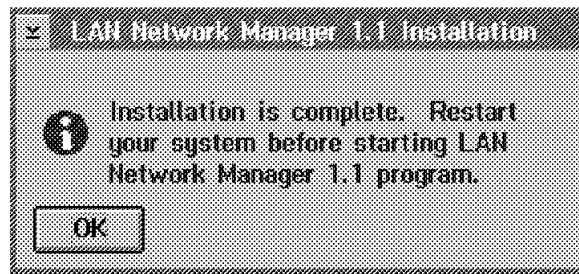


Figure 70. LNM Installation Complete

3.3 LAN Network Manager Configuration

The configuration of the LNM environment involves:

1. Defining LNM for AIX general options
2. Defining each of the LNM OS/2 proxy agents

The configurations defined in Chapter 2 for TCP/IP and SNMP environments have already been defined for the OS/2 and RISC System/6000 systems.

3.3.1 LNM for AIX Configuration

Once LNM for AIX is installed, SMIT is updated with the LNM for AIX options as shown in Figure 71.

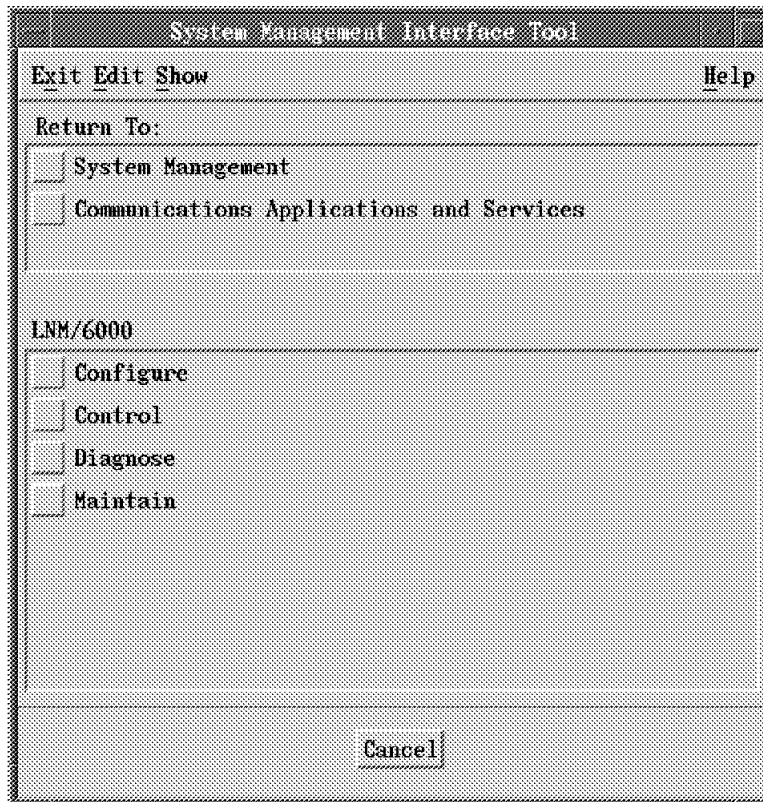


Figure 71. LNM for AIX SMIT Options

When you choose the **Configure** option the screen shown in Figure 72 on page 82 is displayed.

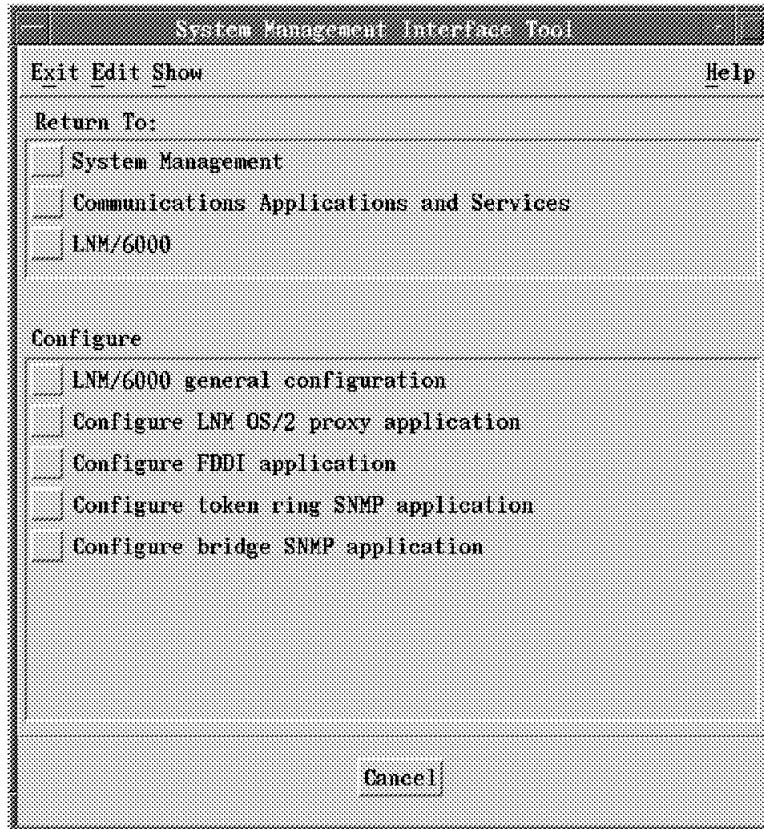


Figure 72. LNM for AIX SMIT Options

When you choose the **General configuration** option, Figure 73 on page 83 is displayed. The *Root Label* field determines the name shown on the AIX NetView/6000 root map for the LNM for AIX ICON. We used **ITSCLAN**. We used default values for the other fields.

Select the **Do** button to update the values.

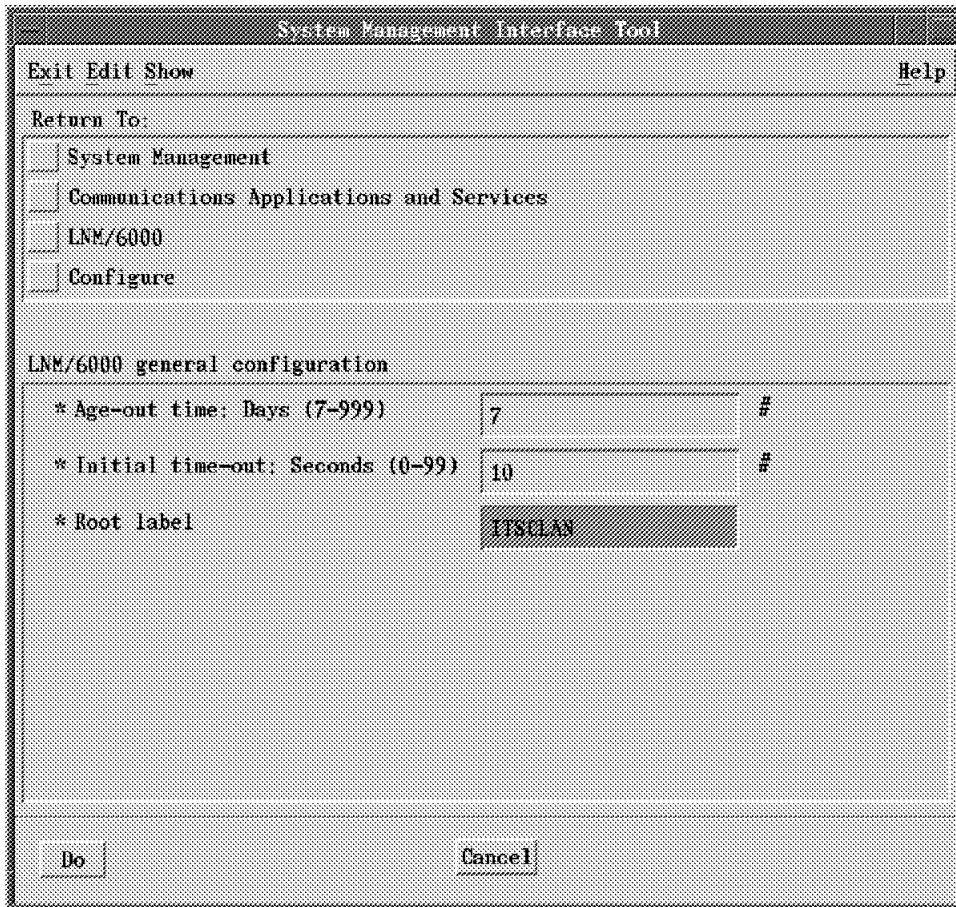


Figure 73. LNM for AIX SMIT General Configuration

Choose the option to configure the LNM OS/2 proxy application. The following screen is then displayed as shown in Figure 74. In our environment *AIXAGENT1* was the LNM OS/2 proxy agent; therefore enter **9.24.104.54** for the IP address. Select the **Do** button to display the screen shown in Figure 75 on page 85.

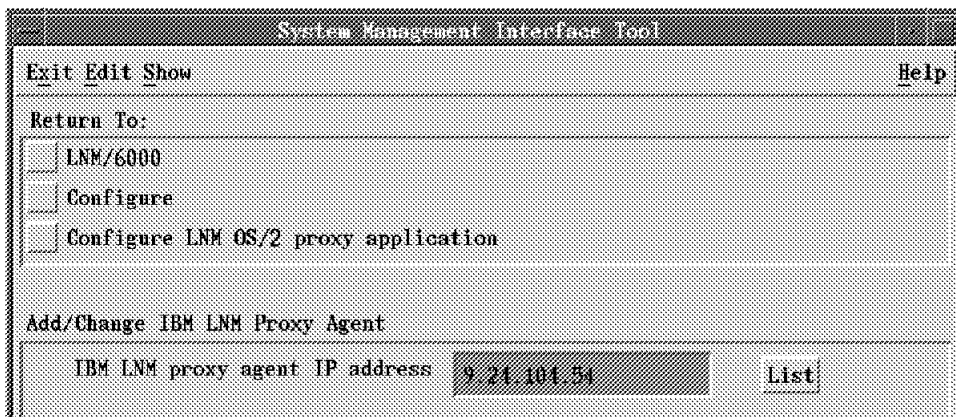


Figure 74. LNM OS/2 Proxy Agent Configuration

This screen enables you to further define additional operational and startup values for the LNM OS/2 proxy agent. The values entered are:

Port number	Enter the value 6005 . This must match the port number used by the LNM proxy agent as defined in the C:\CONFIG.SYS for the OS/2 system.
Automatic agent discovery	Enter the value Yes . This enables LNM for AIX to discover these agents automatically once this definition is completed.
Definitions at startup	Enter the value Remote (proxy agent) . This defines what startup definitions will be used by the OS/2 proxy agent. If you choose the local option instead, you will need to do your LAN definitions at the RISC System/6000.
LNM proxy agent time-out	This value determines the time the LNM proxy agent waits for a response from an adapter before determining the adapter is not active on the LAN segments.
Resync interval	This value determines how often LNM for AIX will synchronize its values. A value of 1 hour was used. If this value is too low then the network will be flooded with LNM for AIX synchronizing with the LNM proxy agent. The proxy agent synchronize time is not affected. That value is configurable from the configuration monitoring screen which is on the agent configuration screen. This determines how often the proxy agent synchronizes the information in its database with the networks it is managing.
LAN subnet name	This value determines the name of the icon that represents the LNM for AIX map. In our environment we entered LABLAN .
Response time-out	This value determines the time LNM for AIX waits for a response from the LNM OS/2 proxy agent before issuing an error. A value of 30 seconds was used.

The values entered are shown below. Select the **Do** button to update the values.

Add/Change IBM LNM Proxy Agent		
* IBM LNM Proxy Agent IP Address	9.24.104.54	
* Port number (5001-65356)	6005	#
* Automatic agent discovery?	Yes	
* Definitions to be used at start-up?	Remote (proxy agent)	
* Automatic bridge link	Inactive	
* LNM proxy agent time-out: Seconds (6-99)	6	#
* Resync interval: Days (0-4)	0	#
* Resync interval: Hours (0-23)	1	#
* Resync interval: Minutes (0-59)	0	#
* LAN subnet name	LABLAN	
* Response time-out: Seconds (6-99)	30	#

Figure 75. LNM OS/2 Proxy Agent Configuration

The information created is stored in the /usr/lpp/lnm6000/conf/lnmlnmemon directory. The configuration files created are based on the IP address of the proxy agent. In our environment the configuration file created was 9.24.104.54.conf.

3.4 Starting LAN Network Manager

To start IBM LAN Network Manager for AIX the following steps are required:

1. In the AIX NetView/6000 management system
 - Ensure AIX NetView/6000 is started.
 - Start LNM for AIX either through a pull-down menu, AIX command shell, or SMIT.
 - Discover the OS/2 LNM proxy agent (if the option to automatically discover agents was not chosen for the proxy agent configuration).
2. In the LNM OS/2 proxy agent:
 - Start OS/2 TCP/IP.
 - Start SNMPD.
 - Start LAN Network Manager.

This could take some time depending on the performance of the OS/2 machine being used. In our environment, using a 386 Model 70, it took 5 minutes to get the proxy agent up and ready to communicate with the AIX NetView/6000 management system.

3.4.1 Starting LNM for AIX

The LNM for AIX application is started through the AIX NetView/6000 graphical user interface. Once AIX NetView/6000 is started an additional menu bar option is available for LNM for AIX. This is the *LAN* option. When AIX NetView/6000 starts, the LNM for AIX daemon *Inm6kd* is automatically started. This can be checked by issuing **ovstatus Inm6kd**. It should be in a *running* state.

If this daemon is not running then start it by entering **ovstart Inm6kd**. To start the additional LNM for AIX application choose the **LAN...Start LNM/6000** option on the pull-down menu as shown in Figure 76.

Choosing to start LNM for AIX through SMIT provides an option to clear the LNM database.

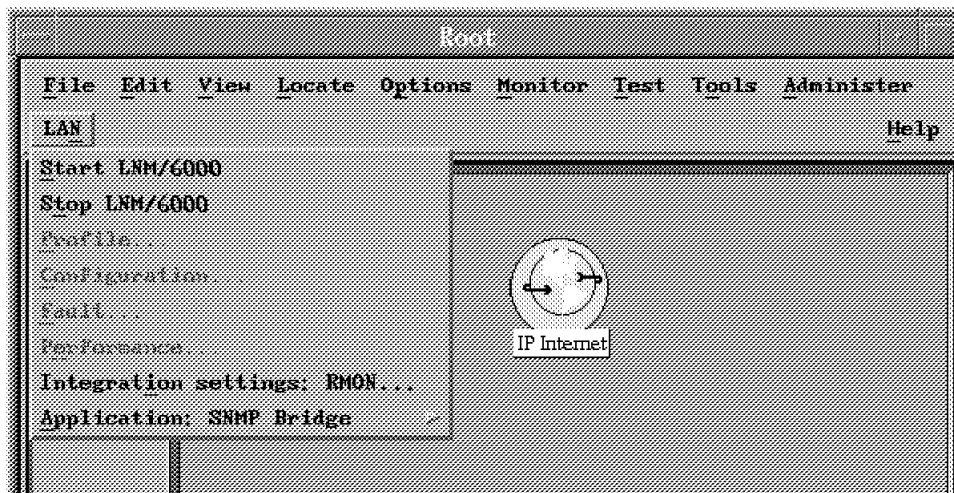


Figure 76. LNM for AIX Startup

Once LNM for AIX is started an additional icon is then displayed on the root map. The name we had entered was *ITSCLAN* as shown in Figure 77 on page 87.

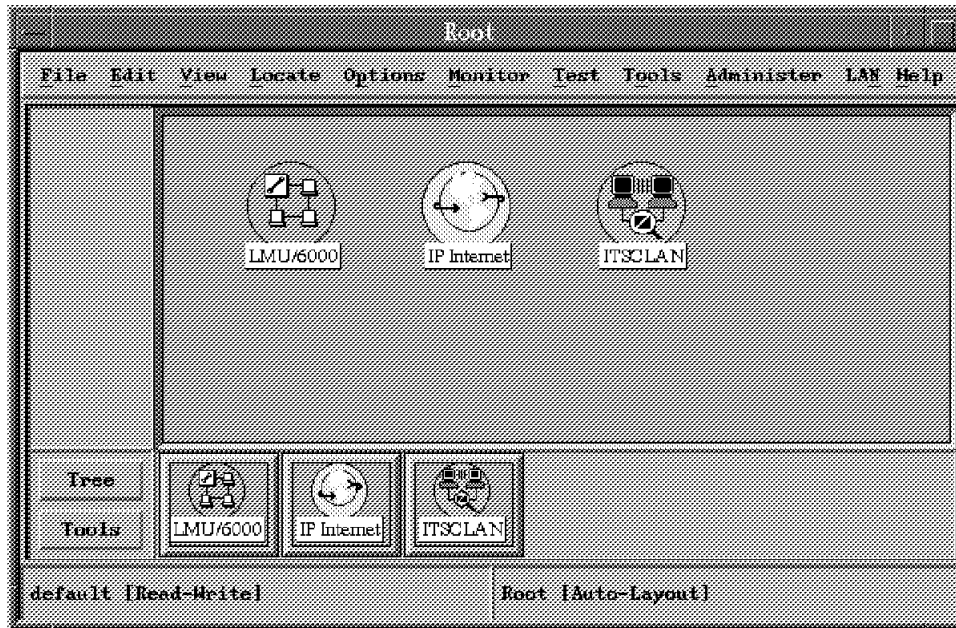


Figure 77. LNM for AIX Started

During the startup of LNM for AIX if the LNM OS/2 proxy agents have been defined to be automatically discovered then the current topology information is retrieved from the proxy agents. As each new LNM OS/2 proxy agent is started LNM for AIX will then retrieve the topology information and update the AIX NetView/6000 topology map. Once the icon on the AIX NetView/6000 root map turns green or yellow (or the individual proxy agents) then you can start retrieving information and checking the status of the LAN.

To verify that LNM for AIX has started properly the following tasks need to be running. These tasks can be displayed by choosing the *Diagnose* option on the LNM for AIX SMIT menu. Figure 78 on page 88 and Figure 79 on page 89 show the result of displaying the status of LNM for AIX.

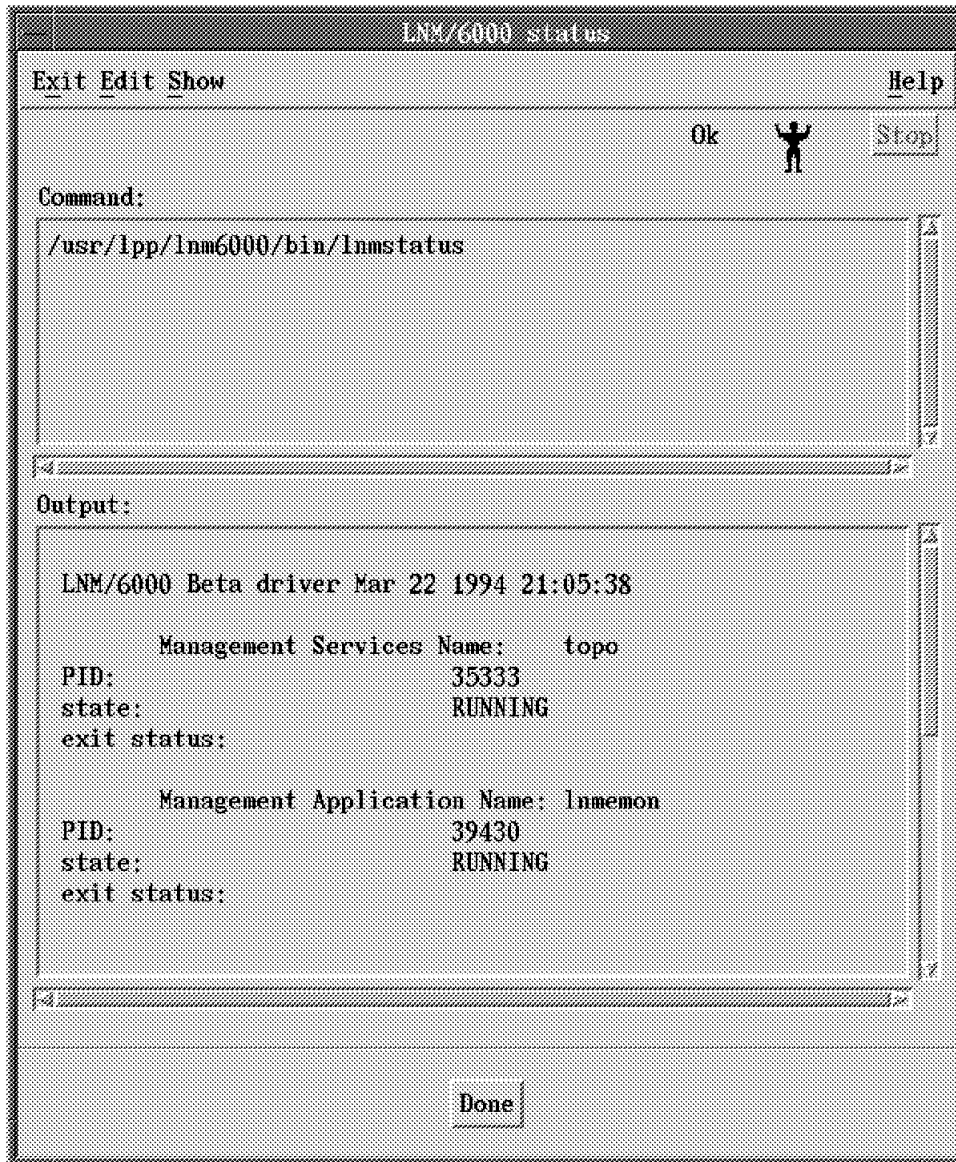


Figure 78. LNM for AIX Tasks Part 1 of 2

```
Output:
      Management Application Name: fddimon
PID:      33799
state:    RUNNING
exit status:

      Management Application Name: brmon
PID:      33032
state:    RUNNING
exit status:

      Management Application Name: trmon
PID:      22025
state:    RUNNING
```

Figure 79. LNM for AIX Tasks Part 2 of 2

3.4.2 Starting the OS/2 LNM Proxy Agent

Since TCP/IP and SNMP were already started (through the configuration in Chapter 2) only the LNM OS/2 proxy agent needs to be started.

To start the LNM proxy agent choose the LNM icon from the LNM folder on the OS/2 desktop.

The OS/2 LNM proxy agent is up and running!

3.5 LAN Network Manager Operations

Following are some of the functions available for LNM for AIX.

There are five levels of hierarchy while navigating through the IBM LAN Network Manager for AIX submaps:

1. Root submap - the highest level, as shown in Figure 77 on page 87
2. Proxy agents submap - this displays each proxy agent defined through the IBM LAN Network Manager for AIX configuration as shown in Figure 75 on page 85
3. Network submap - this displays a detailed view of the network such as the segments and bridges that this proxy agent is managing as shown in Figure 86 on page 96
4. Segment details submap - this displays the individual workstations and CAUs on that segment as shown in Figure 87 on page 97
5. CUA details - this displays the individual ports on the CAU as shown in Figure 88 on page 98

By choosing the icon representing the LNM for AIX submap (*ITSCLAN* in our environment) from the root map of AIX NetView/6000, the various proxy agents are displayed. Only one proxy agent is displayed, as shown in Figure 80 on page 90, in our environment which was defined as *LABLAN*.

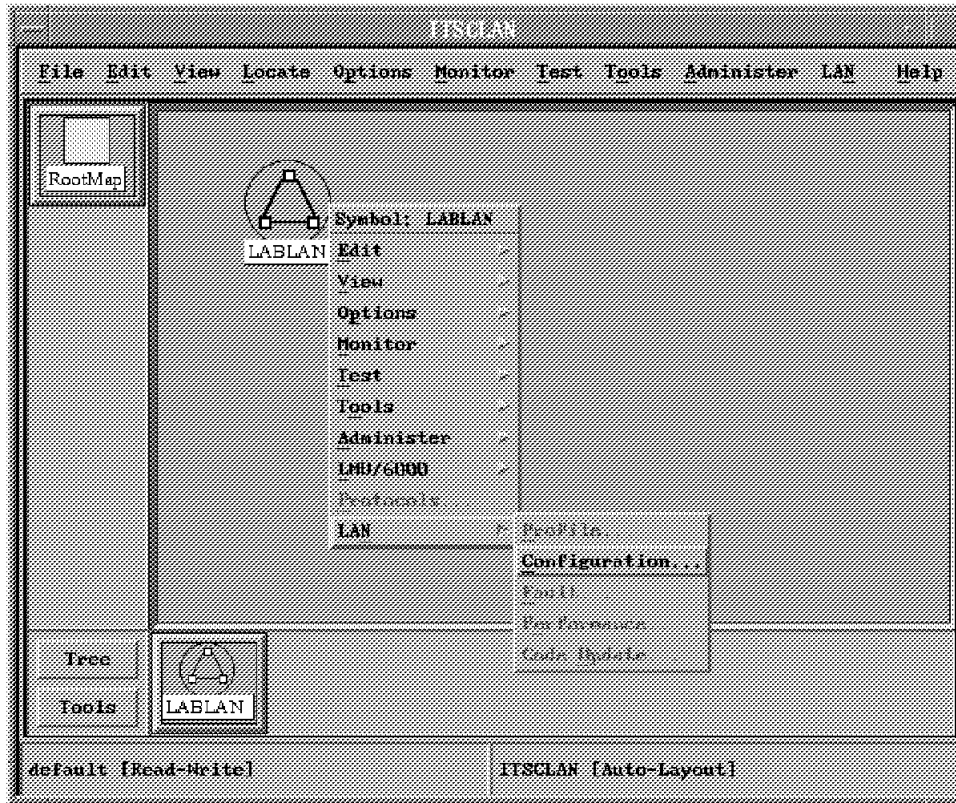


Figure 80. LNM for AIX Proxy Agent

The LNM proxy agent icon's status can be one of several colors. A subset of the colors are:

- Blue - this is the initial color which represents that the IBM LAN Network Manager for AIX and the proxy agent are not communicating.
- Green - this represents that the communication between the IBM LAN Network Manager for AIX and the proxy agent is operational.

The LNM proxy agent configuration information can be retrieved by choosing the right button on the mouse while pointing to the proxy agent icon. Choose the **LAN...Configuration** option from the pull-down menu, as shown in Figure 80.

The LNM proxy agent information is then displayed providing you with the following details:

- Adding definitions for workstations, bridges and Controlled Access Units (CAUs).
- Deleting a CAU qualifier
- Restarting the LNM proxy agent
- Refreshing the view of the network
- Defining access control parameters

Provides the ability for LNM for AIX to detect and remove unauthorized adapters

- Define adapter monitoring

LNМ for AIX will verify that the adapters that are monitored are active on the network; otherwise an error is produced. Provides the ability for critical resources to be monitored on the network.

- Defining general bridge parameters

Defines the way LNМ for AIX communicates with and manages bridges, such as reporting level (control or observing and appropriate passwords), autolink to the bridges and data collection parameters.

- Defining configuration monitoring parameters

This sets an age-out value for an LNМ proxy agent when adapters are inactive for longer than the value defined. Once the adapter ages out of the LNМ proxy agent database the LNМ for AIX age out time takes over. This age out time is set in SMIT under general LNМ for AIX parameters.

- Defining general LNМ parameters

Defines which adapters can perform tracing, thus preventing unauthorized tracing of the network.

- Defining segment parameters

Allows for defining data collection intervals from the network.

From the screen shown in Figure 81 on page 92 the Actions and Parameters pull-down menus enable all the above information to be accessed and modified.



Figure 81. LNM for AIX Proxy Agent Information

The following additional configurations are possible once LNM for AIX and the LNM proxy agents are operational. These configurations are accessed from the LNM proxy agent configuration screen and are only needed if:

1. More than 2 bridges will need to be linked simultaneously within your network. Then the DLC startup value will need to be increased. This is done through the Bridge Parameters screen on LNM for AIX as shown in Figure 82 on page 93. The DLC default value is 2 which only provides a link to a maximum of 2 bridges at any one time. We increased this to 8 for this environment.
2. The Access control and associated passwords to link to the bridges needs to be changed. There is 1 controlling and 3 observing linking levels to the bridges with the default password being 00000000 for all levels. If these values need to be changed they can be accessed through the *System parameters...Bridge parameters* pull down-menu.

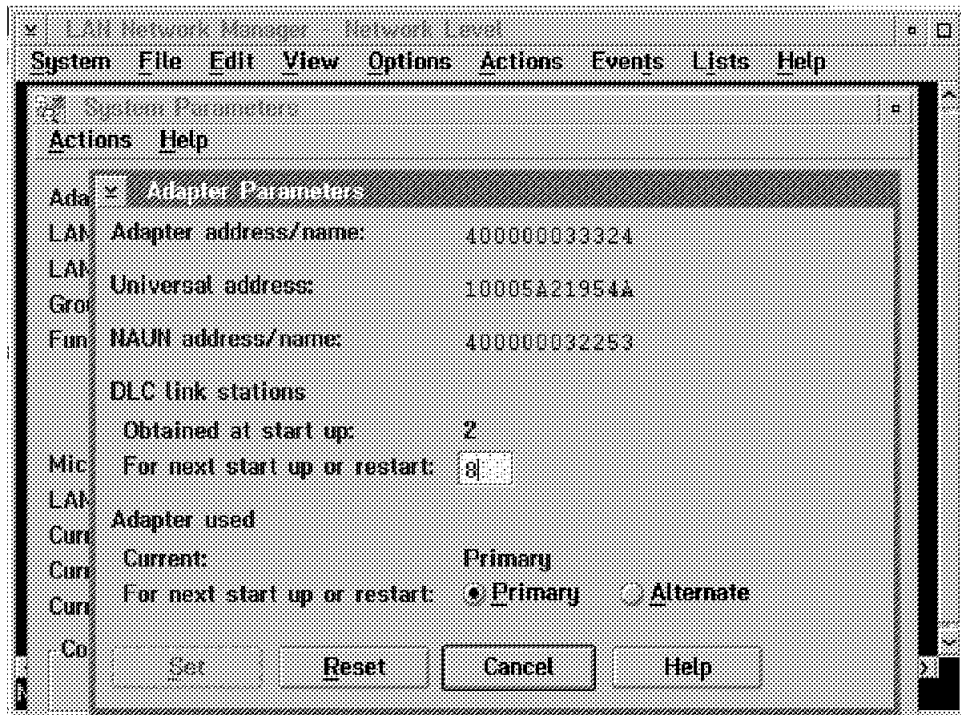


Figure 82. LNM DLC Startup Values Configuration

Both these values require that the LNM OS/2 proxy agent be restarted. If you have changed any of these values then restart the LNM proxy agent from the System pull-down menu.

The screen in Figure 83 on page 94 shows how to add a bridge definition by selecting **Actions...Add Bridge Definition** from the LNM Proxy Agent Configuration screen. The information required to add a bridge is:

- Bridge name: provide a meaningful name to identify the bridges.
- Bridge adapters 1 and 2: the bridge adapter addresses are needed. If they are not entered correctly then the bridge information cannot be retrieved nor can segments beyond that bridge be retrieved. The bridge adapter information can be retrieved by looking at the bridge program and viewing the configuration panel.
- Comments: only displayed when retrieving bridge information.
- Automatic bridge link: define whether you want to link to this bridge automatically or if you want to link to this bridge by specifically issuing the link command.

Choose the **Apply** button to update the LNM for AIX database (that is the GTM and OVW databases of AIX NetView/6000) and the LNM OS/2 proxy agent's database. All the bridges shown in the overall network map in Figure 86 on page 96 were defined in this manner.

Add Bridge Definition

[Help](#)

LAN name

Bridge name

Bridge adapter1

Bridge adapter2

Comments

Automatic bridge link

Description

Figure 83. LNM for AIX Defining a Bridge

Once a bridge is displayed on the network submap of the LNM proxy agent the bridge can be linked to show the networks beyond the current segment.

To link to a bridge, choose to display a list of the defined bridges by selecting **Parameters...List...Bridges** from the LNM Proxy Agent Configuration screen as shown in Figure 81 on page 92. A list of bridges will be displayed that you are able to link or unlink to as shown in Figure 84. An option is also provided to delete the bridge definition.

List of Bridge

[Help](#)

Bridge Name	Bridge Status	LAN Seg	Address1	Bridge Number	LAN Seg	Address2	Auto Link	Performance Link Notification	
BR03EFD	Not Linked	EFD	10005A4D0625	1	FFF	10005A4D0624	No	00	Delete
BR582581	Not Linked	581	10005A8F1E13	7	582	10005A91DDEA	No	00	Link
BR582002	Not Linked	582	10005A00512F	3	002	10005A004F11	No	00	Link
BR582003	Not Linked	582	10005A001FD2	4	003	10005A001F77	No	00	Unlink
BR582FFF	Not Linked	582	4000008250A2	2	FFF	4000008250A1	No	00	

Description

Figure 84. LNM for AIX Bridge List

On the AIX NetView/6000 submap the bridge's status will be color coded. Two of the possibilities are:

- Blue - this is when the bridge is not linked. This will happen when the bridge is initially defined.
- Green - this will occur when the bridge is linked. A trap is sent by the LNM proxy agent to the AIX NetView/6000 event card indicating whether the link was successful or not.

You can also look in /usr/OV/log/trapd.log.

Bridge information can only be displayed once you are linked to the bridge as shown in Figure 85. The bridge being displayed is an 8209 with an Ethernet and token-ring adapter. Additional information can be displayed for the bridge from the Actions and Navigation pull-down menus. For example, bridge performance, filters, forwarding parameters and Source Route Transparent Bridge (SRTB) parameters can be displayed.

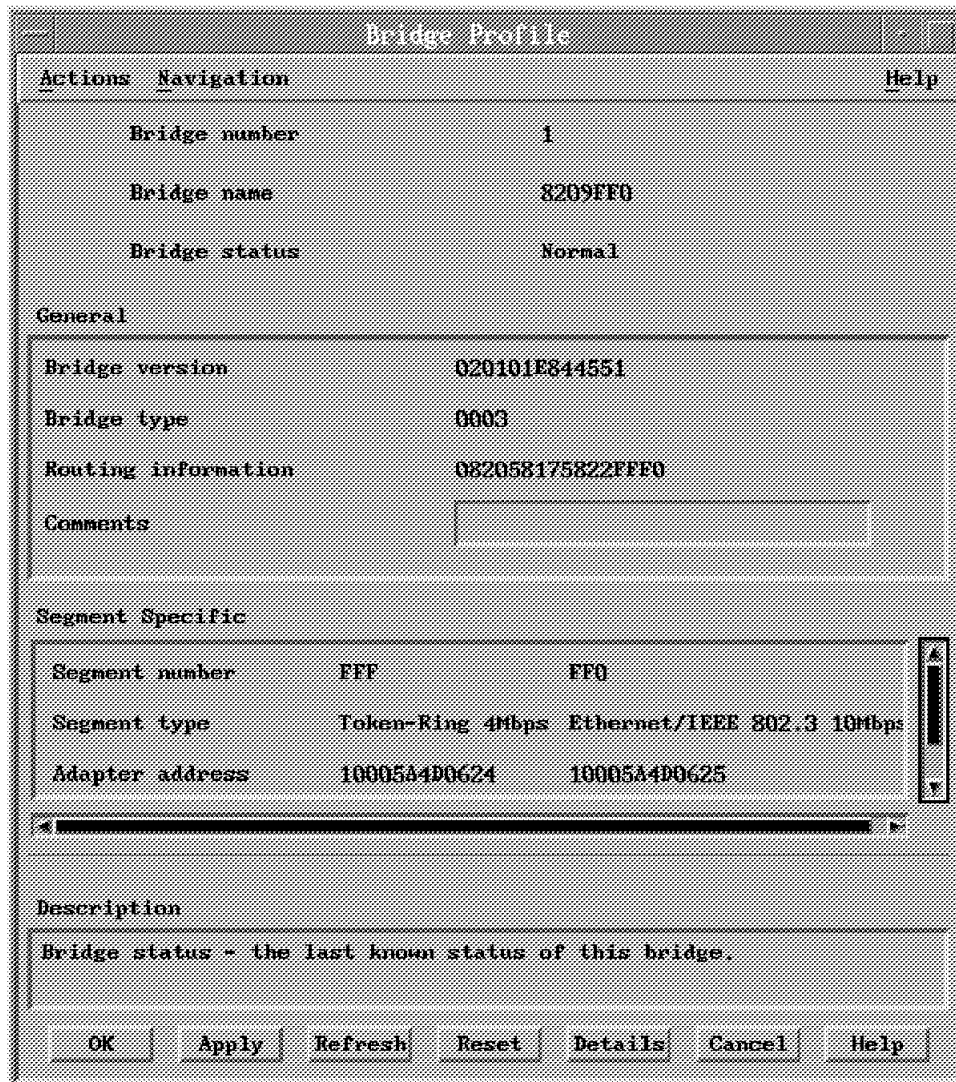


Figure 85. LNM for AIX Bridge Definitions

By selecting the child submap for the LABLAN proxy agent the network is then displayed as shown in Figure 86 on page 96.

In our network the LNM proxy agent is on the token-ring segment 581. To enable LNM for AIX with the ability to discover the complete network map as shown in Figure 86 on page 96 each bridge needs to be defined and linked. Once a bridge is linked this enables the LNM proxy agent to discover the LAN segment beyond that bridge. This is only required to allow the discovery of these segments and to provide current information. Once the segments have been discovered segment detail information is still available without linking to the bridge. This is based on the information last retrieved when the bridge to that segment was last linked. The network map shown in Figure 86 has:

- Local token-ring LAN segments (581) colored green
- All bridges colored blue (not linked)
- All other token-ring LAN segments colored blue since no bridges are linked
- The Ethernet LAN segment, FF0, colored blue since LNM is not able to retrieve Ethernet information

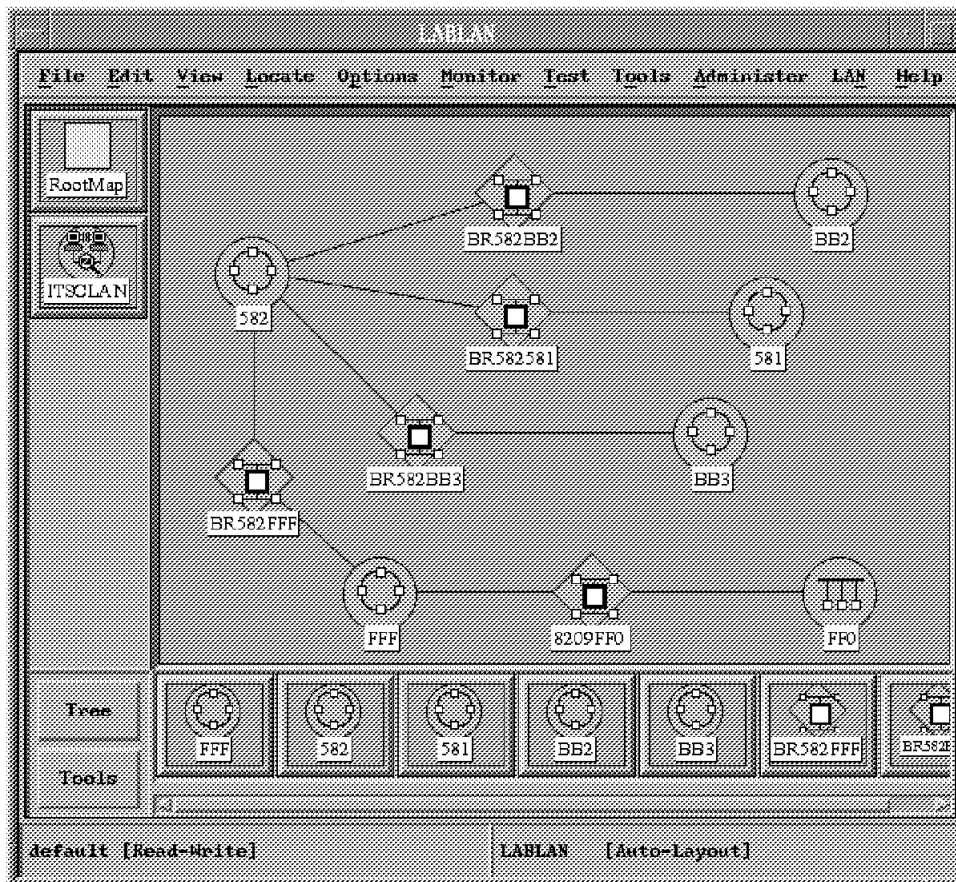


Figure 86. LNM for AIX Network Map

Individual segments can be displayed by selecting the child submap for that segment. The screen in Figure 87 on page 97 shows devices on the segment BB2. In this segment a bridge, workstations and a CAU are displayed.

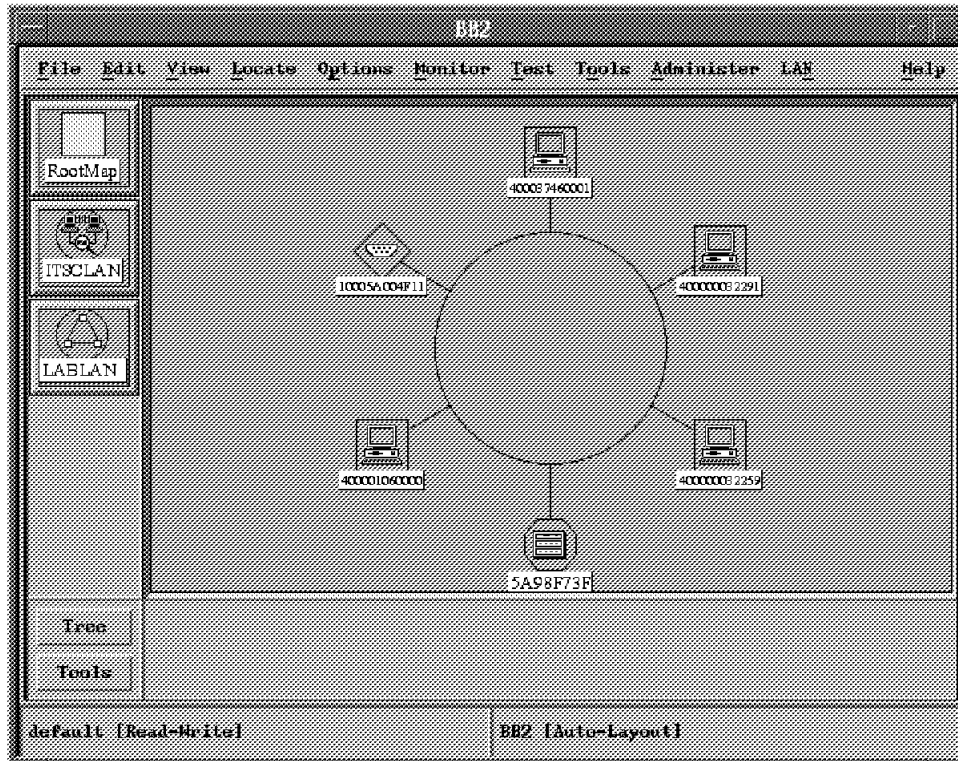


Figure 87. LNM for AIX Segment Details

Details of the CAUs can be displayed by selecting the child submap for a specific CAU. The screen in Figure 88 on page 98 is displaying the CAU that the LNM OS/2 proxy agent is connected to. The icon representing the LNM OS/2 proxy agent is an ellipse. The icons representing standard adapters are square boxes. Individual workstation profile information can be retrieved from any device on the network as shown.

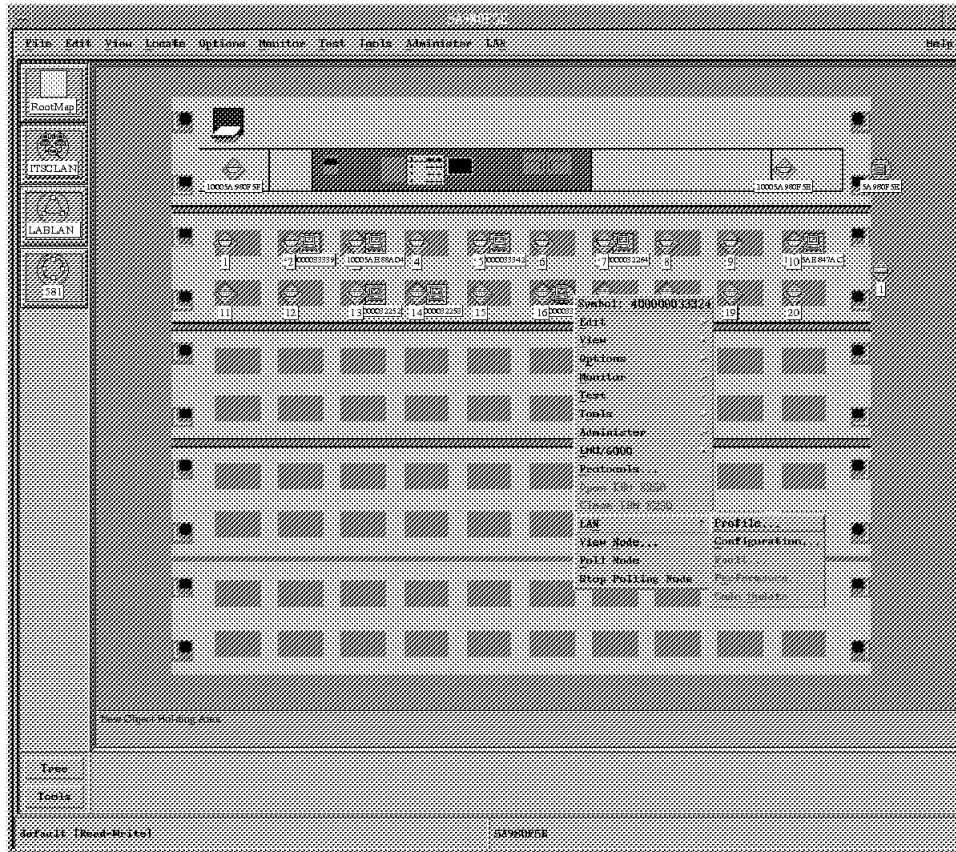


Figure 88. LNM for AIX CAU Details

The integration of LNM for AIX into AIX NetView/6000 enables traps sent by the LNM proxy agent to update the event cards managed by AIX NetView/6000. The screen in Figure 89 on page 99 shows the events listed for LNM for AIX. The current card shows that the performance threshold of bridge BR582BB2 has been exceeded.

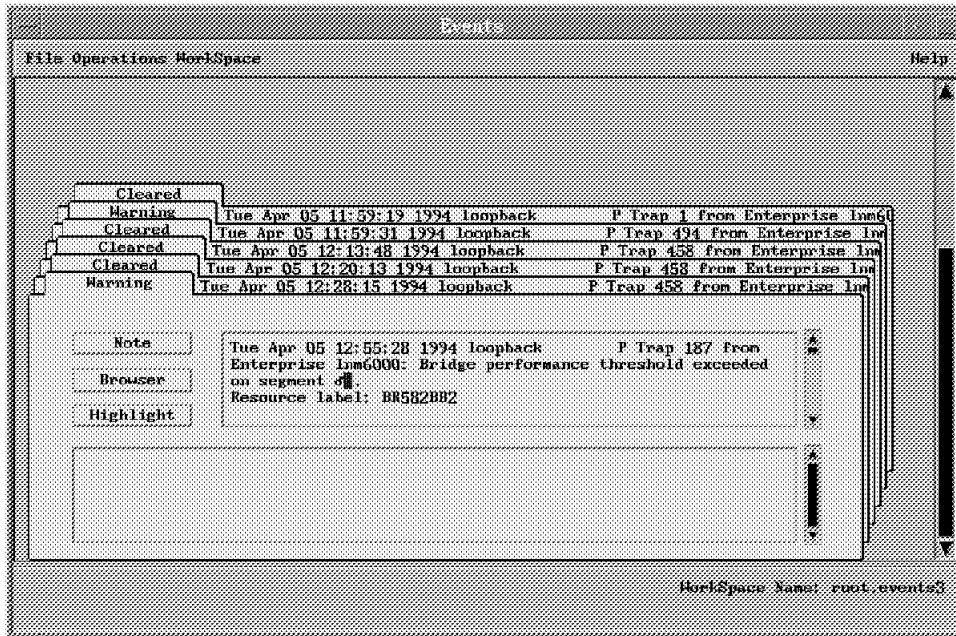


Figure 89. LNM for AIX Events

Chapter 4. RMONitor for AIX

This chapter describes how you can use RMONitor for AIX. Topics include:

- Installation
- Configuration
- Operation

The RMONitor for AIX product integrates its features into the AIX NetView/6000 management platform. RMONitor for AIX collects, monitors and indexes (thresholds) statistics from token-ring and Ethernet LAN segments. These statistics, collected from standardized probes (known as agents) on the LAN, include packet, octet and error counters. RMONitor for AIX provides the AIX NetView/6000 user with complementary performance, operational and problem management functions that extend the capabilities of the overall management system.

RMONitor for AIX works in conjunction with RMON compliant agents, such as RMONitor Agent for OS/2 to form a distributed management structure. The agents can vary from stand-alone probes to integrated hub agents. An RMON-compliant agent is defined as a device that implements the following Internet-standard Remote Network Monitoring (RMON) MIB specifications:

- RFC 1271, Remote network monitoring (RMON) MIB for Ethernet
- RFC 1513, Token-ring extensions to the RMON MIB
- RFC 1213, Management Information Base for network management of TCP/IP-based Internets: MIB-II

RMONitor for AIX interoperates with any RMON-compliant agent and it is possible to program the agent to locally monitor particular segment level statistics, such as utilization, collisions, and packet traffic, and determine when these statistics reach a marginal and critical threshold.

Communication between RMONitor for AIX and the agent is based on the SNMP standard. These agents, located throughout a network and on various platforms, take on the role of an intermediate management data collection point. RMONitor for AIX serves as a central point for managing and consolidating information gathered by the agents located throughout the distributed network. RMONitor for AIX provides invaluable information for those responsible for maintaining the performance of a LAN while enhancing the services the LAN provides.

The RMONitor for AIX application configures agents using policies to provide:

- Threshold monitoring

The RMON agents monitor thresholds and report status changes to RMONitor for AIX using SNMP traps. The agents must support the RMON MIB alarm and events groups, as defined in RFC 1271 and RFC 1513.

- Data collection

The RMONitor for AIX application allows you to define how frequently the data is to be recorded and how frequently the data is to be transferred to RMONitor for AIX.

- LAN segment details

The RMONitor for AIX application provides access to dynamic LAN statistics that are maintained by RMON agents. The dynamic segment data includes the following information:

- Segment throughput and error statistics
- Graphical display of short-term and long-term history
- Graphical display of multiple segments and specified groups of variables in chart form
- Numerical display of LAN statistics

These features, as well as consistent agent control throughout the network, are the RMONitor for AIX application's major advantage.

4.1 RMON Installation

The installation of the RMONitor for AIX environment involves:

1. Installing and tailoring of RMONitor for AIX on the RISC System/6000
2. Installing and tailoring the RMONitor Agent for OS/2 on the OS/2 station
 - Installation of a dedicated adapter
 - Updating CONFIG.SYS with RMONitor Agent for OS/2 requirements

4.1.1 RMONitor for AIX Installation

To install the RMONitor for AIX code use SMIT and the values defined in 1.5.3, "RISC System/6000 Software Installation Procedures" on page 40. The list shown when you prompt for the *SOFTWARE to install* field for RMONitor for AIX is shown in Figure 90 on page 103. Select the top item *1.1.0.0 RMONitor/6000 ALL*.

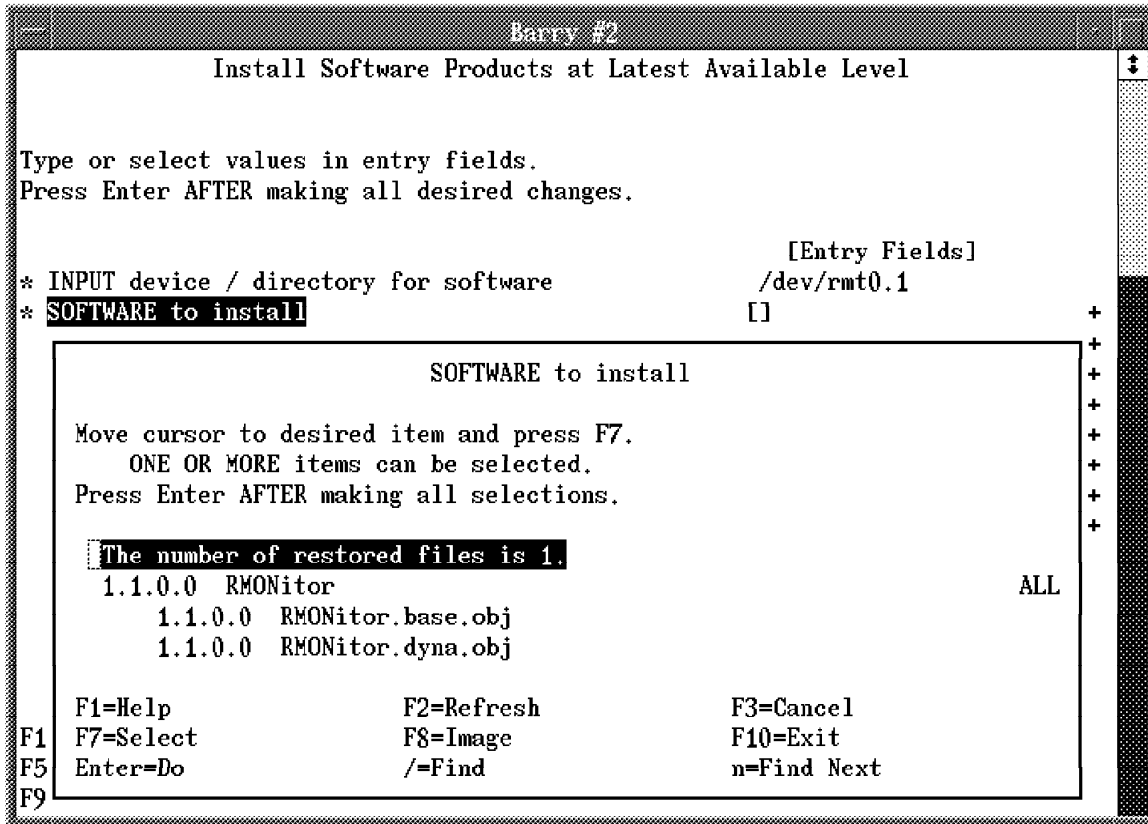


Figure 90. RMONitor for AIX Install List

The installation requires no further interaction.

4.1.2 RMONitor Agent for OS/2 Installation

The installation of the RMONitor Agent for OS/2 involves the following steps:

1. Installation of a dedicated adapter to perform the monitoring functions
2. Installation of the RMONitor Agent for OS/2 code
3. Updating CONFIG.SYS with the RMONitor Agent for OS/2 requirements

The adapter used by RMONitor Agent for OS/2 is dedicated to two tasks:

1. Tracing the network and collecting network statistics
2. Communicating with RMONitor for AIX using SNMP

IBM TCP/IP for OS/2 is not required since RMONitor Agent for OS/2 provides its own TCP/IP stack.

The installation of the RMONitor Agent for OS/2 code is started by keying **A:INSTALL** from an OS/2 window with Disk 1 of 2 in drive A:. The installation of RMONitor Agent for OS/2 uses Software Installer as shown in Figure 91 on page 104. Choose the **Continue** button to proceed with the installation.



Figure 91. RMONitor Agent for OS/2 Software Installer Screen

The next window to appear will have an option to overwrite CONFIG.SYS, as shown in Figure 92. Choose the option to *Update CONFIG.SYS*, then choose **OK** to continue.

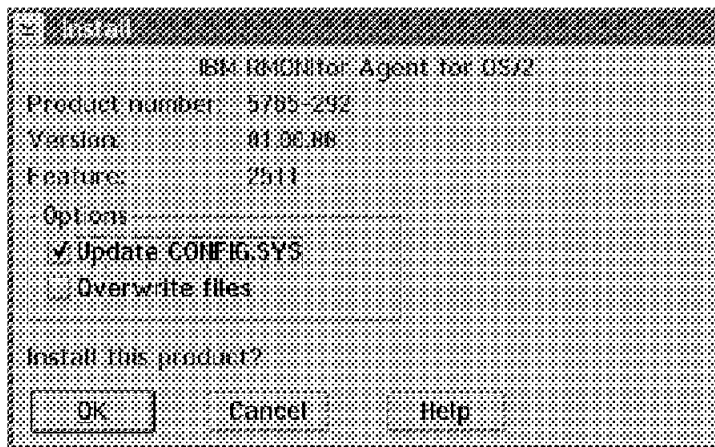


Figure 92. RMONitor Agent for OS/2 Install Window

Select the drive and directories where you want to install the RMONitor Agent for OS/2 files. In our environment the D: drive was selected; to change the drives choose the **Disk space...** option.

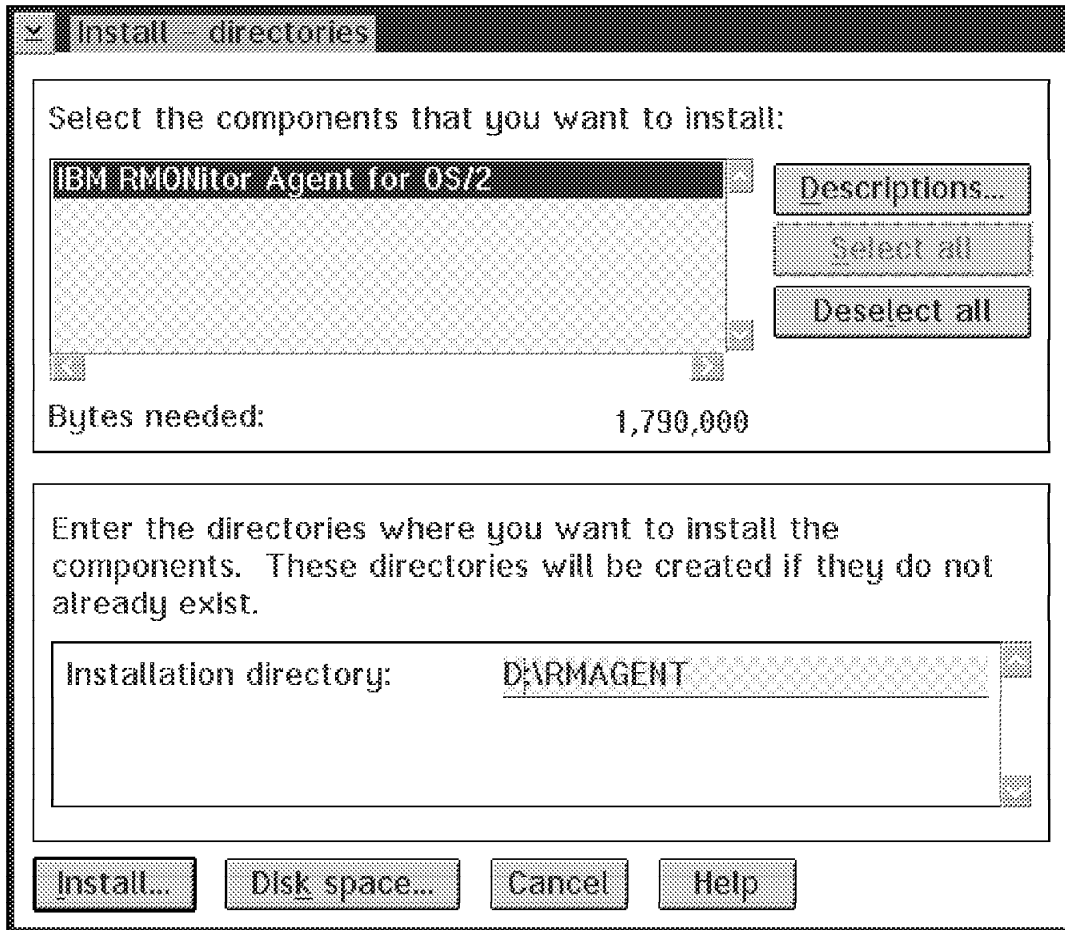


Figure 93. RMONitor Agent for OS/2 Install Directories

The next screen, shown in Figure 94 on page 106, is displayed. Choose the drive which has sufficient spare disk capacity to install the RMONitor Agent for OS/2 files. In addition to changing to the D: drive, we can select the directory to install the code in. Choose the **OK** button to return to the *Install - directories* window.

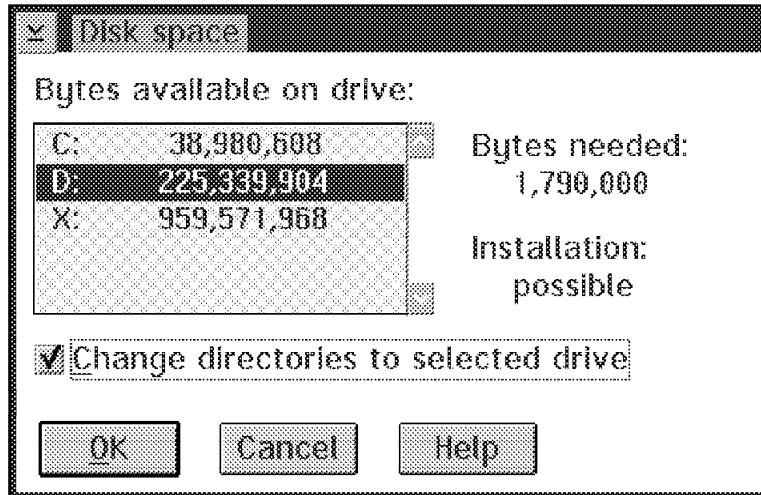


Figure 94. RMONitor Agent for OS/2 Disk Space

Choose the **Install** option to start the installation of the RMONitor Agent for OS/2 code. A screen will appear showing the progress of the installation process. You will be prompted for the second RMONitor Agent for OS/2 diskette.

Once the installation is complete, the following screen, as shown in Figure 95, is displayed.

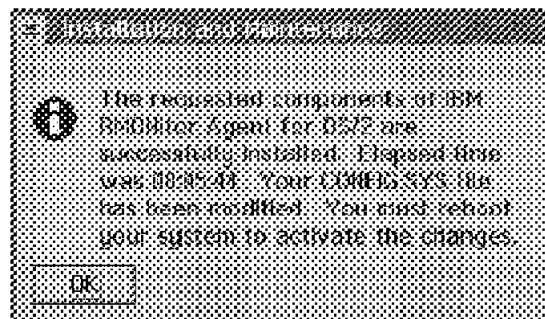


Figure 95. RMONitor Agent for OS/2 Install Successful

The updates to C:\CONFIG.SYS that were done by the installation are:

- Appended the RMONitor Agent for OS/2 directories to the following statements:


```
SET PATH=D:\RMAGENT;
LIBPATH=D:\RMAGENT\DLL;
SET HELP=D:\RMAGENT;
```
- Added the following environment variable:


```
SET RMAGENT=D:\RMAGENT
SET TMP=D:\RMAGENT\TEMP
```

If the TMP variable is already set by some other product then the existing value of the TMP variable can be used. For example, IBM TCP/IP for OS/2 sets the TMP variable to D:\TCP/IP\TMP.

The OS/2 workstation needs to be restarted for the new configuration to be activated.

4.2 RMONitor Configuration

The configuration of RMONitor requires you to customize:

1. RMONitor for AIX configurations
 - General configurations
 - Agent seed file configurations
2. RMONitor Agent for OS/2 configurations
 - TCP/IP environment
 - Configure adapter
3. Defining policies

4.2.1 RMONitor for AIX Configurations

The configuration of RMONitor for AIX involves:

1. Defining RMONitor for AIX configurations - general and EUI connection
2. Defining RMONitor for AIX agent seed file

Once RMONitor for AIX is installed, SMIT is updated with the RMONitor for AIX options as shown in Figure 96 on page 108.



Figure 96. RMONitor for AIX SMIT Options

Choose the **Configure** option to display the possible configuration steps. We selected the default option for the first two entries:

1. RMONitor for AIX general configuration, as shown in Figure 97 on page 109.

The policy file determines where the policies are to be stored. The location of this file is in the directory `/usr/lpp/RMONitor/conf`. The default policy file `RMNPol.dat` was used.

RMONitor for AIX uses two methods for discovering the RMON agents.

- a. Automatic discovery based on input from AIX NetView/6000
- b. Manual/promiscuous discovery based on a seed file

RMONitor for AIX permits the two agent discovery mechanisms to be used simultaneously by using a value of *yes* for the *Automatic discovery* option.

2. RMONitor for AIX EUI connection configuration, as shown in Figure 98 on page 110.

We used the default values.

The above two options need to be configured, even though defaults were taken. This requires you to press the Enter key when you have these windows open on your display.

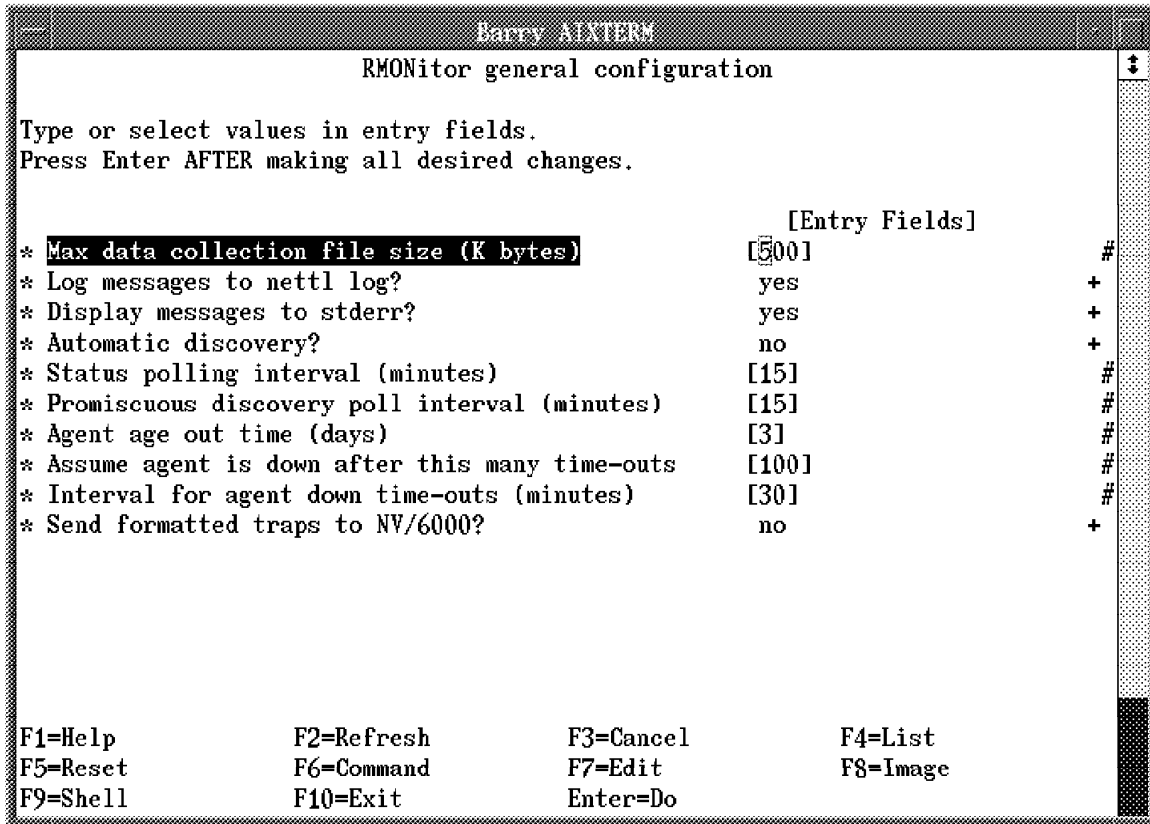


Figure 97. RMONitor for AIX General Configuration

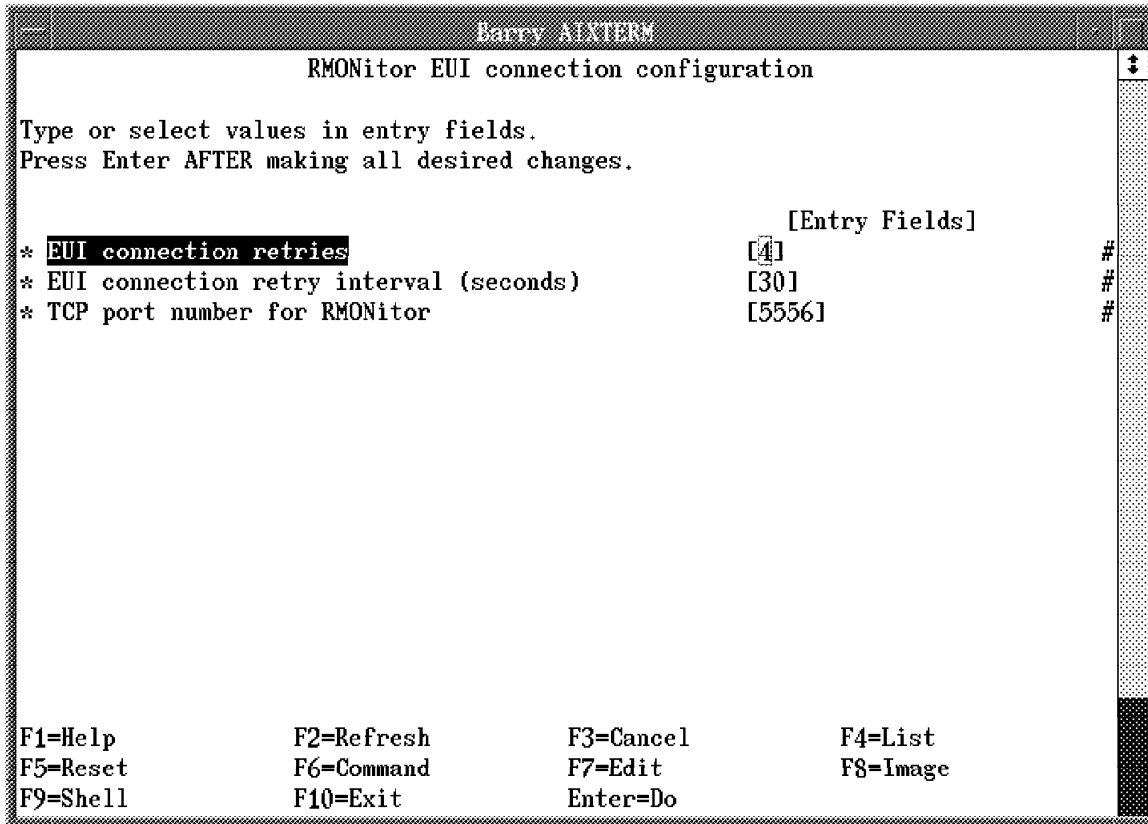


Figure 98. RMONitor for AIX EUI Connection Configuration

Select the RMONitor for AIX agent discovery and file configuration option, then choose the **Add IP address to agent discovery seed file** option. The IP addresses of the RMONitor Agent for OS/2 workstations will need to be entered. The file used to store this information is /usr/lpp/RMONitor/bin/RMONseed.dat. In our environment we had 2 RMON agents:

1. RMAGENT1 with IP address of 9.67.32.87 for the Ethernet network. A 3COM EtherLink/MC adapter was used, as shown in Figure 99.
2. RMAGENT2 with IP address of 9.24.104.72 for the 4Mbps token-ring network. An IBM LANStreamer adapter was used.

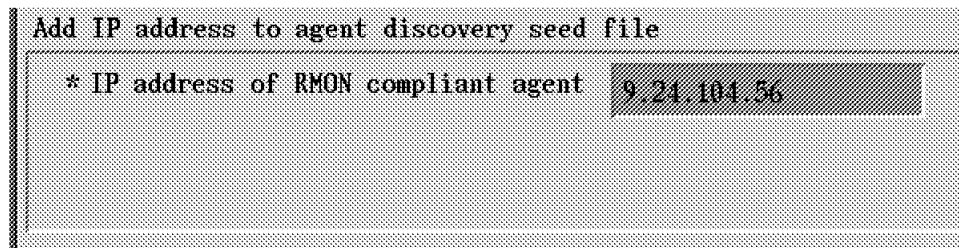



Figure 99. RMONitor for AIX Add RMONitor Agent for OS/2 IP Address

4.2.2 RMONitor Agent for OS/2 Configuration

The configuration of the RMONitor Agent for OS/2 code involves the following:

1. Configuring the RMAGENT TCP/IP environment
2. Configuring the adapter that will perform the monitoring
3. Defining systems that will receive the SNMP traps

All the configurations for the RMONitor Agent for OS/2 code are done through the *Configuration and Setup* utility provided with RMONitor Agent for OS/2. To

start the configuration select the RMONitor Agent for OS/2 icon,  , from the RMONitor Agent for OS/2 folder on the OS/2 desktop. The RMONitor Agent for OS/2 main window is displayed in Figure 100.

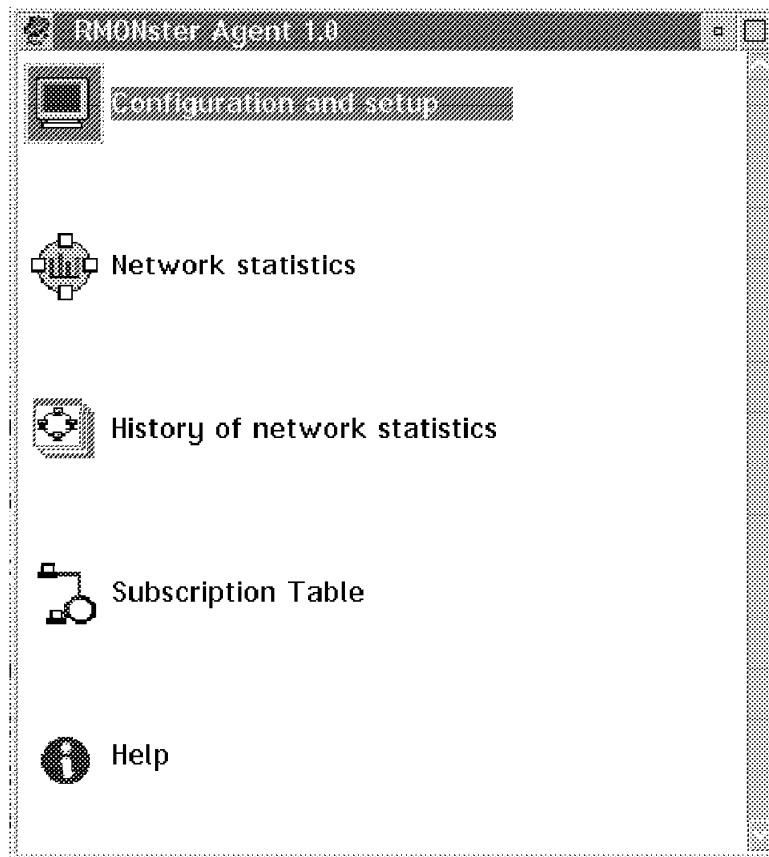


Figure 100. RMONitor Agent for OS/2 Main Window

Choose the *Configuration and setup* option to start the configuration process. An OS/2 notebook, as shown in Figure 101 on page 112, is displayed. The values entered are:

- System name: RMAGENT1.
- IP Address: 9.67.32.87
- Location: Raleigh BLD 657 Room AA137
- Contact: Shiguelo Suzuki
- Local router: 9.67.32.84

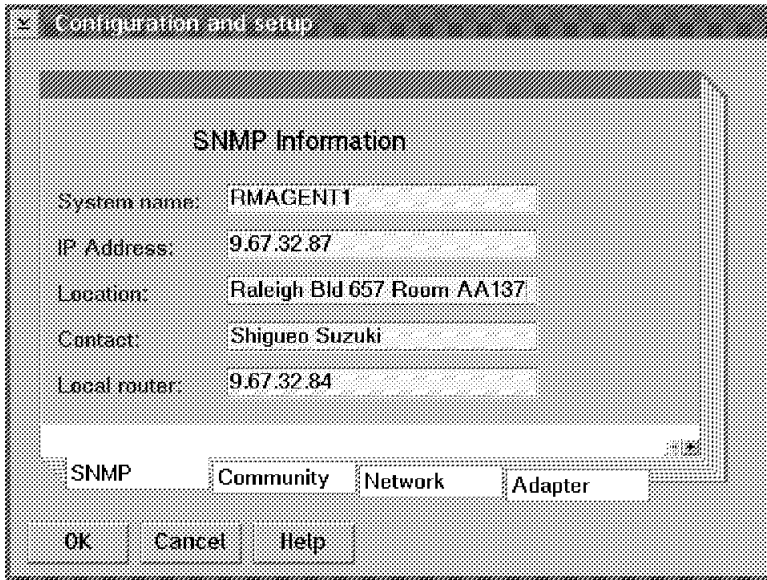


Figure 101. RMONitor Agent for OS/2 SNMP Configuration

Choose the **Community** tag to enter the following information, as shown in Figure 102:

- Get community name: The community name *public* was used.
- Set Community Name: The community name *public* was used.

Note: Since we used pre-release code for this project, we were not able to use ITSC as our community name.

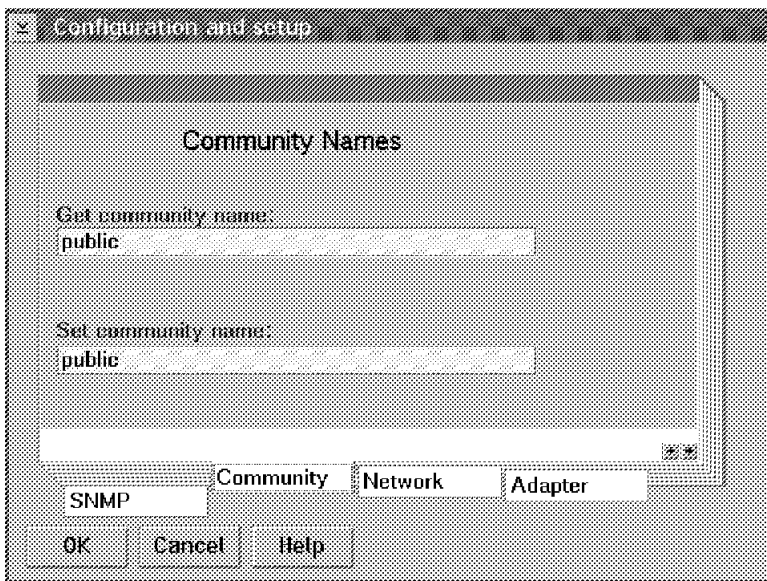


Figure 102. RMONitor Agent for OS/2 Community Configuration

Select the **Adapter** button to enter the following information, as shown in Figure 103 on page 113:

- Adapter: We used a 3COM EtherLink/MC adapter.
- Slot number: The adapter was in slot 3.

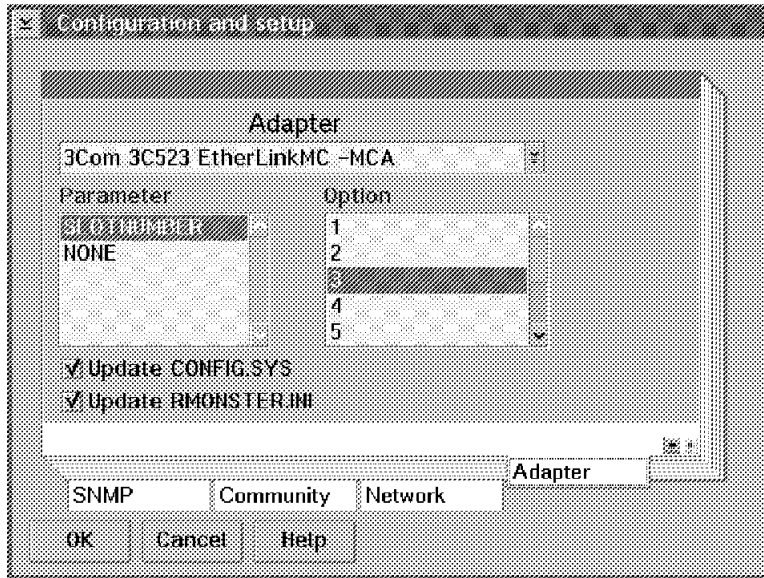


Figure 103. RMONitor Agent for OS/2 Network Configuration

Select the **OK** button to save all the configurations.

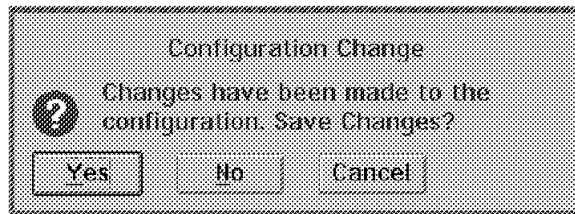


Figure 104. RMONitor Agent for OS/2 Save Configuration

Two device driver statements are added to the C:\CONFIG.SYS file as shown below for each RMONitor Agent for OS/2 configuration:

1. Ethernet RMAGENT1:

```
DEVICE=D:\RMAGENT\RP32.SYS D:\RMAGENT\DRIVERS\RMONSTER.INI
DEVICE=D:\RMAGENT\DRIVERS\ELNKM.COS2 /p:PROTOLY$
```

2. Token-Ring RMAGENT2:

```
DEVICE=D:\RMAGENT\RP32.SYS D:\RMAGENT\DRIVERS\RMONSTER.INI
DEVICE=D:\RMAGENT\DRIVERS\IBMPRO.OS2 /p:PROTOLY$
```

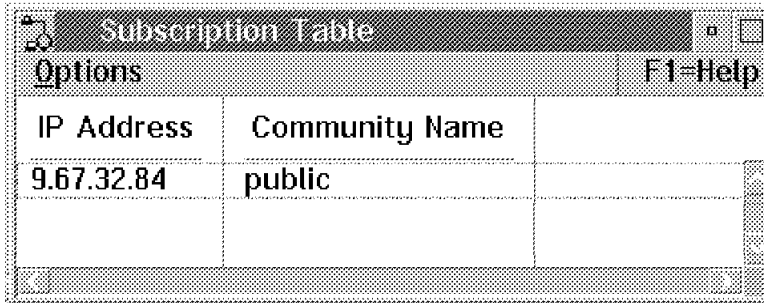
Note: Make sure that the two statements in CONFIG.SYS remain next to each other.

4.2.3 Configuring Trap Information

Defining the systems that are able to receive traps from RMONitor Agent for OS/2 is done through the *Subscription Table* option on the RMONitor Agent for OS/2 main menu as shown in Figure 100 on page 111. If this table is not configured RMONitor for AIX is still able to retrieve information from RMONitor Agent for OS/2; however, it will not receive traps when error conditions occur. When this option is chosen the *Subscription Table* screen is displayed, as shown in Figure 105 on page 114. On our screen we have already entered the IP address of the RISC System/6000 Ethernet adapter. To enter this information

choose the **Options...Add entry** options from the pull-down menu and enter the IP address of the RMONitor for AIX system for that interface:

1. 9.67.32.84 is the IP address of the Ethernet interface on the RMONitor for AIX for RMAGENT1.
2. 9.24.104.25 is the IP address of the token-ring interface on the RMONitor for AIX for RMAGENT2.



IP Address	Community Name
9.67.32.84	public

Figure 105. RMONitor Agent for OS/2 Subscription Table

The OS/2 workstation needs to be restarted to activate the configuration.

4.2.4 Defining Policies

To control communication between RMONitor for AIX and RMONitor Agent for OS/2 *policies* and *rules* need to be defined.

4.2.4.1 Policies

To directly control RMONitor for AIX and RMONitor Agent for OS/2's operations, rules need to be assigned and referenced. Policies are used to assign and implement the rules for RMONitor for AIX and each RMONitor Agent for OS/2.

There are two different types of policies:

- Agent policies - implement agent rules and threshold rules
- Collection policies - implement collection rules

The RMONitor for AIX application comes with a policy editor that allows you to define policies using a graphical interface. You can define specific policies for individual agents as well as collective policies for a subset of agents.

4.2.4.2 Rules

Rules are used to establish operational guidelines between RMONitor for AIX and the RMONitor Agent for OS/2s. You can define multiple rules.

The rules are categorized into:

- Agent rules
- Threshold rules
- Collection rules

Agent Rules: Agent rules define the agent characteristics that you want to monitor. You can set up rules to monitor the RMON statistics, such as: segment group, host group, conversation matrix group, ring station group, time interval sampling and the number of samples to collect for short-term and long-term history.

Threshold rules: Threshold rules define the terms and actions for monitoring the RMON statistics. You can define rising or falling thresholds (that is whether the polled values retrieved from the network are above or below the thresholds defined), marginal or critical thresholds. How frequently the agent checks a statistic against its threshold, and what action to take when a threshold is exceeded are also set up in the threshold rules.

Collection Rules: Collection rules define how often the information gathered by the agents is to be transferred to RMONitor for AIX, when the transfer should take place, whether you want short or long history, and which RMON statistics are gathered. This information is placed in the directory /usr/lpp/RMONitor/databases.

To start the policy editor choose the **Tools...RMONitor...Policy Editor** options from the AIX NetView/6000 pull-down menu, as shown in Figure 106.

Note: The RMONitor for AIX daemons do not need to be started to enable the editing of policies.

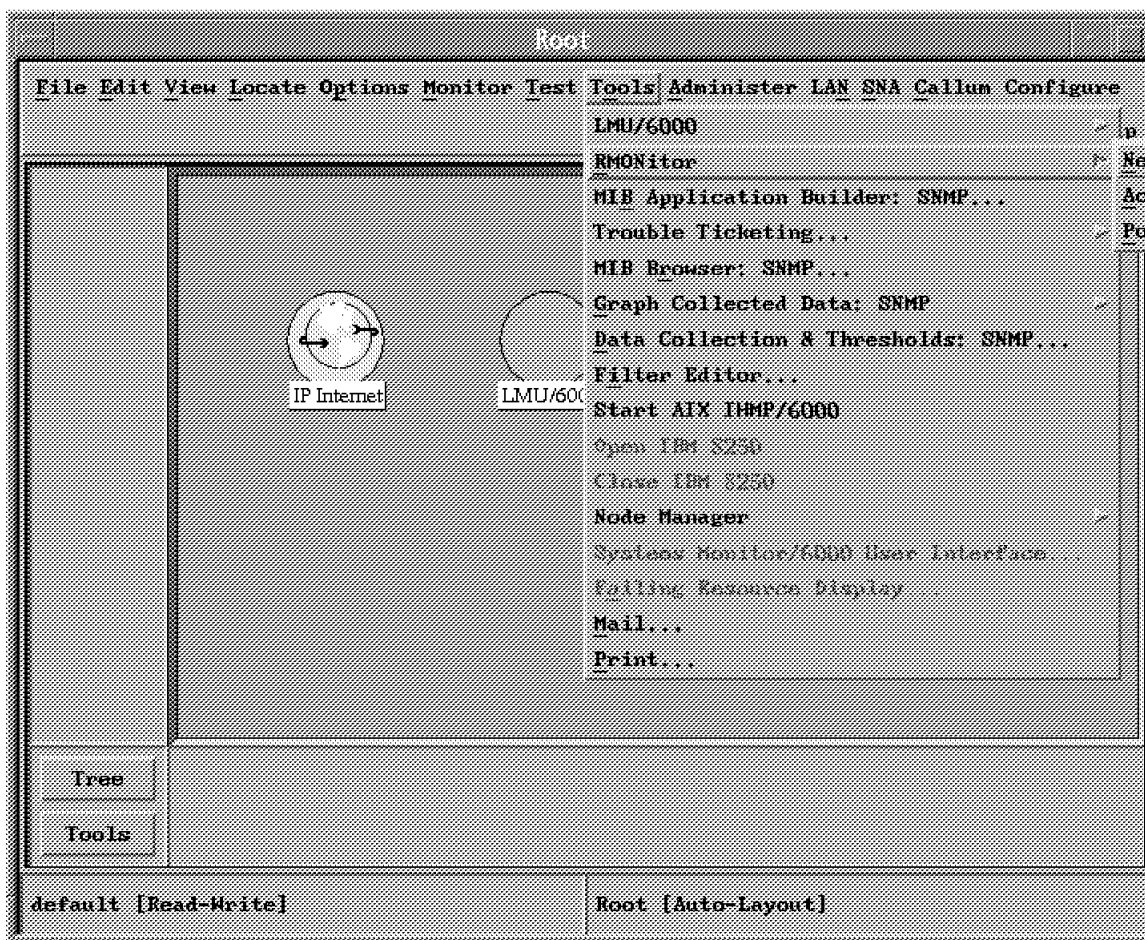


Figure 106. AIX NetView/6000 Starting RMONitor Policy Editor

After selecting the policy editor from the pull-down menu, the RMONitor for AIX Policy Editor window is displayed. The name of the file, RMONPol.dat containing this policy information is also displayed on this window, as was configured earlier. The screen shown in Figure 107 on page 117 already contains the rules information as summarized below:

<i>Table 1. Agent Policies</i>		
Fields	Policies	
Policy Name	RMON1	RMON2.
Agent Selection	9.67.32.87 and Ethernet	9.24.104.72 and Token-Ring
Agent Rules	LongHistory	LongHistory
Threshold Rules	All-Ethernet	Some-TokenRing

<i>Table 2. Collection Policies</i>		
Fields	Policies	
Policy Name	RMON_Ethernet	RMON-TokenRing
Agent Selection	9.67.32.87 and Ethernet	9.24.104.72 and Token-Ring
Collection Rules	ALL_LONG	ALL_LONG

Rules are defined by choosing the appropriate button for each rule. We defined several rules as listed below:

1. Agent Rules: SmallHistory and LongHistory
2. Threshold Rules: All-Ethernet and Some-TokenRing
3. Collection Rules: All_LONG

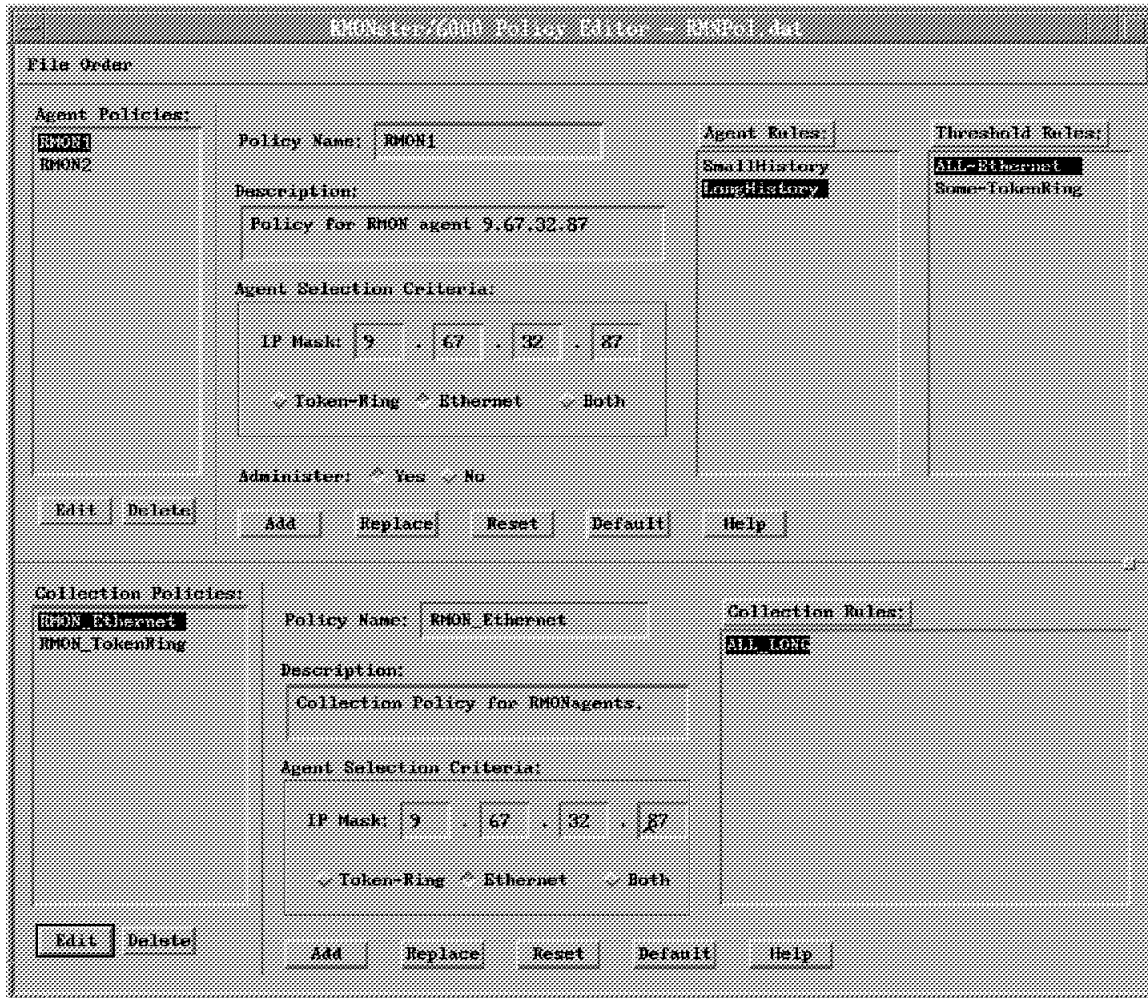


Figure 107. RMONitor for AIX Policy Editor Main Screen

4.2.4.3 Defining Agent Rules

Click on the **Agent Rules** button to begin defining these rules. To define the SmallHistory rule do the following:

- Enter SmallHistory in the Rule Name field.
- Click on all the options in the statistics area. We will collect all the statistics possible from the RMONitor Agent for OS/2.
- Enter **60** for the sample interval and **5** for the number of samples in the short history area. This results in 5 samples, each taken at 60-second intervals to be retained. This provides a total of 5 minutes of short history information.
- Enter **15** for the sample interval and **5** for the number of samples in the long history area. This results in 5 samples, each taken at 15-minute intervals to be retained. This provides a total of 1 hour and 15 minutes of long history information.
- Once this is entered choose the **Add** button to accept this information.

Repeat the above steps to enter the LongHistory rule, as shown in Figure 108 on page 118, with the following information:

- Rule Name: LongHistory

- Choose all statistics
- Short history: 50 samples at 30 second intervals
- Short history: 50 samples at 30 minute intervals

Once completed choose **Close** to complete the agent rule definition.

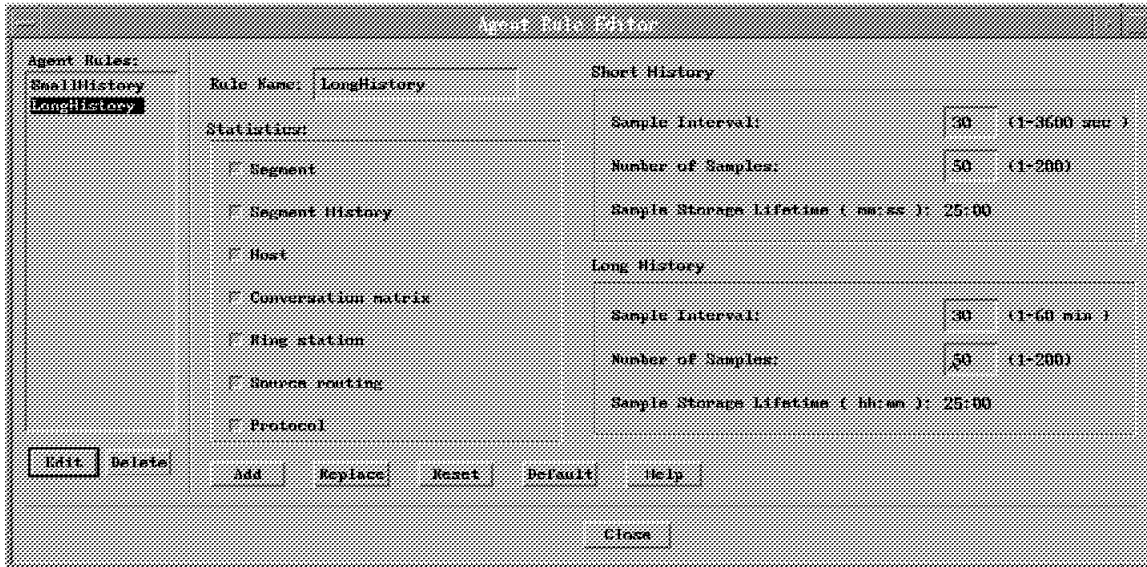


Figure 108. RMONitor for AIX Agent Rules

4.2.4.4 Defining Threshold Rules

Click on the **Threshold Rules** button to begin defining these rules. To define the All-Ethernet rule:

- Enter **All-Ethernet** in the Rule Name field.
- Choose **Ethernet** for the media type.
- Click on the **Add** button to enter this rule and to begin defining the thresholds.
- To define the EN_Utilization thresholds do the following:
 - Click on the **EN_Utilization** in the Available Data Types box.
 - Choose **Rising** as the threshold type. We want to be notified when values are above the thresholds defined. Falling indicates a notification will be sent when the values are below the thresholds defined.
 - Enter **30** for the Agent Sample Interval. This indicates how often the agent compares the values from the network against the thresholds defined.
 - Choose the **Marginal** option in the Thresholds area to define the marginal threshold.
 - A default threshold value is entered; change this value if required.
 - Ensure that the *trap* option is selected. When the value from the network is greater than the threshold value entered a trap will be sent to RMONitor for AIX
 - Click on **Apply** to activate this value.
 - Choose the **Critical** option in the Thresholds area to define the critical threshold.
 - A default threshold value is entered; change this value if required.

- Ensure that the *trap* option is selected. When the value from the network is greater than the threshold value entered a trap will be sent to RMONitor for AIX.
- Click on **Apply** to activate this value.

This process is then repeated for each statistic you want to set thresholds against.

The screen shown in Figure 109 has all the possible statistics defined for the All-Ethernet threshold rule.

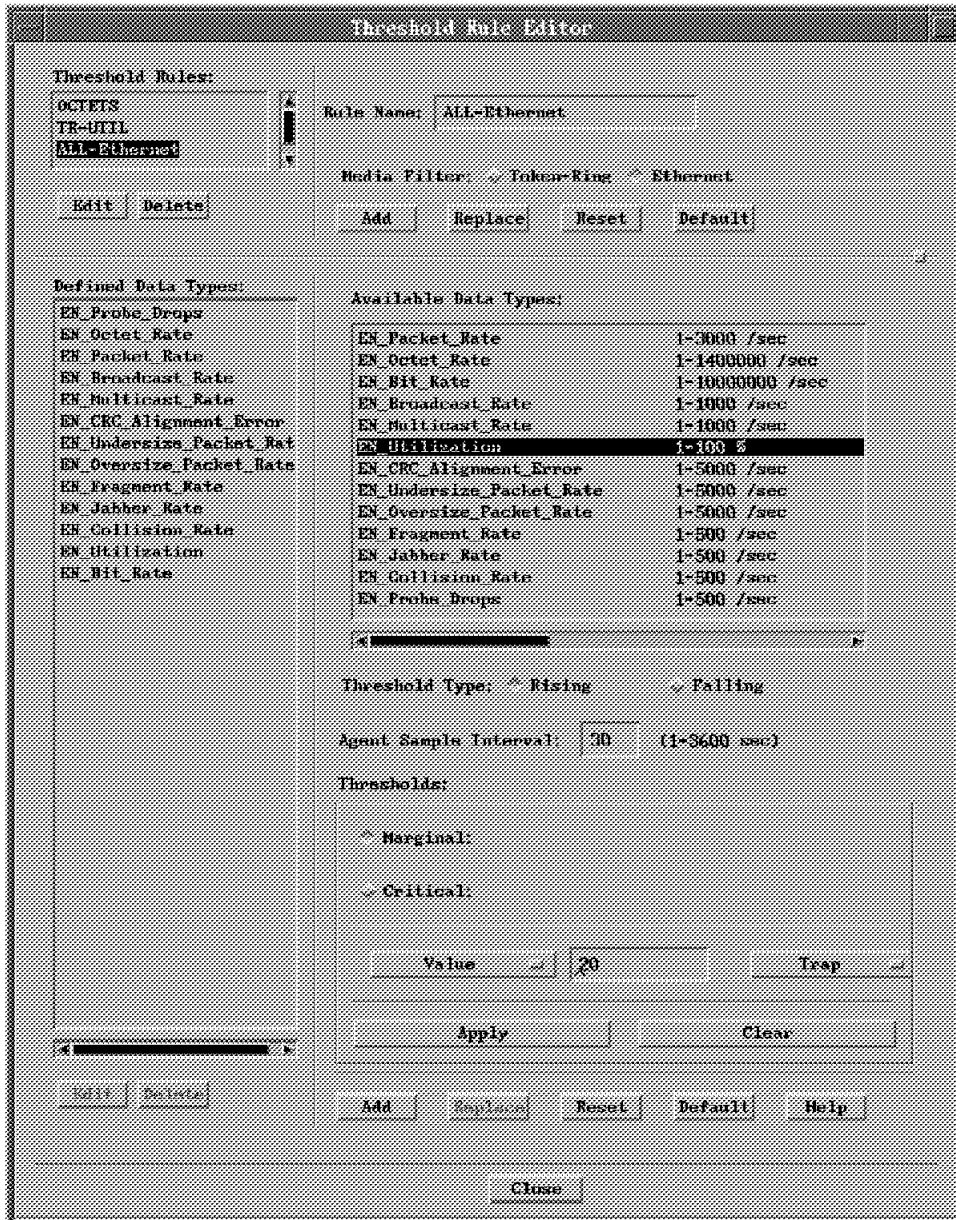


Figure 109. RMONitor for AIX All-Ethernet Threshold Rules

In addition, we have defined the Some-TokenRing threshold rule to include some of the token-ring network statistics as shown in Figure 110 on page 120.

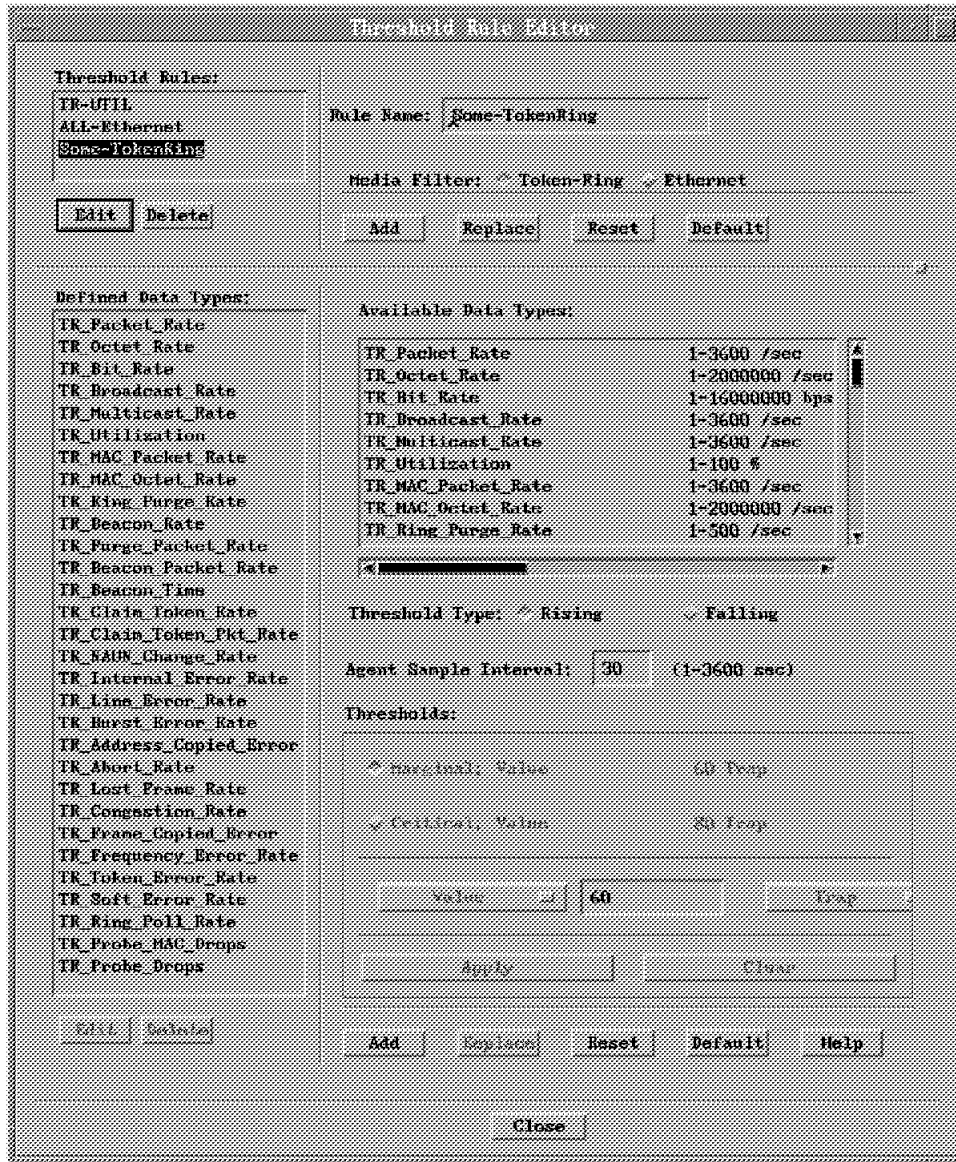


Figure 110. RMONitor for AIX Some-TokenRing Threshold Rules

Once completed choose **close** to complete the threshold rules definition.

4.2.4.5 Defining Collection Rules

Click on the **Collection Rules** button to begin defining these rules. To define the All_LONG rule, as shown in Figure 111 on page 121:

- Enter **All_LONG** in the Rule Name field.
- Select all the options in the **Apply to** list box . This indicates that all the information from the agents will be collected and stored on the RISC System/6000. This information is stored in the /usr/lpp/RMONitor/databases directory. The name of the file is based on the name of the collection rule. In our environment the file would be ALL_LONG.collect. As the file becomes full, based on the maximum size we had configured earlier, a numeric suffix is added, for example ALL_LONG.collect.0.
- Click on the **Long History** button, indicating that you would like to retrieve information based on the long history defined in the agent's rules. We will

retrieve the information every 30 minutes from the agents, since our long history is set to 30 minutes.

- In the *Forced Collection Times* area choose the **11:00** option. This means that the collection of information will begin at 11 a.m., in addition to the long history collections.
- Choose **Add** to accept this definition.
- Non-history data is collected every 30 minutes, and the history data is off-loaded to the long history category.

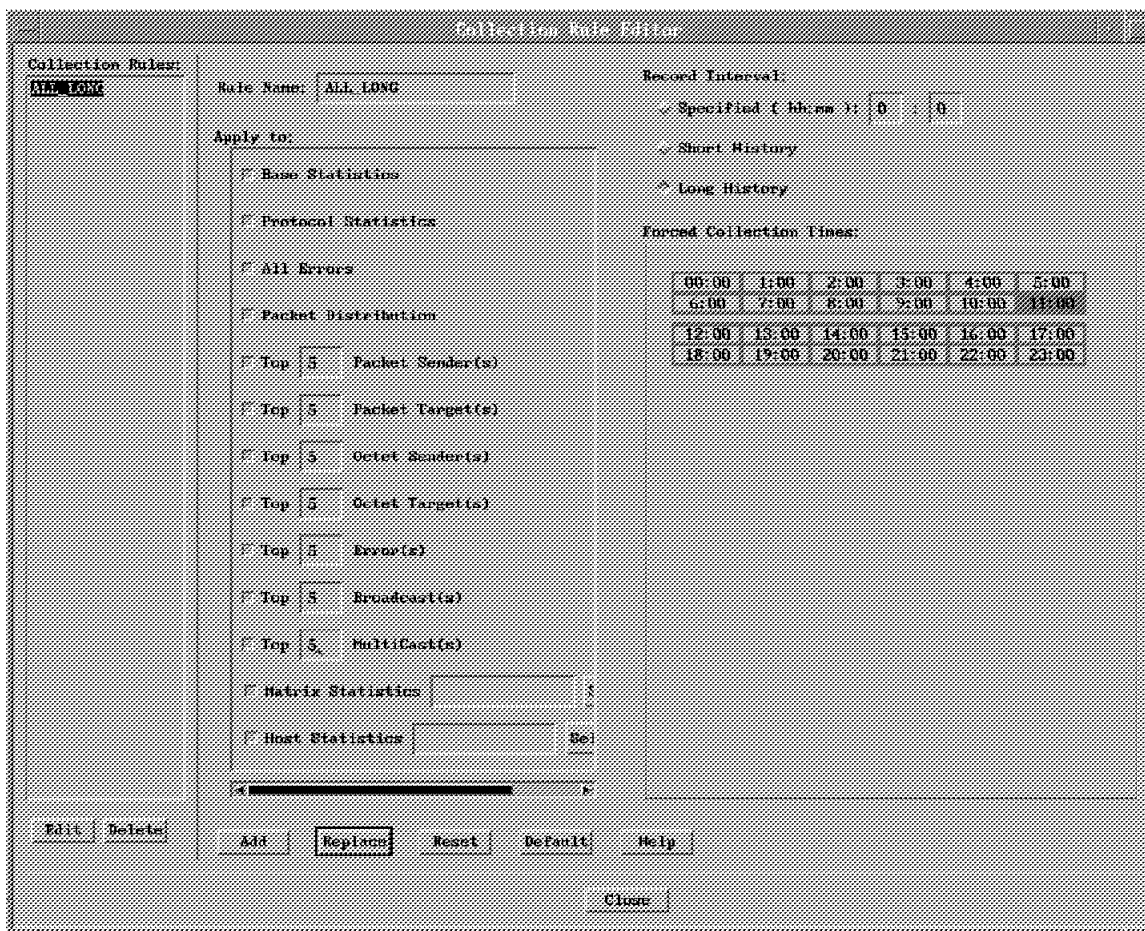


Figure 111. RMONitor for AIX All_LONG Collection Rules

After the individual rules have been defined, you will need to associate those rules with the policies, as shown in Figure 107 on page 117.

To define the agent and collection policies for RMONitor Agent for OS/2, perform the following steps:

1. Agent policies
 - Enter **RMON2** in the policy name.
 - Enter a description.
 - Enter the IP address of your RMONitor Agent for OS/2. In our environment we used **9.24.104.72**.
 - Choose the type of agent. In our environment **Token-Ring** was selected.
 - Choose the **Administer** option to enable this policy to control the RMONitor Agent for OS/2 with the options specified in the rules.

- Choose the agent rules in the list box. In our environment we selected **LongHistory**.
 - Choose the Threshold rules in the list box. In our environment we used **Some-TokenRing**, since this is a token-ring RMONitor Agent for OS/2.
 - Click on the **Add** button to update the information.
2. Collection policies
- Enter **RMON-TokenRing** as the policy name.
 - Enter a description.
 - Enter the IP address of your RMONitor Agent for OS/2. In our environment we used **9.24.104.72**.
 - Choose the collection rules in the list box. In our environment we used **ALL_LONG**.
 - Click on the **Add** button to update the information.

Similar steps were also done to then define the agent and collection policies for RMON1, as shown in Figure 107 on page 117.

Save the policy information in the RMNPol.dat file by selecting the **File...Save** options from the pull-down menu.

After the policy information is defined, RMONitor for AIX will apply these rules for the agents defined.

4.3 Starting RMONitor

To start RMONitor for AIX the following steps are required:

1. Make sure that the AIX NetView/6000 daemons are started.
2. On the AIX NetView/6000 management system start RMONitor for AIX.
3. Start the RMONitor Agent for OS/2.

If the RMONitor Agent for OS/2 is not running when the RMONitor for AIX application is started, the *Discovery polling interval* determines when RMONitor for AIX will try again to find the RMONitor Agent for OS/2. The *Mark agent down after this many timeouts* determines how often RMONitor for AIX will try before determining that the agent is down.

It is probably easier to start the RMONitor Agent for OS/2 first so the agent will be waiting for the RMONitor for AIX application. When RMONitor for AIX starts it will try to then apply the rules against the active RMONitor Agent for OS/2s.

4.3.1 Starting RMONitor for AIX

Before you start RMONitor for AIX, ensure that the following AIX NetView/6000 background processes (daemons) are running:

- ovesmd
- netmon
- snmpd

The RMONitor for AIX application can be started through SMIT by selecting the RMONitor options in SMIT and choosing the control option. Choose to start the RMONitor processes, as shown in Figure 112 on page 123.

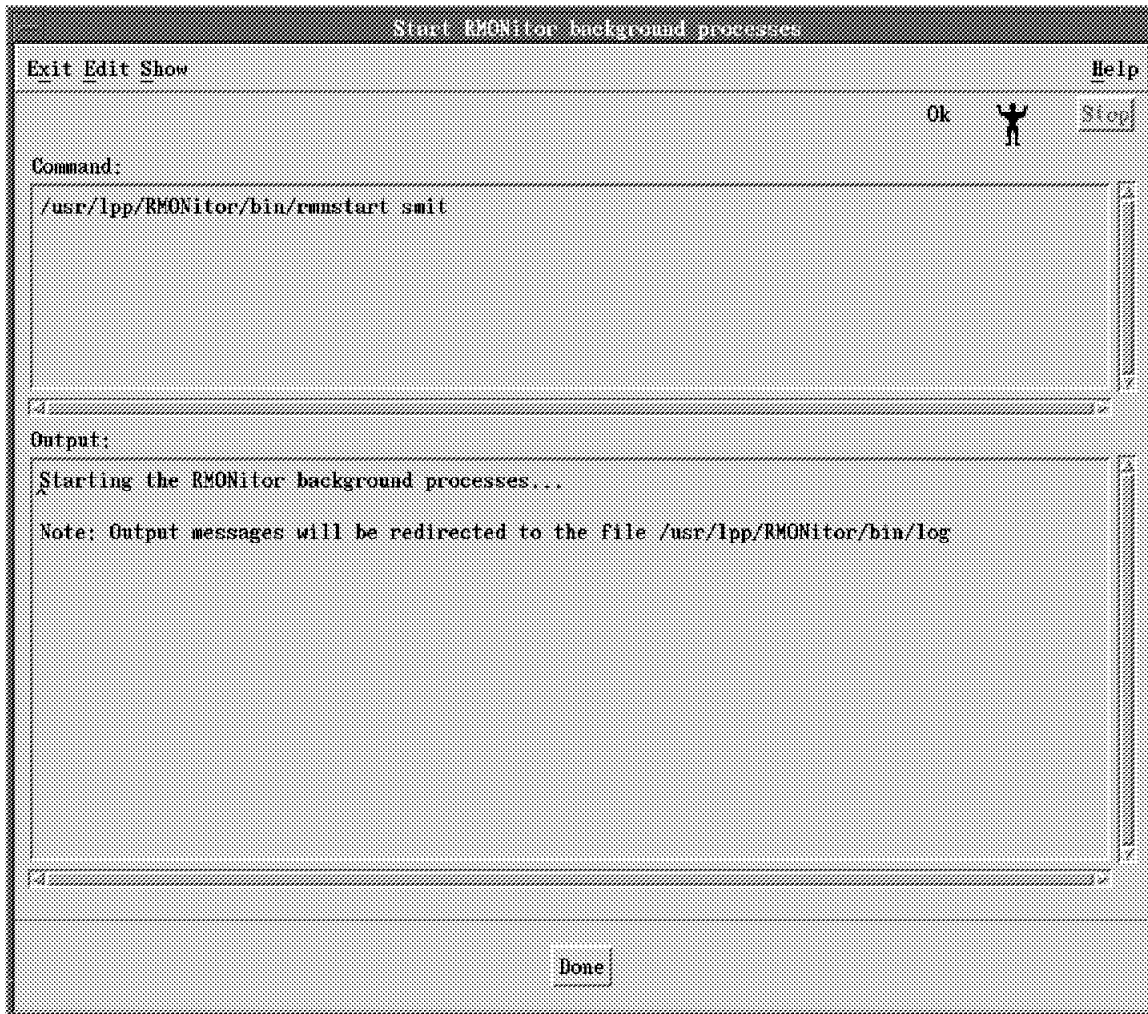


Figure 112. RMONitor for AIX Processes Starting

To display the status of the RMONitor for AIX processes, use the diagnose option from the SMIT menu. The screen displayed when all processes are up and running is shown in Figure 113 on page 124.

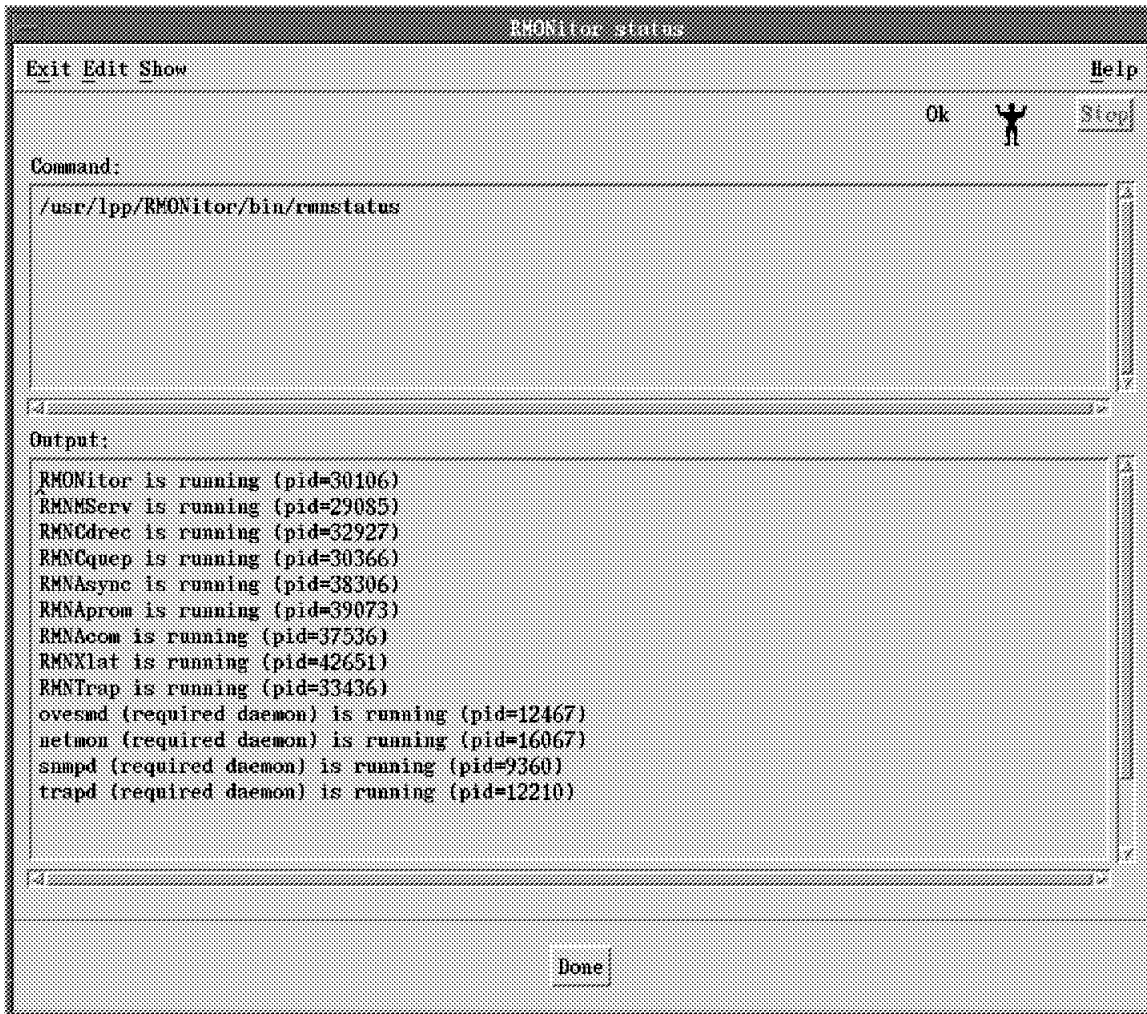


Figure 113. RMONitor for AIX Processes Running

4.3.2 Starting RMONitor Agent for OS/2

To start the RMONitor Agent for OS/2 choose the RMONitor Agent for OS/2 icon,



, from the RMONitor Agent for OS/2 folder on the OS/2 desktop. The RMONitor Agent for OS/2 main window is displayed, as shown in Figure 100 on page 111.

Choose the *Network statistics* icon to verify that the RMONitor Agent for OS/2 code is collecting and displaying the network statistics as shown in Figure 114 on page 125. If this screen is not being updated with the information that the RMONitor Agent for OS/2 is collecting from the network then the RMONitor Agent for OS/2 application is not operational.

The screenshot shows a window titled "Ethernet statistics" with a menu bar containing "File", "Options", and "F1=Help". The main content is a table with two columns: "MIB Variable" and "Value".

MIB Variable	Value
Drop events	0
Octets	9008
Packets	126
Broadcast packets	14
Multicast packets	101
CRC align errors	0
Undersize packets	0
Oversize packets	0
Fragmented packets	0
Jabbers	0
Packet collisions	0
Packet size (in octets)	
65 - 127	21
128 - 255	0
256 - 511	0
512 - 1023	0
1024 - 1518	0

Figure 114. RMONitor Agent for OS/2 Network Statistics

4.3.3 RMONitor Operations

Following are some of the functions available from RMONitor for AIX.

The RMONitor for AIX application provides a way for you to start the RMONitor for AIX graphical application interface without first starting AIX NetView/6000.

RMONitor for AIX provides many windows to monitor thresholds. This allows you to observe the threshold states from a high level using the Network Monitor and Active Monitor windows, down to a detailed level using the various Threshold detail windows.

Network Monitor Window: The first window displayed in RMONitor for AIX is the Network Monitor window. From this window all of the RMONitor for AIX functions can be accessed. We will start this window from AIX NetView/6000, as shown in Figure 115 on page 126, by choosing **Tools...RMONitor...Network Monitor** from the pull-down menu. The Network Monitor window will default to connecting to the *localhost* if no local host has been predefined.

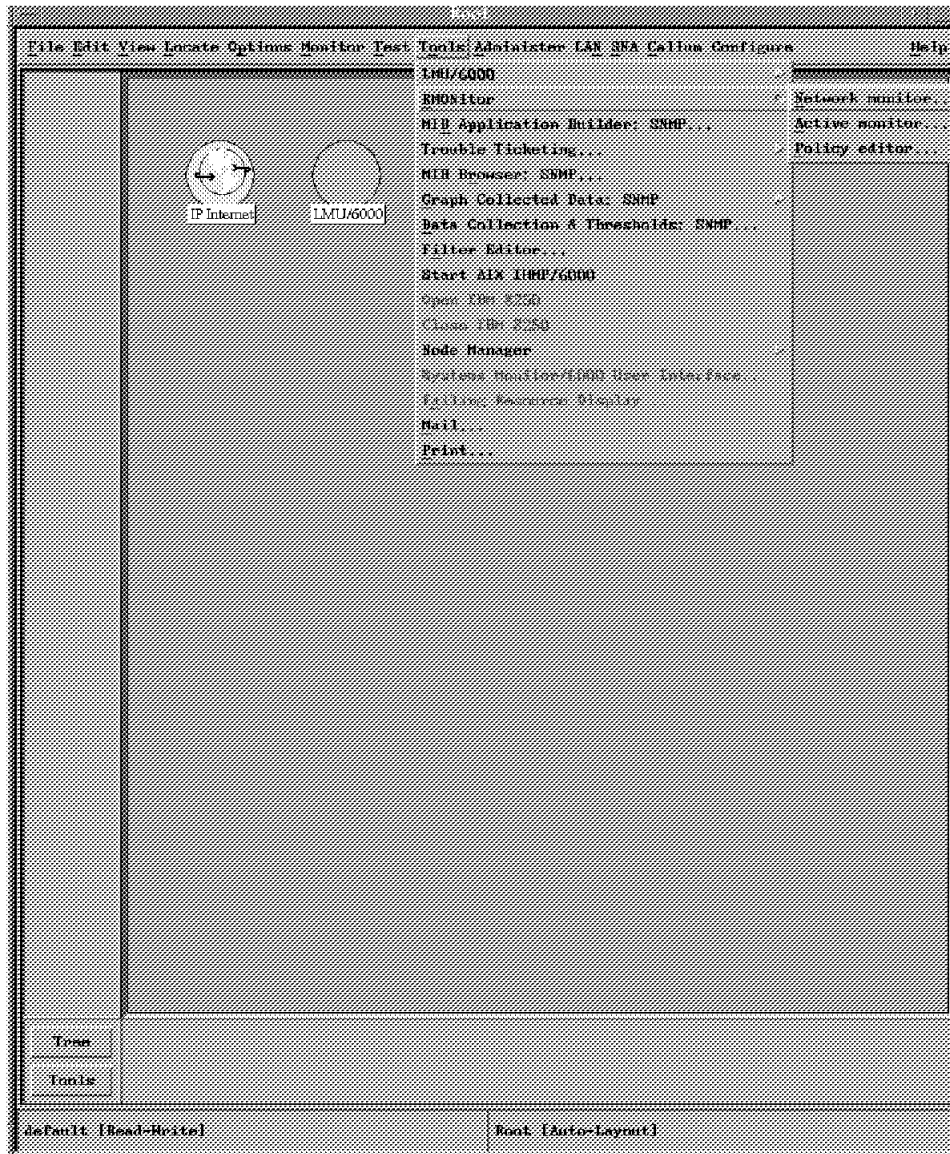


Figure 115. Starting RMONitor for AIX Network Monitor

The Network Monitor screen displays a summary of all RMON agents discovered and their overall states. Additional RMONitor Agent for OS/2 agents will be added to this list as they are discovered. In our environment 5 RMON agents have been identified. This screen provides an overall status of each agent as described:

- Red** Represents an agent experiencing critical conditions.
- Yellow** Represents an agent experiencing a warning (marginal) conditions.
- Green** Represents an agent operating in a normal state.
- Blue** Represents an unknown agent. No connectivity currently exists between the manager and the agent.
- Gray** Represents an unmanaged agent. No thresholds were defined, or successfully setup at this agent. All of the other functions can be executed.

You can choose to display only nodes in a specific state by enabling the appropriate toggle buttons in the criteria area. In our Network Monitor window the toggle buttons for all states are enabled. In our environment there were 5 RMONitor Agent for OS/2s discovered as shown in Figure 116 on page 127:

- 9.24.104.72 - which is our RMONitor Agent for OS/2 monitoring the 4Mbps token-ring network, which is in a marginal state.
- 9.67.32.87 - which is our RMONitor Agent for OS/2 monitoring the Ethernet, which is in a critical state.
- An additional 3 RMONitor Agent for OS/2s from the IBM Research Triangle Park network, are in an unknown or unmanaged state since no policies have been defined for these agents.

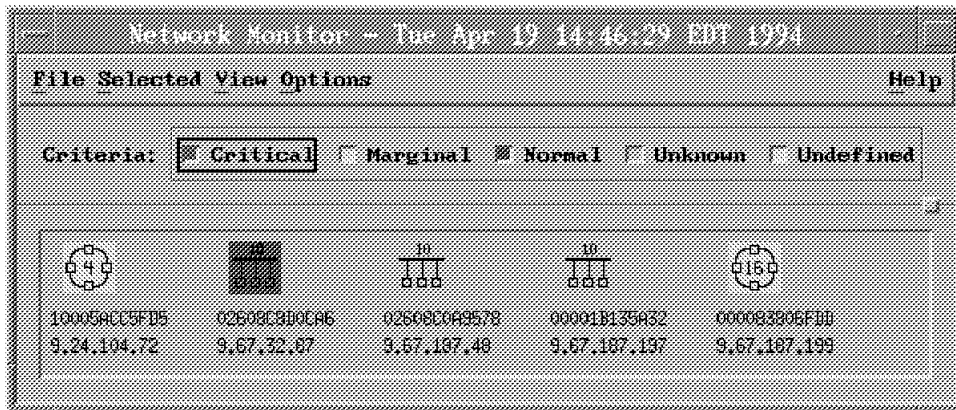


Figure 116. RMONitor for AIX Network Monitor

Active Monitor Window: The Active Monitor window, as shown in Figure 117 on page 128, allows the user to focus attention on a particular set of segments. In addition to displaying the overall segment status, the Active Monitor window shows the threshold categories for media and extensions and their states. This allows for a quick assessment of the threshold status. Utilization of the segment is also displayed. This is evaluated against the marginal and critical thresholds and the status is reflected on the meter.

To display the Active Monitor window do the following:

- Click on the agent(s) you want to selected.
- Choose **Selected...Active Monitor** from the Network Monitor window.

The Network Monitor window will then contain the agents you have selected. In our environment we have chosen two RMONitor Agent for OS/2s to be in our active window. The information shown about these agents includes:

1. Ethernet agent: The agent is in a normal state as are the *Thruput* and *Errors* categories. The utilization of this segment is in a normal state. Remember that the marginal and critical thresholds are determined by the values you entered when defining the policies.
2. Token-ring agent: The agent is in a critical state as are the *Thruput* and *Errors* categories. The utilization of this segment is in a critical state.

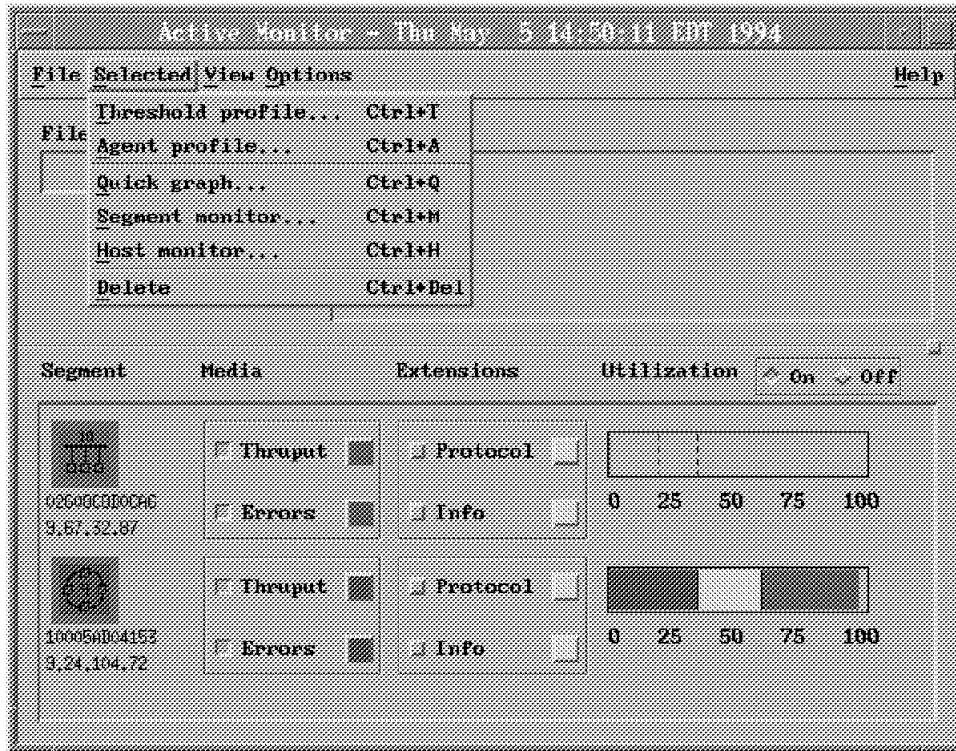


Figure 117. RMONitor for AIX Active Monitor

We will use this window to access all the other functions available within RMONitor for AIX. As shown in Figure 117 the *Selected* pull-down menu enables access to the other monitoring and graphing functions. Selecting an item from this menu requires you to select the agent(s) and then the menu option.

To display the Agent Profile window do the following:

- Click on the agent you want selected.
- Choose **Selected...Agent Profile**.

The Agent Profile window, as shown in Figure 118 on page 129, displays information about the RMONitor Agent for OS/2. This window shows general information about the agent as is shown on the top half of the screen and the functions supported by the agent as is shown by the ticks and crosses under the *Supports* heading. The *Policies* heading indicates the functions that were defined in the policy for this agent. In our environment the RMONitor Agent for OS/2 agent does not support the *Protocol* option; however, this was requested by the policy (as we had configured earlier).

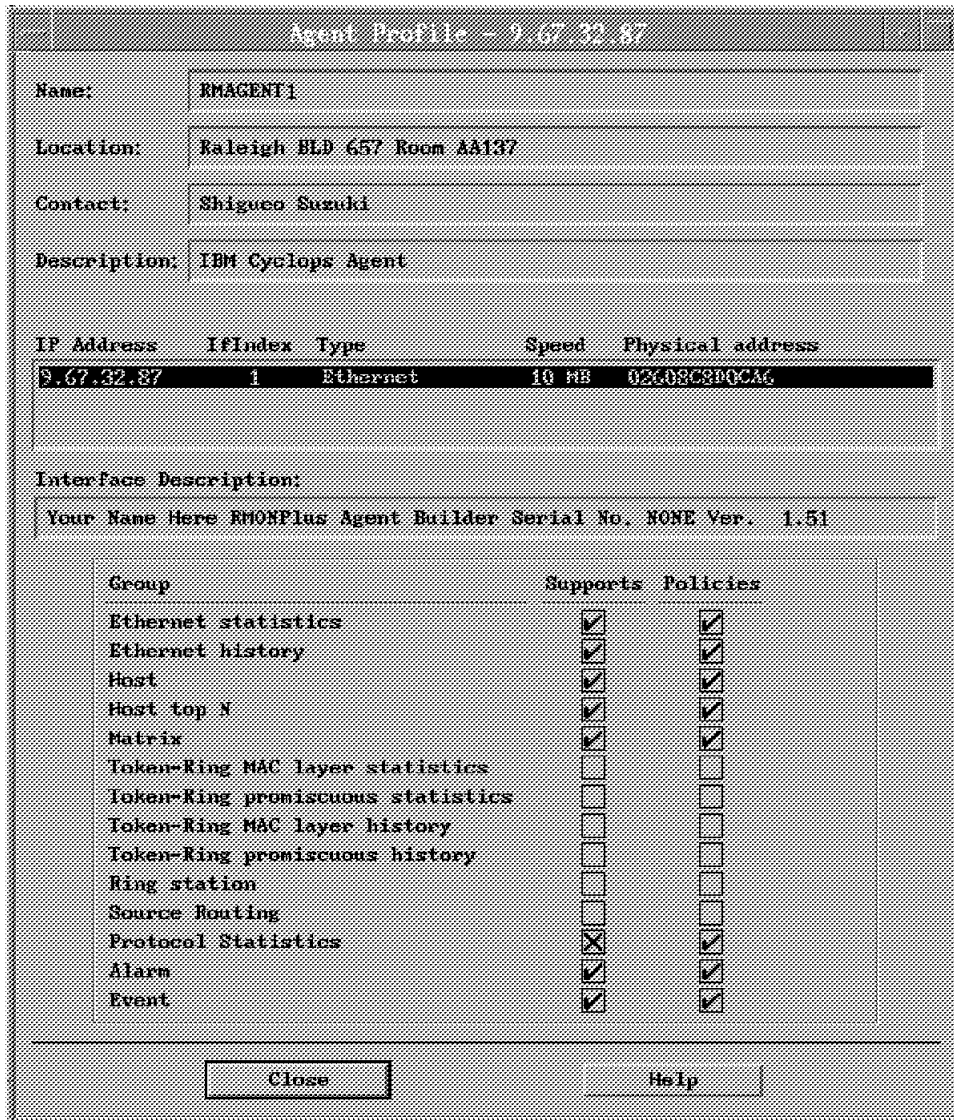


Figure 118. RMONitor for AIX Agent Profile

Threshold Windows: From the Active Monitor window, select the buttons to the right of either the Thruput or Errors labels to display the detailed threshold windows, as shown in Figure 119 on page 130. The detailed threshold window that is displayed shows you the values that the RMONitor for AIX application uses to calculate the status for the Thruput label.

The information displayed for each statistic monitored is:

- State of the statistic(s): the same color scheme is used to indicate whether the counter is in a normal, marginal or critical state.
- Rising or Falling threshold: if the triangle points up it is then a rising threshold, as all our thresholds are. For a falling threshold the arrow will point down.
- The individual statistics displayed are the statistics defined in the policy applied to the RMONitor Agent for OS/2. In our environment we had defined all the statistics as shown.

- Polled Value: this is the value that has been retrieved for the RMONitor Agent for OS/2 at the last poll.
- Trap Value and Time/Date: this is the value of the last trap sent to RMONitor for AIX. The date and time of the trap is also displayed.
- Marginal and Critical thresholds: the current thresholds being used for each statistic. These threshold values are defined in the policy applied to the RMONitor Agent for OS/2. In our environment these were defined in the *All-Ethernet* threshold rules.
- Counters: this shows the number of traps that have been sent in the last 10, 20 and 30 minutes that indicate a worsening condition.

Thruput - 9.67.32.37/0260NCS00CA6									
Options Help									
	Polled Value	Trap Value	Trap Time/Date	Marginal Threshold	Critical Threshold	Counters			
						-10 min	-20 min	-30 min	
<input checked="" type="checkbox"/> A Packet Rate	237/s			2000/s	3000/s				
<input checked="" type="checkbox"/> A Octet Rate	24539/s			150/s	250/s				
<input checked="" type="checkbox"/> A Bit Rate	196316bs	13616bs	Thu May 5 12:15:35 EDT 1994	1500bs	3000bs	1	0	0	
<input checked="" type="checkbox"/> A Broadcast Rate	57/s	54/s	Thu May 5 12:32:34 EDT 1994	50/s	100/s	2	0	0	
<input checked="" type="checkbox"/> A Multicast Rate	1/s			50/s	100/s				
<input checked="" type="checkbox"/> A Utilization	1.96%	0.32%	Thu May 5 12:15:27 EDT 1994	20.00%	35.00%	1	0	0	

Figure 119. RMONitor for AIX Ethernet Thruput Threshold Details

In addition, by double clicking on the RMONitor Agent for OS/2 symbol, a new window detailing the thresholds for all statistics defined in the policy applied to the RMONitor Agent for OS/2, as shown in Figure 120 on page 131 will appear. In our environment all the statistics to be monitored for the token-ring RMONitor Agent for OS/2 are displayed. This was defined in our *Some-TokenRing* threshold rules.

Threshold Profile - 9.24.104.72/100054004153						
Options	Pulled Value	Trap Value	Trap Time/Date	Marginal Threshold	Critical Threshold	Help
▲ Packet Rate	109/s	85196/s	Thu May 5 12:39:00 EDT 1994	2000/s	2000/s	
▲ Octet Rate	15723/s			20000/s	30000/s	
▲ Bit Rate	125790bs			480000bs	960000bs	
▲ Broadcast Rate	2/s			500/s	600/s	
▲ Multicast Rate	42/s			500/s	600/s	
▲ Utilization	3.14%			35.00%	60.00%	
▲ MAC Packet Rate	4/s			50/s	200/s	
▲ MAC Octet Rate	134/s			90000/s	180000/s	
▲ Ring Purge Rate	0/s			350/s	450/s	
▲ Beacon Rate	0/s			350/s	450/s	
▲ Ring Purge Packet Rate	0/s			350/s	450/s	
▲ Beacon Packet Rate	0/s			350/s	450/s	
▲ Beacon Time	0.00%			8.00%	9.00%	
▲ Claim Token Rate	0/s			30/s	45/s	
▲ Claim Token Packet Rate	0/s			60/s	80/s	
▲ Name Change Rate	0/s			160/s	180/s	
▲ Internal Error Rate	0/s			350/s	450/s	
▲ Link Error Rate	0/s			350/s	450/s	
▲ Burst Error Rate	0/s			350/s	450/s	
▲ Address Copied Error Rate	0/s			3500/s	4500/s	
▲ Abort Error Rate	0/s			350/s	450/s	
▲ Lost Frame Rate	0/s			500/s	600/s	
▲ Congestion Rate	0/s			1400/s	1800/s	
▲ Frame Copy Rate	0/s			1400/s	1800/s	
▲ Frequency Rate	0/s			1400/s	1800/s	
▲ Token Error Rate	0/s			350/s	450/s	
▲ Soft Error Rate	0/s			350/s	450/s	
▲ Ring Full Events Rate	0/s			500/s	600/s	
▲ MAC Probe Drop Rate	0			350	450	
▲ Promiscuous Probe Drop Rate	0			350	450	

Figure 120. RMONitor for AIX Token-Ring All Threshold Details

Segment Monitor: The Segment Monitor window, as shown in Figure 121 on page 132, provides the ability to view specific attributes of segment information in either a table or graph format. The information that you view can be from RMONitor Agent for OS/2's long or short history, or the real-time statistics. The attributes contain a group of statistics relevant to that attribute; for example, the *Token-ring Base Stats* attributes display the following statistics:

- Packet Rate
- Octet Rate
- Bit Rate
- Broadcast Rate
- Multicast Rate
- Utilization
- MAC Packet Rate
- MAC Octet Rate

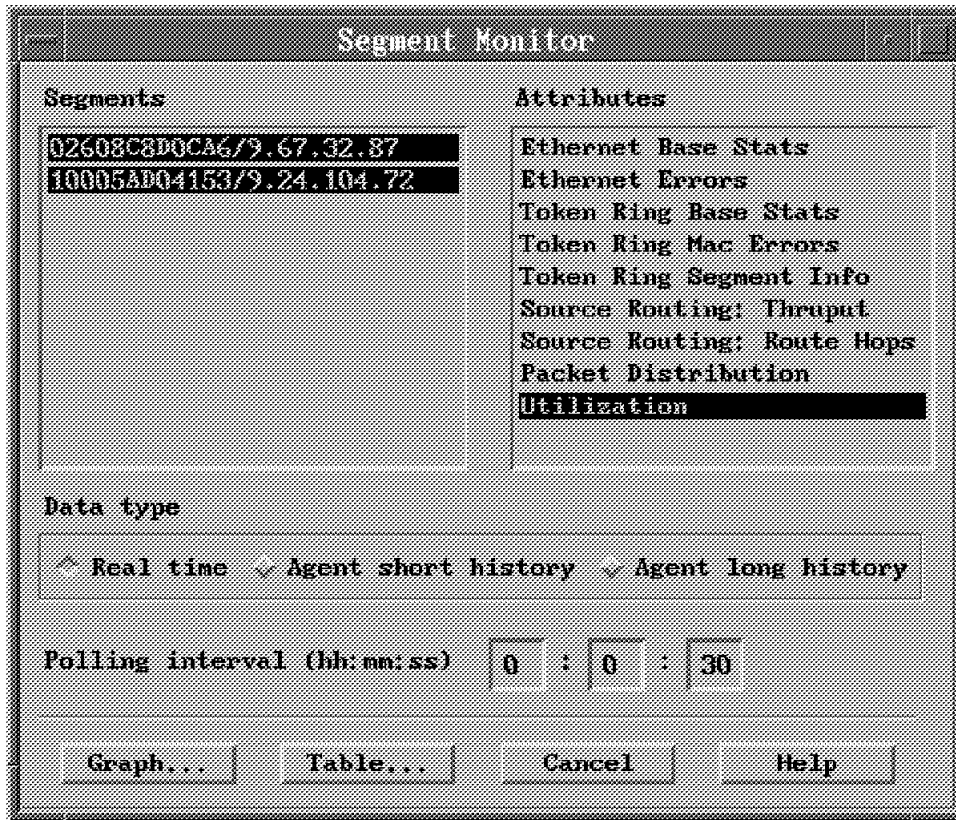


Figure 121. RMONitor for AIX Segment Monitor

We have chosen to display the token-ring's short history information for the token-ring Base Stats attribute. This was displayed by doing the following:

- Click on the token-ring RMONitor Agent for OS/2, which in our environment was the 9.24.104.72 segment.
- Choose the **Agent short history** to indicate we want the information retrieved from the RMONitor Agent for OS/2's short history.
- Choose **token-ring Base Stats** for the attributes we want displayed.
- Choose the **Table** or **Graph** push button to display the information.

We have chosen to display the information in a table, as shown in Figure 122 on page 133, and a graph format, as shown in Figure 123 on page 133.

The information is displayed in 30-second intervals since we have specified the sample interval to be 30 seconds in the *LongHistory* agent rules, as shown in Figure 108 on page 118.

9.24.104.72/10005AD04153					
Options Help					
	19:01:53	19:01:23	19:00:53	19:00:23	18:59:
Packet Rate	174/s	154/s	163/s	159/s	19
Octet Rate	276504/s	272543/s	274067/s	274813/s	27704
Bit Rate	2212035bs	2180346bs	2192542bs	2198509bs	221638
Broadcast Rate	76/s	76/s	76/s	76/s	7
Multicast Rate	44/s	37/s	36/s	34/s	3
Utilization	55.30%	54.50%	54.81%	54.96%	55.
MAC Packet Rate	4/s	3/s	3/s	4/s	
MAC Octet Rate	150/s	120/s	120/s	150/s	12

Figure 122. RMONitor for AIX Token-Ring Base Stats Table

The graphing facility of RMONitor for AIX uses the xnmgraph facility provided by AIX NetView/6000. In the graph displayed we made the graph lines thicker and changed some of the colors through the features provided by xnmgraph.

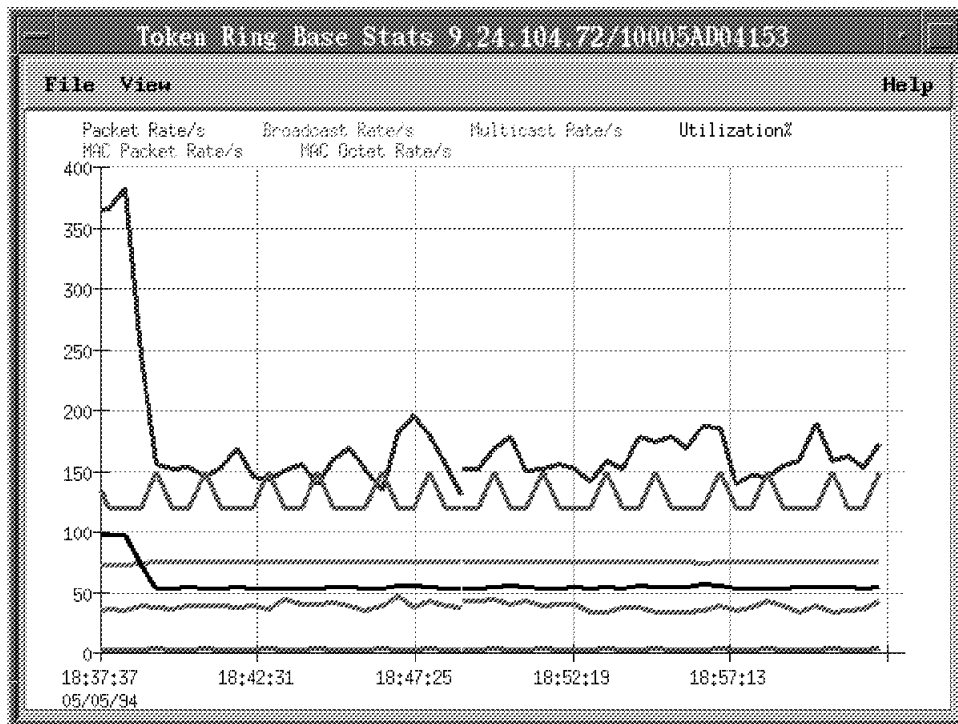


Figure 123. RMONitor for AIX Host Monitor Window

Host Monitor: The Host Monitor window, as shown in Figure 124 on page 134, provides the ability to view information about hosts (adapters) on the segment. The type of information displayed is based on the *Attributes* you want monitored, such as:

- Packet Rate In or Out
- Octet Rate In or Out
- Errors

- Broadcast
- Multicast

Based on one of the attributes listed above the hosts are displayed either as a table, list or graph. The information can be displayed in the following ways:

- All segment stations: displays all hosts on the segment retrieving the specific attribute information.
- Any station addressing: displays the specific host entered when it is either a destination or source.
- Station pair: displays the traffic between the pair of hosts entered.
- Station: displays all the information about the host entered.
- Top N Stations: displays the information about the top N stations.

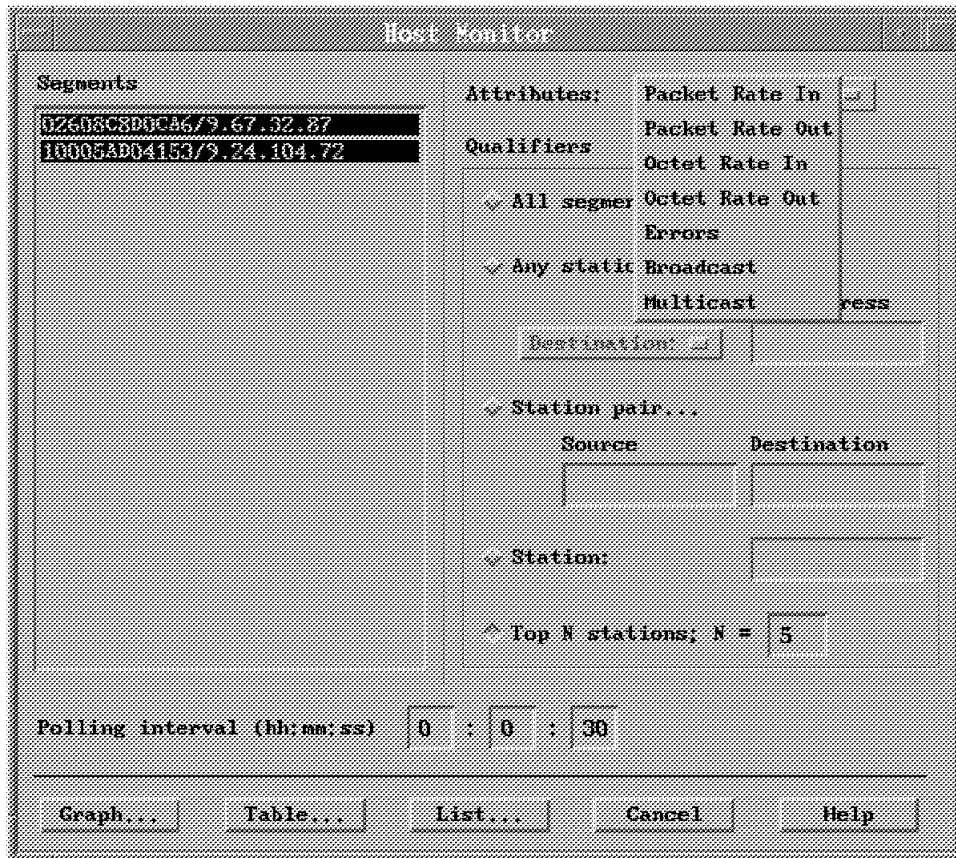


Figure 124. RMONitor for AIX Host Monitor Window

We chose to display the **Packet Rate In** attribute for all stations on the segment as a graph by using the following steps:

- Click on the token-ring RMONitor Agent for OS/2. In our environment that was the 9.24.104.72 segment.
- Choose the **Packet Rate In** attribute.
- Click on the **All segment stations** option.
- Click on the **Graph** push button to graph this information, as shown in Figure 125 on page 135.

The xnmgraph facility was used. We chose only to display the four stations listed. We increased the thickness of the graph lines and changed the colors by using the facilities provided by xnmgraph.

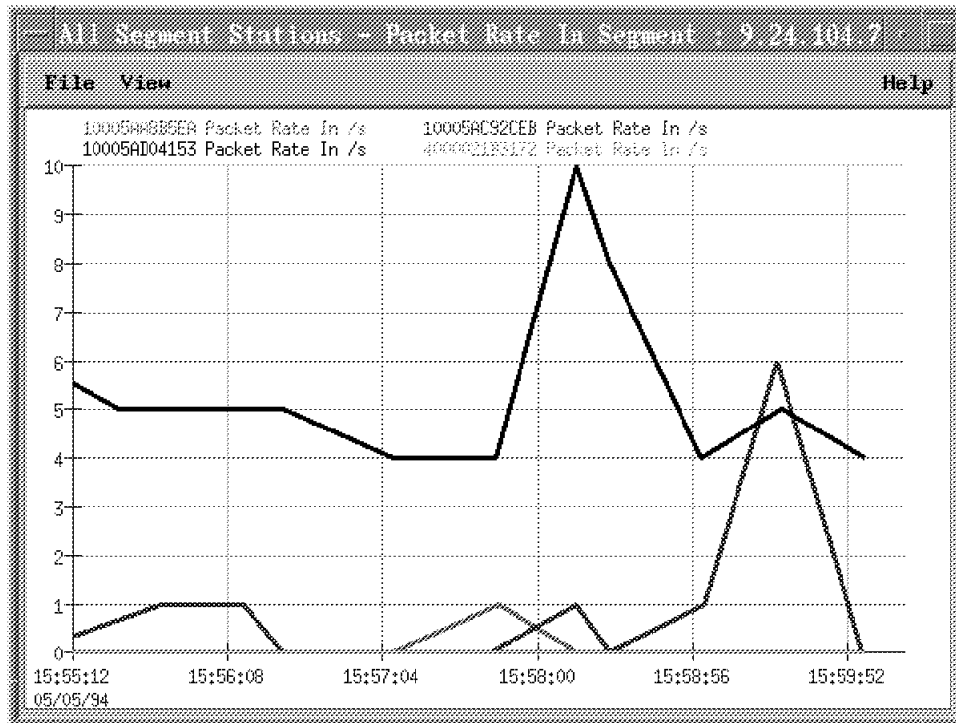


Figure 125. RMONitor for AIX Host Monitor Graph

Quick Graph: The quick graph feature allows you to graph frequently used segment information. The information that you can graph is defined through the Quick Graph Setup window, as shown in Figure 126 on page 136. This window is accessed through the **Options...Quick Graph Setup** pull-down from the Active Monitor window. In this window the attributes that you want graphed for each of the four categories are defined. To graph this information you select the RMONitor Agent for OS/2 and then choose **Selected...Quick Graph** option from the Active Monitor window, and the predefined graph will be displayed. In our environment the attributes we defined for each of the categories were:

1. TR Thruput Family - Packet rate, broadcast rate and utilization
2. TR Errs Family - Congestion rate, token error rate and soft error rate
3. EN Thruput Family - Packet rate, broadcast rate and utilization
4. EN Errors Family - Collision rate

In addition, the polling interval at which you want to retrieve the information from the RMONitor Agent for OS/2 is also defined. In our environment we used the default value of 30 seconds.

Once the definitions are entered choose the **Apply** push button to save the quick graph definitions.

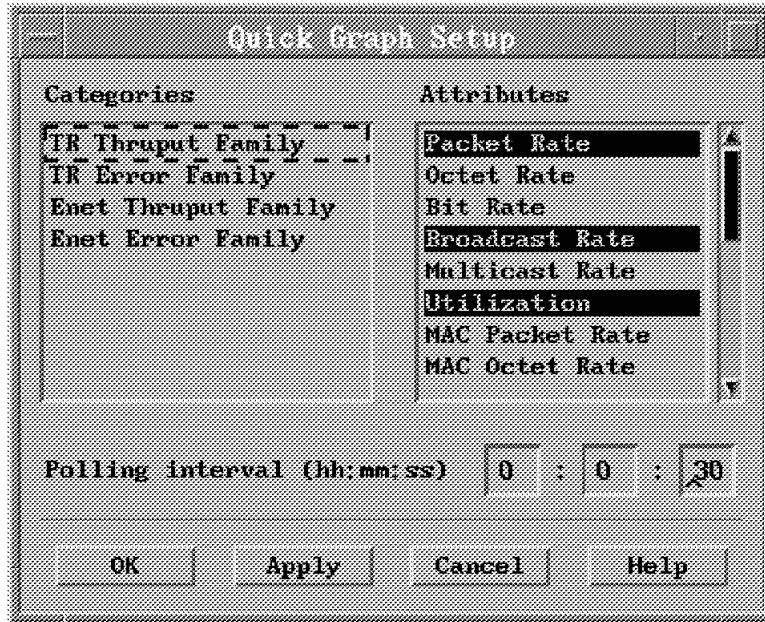


Figure 126. RMONitor for AIX Quick Graph Setup

Therefore, when we choose to display the quick graph for the throughput values of our token-ring RMONitor Agent for OS/2 the graph shown in Figure 127 on page 137 will be displayed.

To display this graph do the following from the Active Monitor window:

- Click on the RMONitor Agent for OS/2; in our case the 9.24.104.72 agent.
- Click on the toggle button to the left of the thrupt label.
- Choose the **Selected...Quick Graph** option from the pull-down menu.

Only the Packet Rate/s, Broadcast Rate/s and Utilization% are displayed, as we had defined earlier.

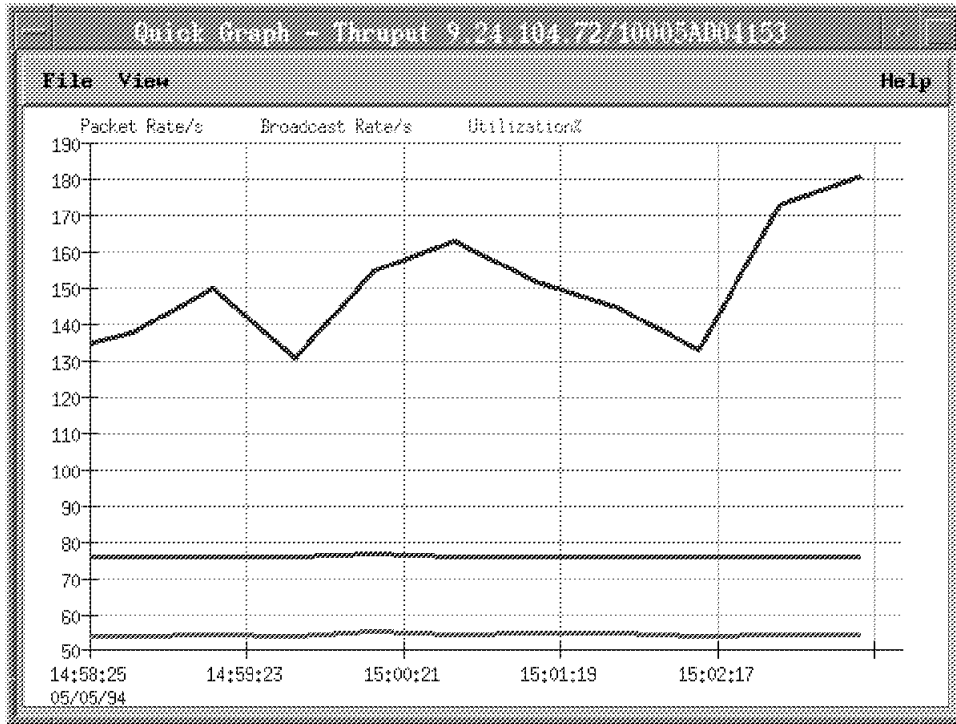


Figure 127. RMONitor for AIX Token-Ring Thruput Category Quick Graph

In addition, multiple options can be selected as shown in Figure 128 on page 138. In that graph all the throughput and error categories are displayed for both of our RMONitor Agent for OS/2s. To display this graph do the following:

- Click on both RMONitor Agent for OS/2s; in our case the 9.24.104.72 and the 9.67.32.87 agents.
- Click on all the toggle buttons to the left of the thruput and error labels.
- Choose the **Selected...Quick Graph** option from the pull-down menu.

We customized the graph through the functions provided with the xnmgraph facility to show the information displayed.

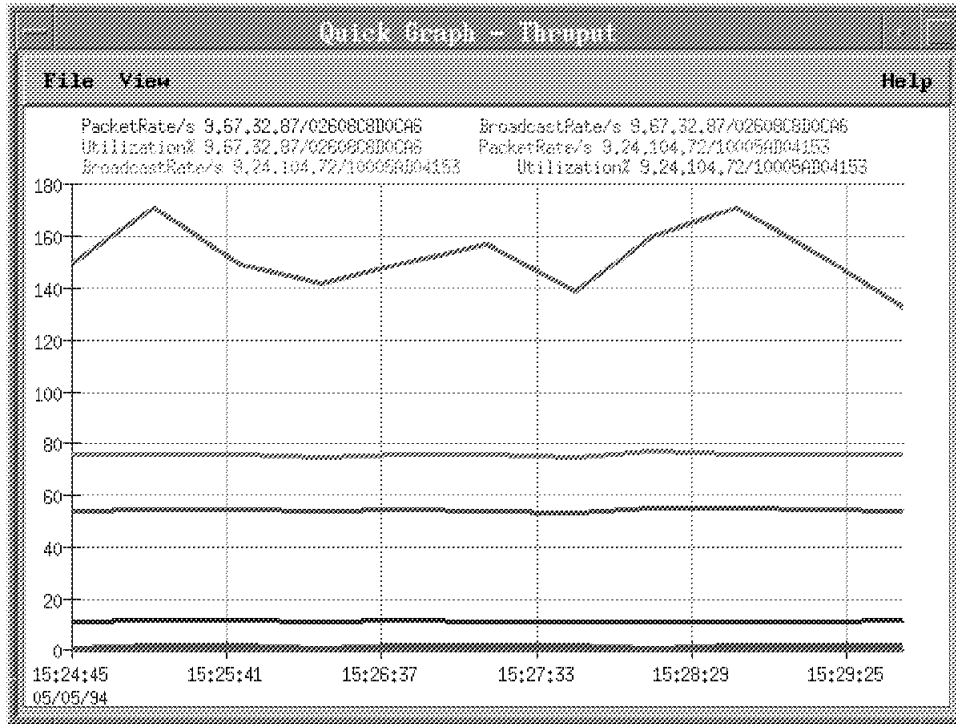


Figure 128. RMONitor for AIX All Categories Quick Graph

Chapter 5. IHMP/6000

The IBM Hub Management Program/6000 (IHMP/6000) provides a comprehensive solution to managing all major LAN types with the IBM 8250 Multiprotocol Intelligent Hubs. IHMP/6000 improves network support productivity by providing an easy-to-use graphical interface for the following management functions: fault, configuration, operations and change.

IHMP/6000 aids in LAN and Hub management by collecting and reporting statistics per hub port and per LAN, and offering LAN level security by preventing unauthorized users from accessing the network. The generic network management functions that are directly available from AIX NetView/6000 are exploited.

IBM has three Hub Management Program offerings which provide a full range of flexibility and function to help manage the IBM 8250 Multiprotocol Intelligent Hub. They are the:

- **IBM AIX NetView Hub Management Program/6000 (IHMP/6000)**
- **IBM AIX NetView Hub Management Program/6000 Entry (IHMP/6000 Entry)**
- **IBM Intelligent Hub Management Program/DOS Entry (IHMP/DOS Entry)**

5.1.1 Highlights of IHMP/6000

Enhances network management for 8250 hubs and improves network support productivity by providing an easy-to-use graphical interface for the following management functions: fault, configuration, operations, and change.

- Provides an expanded view of 8250 hubs with realistic graphics of various components, and color coded status for straightforward operations and status notification.
- Exploits the capabilities of the 8250 hub and its simple network management protocol (SNMP) extended MIB to provide maximum flexibility in assigning individual ports or modules to a LAN, or to isolate any module from the back-plane for troubleshooting purposes.
- Automatically discovers the models of 8250 hubs and their installed modules.
- Leverages the operating environment of AIX NetView/6000, IBM's platform for the management of multi-vendor transmission control protocol/internet protocol (TCP/IP) networks, including the IBM 6611 Network Processor and the IBM 8240 FDDI Concentrator.
- Provides network security by preventing unauthorized users from accessing the network.
- Provides an easy to use, context sensitive online help facility.
- Simple Network management Protocol (SNMP) support in the 8250 Hub permits remote, permanent monitoring with IHMP/6000 for managing from any SNMP management station.

IHMP/6000 Entry provides the same set of comprehensive management functions as the IHMP/6000 licensed product, with the exception of the enhanced security function (more than one MAC address authorized per port) and Time Of Day (intrusion protection based on time of day). Additionally, the lower-priced IHMP/6000 can support up to six 8250s.

5.1.2 Description

The IHMP/6000 and IHMP/6000 Entry graphical user interface was designed to reduce user actions needed to configure a component or identify a failed one, and minimize unnecessary window management. The expanded view of 8250 hubs with mouse clicking on selected components provides the user with a concise and simple display from which the various tasks can be performed for workgroups and small department connectivity.

The user is provided with the following major management functions:

- Automatic discovery of various hubs and installed modules
- Monitoring and display functions
- Configuration and control of modules in the concentrator

5.2 Intelligent Hub Management Program/DOS Entry

The IBM Intelligent Hub Management Program/DOS Entry (V1.0) facilitates and expands the management of local area networks (LANs) with IBM 8250 multiprotocol intelligent hubs. This program operates on a PS/2* with DOS/Windows operating system.

IHMP/DOS Entry can be of particular value to both smaller companies or large enterprises with a large number of branch offices as a solution for the management of smaller hubs and LANs. Also, IHMP/DOS Entry is recommended for those customers who have used ASCII terminals to manage their 8250s, or who prefer an Intel**-based solution.

IHMP/DOS Entry provides an easy-to-use graphical management tool and a very attractive solution for managing a small LAN network of 8250 hubs from a PS/2 connected to this network. These tools are directly available from AIX NetView/6000, and work in conjunction with all of the management modules of the 8250, namely:

- Advanced and basic Ethernet management modules
- Advanced and basic token-ring management module
- FDDI management module

5.2.1 Highlights of IHMP/DOS Entry

The IHMP/DOS Entry package includes both the TCP/IP and SNMP stacks with some utilities, and the following management functions:

- Graphic hub display for configuration with point and click operations at the port level
- Display of alarms and events
- Telnet command from the application
- Hub microcode down-loading from the station
- Online dynamic help facility

Also, IHMP/DOS Entry provides the following functions:

- Provides a realistic expanded view of the 8250 hub with color coded status.
- Graphic resolution is customized depending on the resolution of the terminal display.
- Point and click operations with the mouse.
- Display of events and alarms in a circular queue.

- Online dynamic help facility.
- Telnet command accessible from the application.
- FTP, PING and ECHO commands and microcode downloading application accessible from the station.

The following configuration and change management operations are provided via a realistic graphic view of the hub and mouse clicking on selected components:

- Display of configuration with color codes on the expanded view.
- Display of the status on hub components at the level of the port, module, hub, and LAN via forms.
- Reconfiguration of the various elements of the hub: reset of modules and reassignment of modules and ports when applicable.
- Configuration of the fault tolerant operations on the media modules.
- Online dynamic Help facility.
- Downloading of the microcode of the hub management modules.
- Remote login via TELNET to manage modules, bridge modules etc.

LAN reconfigurations, such as user port re-assignment, are done more quickly with fewer errors using the enhanced user interface. Network component status is reported with a color coding system that lets the user determine with a single view the status of each component. Corrective actions can be done rapidly.

As the access to all the new functions is possible with simple point and click operations, the operator can be educated very quickly on the new functions brought by the new 8250 features.

IHMP/DOS Entry also has an online dynamic help facility. General help displays allow the user to get familiar with IHMP/DOS Entry functions, and module level help displays explain the detailed operations for each module. Also, general help screens explain in detail how to use the various help windows.

5.3 IHMP/6000 Installation

To install the IHMP/6000 code use SMIT and the values defined in 1.5.3, "RISC System/6000 Software Installation Procedures" on page 40. The list shown when you prompt for the *SOFTWARE to install* field for IHMP/6000 is shown in Figure 129. Select the top item *1.1.0.0 IHMP/6000 ALL*.

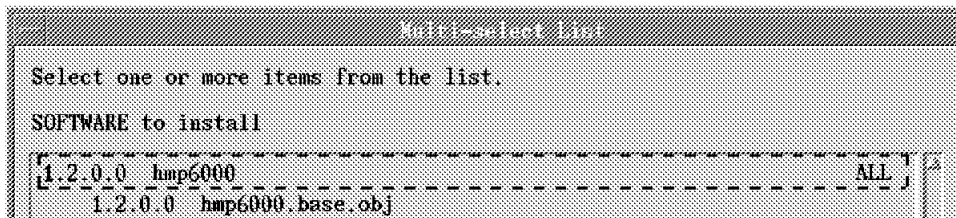


Figure 129. IHMP/6000 Install List

The installation requires no further interaction.

5.4 IHMP/6000 Configuration

The main configuration process is to ensure that the AIX NetView/6000 management system has the authority to access the SNMP information from the 8250 Hub. The following steps are required to configure this:

1. Access the 8250 Hub through telnet or via a directly-attached ASCII terminal.
2. Set the community name.

When AIX NetView/6000 has identified the hub on the IP topology map, you will be able to telnet to the hub and perform administration functions. The initial symbol provided for the 8250 Hub is the computer symbol (a square). This indicates that the community information is not correct between the 8250 Hub and the AIX NetView/6000 management system.

Telnet into the 8250 Hub using the **Administration...Telnet (aixterm)** option on the pull-down menu, as shown in Figure 130. This menu is accessed by clicking on the hub symbol with the right mouse button.

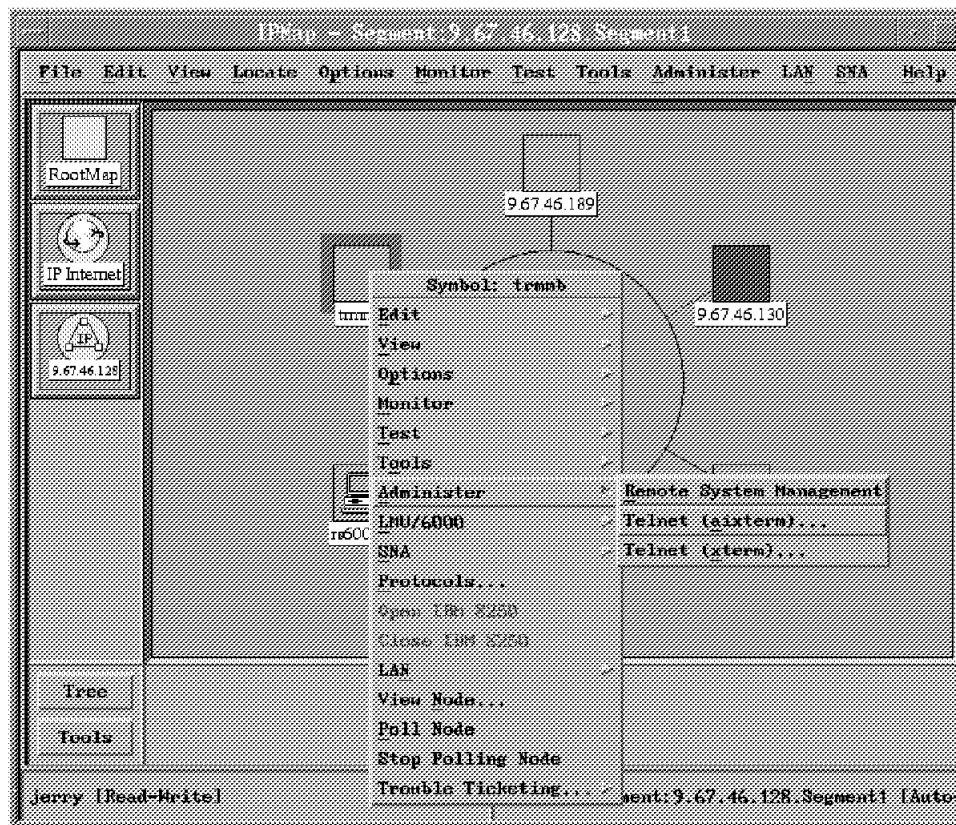


Figure 130. AIX NetView/6000 Selecting Administration Options

Enter the password required to access the administration user ID for the 8250 Hub. The command used to set the community information was:

```
set community public 9.67.46.170 all
```

To show that this has been entered correctly the command is:

```
show community
```

The information you just entered should now be displayed in the community table on the 8250 Hub, as shown in Figure 131 on page 143. In our environment the 8250 Hub sends SNMP information to more than one management system. Our entry is on Index 9. If no entries are available then you will have to clear an entry before entering your community information. To clear community entry 4 you would enter:

```
clear community 4
```

```

Connected to trmmb.
Escape character is '^]'.

TRMMB
Token Ring Management Module (v2.10-A)
Copyright (c) 1993 Chipcom Corporation
Password:

Welcome to the system administrator services on TRMMB.
TRMMB show community
      Index  Community Name      IP Address      Access
      -----  -
      1  ITSC                009.067.038.073  All
      2  ITSC                009.067.046.020  All
      3  ITSC                009.067.046.158  All
      4  ITSC                009.067.046.159  All
      5  ITSC                009.067.046.157  All
      6  ITSC                009.067.038.067  All
      7  public              009.067.046.190  All
      8  public              009.067.046.189  All
      9  public              009.067.046.170  All
     10  [empty]
TRMMB _

```

Figure 131. 8250 Hub Community Information

Save the configuration by entering **save all**, then enter **logout**. The 8250 Hub does not need to be restarted since the community information is dynamically updated.

Note: Though we are using a community name of ITSC throughout our network only the community name of *public* enabled everything to work as expected. This was due to the fact that we were using early beta code.

To check that the community information is correct perform a *Demand Poll* against the 8250 Hub symbol, as shown in Figure 132 on page 144. The Demand Poll performs a ping and retrieves SNMP information from the device. If the Demand Poll is successful the symbol for the 8250 Hub should change to the symbol as shown in Figure 133 on page 144.

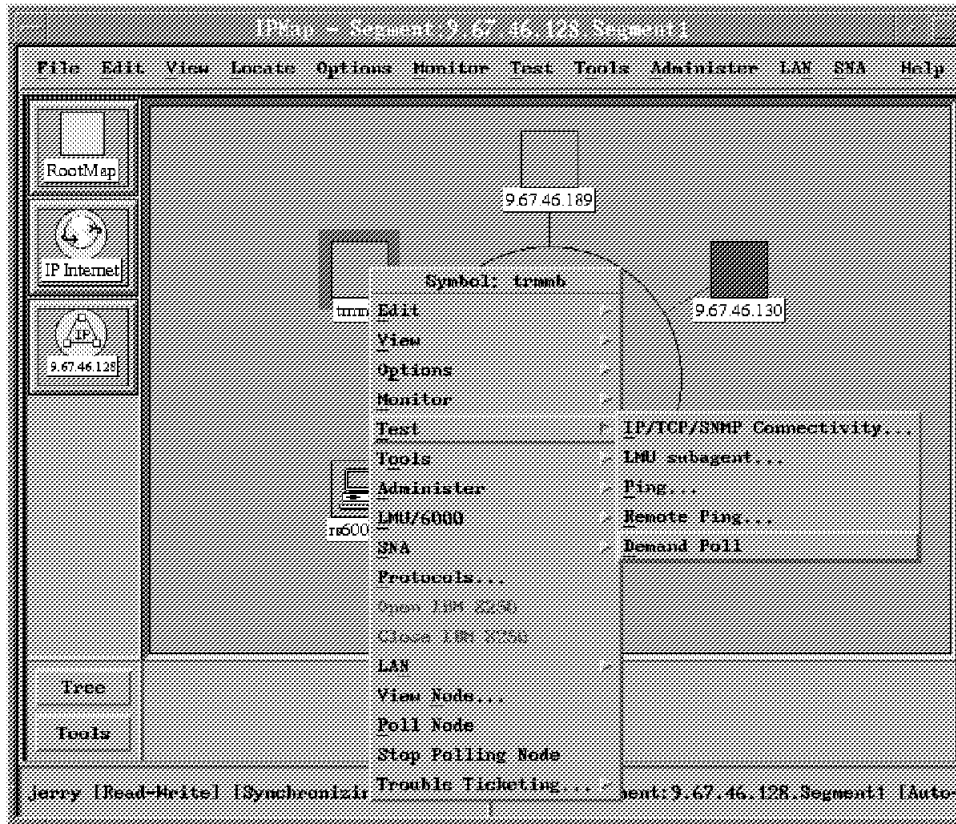


Figure 132. AIX NetView/6000 Demand Poll

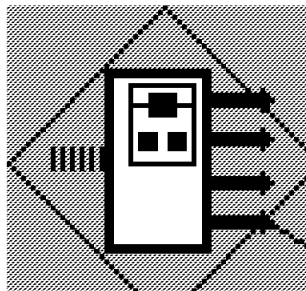


Figure 133. 8250 Hub Symbol

5.5 IHMP/6000 Startup

To start IBM Hub Management Program/6000 the following steps are required:

1. Ensure AIX NetView/6000 daemons are started.
2. Start IHMP/6000.

The IHMP/6000 application can be started through the AIX NetView/6000 graphical user interface, or through SMIT. AIX NetView/6000 does not need to be started to enable the IBM Hub Management Program/6000 application to operate; only the AIX NetView/6000 daemons need to be active. Once AIX NetView/6000 is started additional options are available on the Tools and

Administer pull-down menus. To start IHMP/6000 choose the *Tools...Start IHMP/6000* menu options, as shown in Figure 134 on page 145.

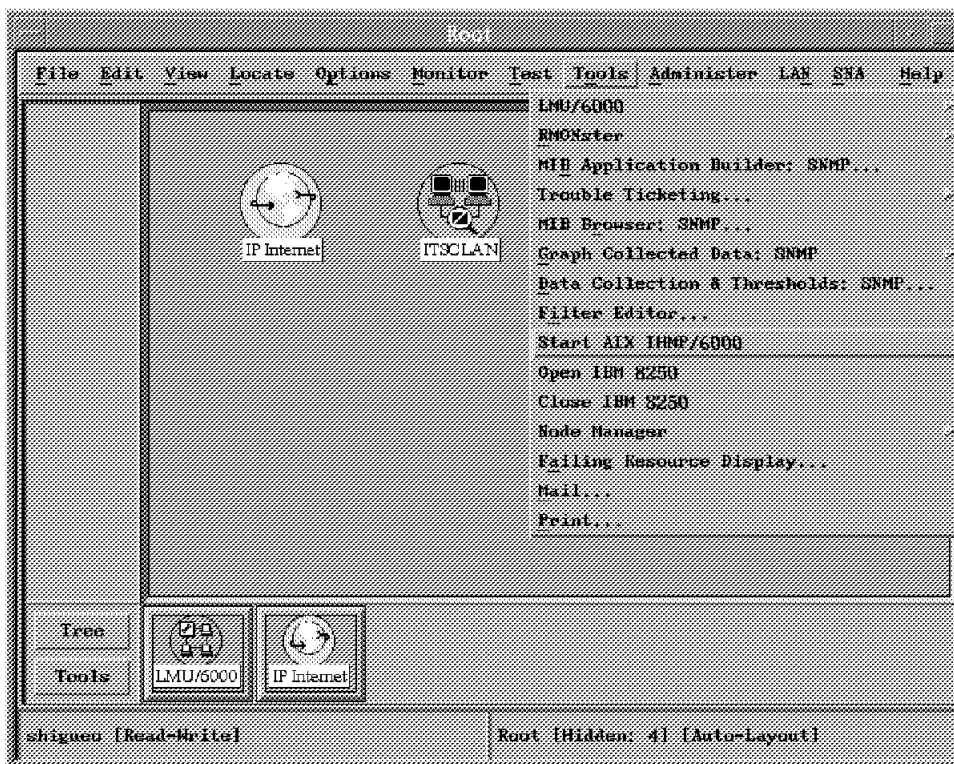


Figure 134. AIX NetView/6000 Additional Menu Options

The IHMP/6000 main screen, as shown in Figure 135 is displayed. This screen is initially empty since no hubs have been defined in the IBM Hub Management Program/6000 configuration file. The message shown at the bottom of the window indicates the file used, which is: `/usr/etc/hmp/data/hmp.cfg`.



Figure 135. IHMP/6000 Main Screen

To verify that the IHMP/6000 application has started correctly the diagnose option within the IHMP/6000 SMIT option displays the status of the IHMP/6000 daemons, as shown in Figure 136 on page 146.

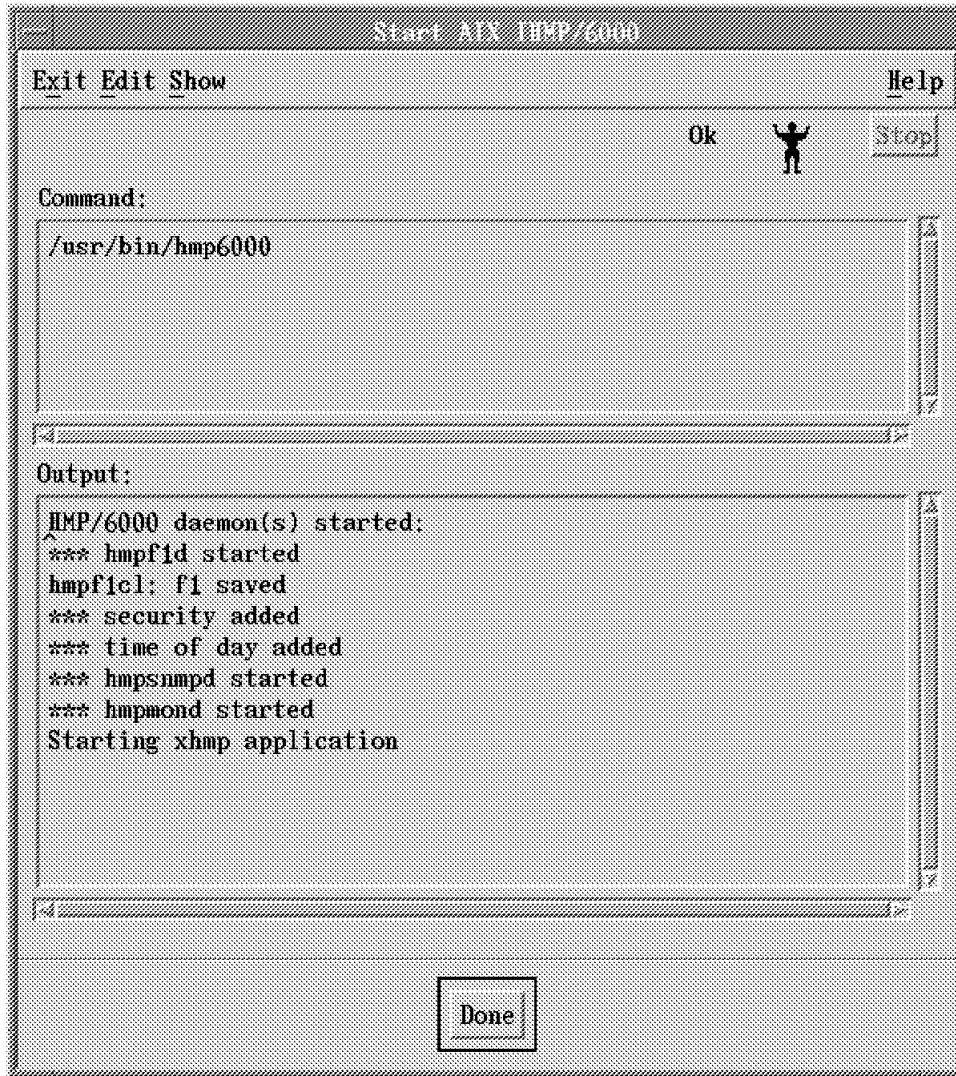


Figure 136. IHMP/6000 Daemons Status

To enter the 8250 Hubs into this main screen you need to retrieve the 8250 Hubs that AIX NetView/6000 has discovered within its IP network. To start this process, choose the **File...Agents** pull-down menu and the Agents Form window will be displayed, as shown in Figure 137 on page 147. From this screen the AIX NetView/6000 database will be interrogated to identify 8250 Hubs that have been discovered by AIX NetView/6000. From the *Agents from external database* area choose the **Get Agents** option. This will take some time while the IHMP/6000 application interrogates the AIX NetView/6000 database. The 8250 Hubs identified will be displayed. To Add the 8250 Hubs to the IHMP/6000 database:

1. Select the 8250 Hubs discovered from the external database.
2. Click on the **Add** option.

The screen will then have the IBM Intelligent 8250 Hubs displayed in the *Current Agents* area indicating that the 8250 Hubs have been added to the IHMP/6000 database (that is the hmp.cfg file), as shown in Figure 137 on page 147.

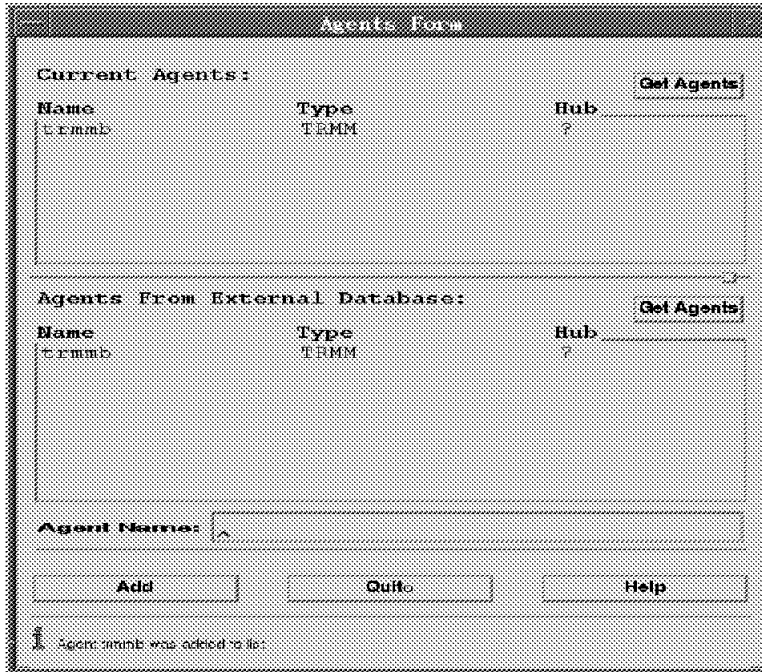


Figure 137. IHMP/6000 Agents Form Window - 8250 Hub Discovered

Select **Quit** to exit this window. You will return to the initial screen with a diagram of the hub, as shown in Figure 138.

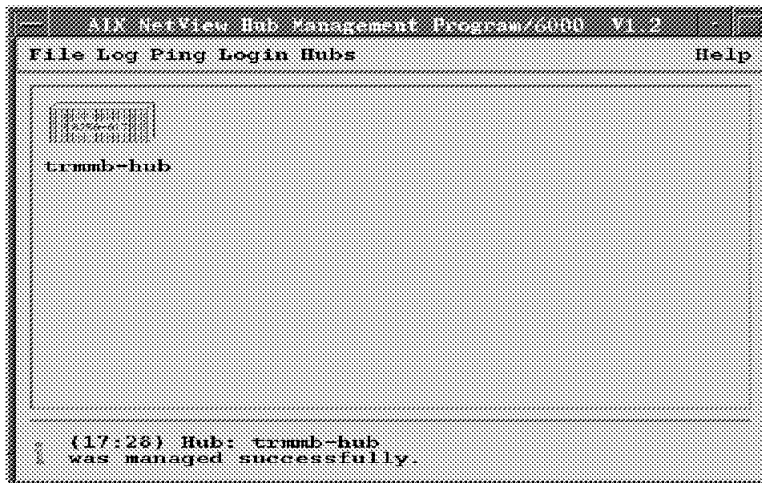


Figure 138. IHMP/6000 8250 Hub Identified

To start the Detailed Hub display:

1. Click on the hub in the hub main window.
2. Click on the hub icon on the AIX NetView/6000 topology map.

For integration purposes we chose the second option. This involved changing the icon symbol behavior on the AIX NetView/6000 topology map from *explode* (that is, display a child map) to *execute* (that is, execute a program). Therefore, when this symbol is selected, instead of going to a submap for IHMP/6000, it will instead perform an execute function which will have the application display the detailed hub display window, as shown in Figure 143 on page 150.

The steps involved are as follows:

1. Change the icon to *executable*.

This is done by selecting to modify the symbol, which is on the *Edit...Modify/Describe...Symbol* options on the pull-down menu, as shown in Figure 139. This menu is accessible by using the right mouse button on the 8250 Hub icon.

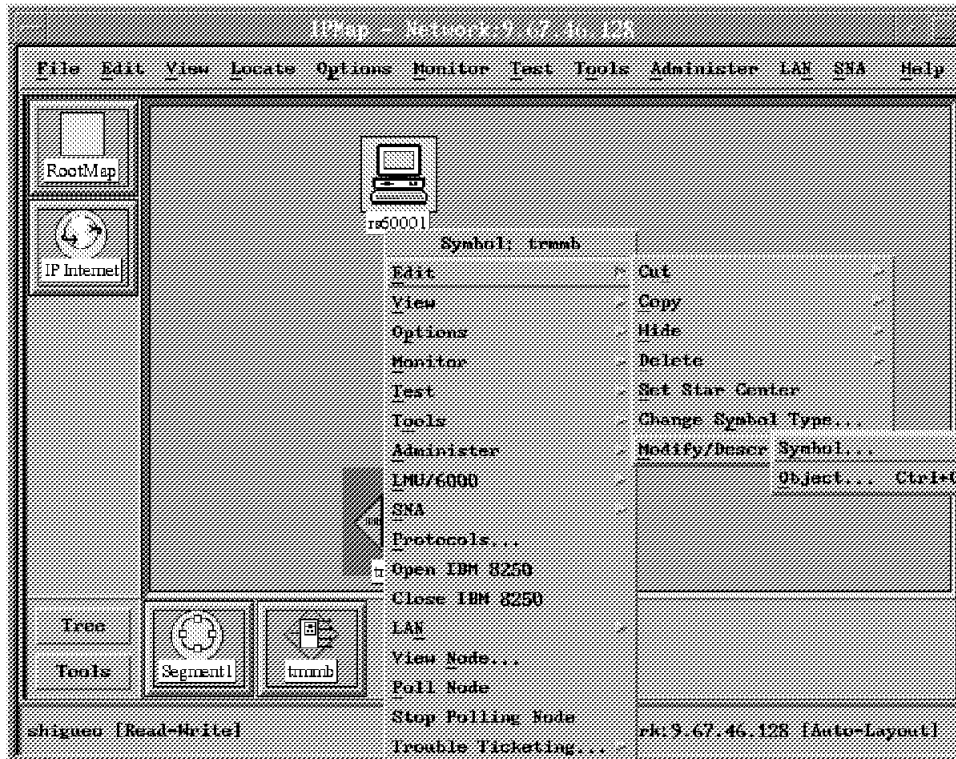


Figure 139. AIX NetView/6000 Selecting Modify Symbol Screen

From the symbol description screen choose the **execute** option for the *behavior* characteristic, as shown in Figure 140 on page 149.

2. Select the application to execute.

When you choose the execute attribute, additional options are set up for the application you want to execute. Choose the **AIX IHMP/6000 : nv6k to hmp open** application, as shown in Figure 140 on page 149.

3. Select the target that will execute the IHMP/6000 application.

The default is to not execute the IHMP/6000 application on this icon. Choose the **Target objects** button. The Target objects for the trmb screen are displayed, as shown in Figure 141 on page 149. Choose to **Add** trmb as the target.

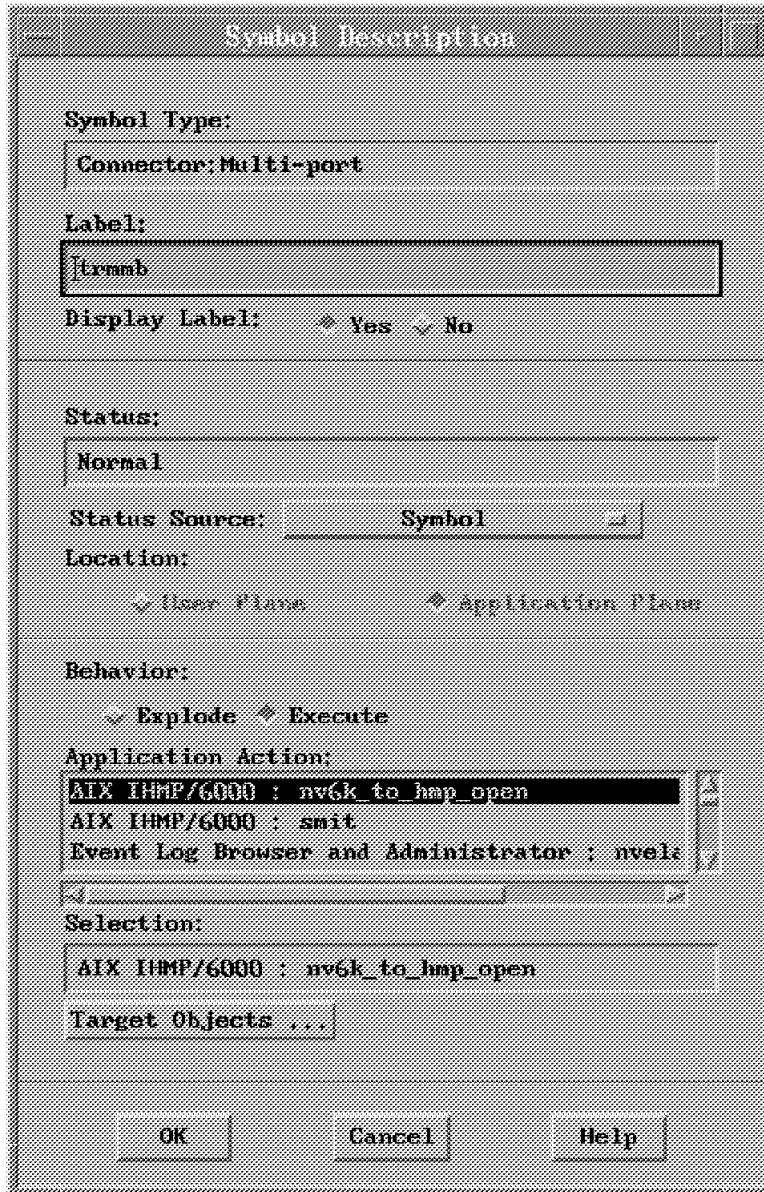


Figure 140. AIX NetView/6000 Changing Symbol to Executable

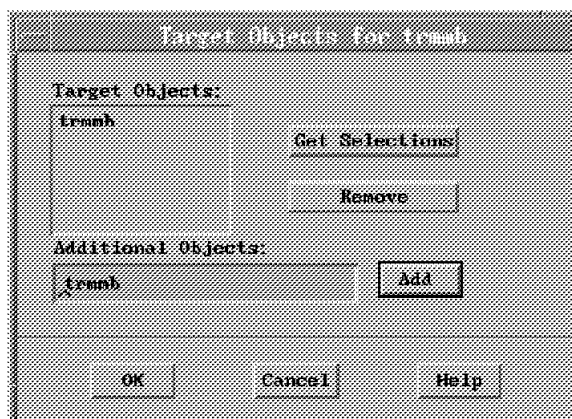


Figure 141. AIX NetView/6000 Defining Target for IHMP/6000 Application

Once this has been completed the icon on the AIX NetView/6000 topology map changes, as shown in Figure 142 on page 150, indicating that this symbol will now execute an application.

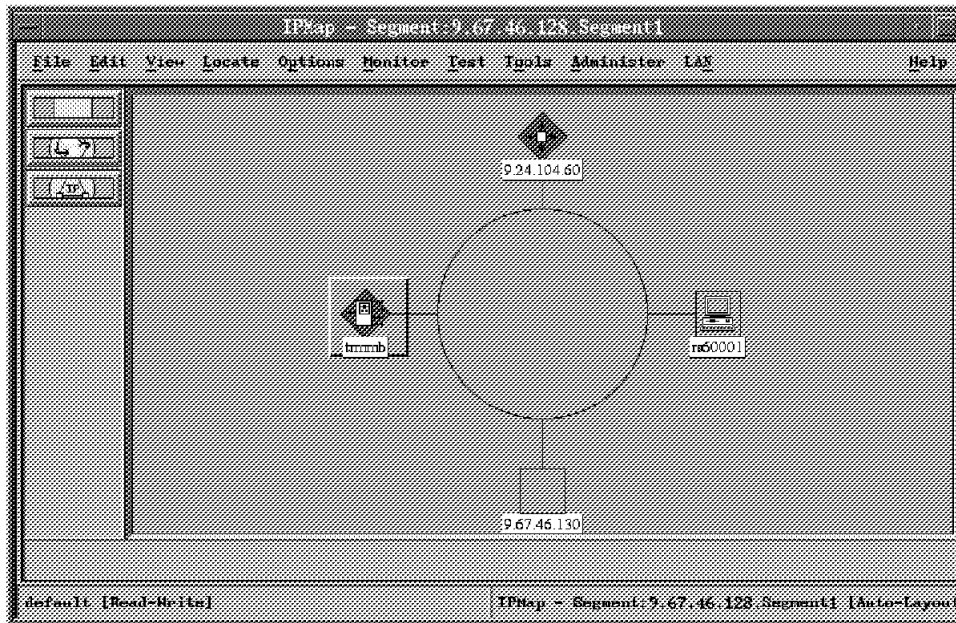


Figure 142. AIX NetView/6000 Hub Icon as Executable

To then start the IHMP/6000 application double click on the hub icon. The IHMP/6000 application is started as shown in Figure 143. From this screen all configurations can be performed.

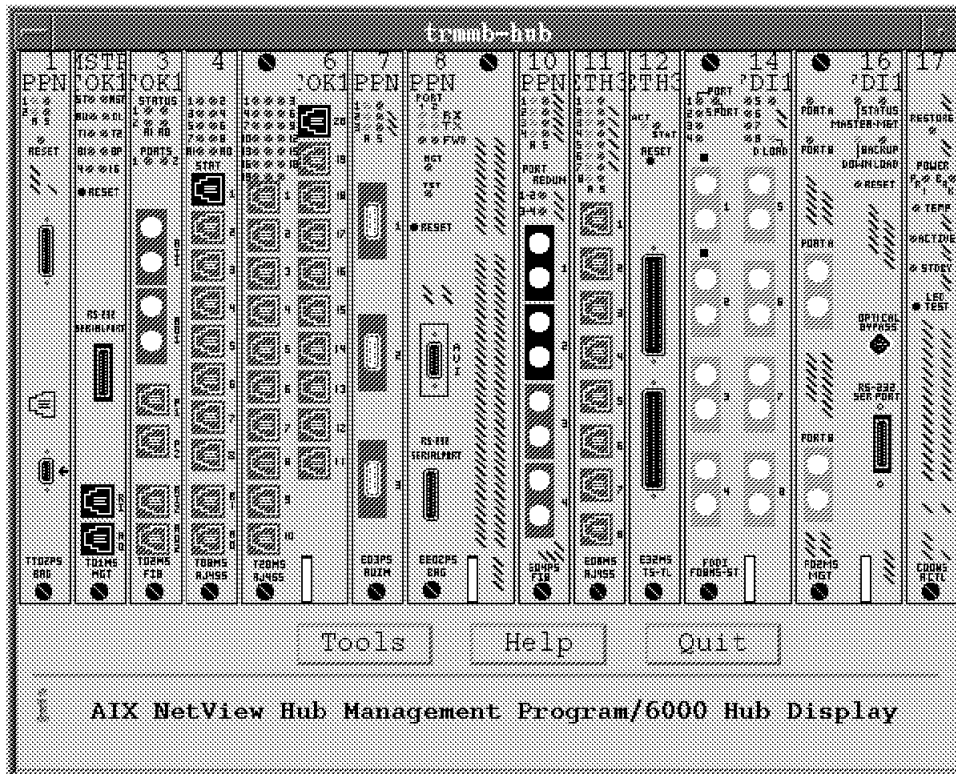


Figure 143. IHMP/6000 Detailed 8250 Hub Display

5.6 IBM Hub Management Program Family for the IBM 8260

To manage an IBM 8260 hub, a single DMM or EC-DMM will be able to provide the necessary information to IHMP/6000. There are some instances which might require multiple management modules, for example, an 8260 EC-DMM and Ethernet EMAC daughter cards for Ethernet LANs, and perhaps an 8250 EMM to support the 8250 10BaseT Security Module or an 8250 Token-Ring Management Module (TMM).

When multiple management modules are present in a single chassis, only one management module is identified as a master management module.

5.7 IHMP/6000 Version 2

IBM Intelligent Hub Manager for AIX Version 2 is the IBM strategic hub network management product on AIX. This is the follow-on product to IHMP/6000 V1. IHMP for AIX V2 provides significant enhancements over IHMP/6000 V1.

Examples of this are:

- Integration with other NetView/6000 LAN applications. Examples of this would be LNM for AIX, and RABM/6000.
- Integration of the hub topology with NetView/6000's topology database.
- An entry-level version of IHMP for AIX that will provide management capability for six hubs. All of the IHMP functions will be enabled for managing the six hubs.

From an end-user perspective, IHMP for AIX, RABM/6000 and LNM for AIX will appear as a single application. You navigate between views provided by each product by simple point-and-click operation as if you were using a single product. All the views and panels of these products have a common format. This makes the IBM LAN network management offering much more powerful and attractive, since the complexity of using the product functions is hidden from the user.

Merging all of the topology databases permits protocol switching to be used, which will automatically highlight a resource on all the topology submaps where the resource resides (IP, hubs, LNM and later on ATM topologies). This is a very efficient way to quickly locate and identify devices in the network.

The integration with LNM for AIX and the integration of the hub topology with NetView/6000 topology makes network problem identification and resolution much easier and quicker than with Version 1.

The full integration with NetView/6000 also greatly improves the usability of the product, since Hub Manager for AIX, LNM for AIX and NetView/6000 use the same common format for graphical interface panels. New 8250 or 8260 customers who obtain IHMP for AIX V2 can take full advantage of all the management features through an easy-to-use and efficient graphical interface.

IHMP for AIX V2 offers a new easy-to-use, context-sensitive, MOTIF-based user interface with three main views: Hub Topology View, Hub Level View and Module Level View. Resources icons are also easy to identify for system status at a glance and real-time problem detection.

Migration to NetView for AIX V3 will require upgrading to IHMP for AIX V2, since the earlier versions will not run on NetView for AIX V3.

Chapter 6. Router and Bridge Manager/6000

Router and Bridge Manager/6000 is a network management application designed to run on the AIX NetView/6000 platform. This application manages both networks of IBM 6611s and individual 6611s using an integrated graphical end user interface by providing the ability to monitor each 6611's aggregate health of its protocols, network interfaces and system functions in a single view.

The Router and Bridge Manager/6000 application contains the following functions:

- Polls a list of selected nodes, analyzes the data received and determines the operational status of those nodes. When status changes in a node occur, Router and Bridge Manager/6000 detects these status changes using thresholds, changes in the operational status, or traps generated by nodes.
- The polling list monitor allows you to view only those nodes that you have selected to be polled, rather than dealing with the full AIX NetView/6000 topology.
- The node monitor allows you to view the status of all protocols and interfaces within a selected node. The node monitor allows you to quickly descend into the problem area for each resource within the node.
- It provides statistics for all 6611s in a network. On a single screen, each 6611 icon in the network displays the aggregate "health" (system, interface adapters and protocols), not just the IP connectivity status.
- Manages all models of the IBM 6611 Network Processor for any Multiprotocol Network Program (MPNP) release level.
- Manages the IBM Data Link Switching (DLSw) and Advanced Peer-to-Peer Networking (APPN) protocols.
- Supports submission of 6611 System Manager fast path commands.
- Manages bridge ports for both source-route bridging (token-ring) and transparent bridging (Ethernet).
- Provides historical performance data, independent of status windows being open or closed, not just current snapshot data.
- Allows dynamic customization of polling rates, data to be collected, and thresholds.

6.1 RABM/6000 Installation

The installation of the RABM/6000 environment involves:

1. Installing RABM/6000 on the RISC System/6000.

To install the RABM/6000 code use SMIT and the values defined in 1.5.3, "RISC System/6000 Software Installation Procedures" on page 40. The list shown when you prompt for the *SOFTWARE to install* field for RABM/6000 is shown in Figure 144 on page 154. Select the top item *1.1.0.0 RABM/6000 ALL*.

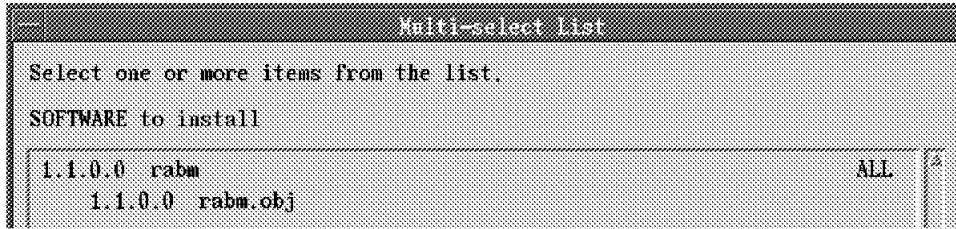


Figure 144. RABM/6000 Install List

The installation requires no further interaction.

6.2 Router and Bridge Manager/6000 Configuration

With the installation of RABM/6000, menu items are added to the AIX NetView/6000 pull-down main menu and to the context menus associated with each router or bridge node. All the RABM/6000 menus are grouped under the *Node Manager* option of the AIX NetView/6000 Tools pull-down menu.

The RABM/6000 application is ready to use without any further configuration processes. The defaults provided are sufficient. However, we configured the option to enable all IBM 6611 Routers discovered in AIX NetView/6000 to be automatically included into the list of nodes to be managed by RABM/6000. Choose **Tools...Node Manager...Setup...Global Configuration** as shown in Figure 145.

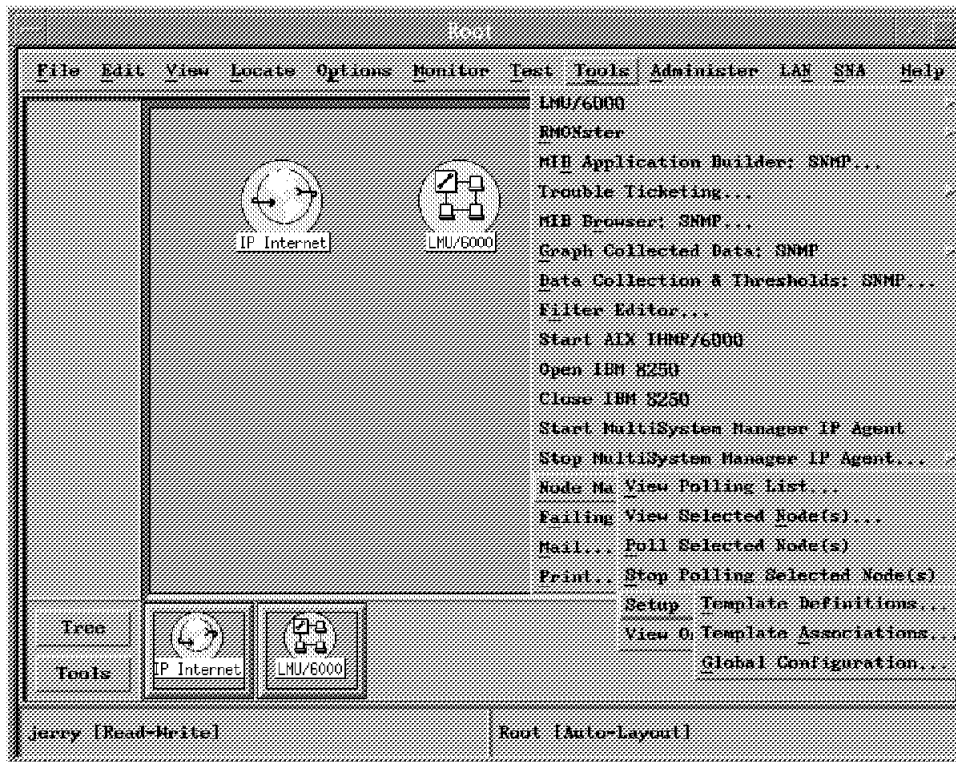


Figure 145. RABM/6000 Pull-Down Menu Options

You should then select the Global Definitions screen, as shown in Figure 146 on page 155, in this screen:

- Choose the **Enable** option to have the RABM/6000 automatically add new nodes to the polling list as AIX NetView/6000 discovers them.
- Select **IBM 6611** in the Complete Device List area. This list displays all nodes that will be dynamically added to the RABM/6000 polling list. Currently only the IBM 6611 Router is defined.
- Choose **Router** from the Default Template to indicate that the router template will be used with any IBM 6611 Router as they are dynamically added to the RABM/6000 polling list.
- Click on **Add** to update the global definitions.
- Choose **OK** to close the Global Definitions screen.

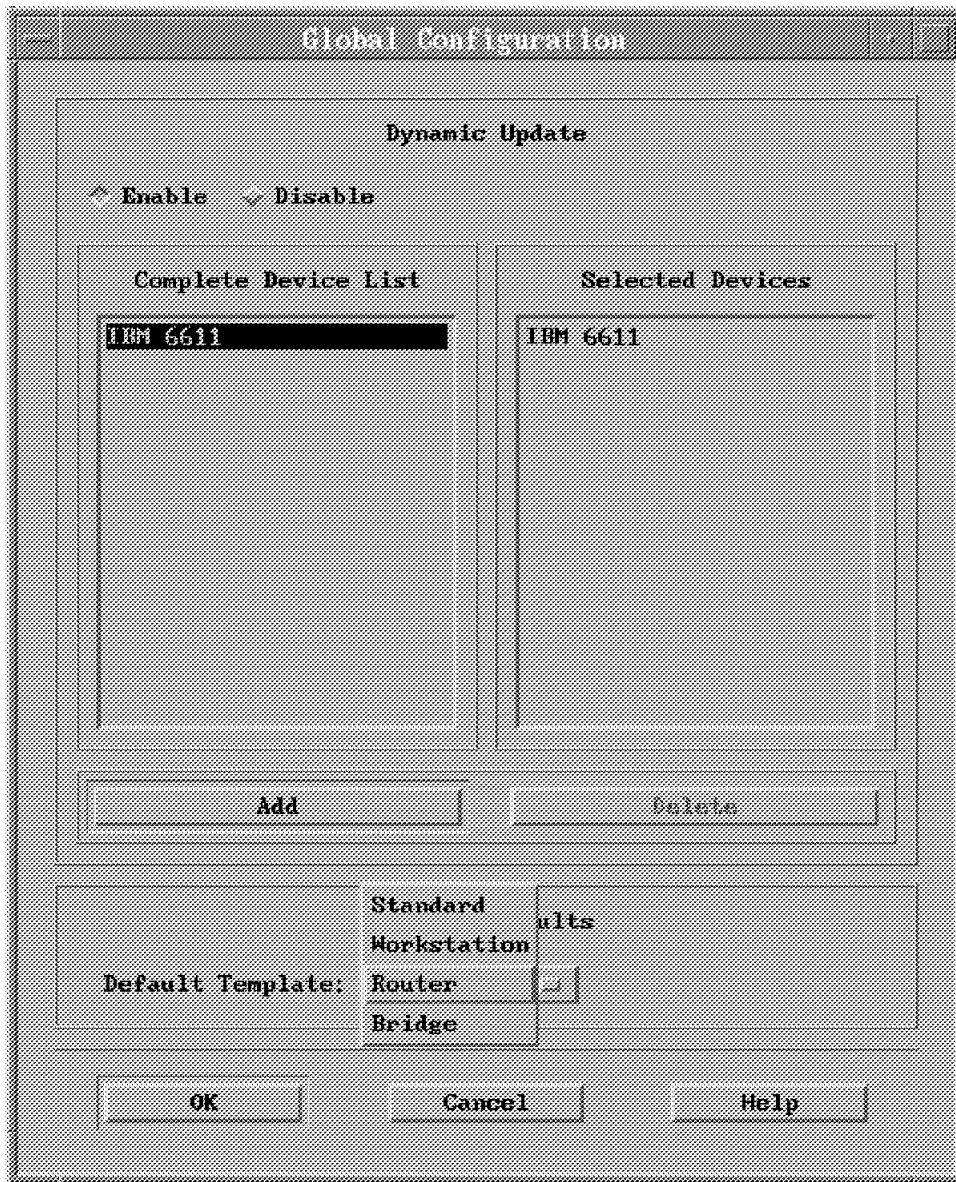


Figure 146. RABM/6000 Global Definitions

6.3 Starting Router and Bridge Manager/6000

To start the RABM/6000 application, select **Tools...Node Manager...View Polling List** from the AIX NetView/6000 main menu bar. The Polling list window is then displayed, as shown in Figure 147 on page 157.

The daemons required for RABM/6000 are automatically started when AIX NetView/6000 is started. The daemons are:

- **rv** - this is the main daemon started when AIX NetView/6000 is started. If this daemon is not started when AIX NetView/6000 starts, the command `ovstart rv` can be used. This daemon will then spawn the following daemons:
- **datacoll**
- **mibsvc**
- **trapsvc**
- **eventsvc**

The Polling List window is the main window for the RABM/6000 application. This window is a summary of all nodes being polled and their overall states. Nodes will be added to this list as the IBM 6611 Routers are discovered by AIX NetView/6000. In our environment there are two IBM 6611 Routers that were discovered:

1. 6611ral
2. 9.24.1.1

As RABM/6000 detects changes in the status of a node on the polling list, the node's new status will be represented by a change in the node color on the polling list window. This color scheme is also used within the Node Monitor window to reflect the status of each component within the node. The color of the node icon reflects the polling status of the nodes:

- Red** Represents a node experiencing critical conditions.
- Yellow** Represents a node experiencing warning (marginal) conditions.
- Green** Represents a node operating in a normal state.
- Blue** Represents an unknown node (a node not responding to polled requests). Any node not supporting the MIB-II definitions would be unknown.
- Brown** Represents an unmanaged node (a node no longer selected to be polled).

You can choose to display only nodes in a specific state by enabling the appropriate toggle buttons in the criteria area. In our Polling List window the toggle buttons for all states are enabled. The two routers displayed in our list are:

- 6611ral** This is in a normal state (green).
- 9.24.1.1** This is in a marginal state (yellow).

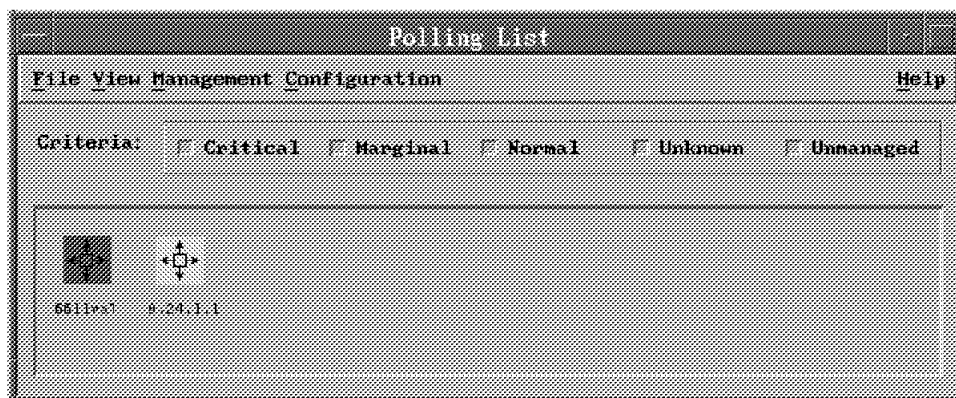


Figure 147. RABM/6000 Polling List

Detailed information is possible through the Node Monitor window. This is accessed by double clicking on one of the nodes displayed in the Polling List window, as shown in Figure 148 on page 159.

The Node Monitor window provides you with a detailed view of each node you are monitoring. The Node Monitor window displays information in three sections:

- The top section is used to reflect information about the system, with an icon graphically representing whether the node is a router, bridge/router or bridge.
- The middle section contains information about the interfaces. An icon and a label are displayed indicating the interface and its speed, such as token-ring at 4Mbps, Ethernet at 10Mbps and serial interface at 1.544Mbps.
- The bottom section contains information concerning protocols; an icon and a label are displayed for each protocol supported: IP, DLSw, APPN, IPX, XNS, AppleTalk, DECnet, Banyan VINES, SRB and TB.

Most of the information contained in these sections are formatted in a "slice". Each "slice" reflects important information about the node. There is one slice representing the overall state of the node in the system section and one slice representing each interface and protocol in their respective sections. Each slice contains:

- An icon which represents the status of the slice through the color schemes described earlier.
- For error and performance information, there are two buttons for each label:
 1. Left push buttons: these start the logging of information based on the polled interval of the node. The information is placed into the file based on the name of the node. In our environment the file was `/usr/OV/log/DATA_6611ra1.log`. You must enable logging on the Node Monitor window to use the Router and Bridge Manager/6000 graphing facility.
 2. Right push buttons: these display more detailed information of the error and performance counters. When these push buttons are pressed, the user will be presented with an analysis window for errors or performance, respectively. The color of the push button indicates the status of the errors and performance for the system, interface or protocol.

- Throughput and utilization meter: the current throughput value is evaluated against the marginal and critical thresholds and the status is reflected on the meter. These marginal and critical thresholds are defined as a percentage of the base value, which is shown below the meter. The dark vertical lines on the meter indicate the marginal and critical thresholds. These can be adjusted by holding down the CTRL key and dragging the threshold using the left mouse button. By double-clicking on the throughput meter, you can view the last five values that were retrieved from the node for that slice, as is done in our screen for the *tk1-16Mbps* interface.

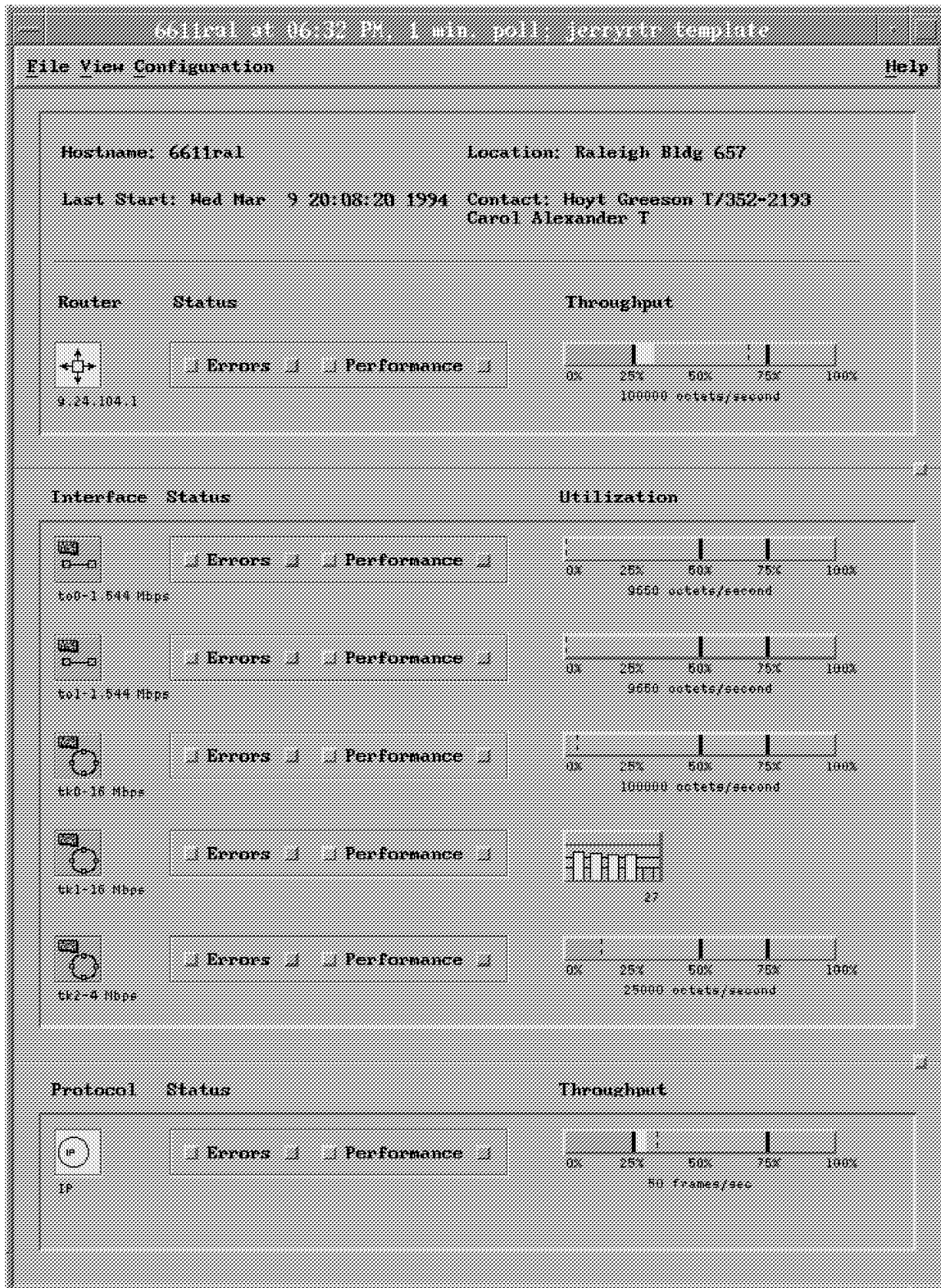


Figure 148. RABM/6000 Node Monitor

Context Menus: You can access context menus, as shown in Figure 149 on page 160, from the system slice and from each interface and protocol slice by pressing the right mouse button while the cursor is on a system, interface or

protocol icon. The values displayed in the windows are retrieved using SNMP requests when the menu item is selected.

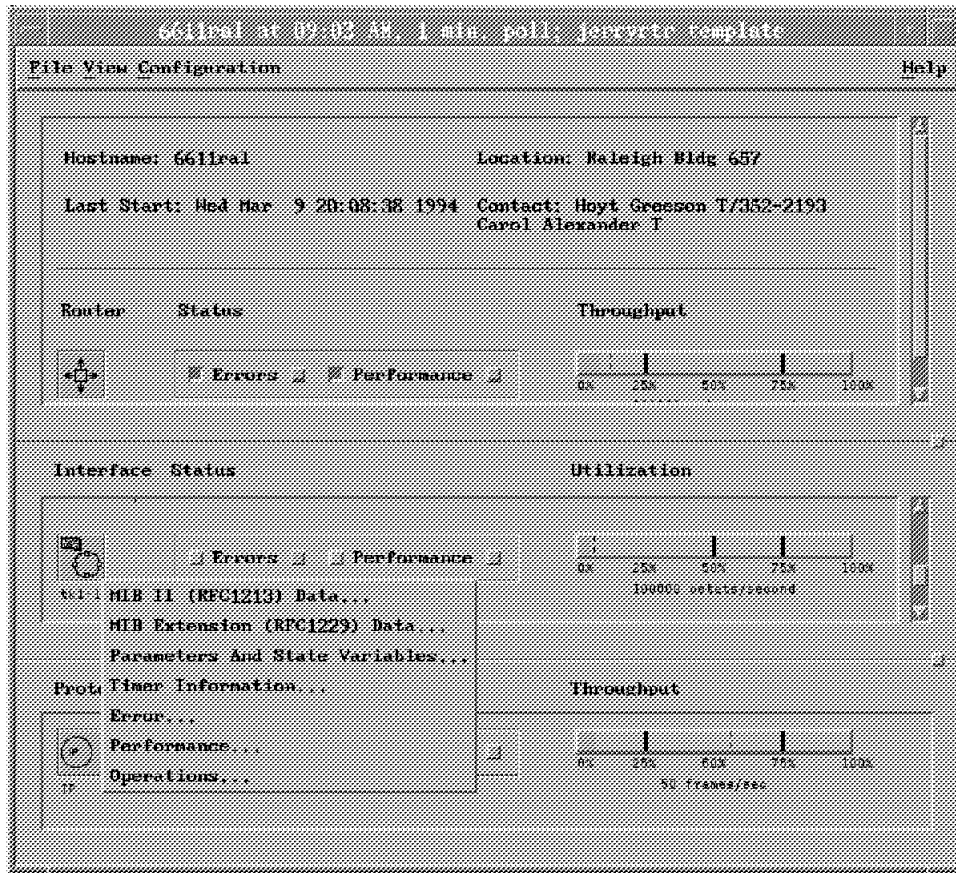


Figure 149. RABM/6000 Context Menu

Analysis Windows: From the Node Monitor window, select the push buttons to the right of either the Error or Performance labels to display the detailed analysis windows, as shown in Figure 150 and Figure 151 on page 161. The detailed analysis windows that are displayed show you the values that the Router and Bridge Manager/6000 application uses to calculate the status for the Error and Performance labels.

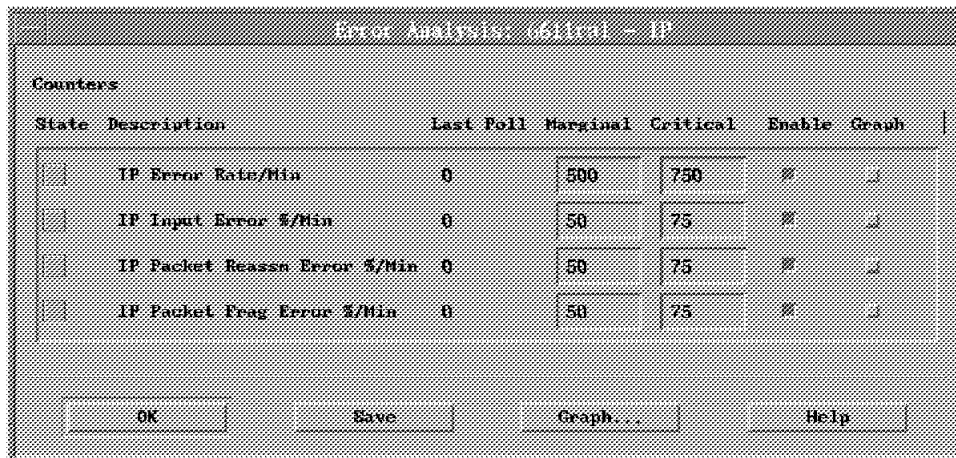


Figure 150. RABM/6000 Error Analysis

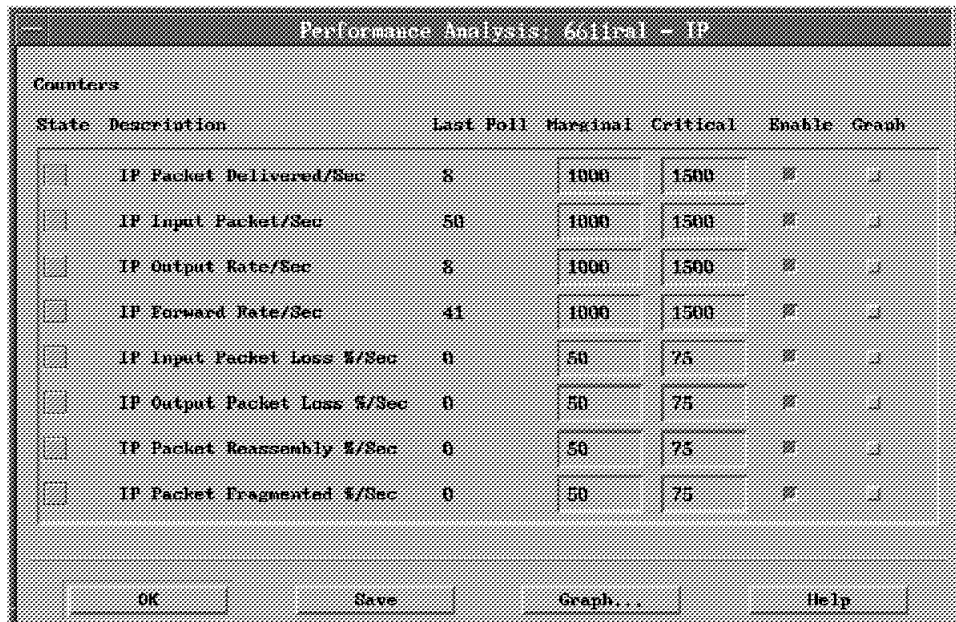


Figure 151. RABM/6000 Protocol Analysis

The information displayed for the counters monitored are:

- State of the counter: the same color scheme is used to indicate whether the counter is in a normal, marginal or critical state.
- Name of the counter: the information being monitored.
- Each counter's last polled value: this is the value that has been retrieved for the node at the last poll.
- Marginal and critical thresholds: these are the current thresholds being used for the counter. You can modify these thresholds by clicking on the respective box and typing the desired value.
- Enable toggle button: if you do not want to include any of the listed counters in the status propagation, you may disable the counter by turning the Enable toggle off. The status of the counter will be Unknown (blue) when the counter is disabled.
- Graph toggle button: enable the Graph toggle button to indicate which counters you want to graph. Select the Graph push button to display a graph of the counters you have selected.

Graphing: The Router and Bridge Manager/6000 graphing utility allows you to monitor and analyze data from the error or performance logging session, as shown in Figure 152 on page 162. The graphing utility uses the log file created by the logging function. The logging function is started by enabling the toggle button to the left of the error or performance counters in the Node Monitor window. In the analysis window displayed in Figure 151, do the following:

- **Enable** the toggle buttons for the first four counters.
- Choose the **Graph** push button to graph the data.

To zoom in for a close-up view of the graph, use the left mouse button to drag a box around the portion that you want to magnify. We are currently viewing only 0.82% of the total graph as is indicated in the top left-hand corner of the graph by the *View* value. When you are viewing a portion of the graph the arrows

enable you to move around and view different parts of the graph, while maintaining the view percentage. The *Full Picture* push button returns the view of the graph to 100%.

Use the mouse to move the vertical index line on the graph and pinpoint a specific date and time. The date and time of when that variable data was collected is indicated at the top of the line. As you move your mouse across the graph, the values displayed beside the variable name changes to reflect the value of the variable.

In our graph the index line is showing information for May 4/94 at time 10:01:15 and the values for the variables at that time were:

IP Packets Delivered/Sec	4
IP Input Packet/Sec	9
IP Output Rate/Sec	5
IP Forward Rate/sec	4

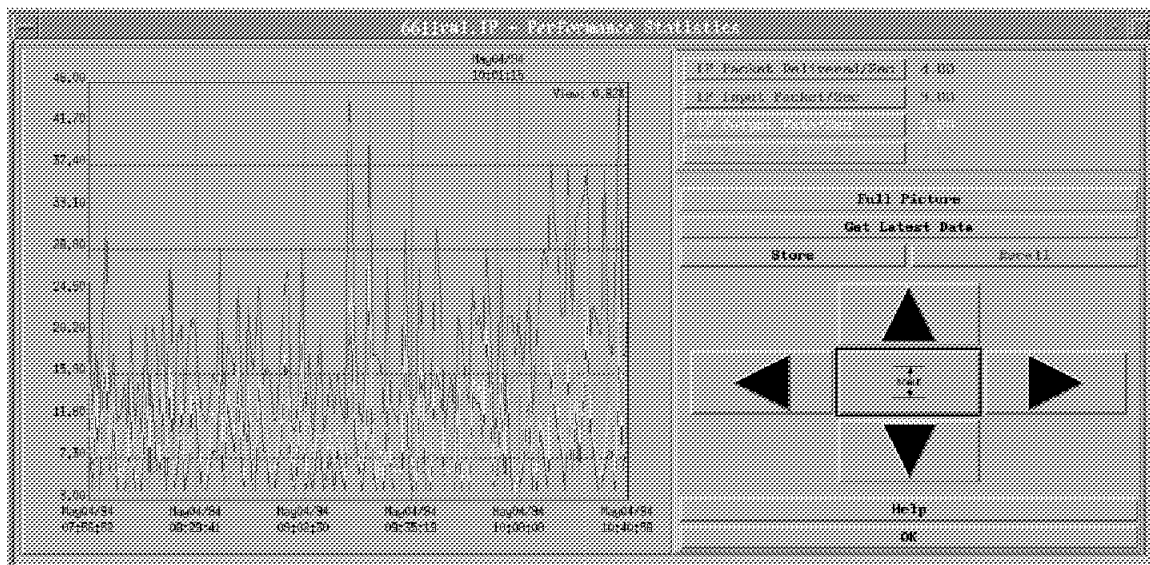


Figure 152. RABM/6000 Graph

Counter Details: At the top right-hand side of the Graphing Utility window, there is a push button for each selected counter labeled with the name of the counter. Click on the counter name push button to display detailed information about that counter, as shown in Figure 153 on page 163.



Figure 153. RABM/6000 Detail Graph Information

Multiple User Considerations: The first person to invoke the Router and Bridge Manager/6000 on a management station obtains read/write authority. The Router and Bridge Manager/6000 application is automatically invoked by starting the AIX NetView/6000 application. Subsequent users have read-only authority.

If the user with read/write authority shuts down AIX NetView/6000, the next user that invokes the Router and Bridge Manager/6000 application inherits read/write authority automatically. A screen will be displayed indicating that you have inherited read/write authority as shown in Figure 154.



Figure 154. RABM/6000 Inheriting Read/Write Authority

Chapter 7. Trouble Ticket/6000

This chapter gives a brief overview of the installation, configuration and operation of AIX Trouble Ticket/6000. It is not intended to cover all the issues related to these matters. Its purpose is to explain how to build a sample trouble ticket environment.

For more detailed information, refer to the documents: *AIX Trouble Ticket/6000 At a Glance Version 1.2 and Version 2.0*, *AIX Trouble Ticket/6000 User's Guide Version 1.2 and Version 2.0* and *Network Problem Management Examples Involving AIX Trouble Ticket/6000*.

7.1 Capabilities

AIX Trouble Ticket/6000 is a software application that works in conjunction with AIX NetView/6000 to provide a comprehensive problem management tool. It includes incident reporting and trouble ticketing with automatic notification and escalation.

An incident report is any abnormal event that has been detected in a network. It can be generated automatically from a trap received by AIX NetView/6000 or can be created manually by a help desk or a network operator using one of the three interfaces supported: windowed dialog boxes, command line and electronic mail.

A trouble ticket gathers one or more incident reports related to the same problem into a central repository, keeping track of the problem from its identification to its resolution. Upon closure it is kept in a history file to be used for performance analysis or for further research. It can also be re-opened if necessary. A trouble ticket can be managed by the windowed dialog boxes provided by AIX Trouble Ticket/6000, using electronic mail or a command line interface.

Once the trouble ticket is created, the AIX Trouble Ticket/6000 program provides methods to notify the appropriate people to handle the problem. It also keeps a log of the actions taken to help solve the problem.

In addition to problem management, the AIX Trouble Ticket/6000 program also addresses inventory management. This discipline includes maintaining inventory lists of network resources, contacts, vendors, locations, and other network-related entities.

7.1.1 Prerequisites

The minimum hardware components required are:

- RISC System/6000 POWERstation or POWERserver
- 32 megabytes of memory (48MB recommended)
- 65 megabytes of free disk space
- Color display supporting X Window System
- IBM or compatible mouse
- Installation media (disk/tape)

The following software components must be installed, configured and operational:

- AIX Version 3 Release 2 or later
- AIX NetView/6000 Version 1 or later
- AIXwindows Environment/6000 Version 1 Release 2
- TCP/IP

Optionally, the INGRES RDBMS Release 6.4/01 may be used to maintain the AIX Trouble Ticket/6000 database.

7.1.2 Functionality

AIX Trouble Ticket/6000 is designed as a client/server application. One possible scenario is having one machine as the server, maintaining the database and running the daemons, and many clients accessing the services of this server as front-end stations.

The front-end stations will run the application's user interface using a set of dialog boxes that are consistent with the OSF/Motif windowing standard.

In general, these dialog boxes will be either a list of records or a detailed window from which you can access all the data related to a specific record. In the AIX Trouble Ticket/6000 utilization, the following rules apply:

- In a list-type dialog box, if you double-click with the left button on a list item, it will open the detailed dialog box of that record.
- In a detailed dialog box, if you double-click with the left button on a field marked with the ++ sign, it will open an intelligent helper list, containing the available options that can be used in that field. These fields have cross-references to other tables.
- In an intelligent helper list, a double-click with the left button chooses that item while a single-click with the middle button opens the detailed dialog box of that record.
- Fields with a dashed underscore line, highlighted by a light blue color are required fields.
- Fields that appear in the same color as the dialog box's background are view-only fields.

Before you start working with the incident reports and trouble tickets, you should perform a number of steps in order to tailor AIX Trouble Ticket/6000 to your environment. These steps include:

- Populating the inventory tables

During the process of generating a trouble ticket, you might want to know the configuration of a failed device, which vendor should correct the failure and how to notify the vendor. This is only possible if you have all of the following information stored in the inventory tables:

- Network resources
- Contacts
- Locations
- Vendors
- Organizations
- Sites
- Models
- Resource Classes

- Tailoring the internal codes

AIX Trouble Ticket/6000 has internal codes which are used as reference data. They include inventory codes (such as resource families and manufacturer codes) and trouble ticket codes (such as ticket priorities and trouble codes).

- Customizing the automation process

This step includes the definition of:

- Which traps will open incident reports
- Which notification methods will be used
- What will be the notification messages
- What escalation rules will apply to a trouble ticket
- What actions should be performed against an opened trouble ticket
- What will be the system defaults

We will not cover all of these steps as they were not essential in our scenarios, but it is highly recommended that you take the time to tailor your environment.

7.2 AIX Trouble Ticket/6000 Installation

We did not use the INGRES database in our environment but, if you are going to use the INGRES database support it has to be installed and configured before AIX Trouble Ticket/6000.

The installation steps are:

- Code installation
- Server configuration
- Installation of additional clients (if required)

Notice that a machine that is configured as a server is also a client.

7.2.1 AIX Trouble Ticket/6000 Code Installation and Configuration

AIX Trouble Ticket/6000 uses the standard SMIT installation process to install the product. During this process, you will receive the following message:

You must complete the installation for AIX Trouble Ticket/6000 using SMIT before running it.

Select "Communications Applications and Services..TT/6000..Configure.. Set Options for TT/6000"

The SMIT panel referenced in this message is shown in Figure 155.

Remember that this is a mandatory step.

Option	Value	Buttons
* Server/Client	Server	List, Up, Down
* Server name (if client)		
* Collect NetView 6000 events	Yes	List, Up, Down
* Database directory	/usr/lpp/tt6000/site	
* TT/6000 log directory	/usr/lpp/tt6000/log	
* Email user name	trouble	
* Mail spool directory	/usr/spool/mail	
* Trouble Ticket view	NetMgr 1	List, Up, Down
* Semaphore / Shared Memory base	0x4E550000	X
* Rebuild database	Yes	List, Up, Down

Figure 155. AIX Trouble Ticket/6000 Configuration Panel

The options that required more attention were:

- Server/Client
We have configured our station as a server.
- Collect NetView/6000 events

These options determine which events will automatically generate events from AIX NetView/6000. If the option is set to YES, the AIX Trouble Ticket/6000 menus are registered with AIX NetView/6000 in three places:

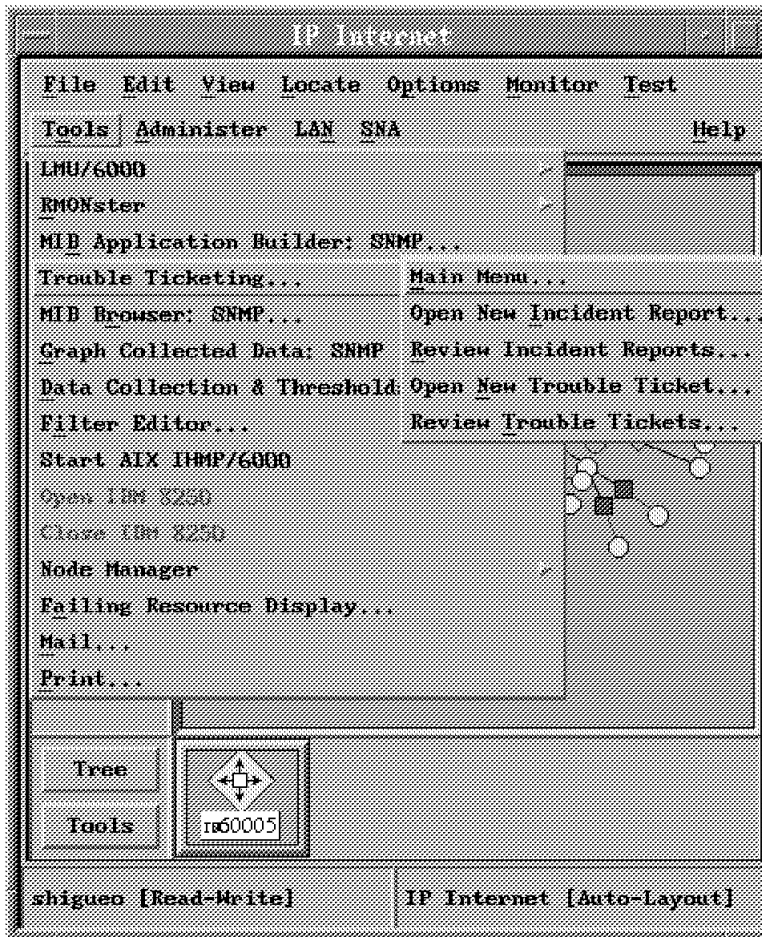


Figure 156. AIX Trouble Ticket/6000 Access from the AIX NetView/6000 Main Menu

1. The main menu, as shown in Figure 156.
2. The context specific menu brought up on the topology display when you click the right mouse button on a node. In this case, you will not be able to access the AIX Trouble Ticket/6000 main application.
3. The tools palette, as shown in Figure 157 on page 170. Notice that you will not be able to access the AIX Trouble Ticket/6000 main application, from the tools palette.

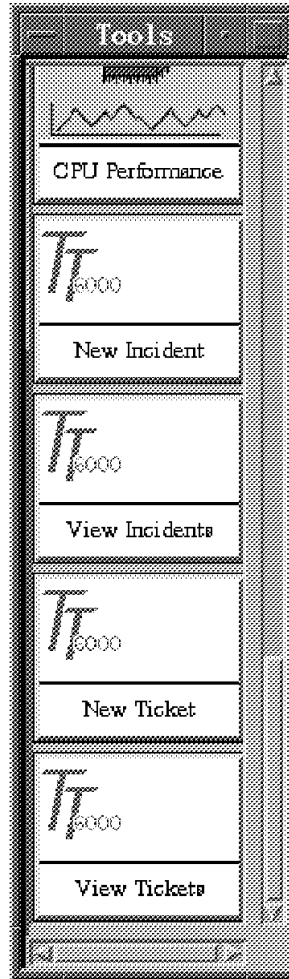


Figure 157. Tool Palette Showing AIX Trouble Ticket/6000 Options

- E-mail user name

If you are going to use AIX Trouble Ticket/6000 along with E-mail, create an AIX user ID to process this mail and fill in this field with this user ID. If you leave this field blank the mail_eater_nxd daemon will not be configured and will not run when you start the AIX Trouble Ticket/6000 daemons.

- Rebuild database

Specify YES if you are reinitializing the database or configuring the server for the first time. If you want to keep the information stored in the database, select NO.

The output of the configuration process is shown in Figure 158 on page 171.

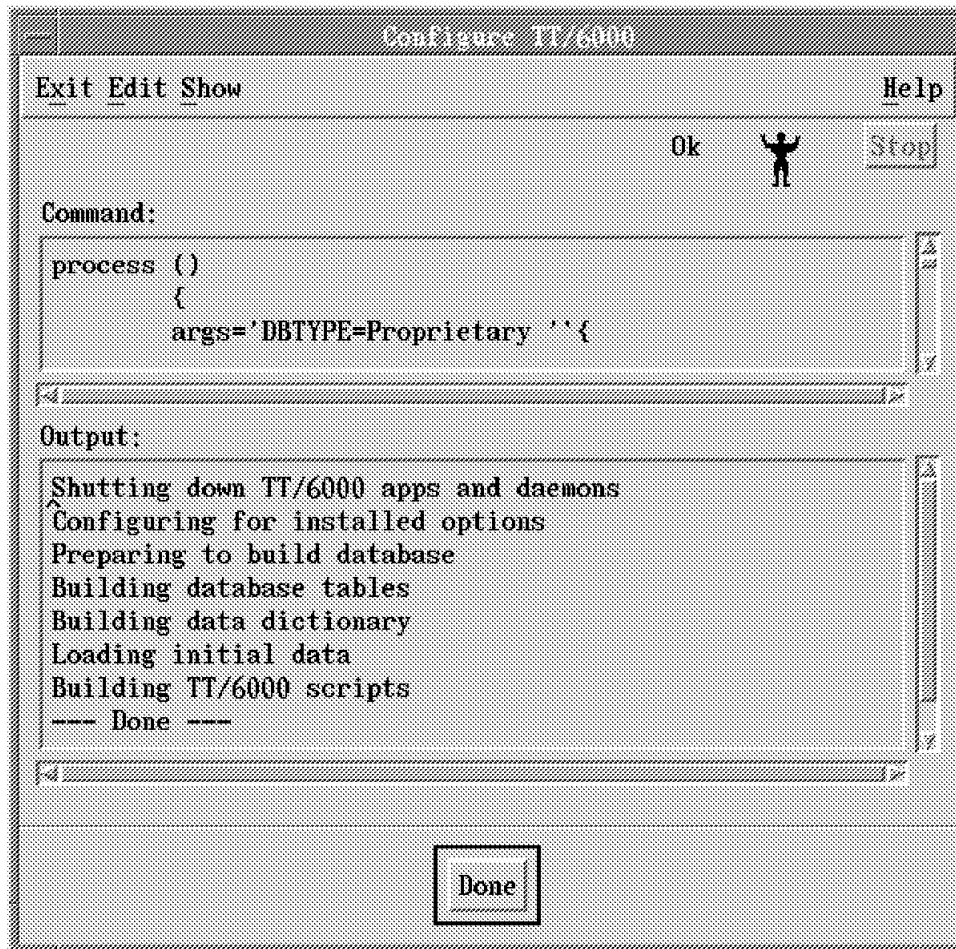


Figure 158. AIX Trouble Ticket/6000 Configuration Output

During this configuration process, one of the steps performed is to register the two TCP/IP sockets (slump and slump_server) used by AIX Trouble Ticket/6000. These sockets are assigned automatically in the /etc/services file, but if you receive a message saying that they were not, do the following:

- Edit the /etc/services file. If you are using NIS, this file resides on the NIS master machine; otherwise, it is on the AIX Trouble Ticket/6000 server.
- Insert these two lines:

```
slump          2100/tcp
slump_server   2101/tcp
```

Make sure that no other entry is using this pair of addresses. If so, you can use another pair of addresses between 2000 and 4999.

Note

All the clients must have the same sockets defined as the server. If you specify different addresses you will receive the following message:

```
TT/6000 daemons are not running. Run nx_init
on the server to start them.
```

- Save the changes and exit.

- If you are using NIS, you must run the following commands as the root user on the NIS server in order to force a reread of the /etc/services file:

```
cd /etc/yp  
make
```

7.2.2 Installing Additional AIX Trouble Ticket/6000 Clients

If you are installing additional clients to access the server, there are two different ways to accomplish this:

1. Install the code and configure it as a client on each additional machine requiring access to the server. This method again uses the SMIT process to install the code as it was done in the server installation. Then the configuration process is different in that you will configure this machine as a client. Using this approach, the AIX Trouble Ticket/6000 software is registered in the vital product database and therefore you will have strict software control of it. This means that you will be able to remove and update the software using the normal AIX procedures.
2. Distribute the client code from the server, by selecting **Communications Applications and Services...TT/6000...Configure...Install TT/6000 client**, as shown in figure Figure 159 on page 173. By using this approach the software is installed using a file transfer to the specified directory and the vital product database is not updated with this installation.

The output messages of this installation method are shown in Figure 160 on page 173.

In this case, if you want to de-install the client code, use the **De-install TT/6000 client** option available in the same SMIT menu.

Note

Do not configure one system to be a client to two servers, because a client cannot access two AIX Trouble Ticket/6000 databases simultaneously.

Do not install a server as a client of another server because the clients installed on the first server will be lost.

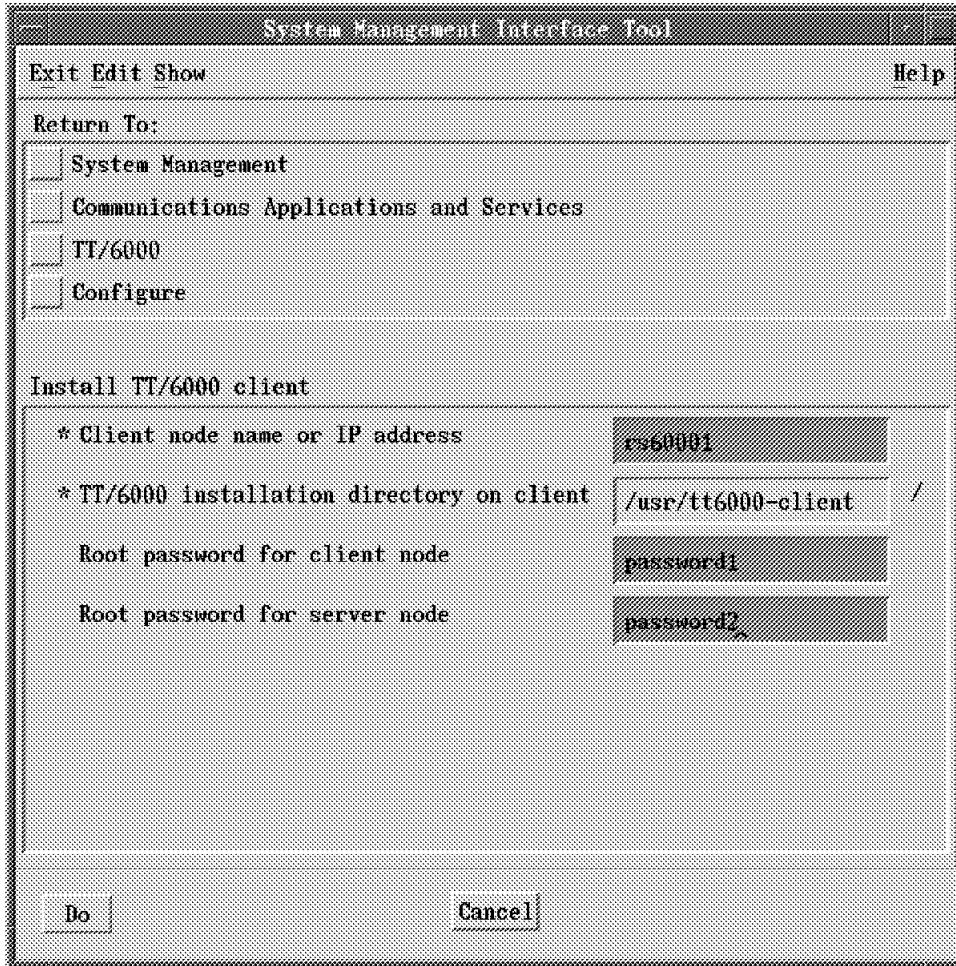


Figure 159. AIX Trouble Ticket/6000 Client Installation Panel

```

---- start ----
Sizing client files
Checking client access
Checking sockets
ypwhich: the domainname hasn't been set on this machine.
slump      2110/tcp      #TT/6000 communication
slump_server 2111/tcp
Checking server access
Transferring client files
93838 blocks
Shutting down TT/6000 apps and daemons
Configuring for installed options
Building TT/6000 scripts
--- Done ---

```

Figure 160. AIX Trouble Ticket/6000 Client Installation Output Messages

Besides these two methods, you can also access the AIX Trouble Ticket/6000 application by remote login clients. In this case, you will only be using the

X-resources of the client machine and will still be using the computational resources of the server machine.

7.3 AIX Trouble Ticket/6000 Startup

The AIX Trouble Ticket/6000 daemons are controlled through the **Communications Applications and Services...TT/6000...Control** SMIT panel, as shown in Figure 161. They do not depend on AIX NetView/6000 daemons to be started or stopped.

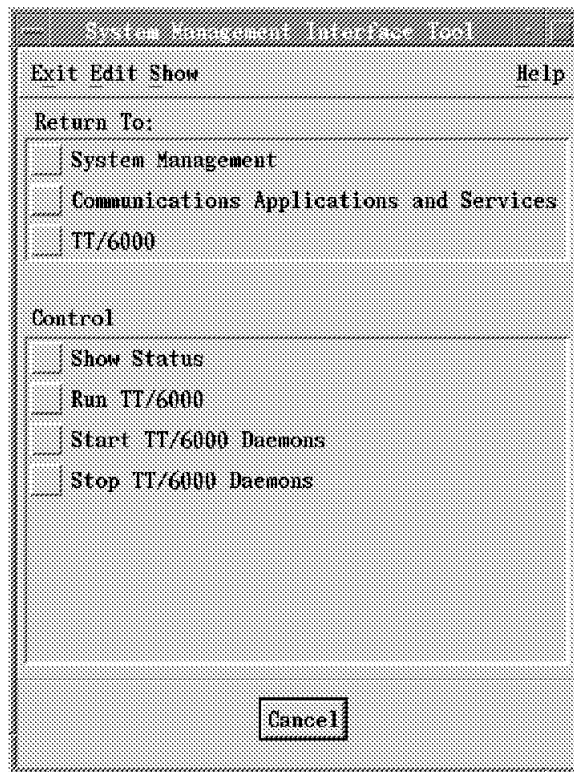


Figure 161. AIX Trouble Ticket/6000 Control Panel

After selecting the option to start the AIX Trouble Ticket/6000 daemons, you will be prompted to start them at the system restart, now or both. Choose one of the options and click on **Do**.

You can check if the daemons are running by selecting the **Show Status** option. The output of this selection should be similar to that shown in Figure 162 on page 175.

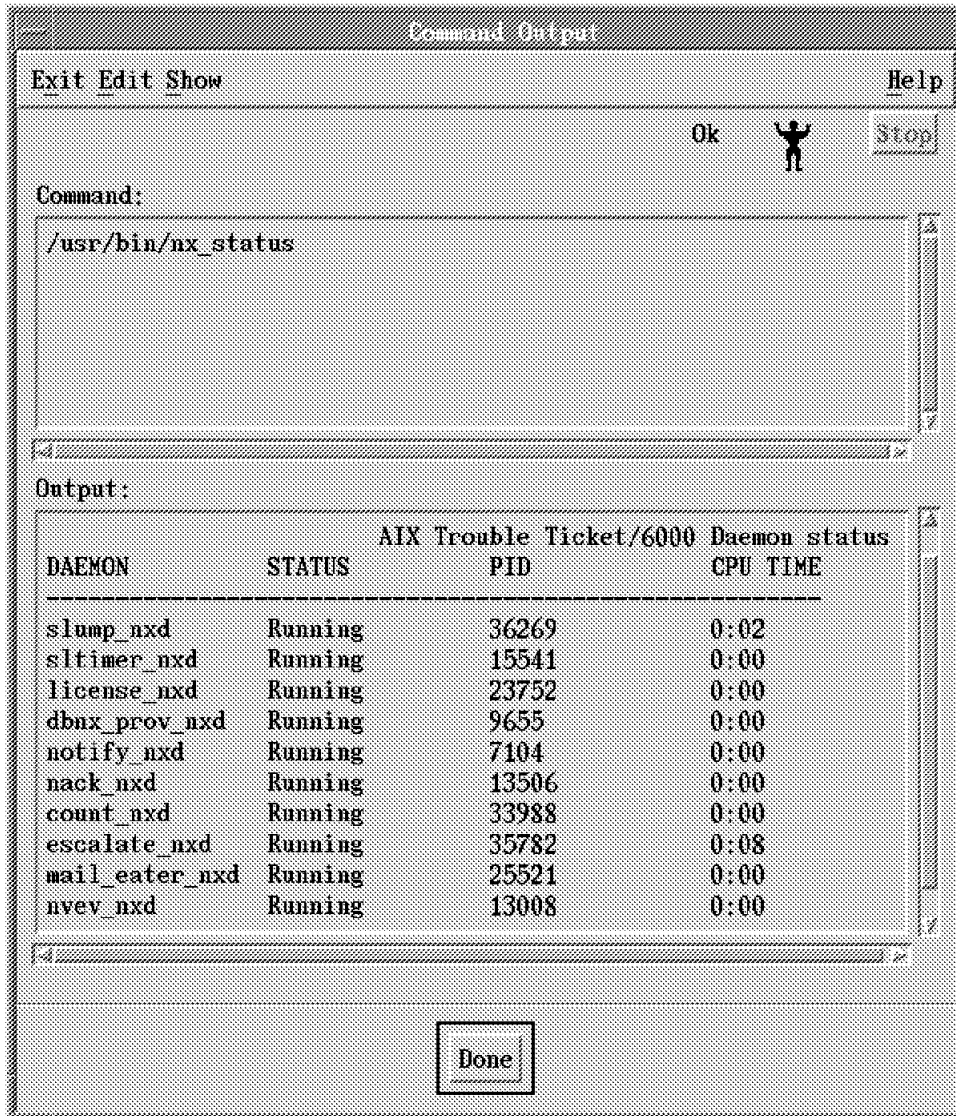


Figure 162. AIX Trouble Ticket/6000 Daemons Status Output

Notice that when you run the AIX Trouble Ticket/6000 application, it will start the daemons automatically even if they are currently stopped.

There are three ways to start the AIX Trouble Ticket/6000 main application:

1. From the command line, type:


```
tt6000
```
2. Select **Tools...Trouble Ticketing...Main Menu** in the AIX NetView/6000 main menu, as it is shown in Figure 156 on page 169.
3. Select **Communications Applications and Services...TT/6000...Control...Run TT/6000** in SMIT, as shown in Figure 161 on page 174.

Once you start the AIX Trouble Ticket/6000 application, it will show a copyright panel indicating that the application is being loaded. The application main panel is shown in Figure 163 on page 176.

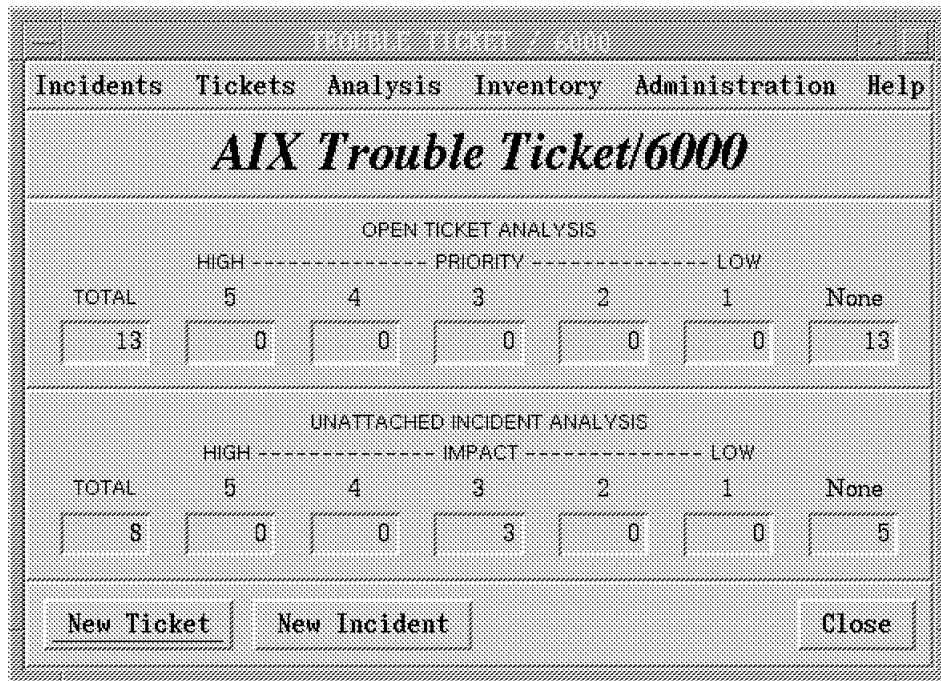


Figure 163. AIX Trouble Ticket/6000 Main Panel

7.3.1 Starting AIX Trouble Ticket/6000 from IBM Xstation

If you try to start the AIX Trouble Ticket/6000 application from an IBM Xstation and receive the message:

Warning: Font "xxxx" is not defined (using "fixed")

Where xxxx is the font being used (12x24 for example), you are running into font incompatibilities. To access the correct fonts, type the following commands from an AIX command prompt:

```
xset +fp /usr/lib/X11/fonts/misc
xset +fp /usr/lib/X11/fonts/100dpi
xset +fp /usr/lib/X11/fonts/75dpi
```

To make these changes effective for the subsequent restart of your Xstation follow these steps:

- Edit the file that displays the X window manager. This file is probably the .xinitrc file. It resides in the home directory of your user.
- Add the three xset commands that access the correct fonts.
- Restart the Xstation.
- When AIX prompts you for the host name, press the Enter key. If you type a host name, this work around may not work correctly. When you type the host name it will issue an rlogin to the specified machine, but the environment variables will not be exported. After you log on to the specified host make sure that you have the DISPLAY variable set to your machine.

In our case, where we were running AIXwindows Environment Version 1.2.3, the xinit program, that usually initializes the Xwindows environment, had been modified and it did not check if it was starting from an Xstation or from an hft

console. This caused some error messages that were fixed by using /usr/bin/X11/startx, which starts the Xclient's applications. We modified our profile file to have these entries:

```
if [ -n "$XSTATION" ]
then
    /usr/bin/X11/startx
fi
```

7.4 The Life Cycle of a Trouble Ticket

In this section we will describe the procedures that we used to prepare our environment in order to handle an incoming problem generated by a trap received by AIX NetView/6000.

A summary of the topics that we will cover include:

- The inventory tables that need to be filled out to have a minimum environment.
This step will also show how to import data from AIX NetView/6000's topology database.
- The additional tables that we used to make our examples more comprehensive.
- How to make a trap received by AIX NetView/6000 generate an incident report automatically.
- How to handle the incident report.
- How to open a trouble ticket.
- Assigning actions to be performed against the trouble ticket.
- Closing the trouble ticket.

Be sure to establish a one-to-one relationship between the AIX Trouble Ticket/6000 users (the ones that will be registered in the contact table) and the AIX users. This is explained later in 7.4.1.1, "The Contact Table" on page 178.

7.4.1 Populating the Inventory Tables

The following two tables are loaded by the product during its installation:

- Reference table

This table contains valid codes to be selected while creating trouble tickets, incident reports, and inventory records. These tables are accessed through the Administration option of the main menu, and include the following information:

Table 3. Reference Table Contents

Inventory codes	Trouble ticket codes
Resource families	Ticket priorities
Manufacturer codes	Ticket status
Contact types	Trouble codes
Location types	Service status
Coordinate types	Action status
Vendor types	Action delay codes
	Escalation levels
	Reason codes
	Incident impacts
	Urgencies
	Severities

- Resource classes table

A resource class identifies general categories of network resources, such as modems, bridges, routers, PCs, workstations, etc. They are categorized as hardware, software, or services.

As you go through this section, you will notice that all inventory table maintenance is done essentially in the same way.

Note

At a minimum, you must populate the Contact table and the Network Resources table with some minimal initial information in order to be able to create and use trouble tickets. However, remember that the more time you spend filling in the inventory tables, the more information you will have available when dealing with your problems.

7.4.1.1 The Contact Table

A contact is a person associated with the management of your network. This can be someone who handles trouble tickets, a technician, a network manager, a vendor, etc.

The steps that we used to configure the Contact table were:

- From the AIX Trouble Ticket/6000 main menu, select **Inventory...Contacts**. The Contact List dialog box is displayed.
- From the Contact List dialog box, select **Object...New**. This will open the Contact Detail dialog box.

At a minimum, fill in the following fields:

- Last (name)
- User ID

Enter a unique AIX user ID for each Contact table entry. If you enter an undefined AIX user ID, you will end up having unknown trouble ticket submitters, denoted by the “,” (comma) symbol.

- Electronic Mail Address

This information will be used to notify the contact person by E-mail, if the Automatic Notification fields are filled to specify E-mail as the notification method.

- Work Phone Number

One example of a contact with the minimum information filled is shown in Figure 164.

The screenshot shows a dialog box titled "CONTACT DETAIL" with a menu bar containing "Object" and "Help...". The main title is "Contact Detail". The form contains the following fields:

Last	First	Middle	Record Status ++
Nusbaum	Barry		Active
Nickname	Type ++	User ID	Electronic Mail Address
Barry		barry	barry@rs60005.itsoral.ibm.com
Functional Organization ++	Administrative Organization ++	Expense Code	
Location ++		Phone Numbers	
		Work	(919) 111-1111 (fictitious)
Postal address		Facsimile	
		Voice Mail	
		Pager	
Contact Notes			
Automatic Notification Methods			
Emergency ++	High Priority ++	Normal ++	Low Priority ++
Log ++			
Close			

Figure 164. Example of a Minimum Contact Entry

- Click on the **Close** button and select to **Save** the modifications made.

The Contact List dialog box will be updated with the new entry as shown in Figure 165 on page 180.

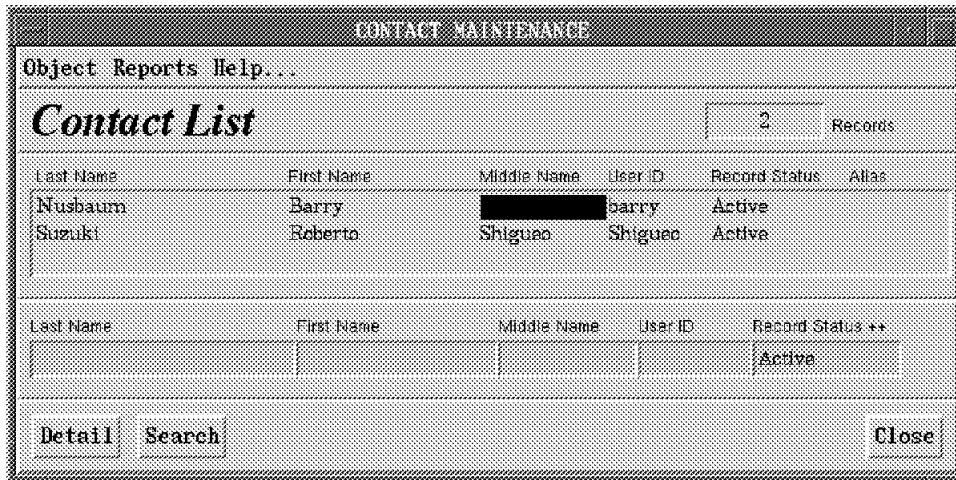


Figure 165. Contact List Dialog Box Updated with the New Entry

Figure 166 on page 181 shows a Contact Detail dialog box filled with additional information. If you are following this chapter step by step, you will notice that it is not possible to fill all these fields at this time because some of them are cross references to other tables (namely the Location and the Organization tables) that have yet to be modified.

CONTACT DETAIL			
Object Help...			
Contact Detail			
Last	First	Middle	Record Status ++
Suzuki	Roberto	Shiguo	Active
Nickname	Type ++	User ID	Electronic Mail Address
Shiguo	User	Shiguo	shiguo@rs60005.itso.ral.ibm.co
Functional Organization ++	Administrative Organization ++	Expense Code	
ITSO Raleigh	ITSO Raleigh	[REDACTED]	
Location ++	Phone Numbers		
IBM ITSC Raleigh	Work	(919) 301-2426 (temporary)	
Postal address	Facsimile		
4912 Green Road	Voice Mail		
Raleigh, NC 27604	Pager		
Contact Notes			
This is just a temporary contact entry. Don't count on that.			
Automatic Notification Methods			
Emergency ++	High Priority ++	Normal ++	Low Priority ++
Email	Email	Email	Email
Log ++			
[Empty Log Area]			
Close			

Figure 166. Contact List Dialog Box with All the Fields Filled

7.4.1.2 The Network Resources Table

Network resources are the devices, software and services that make up a network. These resources can be imported from AIX NetView/6000's topology database and populate essential fields in the Network Resources table. These fields are:

- System ID (the IP address)
- System name
- Name (the same as system name)
- MAC address
- Resource class

This information is retrieved from the General Resource Class (GRC) type information in the topology database. If this type does not match a known value in the Resource Class table the value *Unknown* will be used.

To import this information, Select **Administration...Import/Verify Managed Elements** from the AIX Trouble Ticket/6000 main menu, as shown in Figure 167.

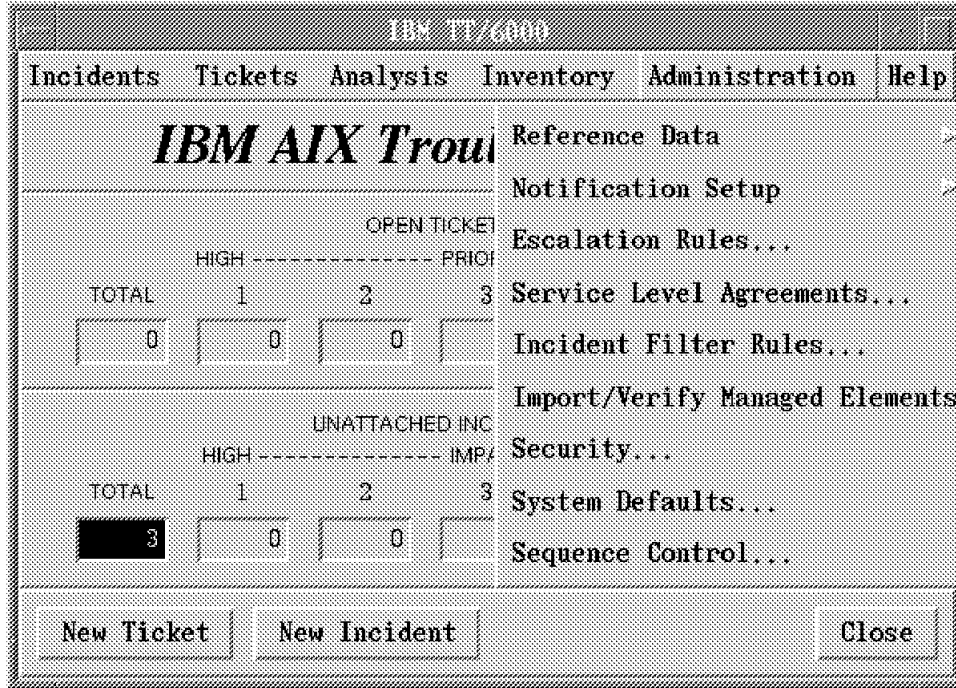


Figure 167. AIX Trouble Ticket/6000 Menu Selection to Import Network Resources from AIX NetView/6000

You will receive the window shown in Figure 168 indicating that the import process is taking place.

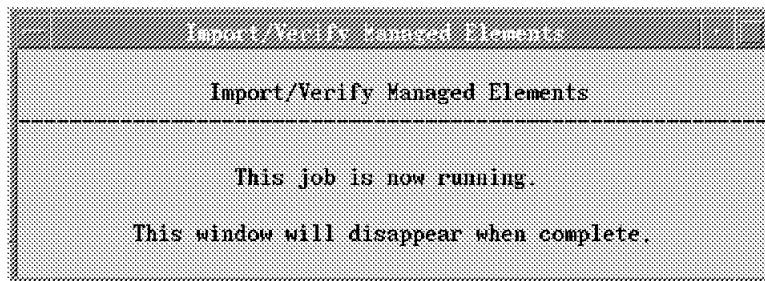


Figure 168. Import/Verify Managed Elements Information Window

This process also verifies the consistency of the inventory against the current state of the network.

To check the imported network resources, select **Inventory...Network Resources** from the AIX Trouble Ticket/6000 main menu. This will display the Network Resource List dialog box as shown in Figure 169 on page 183.

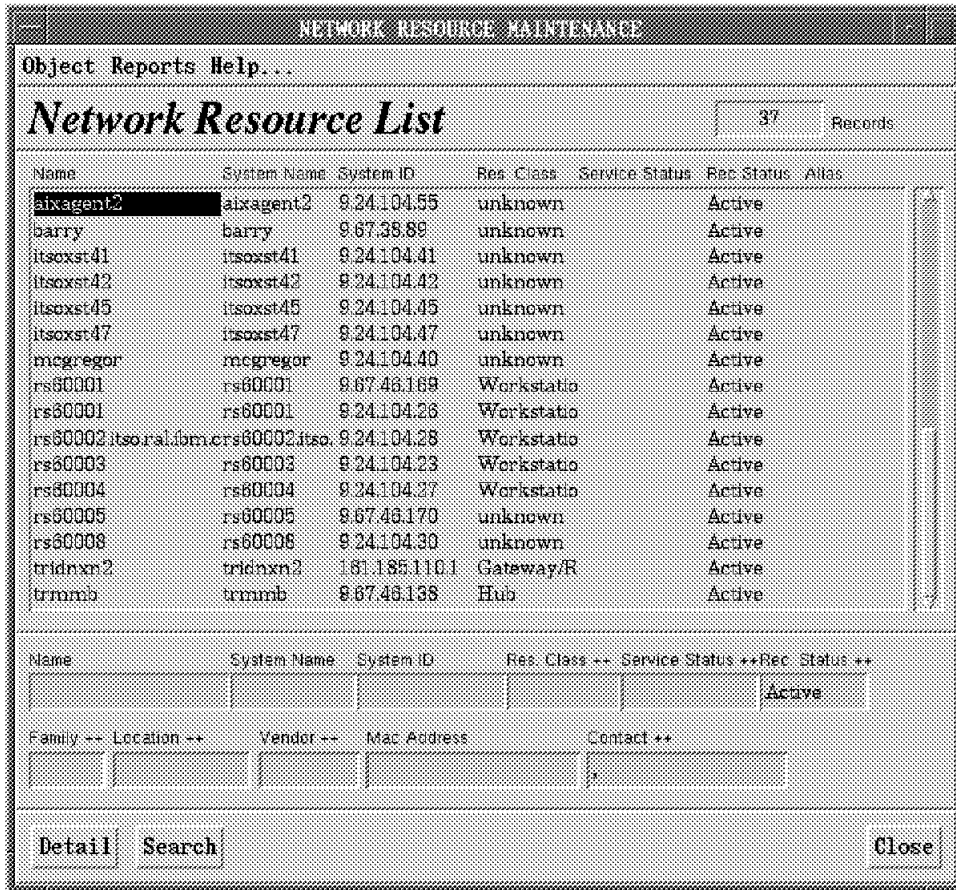


Figure 169. Network Resource List Dialog Box after Importing the Elements

If you double-click the left mouse button on one of the entries in this list or if you select one of the entries and click on the **Detail** button, it will open the Network Resource Detail dialog box, as shown in Figure 170 on page 184.

You might want to fill in the other fields of this table. We have modified the values in the Resource Class field, the Responsible Organization field, the Location field and the Contact Field, as they will appear in the incident report related to any affected machine.

NETWORK RESOURCE DETAIL

Object Help...

Network Resource Detail

Name	System Name	System ID	Record Status ++
aixagent2	aixagent2	9.24.104.66	Active
Resource Class ++	Family	Service Status ++	MAC Address
unknown	H/W		40:00:00:03:33:42
Default Priority ++			
	3		
Model ++	Manufacturer	Release	Serial Number
License Number	Acquisition Date/Time	Expiration Date/Time (license, etc)	
SLA ++	Expense Code	Responsible Organization ++	
Location ++	Floor	Room	
Cabinet	Shelf	Slot	
Contact ++	Phone		
Vendor ++	Maintenance Vendor ++		
Log ++			

Close

Figure 170. Network Resource Detail Dialog Box with the Imported Information from AIX NetView/6000

7.4.1.3 The Organization Table

Organizations describe internal departments and divisions to which trouble ticket responsibility may be assigned. To get to the Organization Detail dialog box where such information can be entered:

- From the main menu, select **Inventory...Organizations**.
It will open the Organization List dialog box.
- From the Organization List dialog box menu, select **Object..New**.
This will open the Organization Detail dialog box.
- In the Organization Detail dialog box fill in the fields:
 - Organization Name
 - Description

- Contact Name

If you double-click on this field, it will show the available options. You should have a panel similar to that shown in Figure 171.

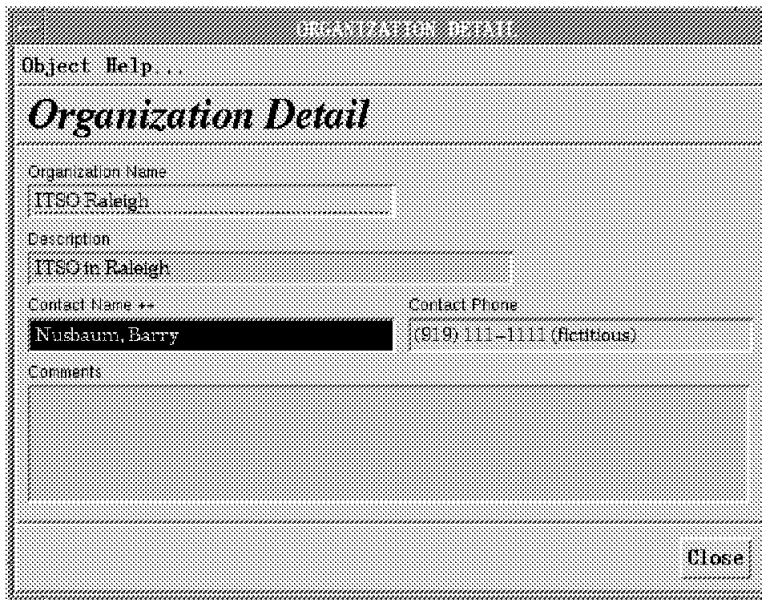


Figure 171. Example of an Organization Detail Dialog Box

- Click on **Close** and select to **Save** the changes made.

Your new entry should be available as shown in Figure 172.



Figure 172. Organization List Dialog Box Showing the New Organization

7.4.1.4 The Site Table

A site is a general grouping of locations, such as a city where several locations exist. To enter the site details:

- From the main menu, select **Inventory...Sites**.
It will open the Site List dialog box.
- From the Site List dialog box menu, select **Object...New**.
This will open the Site Detail dialog box.
- In the Site Detail dialog box fill in the fields:
 - Site Name
 - Long Name
 - Contact Name

If you double-click on this field, it will show the available options.

You should have a panel similar to that shown in Figure 173.

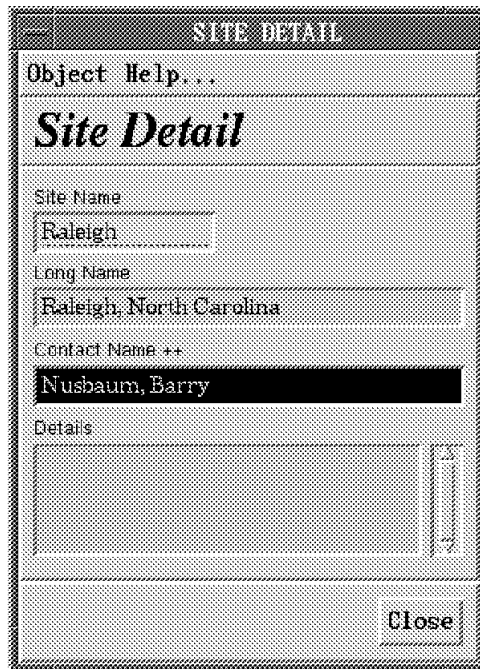


Figure 173. Example of a Site Detail Dialog Box

- Click on **Close** and select to **Save** the changes made.

Your new entry should be available as shown in Figure 174 on page 187.



Figure 174. Site List Dialog Box Showing the New Site

7.4.1.5 The Location Table

A location identifies a specific physical place, that can be of any type, for example, a city, a campus, a building, or a floor of a building. To provide details of your location:

- From the main menu, select **Inventory...Locations**
It will open the Location List dialog box.
- From the Location List dialog box menu, select **Object...New**.
This will open the Location Detail dialog box.
- In the Location Detail dialog box fill in the fields:
 - Location Name
 - Location Type
Double-click on this field to select one of the available options.
 - Site
Double-click on this field to select one of the available sites.
 - Coordinates
This field specifies the type of coordinates that will be used. Select the one that fits your needs.
 - Postal Address

You should have a panel similar to that shown in Figure 175 on page 188.

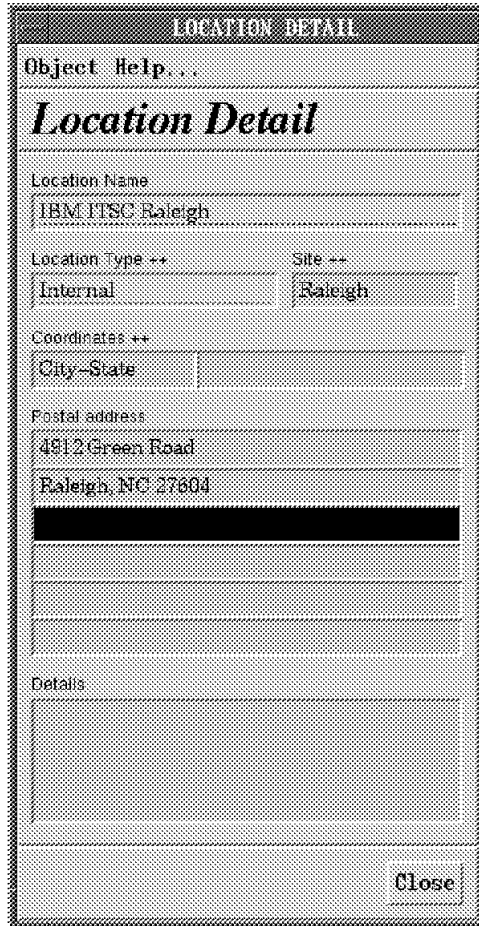


Figure 175. Example of a Location Detail Dialog Box

- Click on the **Close** button and select to **Save** the modifications made.

Your new entry should be available as shown in Figure 176.

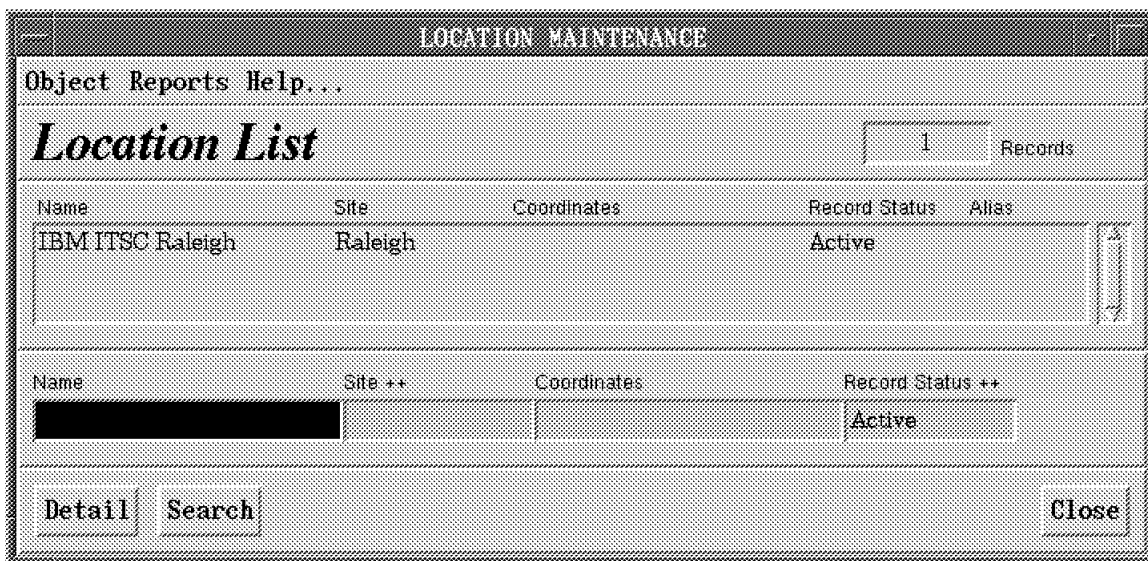


Figure 176. Location List Dialog Box Showing the New Location

7.4.1.6 The Vendor Table

A vendor identifies a company that provides hardware, software or services to your network.

- From the main menu, select **Inventory...Vendors**
It will open the Vendor List dialog box.
- From the Vendor List dialog box menu, select **Object...New**.
This will open the Vendor Detail dialog box.
- In the Vendor Detail dialog box fill in the fields:
 - Vendor Name
 - Also known As
 - Type
 - Contact Name

This can be considered a nickname or an alias for the same vendor.
Double-click on this field to select one of the available types.
Double-click on this field to select one of the available options.

You should have a panel similar to that shown in Figure 177.



Figure 177. Example of a Vendor Detail Dialog Box

- Click on the **Close** button and select to **Save** the modifications made.

Your new entry should be available as shown in Figure 178 on page 190.



Figure 178. Vendor List Dialog Box Showing the New Vendor

7.4.2 Generating Incident Reports from Traps

In order to specify whether an incoming AIX NetView/6000 trap will open a new incident report in AIX Trouble Ticket/6000, you have to customize the Incident Filter Rule table.

In this table, you will specify:

- Which trap is going to be affected by that rule.
- For which device that rule will be valid.
- What action should be taken upon the receipt of this trap.

The procedures to customize a rule are:

- From the AIX Trouble Ticket/6000 main menu, select **Administration...Incident Filter Rules**. It will open the Incident Filter Rules dialog box.
- From the Incident Filter Rules menu, select **Object...New**. It will open the Incident Filter Detail dialog box.
- Double-click on the Enterprise Name field and it will display the available options. We have chosen *Imu2* with the enterprise ID of *1.3.6.1.4.1.2.6.14*
- Double-click on the Generic field to display the available traps. Remember that a trap is defined by a generic and a specific number. We have selected 6 and 10000005, respectively.
- Double-click on Filter name to decide which filter policy you are going to use. We have chosen *Report all events*. Refer to the documentation mentioned in the beginning of this chapter to see all the available options.
- Type the IP address for which this rule will be valid. Leaving this field blank will validate this filter rule for all IP addresses.

At this point you should have a panel similar to that shown in Figure 179 on page 191.

- Click on **Close** and choose to **Save** the changes made.



Figure 179. Example of an Incident Filter Detail Dialog Box

After completing these procedures, your new rule should be present at the bottom of the Incident Filter Rules panel as shown in Figure 180 on page 192.

INCIDENT FILTER RULES					
Object Help...					
<i>Incident Filter Rules</i>					
Enterprise Name	Object ID	Generic	Specific	Device IP Address	Event Description
netView6000	1.361.41.2.8.3	6	58785791		Node Added
netView6000	1.361.41.2.8.3	6	58785795		Node Deleted
netView6000	1.361.41.2.8.3	6	58916865		Node Down
netView6000	1.361.41.2.8.3	6	58916867		Interface Down
netView6000	1.361.41.2.8.3	6	58916868		Segment Critical
netView6000	1.361.41.2.8.3	6	58916869		Network Critical
netView6000	1.361.41.2.8.3	6	58982400		Link Level Address Changed
netView6000	1.361.41.2.8.3	6	58982401		Mismatch of Link Level Address
netView6000	1.361.41.2.8.3	6	58982403		Object Identifier Change
netView6000	1.361.41.2.8.3	6	58982404		System Descr Change
netView6000	1.361.41.2.8.3	6	58982405		System Name Change
netView6000	1.361.41.2.8.3	6	58982410		System Contact Change
netView6000	1.361.41.2.8.3	6	58982411		System Location Change
netView6000	1.361.41.2.8.3	6	58982412		Interface Type Change
netView6000	1.361.41.2.8.3	6	58982413		Interface Descr Change
lmu2	1.361.41.2.6.14	6	1000000592410455		Ln LMU Topology changed. Ln Station \$3 Ln Type \$3 Ln Statu

Enterprise Name ++ Object ID ++ Generic ++ Specific ++ Device IP Address

Detail Search Close

Figure 180. The New Incident Filter Rule Shown at the Bottom of the List

You can specify the default incident reporter for these automated cases. Select **Object...Set Incident Reporter** from the Incident Filter Rules menu and this will open a dialog box in which a contact can be named to be the incident reporter. Double-click in the field and select one of the available entries. Your dialog box should be similar to that shown in Figure 181.

SET INCIDENT REPORTER
Object Help...
<i>Set Incident Reporter</i>
Incident Reporter ++
Suzuki, Roberto Shiguo
Close

Figure 181. Dialog Box to Select a Default Incident Reporter

7.4.3 Receiving an Incident Report

In 7.4.2, “Generating Incident Reports from Traps” on page 190 we created an incident filter rule that would capture a trap, as shown in Figure 182.

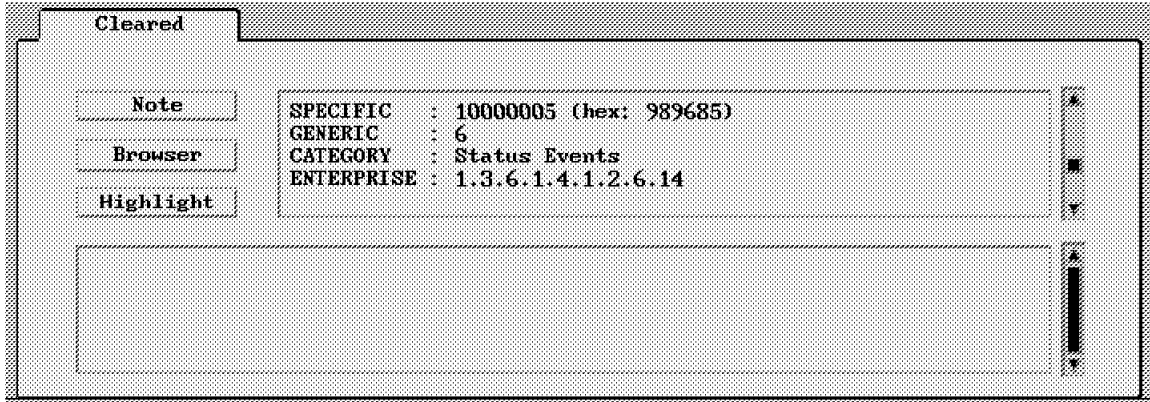


Figure 182. Event Card Showing the Trap that Is Going to Be Treated

To list the generated incident report, select **Incidents...List** from the main menu. This will open the Incident Report List dialog box, as shown in Figure 183.

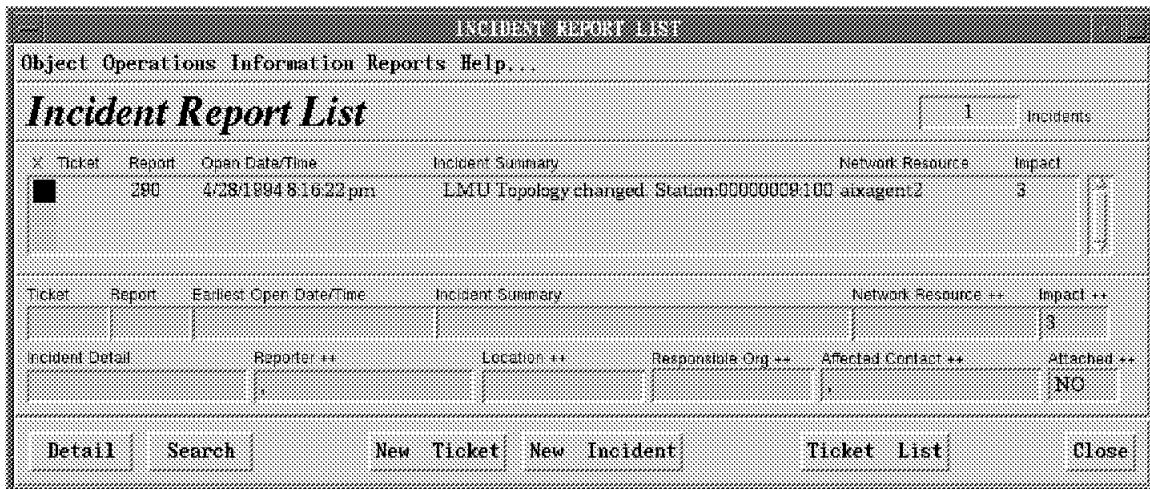


Figure 183. Incident Report List Dialog Box Showing the Trap that Matched the Incident Filter Rule

Double-click on the incident entry or select it and click on the **Detail** button to bring up the Incident Report dialog box, as shown in Figure 184 on page 194.

INCIDENT REPORT			
Object Information Help...			
Report Number	Open date/time	Ticket Number	
290	4/28/1994 8:16:22 pm		
Incident Summary		Network Resource ++	
LMU Topology changed. Station:00000009.10005A31F459 T		aixagent2	
Incident Detail			
<pre>(1.3.6.1.4.1.2.5.3.1.4.1.1):(1.3.6.1.2.1.2.2.1.3.79) (1.3.6.1.4.1.2.5.3.1.4.1.2):00000009.10005A31F459 (1.3.6.1.4.1.2.6.14.4.2.1.3.2):2 (1.3.6.1.4.1.2.6.14.4.2.1.4.2):3 (1.3.6.1.4.1.2.6.14.4.2.1.5.2):10005A31F459 (1.3.6.1.4.1.2.6.14.4.2.1.6.2):1004 (1.3.6.1.4.1.2.6.14.4.2.1.7.2):</pre>			
Observed start date/time	Observed end date/time	Count	Impact ++
4/28/1994 8:16:22 pm	4/28/1994 8:16:22 pm	1	3
Location ++		Site	
IBM ITSC Raleigh		Raleigh	
Affected Contact ++		Phone	Responsible Org ++
Suzuki, Roberto Shiguelo		(919) 301-2426(t)	ITSO Raleigh
Reporter -- last, first, middle ++		Phone	Email
Suzuki, Roberto Shiguelo		(919) 301-2426(t)	shiguelo@rs60005.its
Submit Report		Quick Ticket	
			Close

Figure 184. Initial Incident Report Generated from a Trap

The creation of this incident report is indicated in two ways. Electronic mail is sent to the incident reporter as shown in Figure 185 on page 195, and a notification log is created. This notification log is accessed from the Trouble Ticket main menu, by using the Analysis...Notifications pull-down. If you double-click on a notification entry, you will receive the Notification Detail dialog box as shown in Figure 187 on page 196.

From shiguel Thu Apr 28 20:16:24 1994
 Received: by rs60005.itso.ral.ibm.com (AIX 3.2/UCB 5.64/4.03)
 id AA38672; Thu, 28 Apr 1994 20:16:24 -0400
 Date: Thu, 28 Apr 1994 20:16:24 -0400
 Message-Id: <9404290016.AA38672@rs60005.itso.ral.ibm.com>
 To: shiguel@rs60005.itso.ral.ibm.com
 From: TT6000.Notification
 Subject: Incident Report #290 created.
 Status: RO

This incident occurred at 04/28/1994 20:16:23.
 The reporter is Suzuki, Roberto Shiguel.
 The description follows:

LMU Topology changed.
 Station:00000009:10005A31F459
 Type:2
 Status:3
 NodeAddress:10005A31F459
 NodeType:1004
 Domain:
 Userid:SUPERVISOR
 Managing:00000009:400000033342

Figure 185. E-mail Showing the Incident Report Creation



Figure 186. Notification List Showing that the Incident Report Was Created

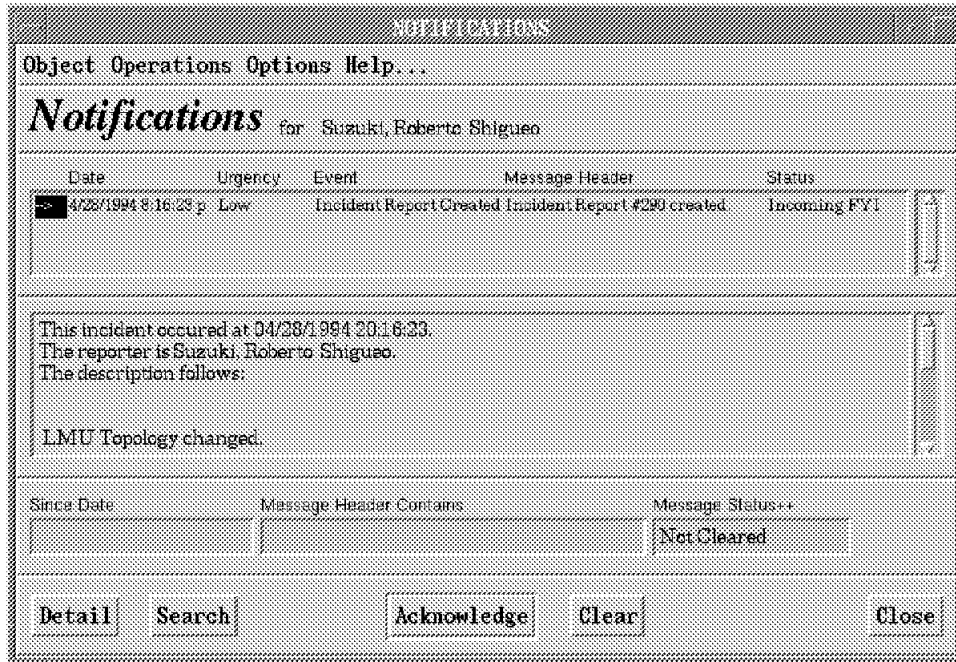


Figure 187. Detailed View of the Notification of the Incident Report Creation

7.4.4 Opening a Trouble Ticket

Once an incident report is created, we can choose to open a trouble ticket that will manage the resolution of the possible problem that has been reported.

There are several ways to open a trouble ticket:

- By selecting a new trouble ticket using one of the AIX NetView/6000 access points to AIX Trouble Ticket/6000 as shown in 7.2, "AIX Trouble Ticket/6000 Installation" on page 167.
- By clicking on the **New Ticket** button of the AIX Trouble Ticket/6000 main panel, or by selecting **Tickets...New**.
- By clicking on the **New ticket** button of the Incident Report List dialog box.
- By clicking on the **New Ticket** button of the Trouble Ticket List dialog box, or by selecting **Object...New**.
- By selecting **Quick Ticket** from the Incident Report dialog box.

We selected the last option because it automatically attaches the incident report that we are viewing to the trouble ticket. If you select any of the other options you will have to mark the desired incident report(s) in the Incident Report List dialog box by double-clicking on it, and then clicking on the **Attach Incidents** button. The new trouble ticket with the incident report attached is shown in Figure 188 on page 197.

TROUBLE TICKET

Object Operations Information Help...

Trouble Ticket

Ticket Number	Open date/time	Priority ++	Esc. Level ++	Status ++
17	4/29/1994 10:16:56 am	3	None	Open

Ticket Summary	Trouble Code ++
LMU Topology changed. Station:00000009:10	SW

Ticket Detail

```

(1.36.1.4.1.2.5.3.1.4.1.1):(1.36.1.2.1.2.2.1.3.79)
(1.36.1.4.1.2.5.3.1.4.1.2):00000009:10005A31F459
(1.36.1.4.1.2.6.1.4.4.2.1.3.2):2
(1.36.1.4.1.2.6.1.4.4.2.1.4.2):3

```

Resource ++	Failed	Chronic	System Name	System ID
aixagent2	NO	NO	aixagent2	9.24.10455

Assignee ++	Responsible Organization ++	External Reference
Suzuki, Roberto Shiguelo	Organization	

Ticket Log ++

Submitted By	Last Modified By	Last Modified date/time
Suzuki, Roberto Shiguelo	Suzuki, Roberto Shiguelo	4/29/1994 10:16:56 am

Figure 188. A New Trouble Ticket with the Incident Report Attached

In order to validate this trouble ticket you will have to select a Trouble code. Double-click on the field and you will receive the available options. Click on the **Submit Ticket** option and it is officially opened. If you select **Tickets...List** from the main panel, the Trouble Ticket List dialog box will be displayed showing the new trouble ticket as in Figure 189 on page 198.

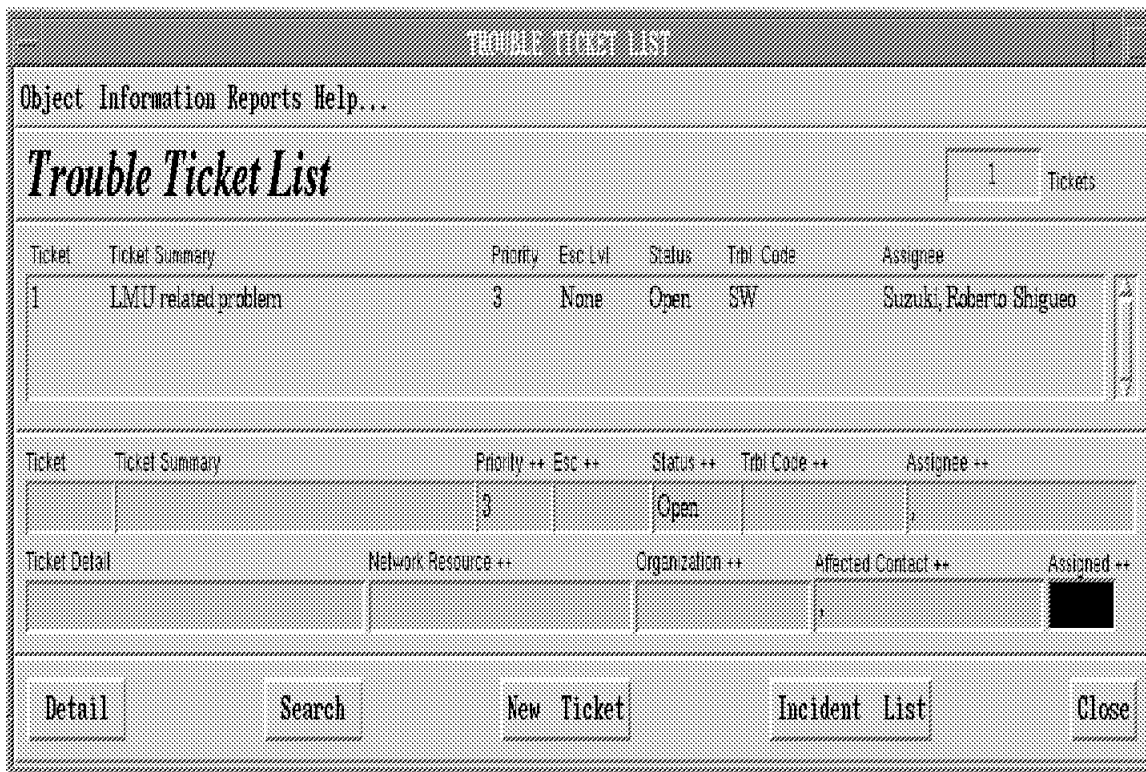


Figure 189. Trouble Ticket List Dialog Box Showing the New Trouble Ticket

The creation of this new trouble ticket is indicated by the following sequence:

- Trouble ticket # created
- Ticket # assigned to contact
- Incident # attached

These notifications are made through electronic mail and notification logs as shown in 7.4.3, “Receiving an Incident Report” on page 193.

7.4.5 Assigning Actions

Now it is time to solve the problem. In order to assign an action against the problem:

- Select **Operations...Define Actions** from the Trouble Ticket dialog box. This will open the Action List dialog box.
- From this dialog box, select **Object...New**. This will open the Action Detail dialog box. Figure 190 on page 199 shows an example of how you can fill in this table with a hypothetical action that could be performed against a problem.

If this action is to be used in other trouble tickets you may save it as a template by selecting **Object...Save Template** in the Action List dialog box.

ACTION DETAIL

Object Information Help...

Action Detail 1 of 1 Status ++ **Delayed**

Action

Fix Resource

Description

Affected Contact ++ Phone Number Expense Code

Suzuki, Roberto Shigueo (919)301-2426

Affected Resource ++ Location ++ Failure? ++

aixagent2 IBM ITSC Raleigh NO

Maintenance Organization ++ Maintenance Vendor ++ SLA ++

ITSO Raleigh IBM

Work Order Number Charge Back? ++

 NO

Action Assignee ++ Scheduled Start Scheduled Finish

Nusbaum, Barry 4/23/1994 12:00:00 am 4/25/1994 12:00:00 am

Down Time SLA Down Time Actual Start Actual Finish

 4/23/1994 5:23:12 pm

Action Writer ++ Assignment Made Assignment Acknowledged

Suzuki, Roberto Shigueo

Results

Action Log ++

Close

Figure 190. Action Detail Dialog Box Showing a Hypothetical Situation

Click on the **Close** button and the new action will be shown in the Action List dialog box, as shown in Figure 191 on page 200.

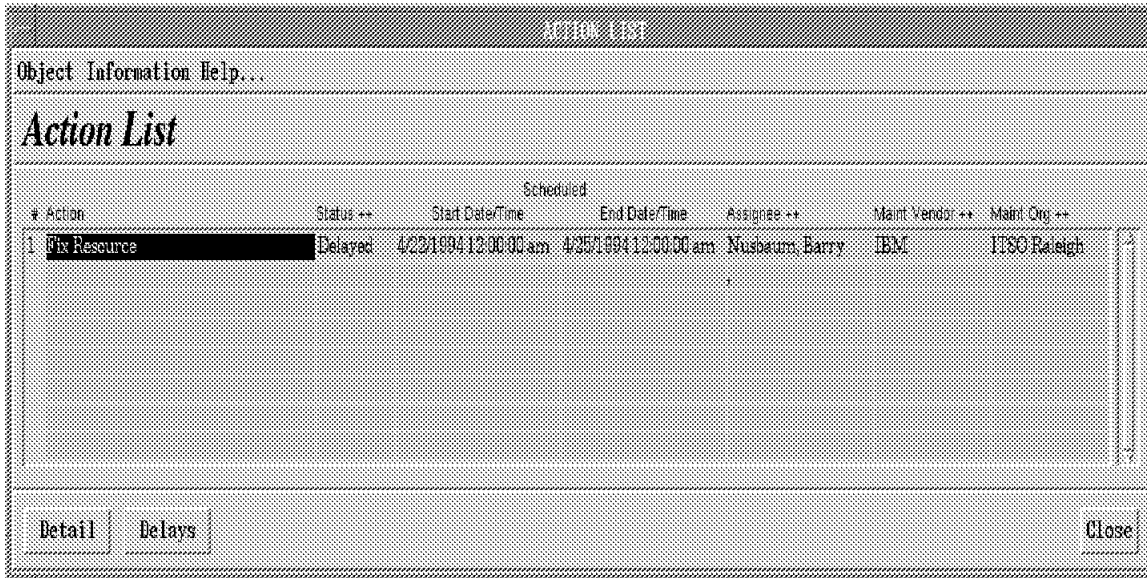


Figure 191. Action List Dialog Box Showing the New Action

In the Trouble Ticket dialog box, click on the **Submit Ticket** button or select **Object...Save** to make these actions effective. This action assignment is indicated in the following places:

- In the Action Assignment Summary, accessible from the AIX Trouble Ticket/6000 main panel by selecting **Analysis...Action Assignment Summary** as shown in Figure 192.
- In electronic mail to the assignee.
- In the notification log.

Assignee	Total	PRIORITY					None	Asg Hrs
		1	2	3	4	5		
Suzuki, Roberto Shiguen	1	0	0	1	0	0	0	5:50:00

Vendor	Total	PRIORITY					None	Asg Hrs
		1	2	3	4	5		
IBM	1	0	0	1	0	0	0	5:50:00

Figure 192. Action Assignment Summary Panel

In the case of an action assignment, the assignee has to acknowledge the receipt of it. In Figure 193 on page 201 you can see that the action assigned notification has the message *Pending ACK* as the status.

To acknowledge it, click on the **Acknowledge** button available in the Notification dialog box and in the Notification Detail dialog box, or select the **Operations...Acknowledge** option in the Notification dialog box.

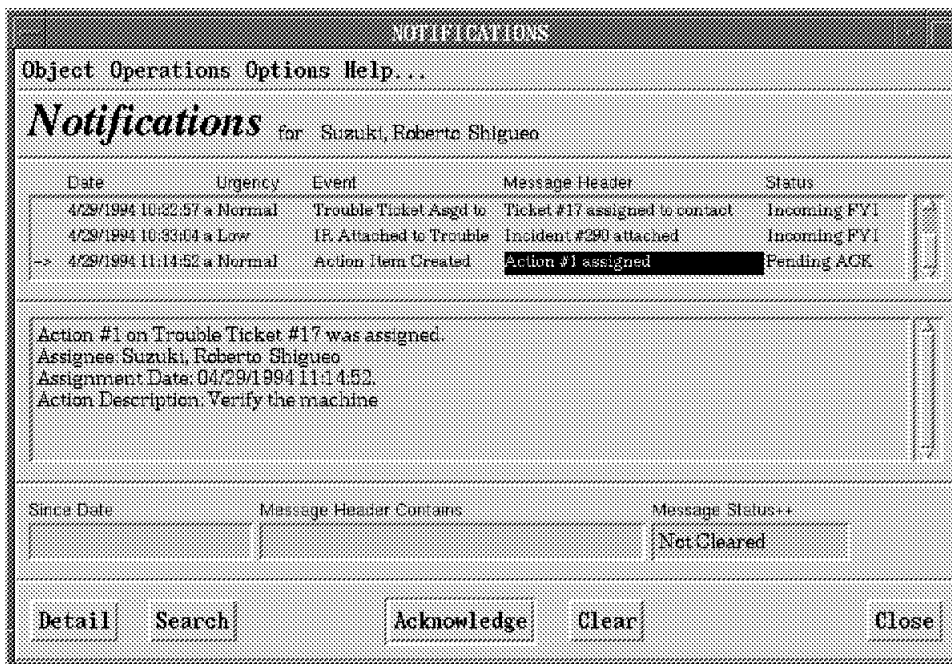


Figure 193. Notification Dialog Box Showing that an Action Assignment Has to Be Acknowledged

7.4.6 Solving the Problem and Closing the Trouble Ticket

The next step in this process is for the assignee to perform the action assigned. The assignee updates the status of the action as either delayed or completed. Also, it is the assignee's task to log comments and results of the action performed. In Figure 194 on page 202, we show the action completed.

ACTION DETAIL			
Object Information Help...			
Action Detail 1 of 1		Status -- Completed	
Action			
Verify the machine			
Description			
Before calling the vendor itself, first we are going to verify the machine. If this does not help then we will escalate the problem.			
Affected Contact --	Phone Number	Expense Code	
Suzuki, Roberto Shigueo	(915) 301-2428 (temporary)		
Affected Resource --	Location --	Failure? --	
aixagent2	IBM ITSC Raleigh	NO	
Maintenance Organization --	Maintenance Vendor --	SLA --	
ITSO Raleigh	IBM		
Work Order Number		Charge Back? --	
		NO	
Action Assignee --	Scheduled Start	Scheduled Finish	
Suzuki, Roberto Shigueo	4/29/1994 11:00:00 am	4/29/1994 5:00:00 pm	
Down Time	SLA Down Time	Actual Start	Actual Finish
1:13:40		4/29/1994 11:02:00 am	4/29/1994 12:14:40 pm
Action Writer --	Assignment Made	Assignment Acknowledged	
Suzuki, Roberto Shigueo			
Results			
The machine is operational.			
Action Log --			
Windows was not running. Probably someone wanted to use pure DOS. We have restarted it. This will solve the problem.			
Close			

Figure 194. Completion of an Action

In this example, the action taken was enough to solve the problem. It could be that the assignee could not solve the problem in time. The next step would then be to escalate the problem to another assignee with more skill.

It is the assignee's task to keep track of the problem resolution by logging all the relevant information. Notice that once a log report is submitted, it can no longer be modified. Any further logs will only be appended to the existing ones. Notice also that the action assignee is not necessarily the same as the assignee of the trouble ticket itself.

As a result of the action performed, another trap was generated and consequently another incident report was opened, this time to indicate that the problem was solved. Whenever an incident report that is related to a trouble ticket is generated, it can be attached to an opened trouble ticket. Refer to 7.4.4, "Opening a Trouble Ticket" on page 196 to see how to attach an incident report to a trouble ticket.

Before closing the trouble ticket it is important to record the cause of failure. This is done by selecting **Operations...Record Causes** in the Trouble Ticket dialog box and an example is shown in Figure 195 on page 203.

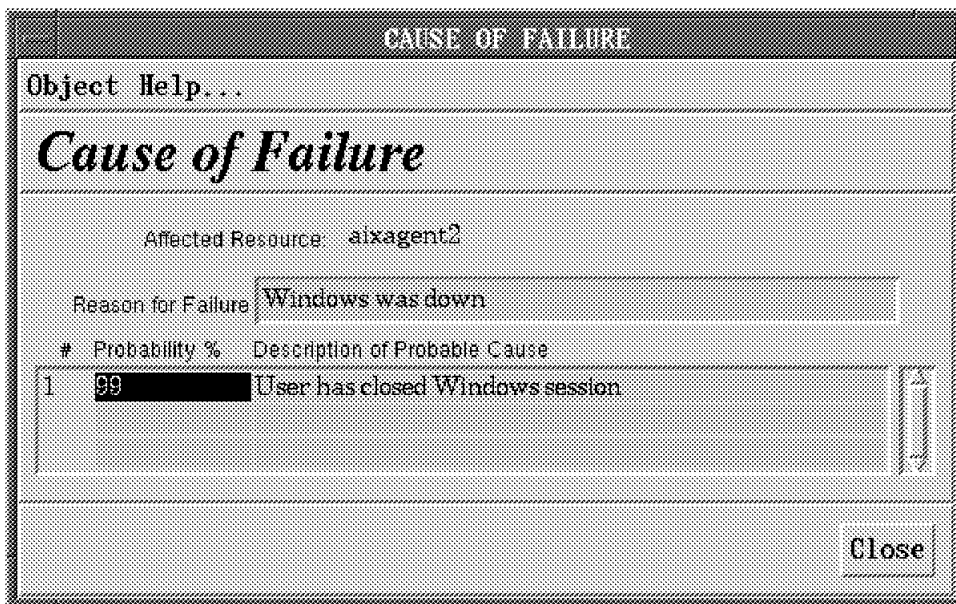


Figure 195. Recording a Possible Cause of Failure

Now we are ready to close the ticket, by selecting the **Close Ticket** button in the Trouble Ticket dialog box. It brings the Status Change Detail dialog box, that we have modified to store the information shown in Figure 196.

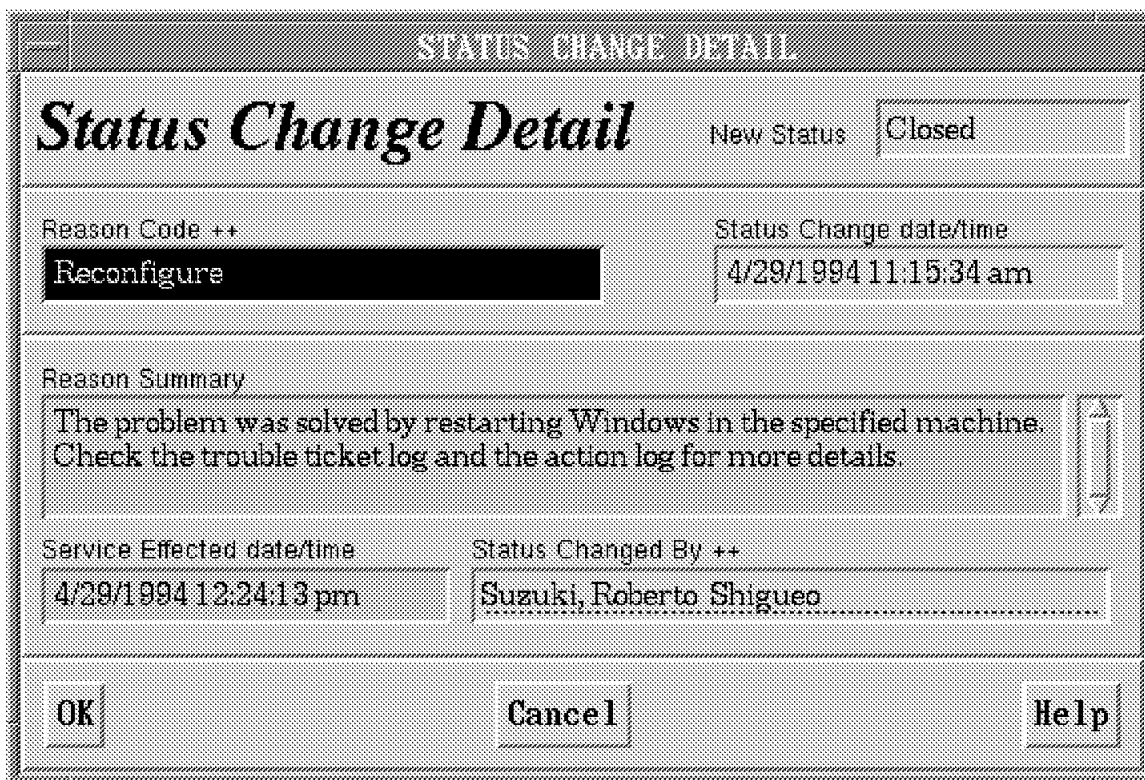


Figure 196. Information Required before Closing a Trouble Ticket

Figure 197 on page 204 shows the final status of the Notification dialog box up to closing of the trouble ticket.



Figure 197. Final Status of the Notification Dialog Box

Chapter 8. Integration Scenarios

Now that we have given an overview of the products, and shown how they work individually, this chapter will show how they can be made to work more closely together.

We have picked some scenarios to demonstrate how the products can be integrated. They are:

- A critical station on the LAN goes down.
- A station is not authorized to access the network.
- A virus is detected on DOS/WINDOWS workstation.

In the scenarios we will show things like:

- Event configuration
- Alert flow
- Execution of shells
- Pop-up windows in AIX and OS/2
- ovobjprint to print a database of LAN objects
- ovtopodump for details of LAN objects

8.1 A Critical Station on the Network Goes Down

IBM LAN Network Manager for AIX provides the ability to monitor adapters on the network and produce SNMP traps when the adapter leaves the network.

If a station is defined as monitored, LNM will periodically send a frame to the adapter. If no response is received LNM will continue to poll that adapter until the number of retries specified on the General Parameters window is reached. The response timeout value determines how long LNM retries to check the adapters that it is monitoring. We will show:

- How to configure IBM LAN Network Manager for AIX to perform this function
- The flow of alerts
- Execution of an AIX shell script

The following steps are required to configure this environment:

- Activate adapter monitoring.
- Define a profile for the adapter and enable the monitoring option for that adapter.

Most configuration options are selected from the pull-down menus of the LNM Proxy Agent Configuration screen. For example, to add a station definition the *Actions...Add Definition...Station* pull-down menu option is taken, as shown in Figure 198 on page 206. These configuration changes can be done from either the AIX GUI interface, or the OS/2 agent GUI interface.



Figure 198. LNM Proxy Agent Configuration Pull-Down Menu Options

Activating adapter monitoring is accomplished through the LNM Proxy Agent Configuration screen by selecting the **Parameters...Adapter Monitoring** pull-down menu.

The *Monitor retries* value determines how many times LNM polls the adapter before determining the adapter is not responding. In our environment, the LNM proxy agent will poll the adapter 4 times. If no response is received during this period of time LNM considers the adapter to be not responding. Choose the **Active** option for Monitor Adapters to enable monitoring, as shown in Figure 199 on page 207. Choose **Apply** to update the configuration then **OK** to exit the screen.

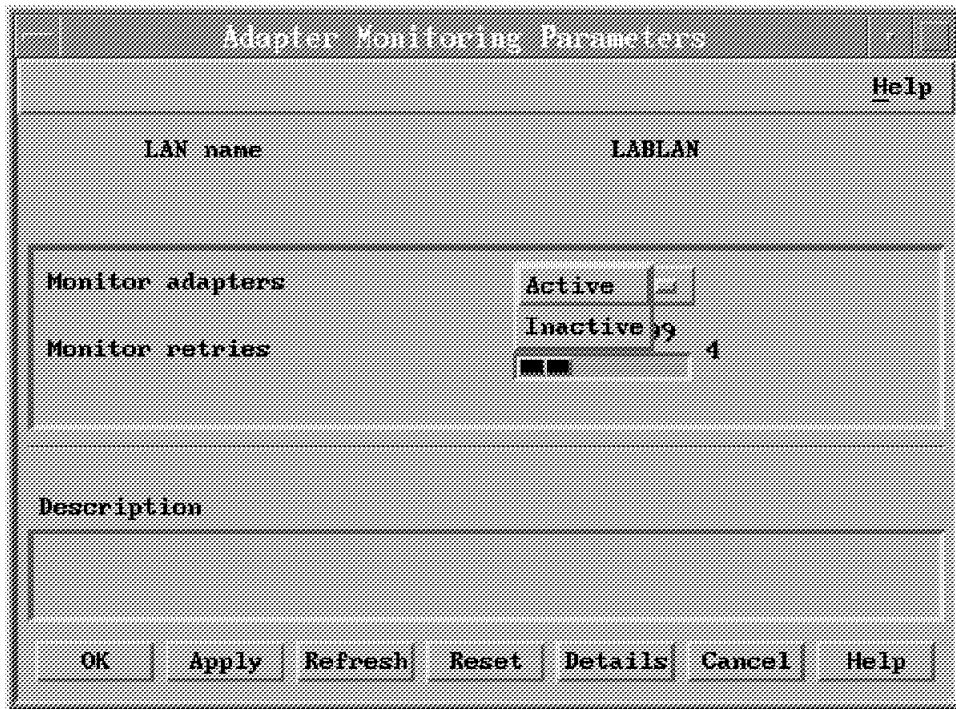


Figure 199. LNM Adapter Monitoring Parameters

The interval at which LNM polls the adapter is determined by either the *Response timeout* value or 15 seconds whichever is greater. This value is in the General Parameters window and can be shown by selecting **Parameters...General Parameters** from the pull-down menu of the LNM Proxy Agent Configuration screen. In our environment 15 seconds was used for the poll interval since our response timeout value was set at 6, as shown in Figure 200 on page 208.

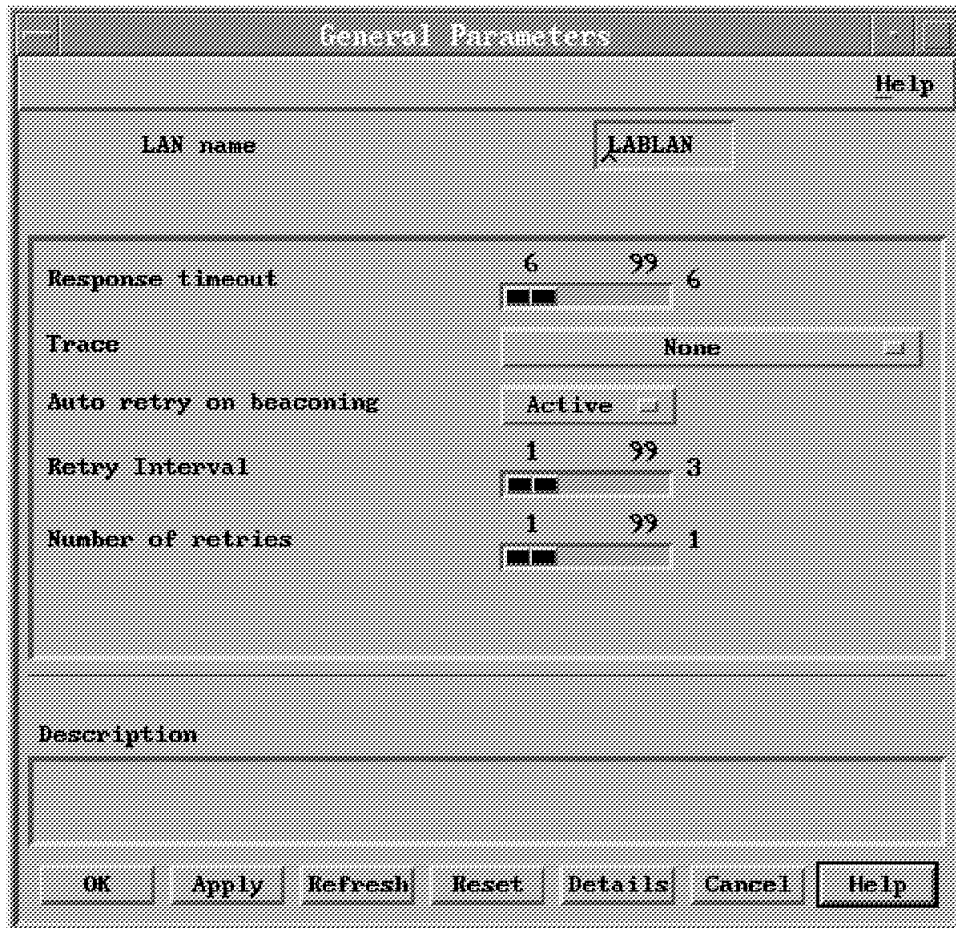


Figure 200. General Parameters

To change the definition of an adapter select **Actions... Add Definition...Station** from the appropriate pull-down menu on the LNM Proxy Agent Configuration screen,

In this screen we entered the following information, as shown in Figure 201 on page 209:

- Adapter Name: DOSWINDOWS
- Adapter Address: 10005A31F459
- Comments: DOS Windows workstation to be monitored
- Monitored: Yes

Choose **Apply** to then update the databases. Choose **OK** to exit this screen.

Add Station Definition Help

LAN name: LABLAN

Adapter name: DOSWINDOWS

Adapter address: 10005A31F459

General

Comments: DOS Windows workstations to be

Monitor: No

Tracing: Yes

Access Control

Time	Day	Hours
From	Sunday	0 24 0
To	Sunday	0 24 24

Description

OK Apply Refresh Reset Details Cancel Help

Figure 201. LNM for AIX Station Profile Details

At this point the LNM environment has been configured to monitor this adapter, which we have defined as DOSWINDOWS.

From the LNM proxy agent configuration screen a list of stations can be displayed (this is to show what adapters are on the network and which have profile definitions):

- Choose the **Lists...Stations** option from the pull-down menu.
- When the Station List screen is shown choose the segment that the adapter is on and select the **Display** button to display a list of the adapters. In our environment LAN segment 581 was selected, as is shown in Figure 202 on page 210

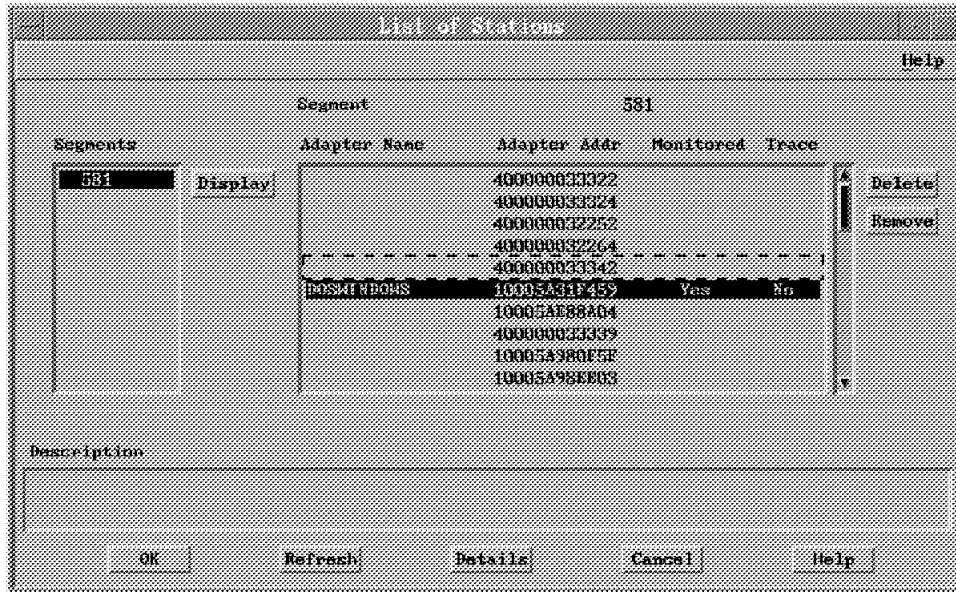


Figure 202. LNM for AIX Station List

Following is a diagram of the environment to illustrate the flow of information in this scenario.

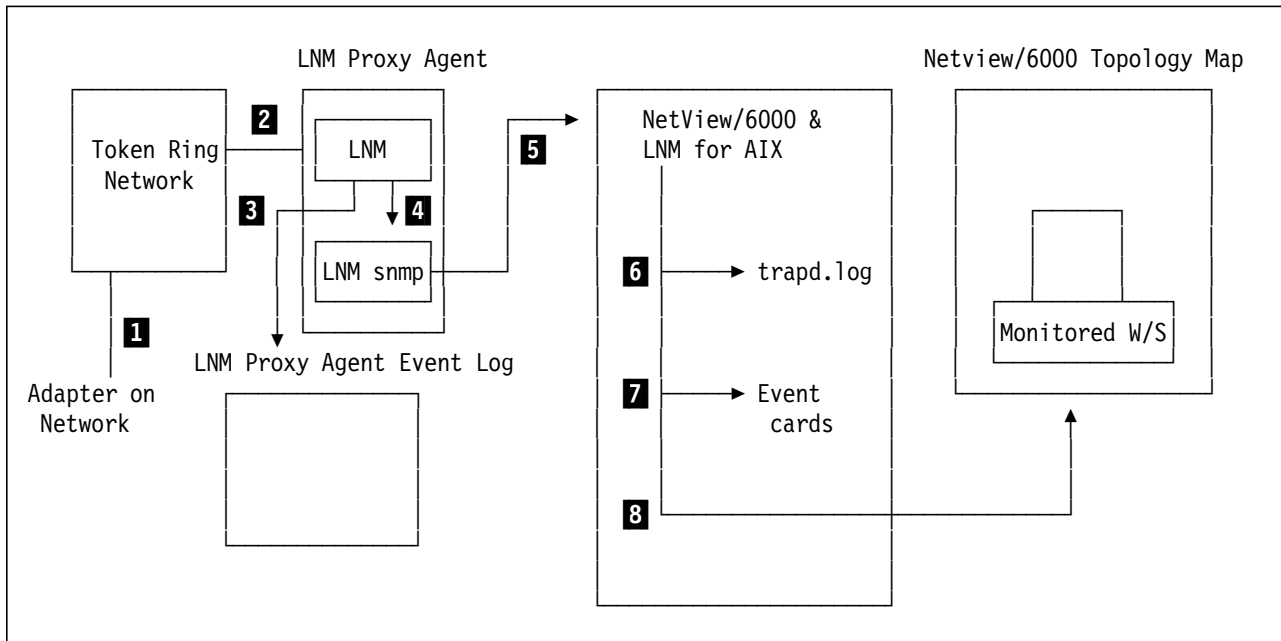


Figure 203. LNM for AIX Environment

- 1** The adapter loses contact with the network. In our environment we powered off the PC.
- 2** The OS/2 LNM proxy agent receives information about NAUN changes on the network. The LNM proxy agent polls the monitored adapter until all timeout and retry values have been exceeded.
- 3 and 4** LNM generates the following alerts:
 - NAUN changes (since adapter has left network).
 - Monitored adapter is not responding.

Each alert is logged in the LNM proxy agent's local event log and sent to the SNMP component of LNM.

- 5** Each alert is converted to an SNMP trap and sent to the AIX NetView/6000 application.
- 6** All traps received are logged in the trapd.log file.
- 7** The major alerts are displayed in the event cards of AIX NetView/6000.
- 8** The workstation color is updated in the AIX NetView/6000 topology to reflect the status of the workstation entering or leaving the network.

All the traps received from the LNM proxy agent are stored in the trapd.log file as shown in Figure 204.

At times alerts appear twice in the trapd.log file as can be seen with the *Monitored adapter not responding* trap. Traps with a level of 7 indicate a *Log Only* trap, whereas traps with values of 2 or 3 will cause event cards to be created in AIX NetView/6000.

```
1
767381667 7 Wed Apr 27 13:19:51 1994 aixagent1 A Trap 220 from Enterprise lnm6000: Naun change for segment 0x05 81.
Station address: 0x40 00 00 03 33 42
767381667 7 Wed Apr 27 13:19:51 aixagent1 A NAUN address: 0x10 00 5a e8 8a 04
2
767381737 7 Wed Apr 27 13:20:58 1994 aixagent1 A Trap 123 from Enterprise lnm6000: Monitored adapter
0x10 00 5a 31 f4 59 is not responding.
3
767381737 2 Wed Apr 27 13:20:58 1994 loopback P Trap 123 from Enterprise lnm6000: Monitored adapter 10005A31F459
is not responding.
767381737 2 Wed Apr 27 13:20:58 loopback P Resource label: 10005A31F459
```

Figure 204. AIX NetView/6000 trapd.log File

The traps received in this scenario are described below:

- 1** A NAUN notification will be sent since adapter 10005A31F459 has left the network. Adapter 40000003342 has a new NAUN which is 10005AE88A04. Since the trap type is 7, this is a log only trap.
- 2** The monitored adapter is not responding. Since the trap type is 7, this is a log only trap.
- 3** The monitored adapter is not responding, however, this trap is also displayed in the AIX NetView/6000 event cards since this was a type 2 trap.

One event is displayed in the AIX NetView/6000 event cards as shown in Figure 205 on page 212.

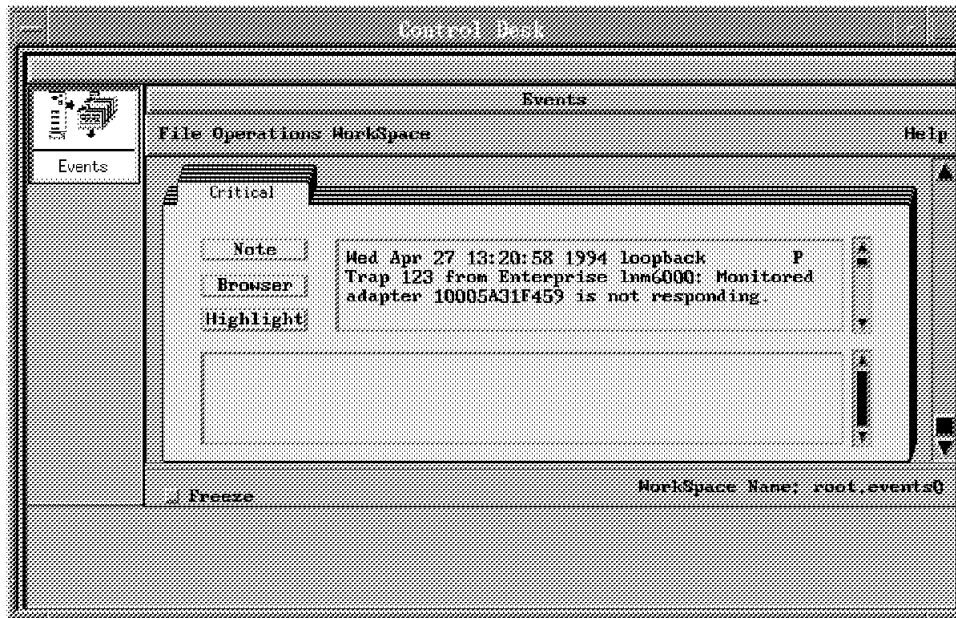


Figure 205. AIX NetView/6000 Event Cards

When the station returns to the network the following is displayed in the AIX NetView/6000 trapd.log file, as shown in Figure 206, and event cards, as shown in Figure 207 on page 213.

1	767381860	7	Wed Apr 27 13:24:45 1994 aixagent1	A Trap 220 from Enterprise lnm6000: Naun change for segment 0x05 81. Station address: 0x10 00 5a 31 f4 59
	767381860	7	Wed Apr 27 13:24:45 aixagent1	A NAUN address: 0x10 00 5a e8 8a 04
2	767381860	7	Wed Apr 27 13:24:45 1994 aixagent1	A Trap 220 from Enterprise lnm6000: Naun change for segment 0x05 81. Station address: 0x40 00 00 03 33 42
	767381860	7	Wed Apr 27 13:24:45 aixagent1	A NAUN address: 0x10 00 5a 31 f4 59
3	767381874	7	Wed Apr 27 13:24:48 1994 aixagent1	A Trap 124 from Enterprise lnm6000: Monitored adapter 0x10 00 5a 31 f4 59 returned to network
	767381874	7	Wed Apr 27 13:24:48 aixagent1	A Segment number: 0x05 81
4	767381874	3	Wed Apr 27 13:24:48 1994 loopback	P Trap 124 from Enterprise lnm6000: Monitored adapter 10005A31F459 returned to network.
	767381874	3	Wed Apr 27 13:24:48 loopback	P Resource label: 10005A31F459
	767381874	3	Wed Apr 27 13:24:48 loopback	P Segment number: 0581

Figure 206. AIX NetView/6000 trapd.log File

- 1** This caused a NAUN notification since adapter 10005A31F459 entered the network. Its new NAUN information is displayed. The NAUN for this adapter is 10005AE88A04. Since the trap type is 7, this is a log only trap.
- 2** This is a NAUN notification. The adapter that had 10005AE88A04 as its NAUN now has 10005A31F459 as its NAUN. Since the trap type is 7, this is a log only trap.
- 3** The monitored adapter has returned to the network. Since the trap type is 7, this is a log only trap.
- 3** The monitored adapter has returned to the network, however, this is also displayed in the AIX NetView/6000 event cards.

One event is displayed in the AIX NetView/6000 event cards as shown in Figure 207 on page 213.

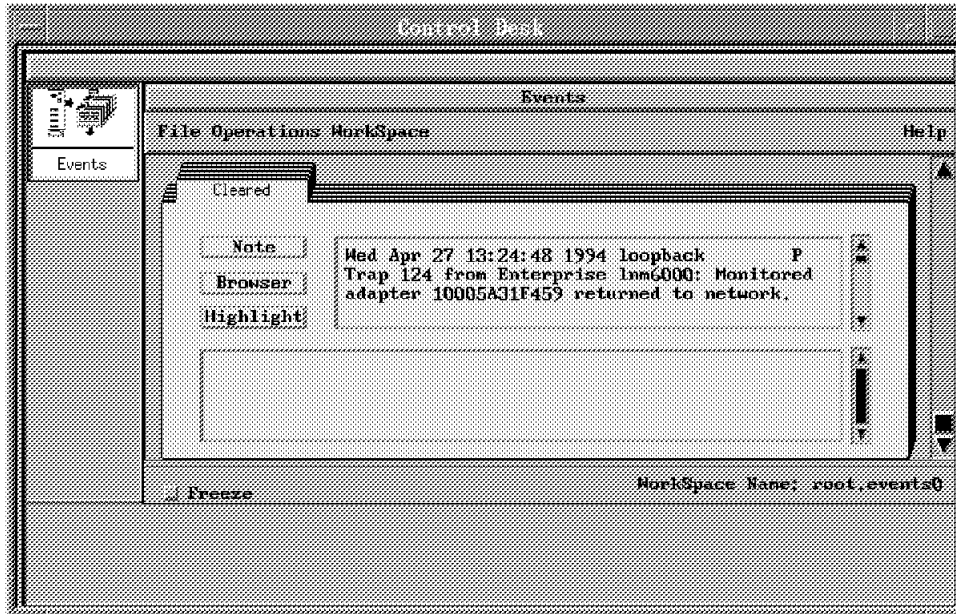


Figure 207. AIX NetView/6000 Event Cards

The IBM LAN Network Manager for AIX object identifying this station on the LNM for AIX topology map is updated in the following manner:

- Adapter leaving the network
 - The object is initially in a normal state (green) when the station is on the network.
 - The object changes to an unknown state (blue) when the trap indicates that the monitored adapter has left the network. The trap number for this state change was 123, as was shown in Figure 207.
- Adapter re-entering the network
 - The object is in an unknown state (blue).
 - The object changes to a normal state (green) when the NAUN changes information for the adapter is received in trap 220. The trap indicating that the adapter has returned to the network does not affect the status of the object on the LNM for AIX map.

8.2 An Unauthorized Adapter Enters the Network

IBM LAN Network Manager for AIX provides the ability to secure the network to prevent unauthorized access.

The possible security options available are:

- The adapter address is unauthorized. Any adapter undefined in the LNM database is not authorized to connect to the network.
- The adapter is on at an unauthorized day/time. An adapter definition is required for each adapter identifying the day/time this adapter is authorized to access the network.

- The adapter has moved (Controlled Access Unit only). This prevents adapters from moving from port to port within the CAU. The offending adapter is removed.
- The adapter is an undefined bridge. This controls which bridges can attach to your network. The offending bridge adapter is removed when the bridge adapter is not defined.
- In addition, the lobes on the CAU can be disabled if any of the above violations occur when attached to the CAU.

In our scenario we will show what happens when an adapter accesses the network at an unauthorized time. We will show:

- How to configure IBM LAN Network Manager for AIX to restrict access by time.
- The flow of alerts.
- Execution of an AIX shell script.

The following steps are required to configure this environment:

- Activate access control security.
- Configure the OS/2 LNM proxy agent to be a controlling LNM station.
- Define configuration information for the adapter entering the authorized day and time for the station.

Configuring the OS/2 LNM proxy agent to be a controlling LNM station is done from the LNM proxy agent configuration screen. Select **Parameters...Bridge Parameters** to display the Bridge Parameters screen, as shown in Figure 208 on page 215.

Change the reporting level to **Controlling**. Enter the controlling level password for the bridges in your network. Then choose **Apply** to update the configuration, and **OK** to exit the screen.

Only an LNM station at the controlling level has the authority to remove adapters from the network. If the LNM station is at one of the other levels, observing 1, 2 or 3, an error will be returned indicating that the LNM station is not a controlling LNM and therefore cannot remove the adapter.

Bridge Parameters

Help

LAN name **LABLAN**

General

Bridge autolink flag Disabled

Autolink timer Controlling 4

Reporting link status Observing1

For next startup or restart Observing2

 Observing3

Password

Data Collection

Time	Day	Hours	Minutes
From	Sunday <input type="checkbox"/>	0 23 0	0 59 0
To	Saturday <input type="checkbox"/>	0 23 0	0 59 0

Description

Figure 208. LNM for AIX Access Control Configuration

The LNM proxy agent needs to be restarted to operate at the new reporting level. Choose **Actions..Restart LNM Proxy Agent** from the LNM Proxy Agent Configuration screen, as shown in Figure 209 on page 216.



Figure 209. LNM for AIX Restart LNM Proxy Agent

A confirmation screen will be displayed. Choose **OK** to restart the proxy agent.

To activate the Access Control Security, select **Parameters...Access Control** from the LNM Proxy Agent Configuration screen.

Select the toggle button to activate **Adapter is on at an unauthorized day/time**. Then select the **Apply** button to update the configuration. To activate access control choose the **Actions...Access Control...Activate** pull-down option, as shown in Figure 210 on page 217. If the refresh button is selected the current configuration will be retrieved from the LNM proxy agent and the screen will be updated.

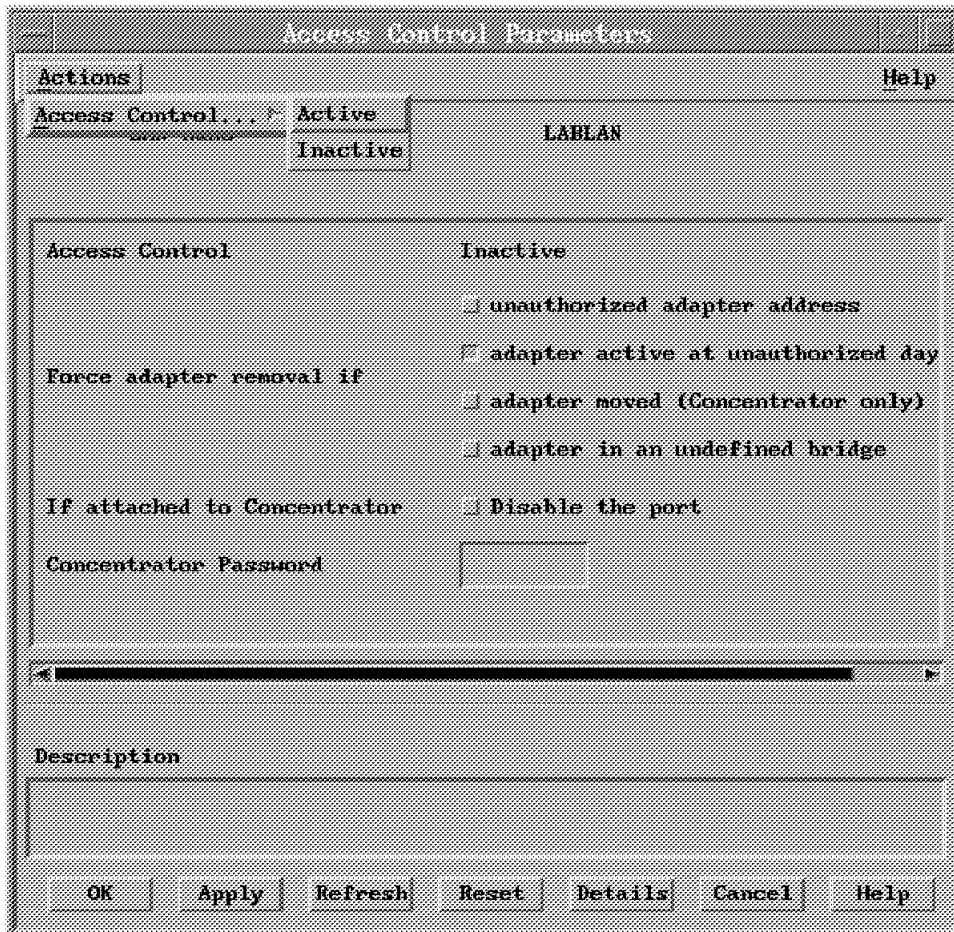


Figure 210. LNM for AIX Access Control Parameters

The next step is to define the adapters for which you want to enforce security access. The access control information is stored in the *configuration* information for the station.

The access control information can be accessed by:

- The LNM Proxy Agent Configuration screen when first creating a station definition.
- The Context pull-down menu on the station in the LNM for AIX topology map.

Note: A profile needs to be created for the station before the configuration information can be entered in this method.

We will access the configuration information by displaying the location of the adapter on the LNM for AIX map and select the **LAN...Configuration** option on the Context pull-down menu, as shown in Figure 211 on page 218. The profile information for this station was created in the monitored adapter chapter.

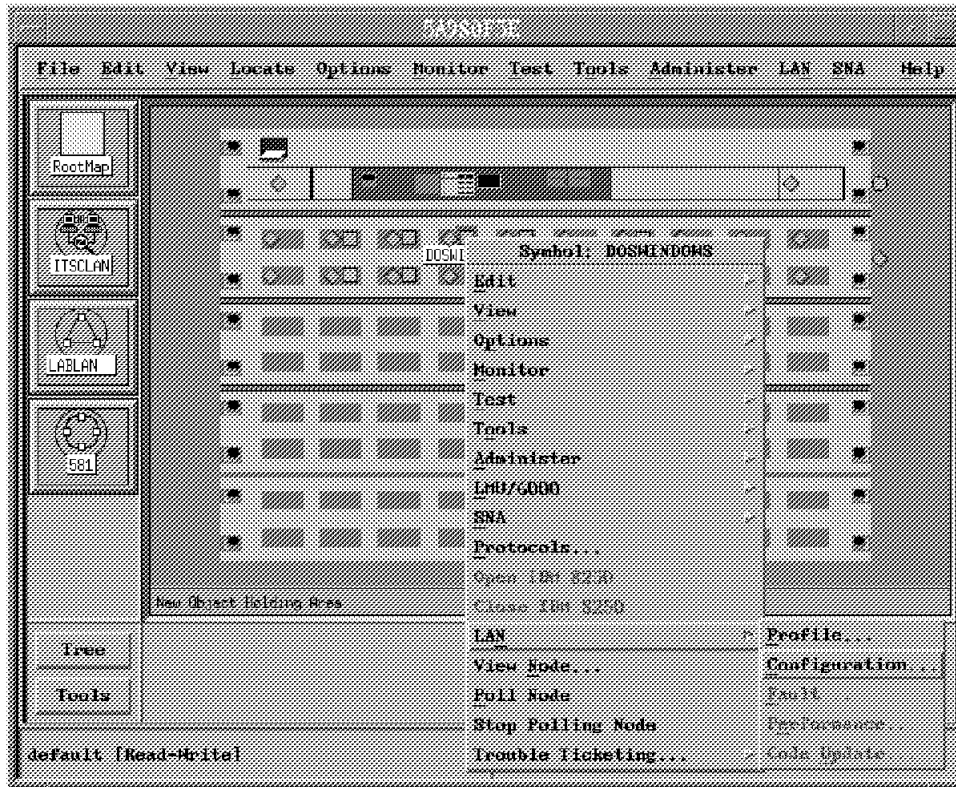


Figure 211. LNM for AIX Context Pull-Down Menu

The Configuration screen will be displayed. The way to define access control is to provide the day/time period that the station will be permitted to have access to the LAN. In our environment we enabled the station to access the network from Sunday morning (0 hours) to Sunday midnight (24 hours), as shown in Figure 212 on page 219. Choose the **Apply** push button to update the configuration and choose **OK** to exit the screen.

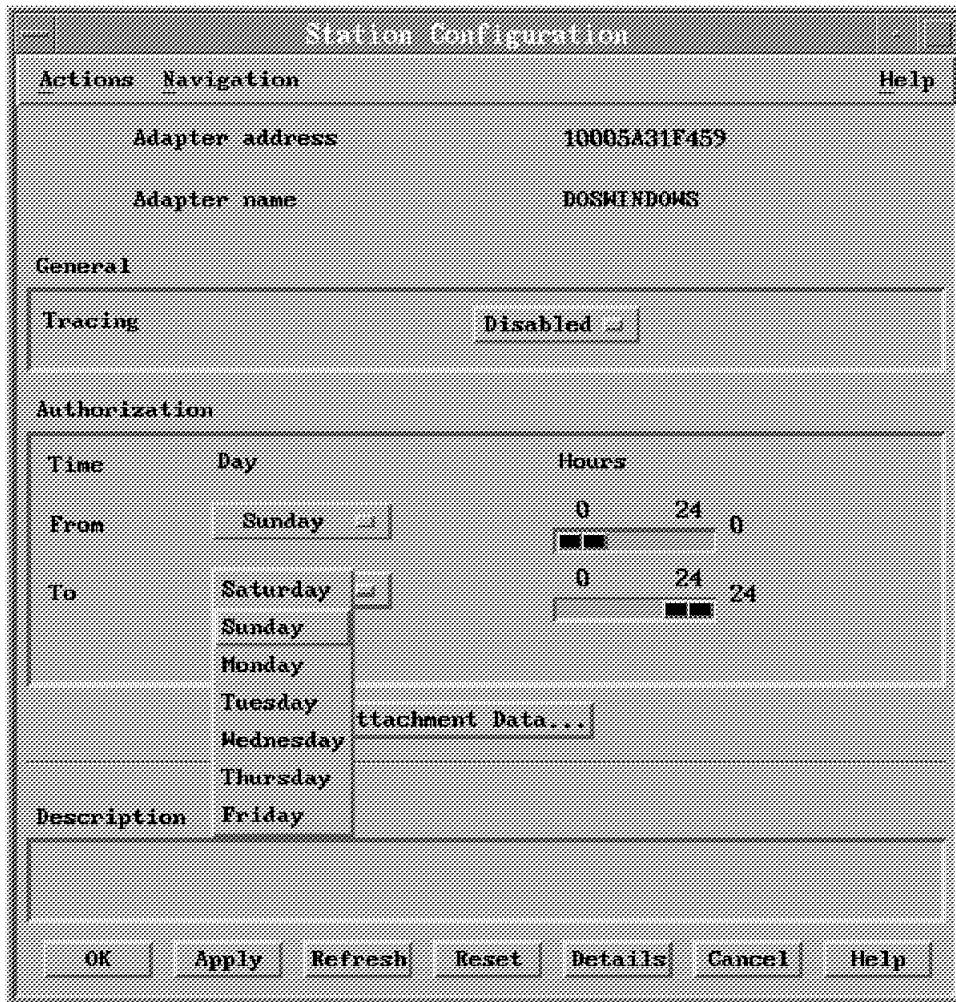


Figure 212. LNM for AIX Context Pull-Down Menu

At this point the LNM environment has been configured to prevent unauthorized access to the network from this station.

Following is a diagram of the environment; we will step through the flow of the information in this scenario.

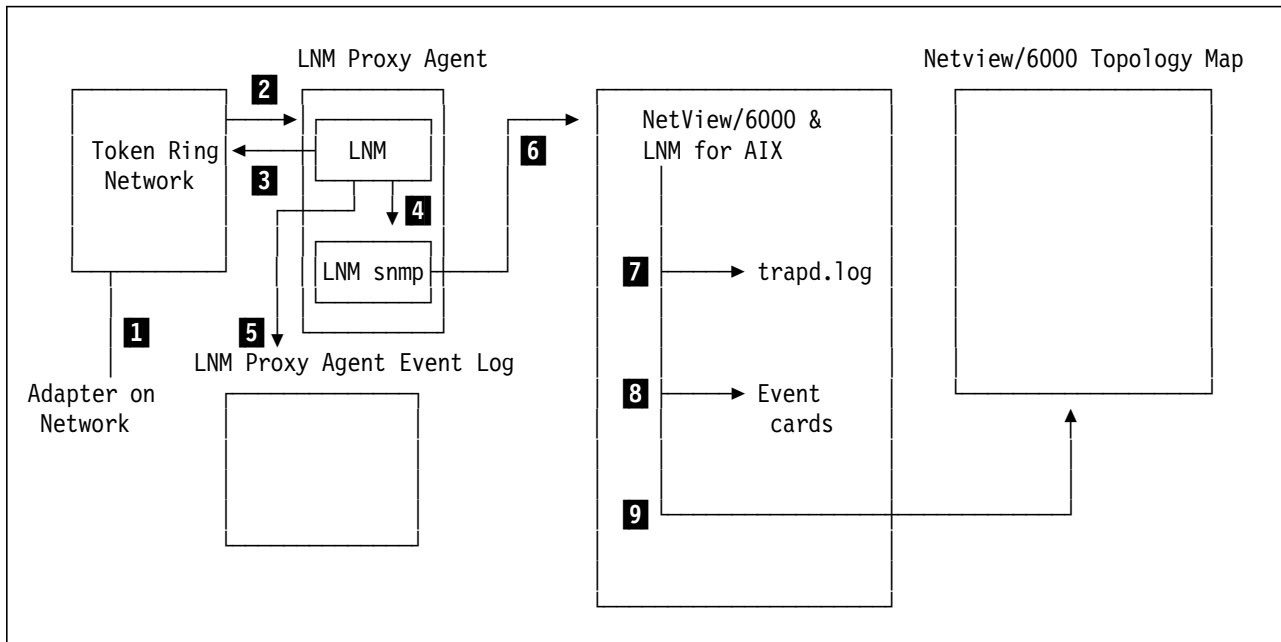


Figure 213. LNM for AIX Environment

- 1** The station is powered up and the adapter inserted into the token-ring network.
 - 2** OS/2 LNM detects that a new adapter has entered the network.
 - 3** OS/2 LNM detects the adapter is unauthorized and disables the adapter.
 - 4 and 5** LNM generates several alerts:
 - NAUN changes (since adapter has left network).
 - Unauthorized adapter on the network.
 - Adapter removed.
- Each alert was logged in the LNM proxy agent's local event log and sent to the SNMP component of LNM.
- 6** Each alert is converted to an SNMP trap and sent to the AIX NetView/6000 application.
 - 7** All traps received are logged in the trapd.log file.
 - 8** The major alerts are displayed in the event cards of AIX NetView/6000.
 - 9** No topology update occurs.

Following are the traps received in the trapd.log file for this scenario, as shown in Figure 214 on page 221.

```

1
767370383 7 Wed Apr 27 14:33:30 1994 aixagent1 A Trap 220 from Enterprise lnm6000: Naun change for segment 0x05 81.
Station address: 0x10 00 5a 31 f4 59
A NAUN address: 0x10 00 5a e8 8a 04
2
767370383 7 Wed Apr 27 13:33:31 1994 aixagent1 A Trap 220 from Enterprise lnm6000: Naun change for segment 0x05 81.
Station address: 0x40 00 00 03 33 42
A NAUN address: 0x10 00 5a 31 f4 59
3
767370383 7 Wed Apr 27 14:33:32 1994 aixagent1 A Trap 449 from Enterprise lnm6000: Adapter inserted on segment
0x05 81 at an unauthorized time or day.
A Adapter address: 0x10 00 5a 31 f4 59
A CAU ID: 0x00 00 00 00
A Lobe receptacle number: 0x00
4
767370384 2 Wed Apr 27 14:33:34 1994 loopback P Trap 449 from Enterprise lnm6000: Adapter inserted on segment
0581 at an unauthorized time or day.
P Resource label: 10005A31F459
P Adapter address: 10005A31F459
P CAU ID: 00000000
P Lobe Attachment Module number: 00
P Lobe receptacle number: 00
767370384 2 Wed Apr 27 14:33:34 loopback
767370384 2 Wed Apr 27 14:33:34 loopback
767370384 2 Wed Apr 27 14:33:34 loopback
767370384 2 Wed Apr 27 14:33:34 loopback
5
767370383 7 Wed Apr 27 14:33:37 1994 aixagent1 A Trap 220 from Enterprise lnm6000: Naun change for segment 0x05 81.
Station address: 0x40 00 00 03 33 42
A NAUN address: 0x10 00 5a e8 8a 04
6
767370392 7 Wed Apr 27 14:33:43 1994 aixagent1 A Trap 225 from Enterprise lnm6000: Adapter removed from segment
0x05 81 by LAN Network Manager.
A Adapter address: 0x10 00 5a 31 f4 59
7
767370392 3 Wed Apr 27 14:33:43 1994 loopback P Trap 225 from Enterprise lnm6000: Adapter removed from segment
0581 by LAN Network Manager.
P Resource label: 10005A31F459
P Adapter address: 10005A31F459
767370392 3 Wed Apr 27 14:33:43 loopback
767370392 3 Wed Apr 27 14:33:43 loopback

```

Figure 214. AIX NetView/6000 trapd.log File

Each log entry that has a value of 7 in the second field is a log- only type entry. A type 2 or 3 will create an event card in AIX NetView/6000.

- 1 and 2** Two NAUN changes as the adapters reflect their new NAUN adapters.
- 3** Adapter 10005A31F459 has been detected as accessing the network at an unauthorized time, the day being Wednesday.
- 4** Adapter 10005A31F459 has been detected as accessing the network at an unauthorized time, the day being Wednesday; this trap is also displayed in the AIX NetView/6000 event cards.
- 5** NAUN change, this indicates that the adapter has just been removed, since the NAUN information is for the adapter that had 10005A31F459 as its NAUN.
- 6** Adapter 10005A31F459 has been removed from the network.
- 7** Adapter 10005A31F459 has been removed from the network; this trap is also displayed in the AIX NetView/6000 event cards.

The two events are displayed in the AIX NetView/6000 event cards as shown in Figure 215 on page 222 and Figure 216 on page 222.

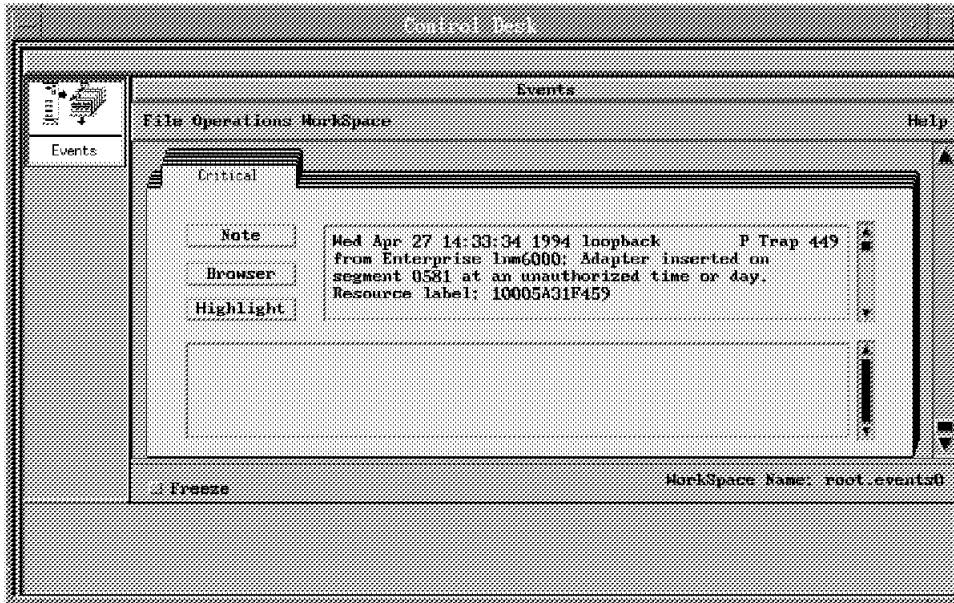


Figure 215. AIX NetView/6000 Unauthorized Access Event Card

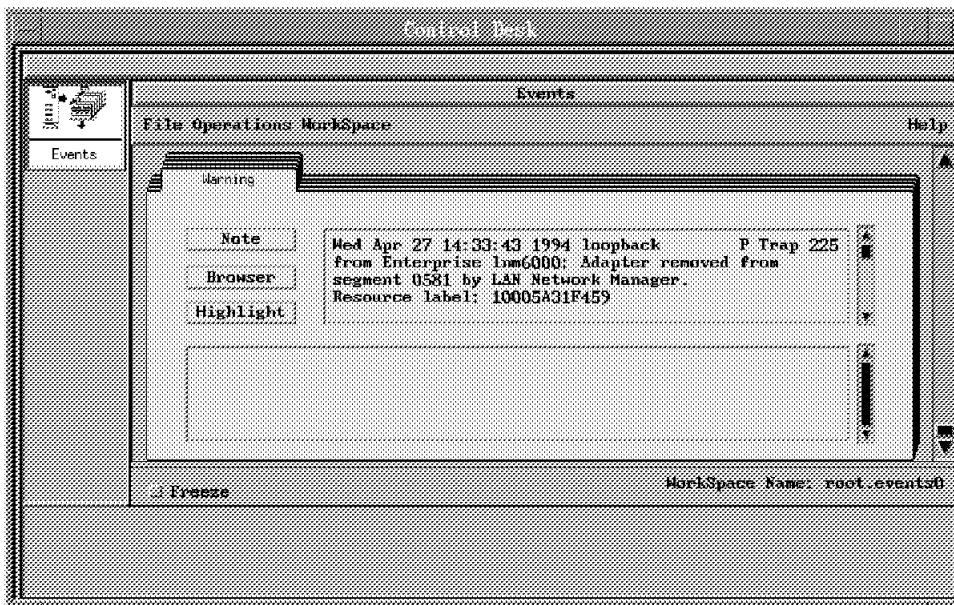


Figure 216. AIX NetView/6000 Adapter Removed Event Card

8.3 Virus Detected on a DOS/Windows Workstation

As we have discussed earlier in 2.5.2, “LMU/2 Configuration for DOS Stations” on page 54, the LMU/2 program provides some utilities to handle the detection of a possible virus. These utilities are DOSVIRGA in the DOS platform and VIRALERT in the OS/2 platform. The function of each of the utilities is the same.

- You have to run a virus-checking program. This means that the two utilities themselves do not detect the virus.
- Check the return code from the virus-checking program for a virus-detected condition (generally, any non-zero return code).
- Run the utility if the virus-detected return code is returned.

We will show an example using a DOS/Windows machine as the infected station. The steps that we will cover are:

- How to configure DOS/Windows station to send the alert.
- How to configure the fault manager station to handle this alert.
- The changes in the NetView/6000 program.
- The actions taken upon receipt of this warning will be:
 - Issue a remote command that will copy standard versions of the autoexec.bat and config.sys files, stored on a network drive, to the machine with the virus. This will not allow the infected machine to call the automatic network login procedures and possibly spread the virus.
 - Display a warning pop-up window in AIX.
 - Open an Incident Report in AIX Trouble Ticket/6000.
 - Disable the infected machine's adapter using IBM LAN Network Manager for AIX.

Refer to Chapter 2, "LAN NetView Management Utilities/6000" on page 43 for more details on the LMU/2 configuration and Chapter 3, "IBM LAN Network Manager for AIX" on page 75 for IBM LAN Network Manager for AIX matters.

8.4 Configuring the DOS/Windows Station

Before running the DOSVIRGA program, you must set the FAULT_MANAGER environment variable to address the fault manager station. This station is the one that you configured using the fault_manager option when running the LMUCUST utility. Use the following command to set this variable:

```
SET FAULT_MANAGER=fault_manager_station
```

Where *fault_manager_station* can be either a computer name if you are in an OS/2 LAN Server environment, or an internetwork address if you are in a NetWare environment.

We decided to create a batch file, called virus.bat, to simulate the virus detection. The content of this file was:

```
SET FAULT_MANAGER=00000009:400000033342
c:\1mu2\DOSVIRGA.COM
```

We decided to manually start this batch file but you might insert these lines in a batch file that would actually run the virus-checking program.

8.5 Configuring the Fault Manager Station

The configuration of the fault manager station consists of preparing a user-defined table to handle the alerts. This table identifies which alerts the fault manager is to process, and what action to take for each alert. The file name and location of this table are specified in the `lmui.ini` file and to modify these specifications, you have to edit the `lmui.ctl` file, and look for the following entry:

```
APP(LMU_UTILITY),
  KEY(FAULT_TABLE),
  ASCIIIZ(d:\LMU2\AUEUSER.TAB);
```

Change the ASCIIIZ entry to point to the file that you are using. Please refer to "Fault Manager-Related File" on page 53 for more details on this table. In the virus case, the entries in the user-defined table are:

# Product/ # Appl Id	Alert Type	Alert Desc	Source	Target	Auto Thresh	Notify Thresh	Auto Timer	Notify Timer	Command
5622153	11	C000	*	*	0000Y	0000Y	0	0	-\$b Alert from -\$c is -\$t
5622153	11	C000	*	00000009:400000033342	0000Y	0000Y	0	0	LMUPOPUP "Alert from -\$c" "-\$t"

The first entry causes the fault manager station to send the virus alert. The token used is:

- \$b** This token indicates that the data from the alert is sent both to the LMU/2 GUI and the LMU/2 SNMP proxy agent.
- \$c** Substitutes the source computer name (computer name or internetwork address) wherever this token appears.
- \$t** Substitutes the SV-Parm subfield 82 text wherever this token appears. In our case, this text warns about the virus.

To make the changes effective, execute the following commands:

```
lmquery /tf auerecvr
detach auerecvr
```

You can include as many entries as you want to execute multiple commands and send multiple alerts. Another alternative is to specify a `.cmd` file to be executed and group all the commands in there.

8.6 Preparing AIX NetView/6000 to Receive a Virus-Detected Trap

Once we have configured the fault manager to send the alert to the SNMP proxy agent machine, this station will convert this alert into a trap and send it to the RISC System/6000 running AIX NetView/6000 and AIX LMU/6000.

The customization that has to be done is to prepare the AIX NetView/6000 program to start a shell script that executes a number of actions upon the receipt of that specific trap.

This customization is accomplished by selecting **Options...Event Configuration...Trap Customization: SNMP** in the AIX NetView/6000 main menu. In the Event Configuration dialog box that is opened, follow these steps:

- Select the **lmui2** enterprise name.

- Select the enterprise specific trap **10000006**. This is the trap that is sent by the SNMP proxy agent. When you make this selection, the format specification session of this dialog box is filled with the information related to that specific trap.

- Insert a command in the Optional Command and Argument Format field. The command that we chose to execute was:

/lmu/virus.detected \$2 \$8 \$10

The parameters that we used were:

\$2 The second parameter passed along with the trap specifies the node that has originated the alert.

\$8 This parameter provides the alert text.

\$10 The alarm time stamp is passed in this parameter.

At this point, the Event Configuration dialog box should look similar to Figure 217.



Figure 217. Event Configuration Dialog Box Showing the Virus Trap Customized

- Click on the **Replace** button on the right side of the dialog box and then click on the **OK** button at the bottom of it.

8.7 Automated Actions Against a Virus Detected-Trap

Following is a diagram of the environment to illustrate the flow of the information in this scenario.

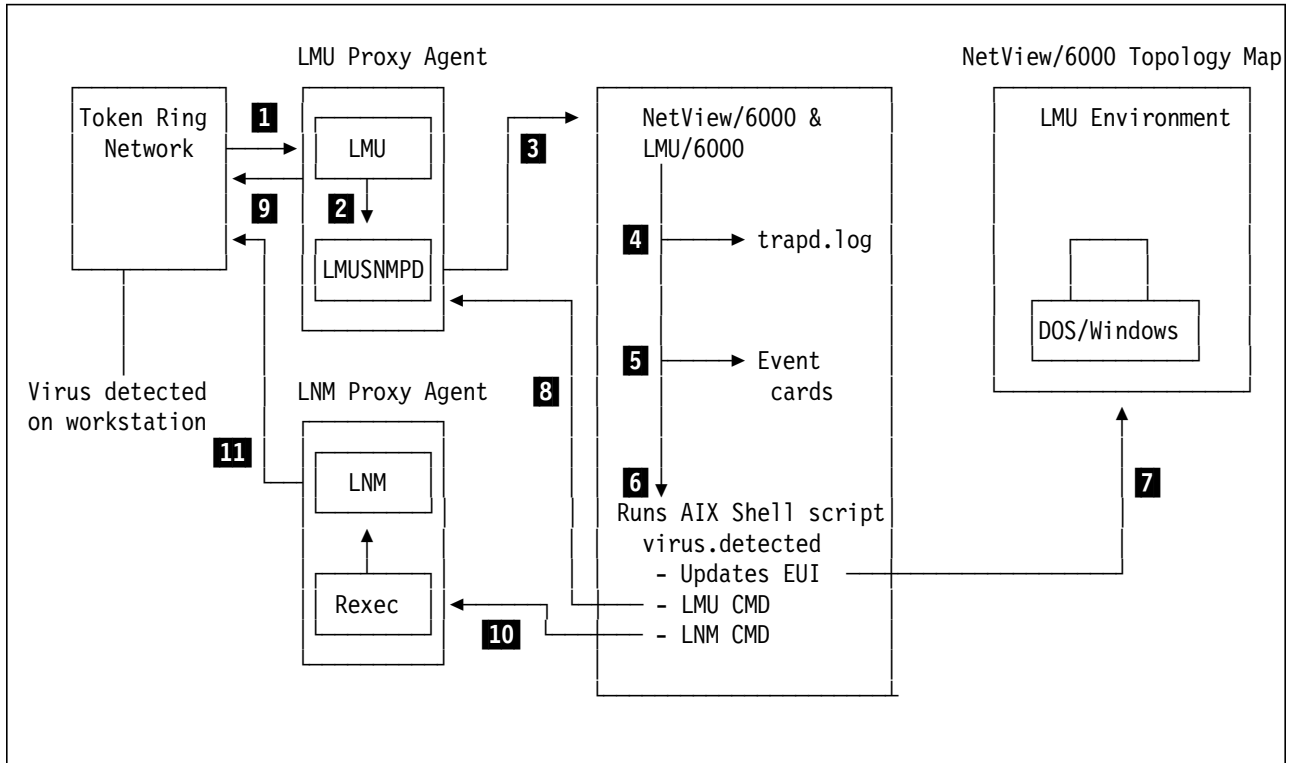


Figure 218. LNM for AIX Environment

- 1** The workstation detects the virus and sends an alert to LMU/2.
- 2** LMU sends this information to the LMU GUI and to the SNMP proxy agent.
- 3** The SNMP proxy agent converts the alert into a trap and sends it to AIX NetView/6000 and to AIX LMU/6000.
- 4** The trap is logged in the trapd.log file.
- 5** The trap is converted into an event card and displayed in the event card application.
- 6** The virus.detected shell script is started.
- 7** The shell script updates the symbol status to a marginal state.
- 8** An LMU/2 remote command is sent to the administrator machine, that happens to be the same SNMP proxy agent, specifying that new config.sys and autoexec.bat files will be copied to the infected station.
- 9** The command is sent to the infected machine and the files are copied.
- 10** An REXEC command is sent to the LNM proxy agent executing an LNM command to disable the workstation's adapter.
- 11** The command is sent to the workstation and its adapter is disabled.

The automated actions that are going to be performed are fully based on the contents of the shell script that you specify in the Event Configuration dialog box.

As soon as the virus alert is sent, the LMU GUI signals with an audible alarm. Its window frame flashes and the icon representing the infected machine becomes striped. If you click on this icon and select **Windows...Display Events** or double click with the right button it will show the events related to that machine, as shown in Figure 219.

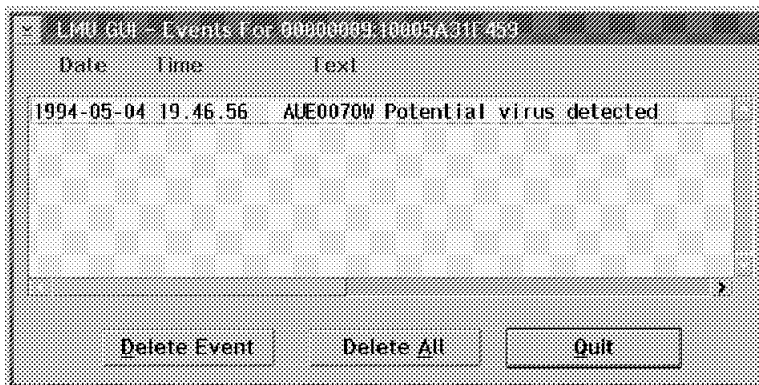


Figure 219. LMU/2 GUI Showing the Virus Event Received

Also the LMUPOPUP utility is executed and the warning window is shown in Figure 220.

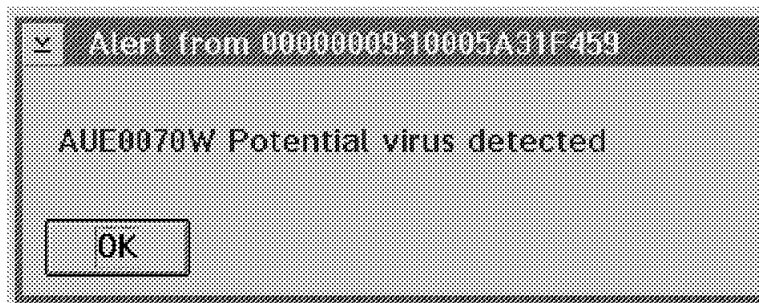


Figure 220. LMUPOPUP Utility Warning about the Virus

All the traps that are received by AIX NetView/6000 are stored in the trapd.log file, located in the /usr/OV/log directory. The entries that show the virus-detected trap coming from the SNMP proxy agent are shown in Figure 221 on page 228.

```

768233751 3 Fri May 06 10:15:51 1994 aixagent2 P
768233751 3 Fri May 06 10:15:51 aixagent2 P LMU Alert.
768233751 3 Fri May 06 10:15:51 aixagent2 P Station:0000
0009:10005A31F459
768233751 3 Fri May 06 10:15:51 aixagent2 P Alert from 0
0000009:10005A31F459 is AUE0070W Potential virus detected
768233751 3 Fri May 06 10:15:51 aixagent2 P Priority:0
768233751 3 Fri May 06 10:15:51 aixagent2 P TimeStamp:19
94-05-06 10.17.12
768233751 3 Fri May 06 10:15:51 aixagent2 P Domain:
768233751 3 Fri May 06 10:15:51 aixagent2 P Userid:
768233751 3 Fri May 06 10:15:51 aixagent2 P Managing:
768233751 3 Fri May 06 10:15:51 aixagent2 P NodeAddress:
10005A31F459

```

Figure 221. Excerpt from the trapd.log File Showing the Virus Trap

This information is also converted into an event card and it is shown in Figure 222.

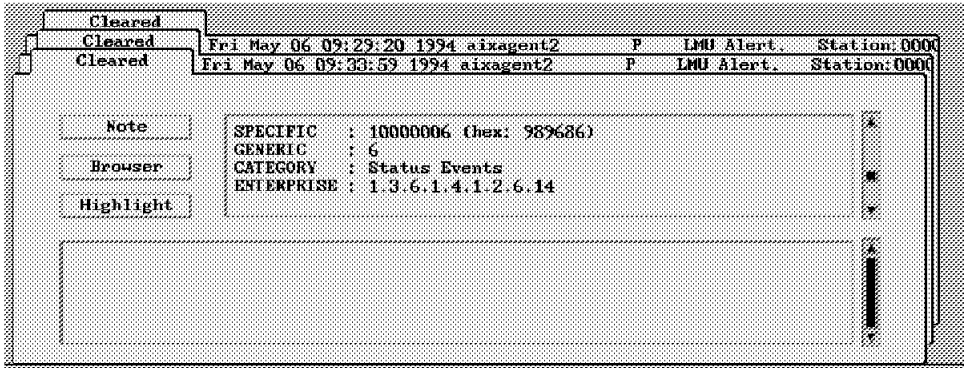


Figure 222. Event Card Showing Additional Information about the Virus Trap

Notice that we have scrolled the event card bar down to the middle to show the enterprise ID (1.3.6.1.4.1.2.6.14), the generic trap (6) and the specific trap (10000006).

As was shown in Figure 218 on page 226 the following steps are commands to be executed by the LMU and LNM proxy agents. We chose to copy new autoexec.bat and config.sys files in order to disable the station to automatically connect to the network at its next startup. And as an immediate action, we disabled the adapter, thus preventing the virus from spreading to other machines in the network.

Appendix A. LMU-Related File

A.1 LMU.CTL File

```
#####
# IDENTIFIES THE PATH AND FILENAME OF THE LMU PROFILE. #
# THE LMU PROFILE MUST RESIDE ON THE OS/2 BOOT DRIVE AND #
# HAVE THE NAME LMU.INI #
#####

DEFINE_PROFILE INI_FILE(C:\LMU.INI)

#####
#
# THE FOLLOWING PARAMETERS DO NOT HAVE A DEFAULT VALUE #
# AND MUST BE MODIFIED BEFORE USING THE COMPONENT WHICH #
# REFERENCES THEM: #
#
# MANAGING_SYSTEM #
# MANAGING_SYSTEM_WITH_DATABASE #
# FAULT_MANAGER #
# GRAPHICAL_USER_INTERFACE #
# SNMP_PROXY_AGENT #
# SNMP_PROXY_INFORMATION #
#
#####

#####
# THE FOLLOWING PARAMETERS APPLY TO ALL WORKSTATIONS. #
#####

# The computername or internetwork address specified
# identifies this workstation's managing system.
# Ex. LMUMANG (IBM requester)
# or
# Ex. 000000A1:100012345678 (NetWare requester)

APP(LMU_UTILITY),
    KEY(MANAGING_SYSTEM),
    ASCIIZ(00000009:400000033342);

# The computername or internetwork address specified
# identifies this workstation's managing system with database,
# which is the system maintaining the LMU database.
# Ex. LMUMANG (IBM requester)
# or
# Ex. 000000A1:100012345678 (NetWare requester)

APP(LMU_UTILITY),
    KEY(MANAGING_SYSTEM_WITH_DATABASE),
    ASCIIZ(00000009:400000033342);

# The computername or internetwork address specified identifies this
```

```

# workstation's fault manager, which is the system to receive alerts
# generated by the LMU applications.
# Ex. FAULTMAN (IBM requester)
#       or
# Ex. 000000A1:100012345678 (NetWare requester)

```

```

APP(LMU_UTILITY),
    KEY(FAULT_MANAGER),
    ASCIIIZ(00000009:400000033342);

```

```

# Identifies the location of the file to contain
# the messages issued by LMU.

```

```

APP(LMU_UTILITY),
    KEY(MESSAGE_LOG),
    ASCIIIZ(d:\LMU2\LMU.LOG);

```

```

# Identifies the LAN adapter used in NetBIOS communications.
# Value 00 indicates the primary adapter and value 01 indicates
# the secondary adapter. This key is optional and if not
# specified the primary adapter (00) will be used.
#
# NOTE: The hexnum value for LAN_ADAPTER must be specified
# as 2 hexadecimal digits (for example, 01).

```

```

APP(LMU_UTILITY),
    KEY(LAN_ADAPTER),
    HNUM(00);

```

```

# Identifies the location in which the *.BND files were
# installed.
# Managing System and SNMP Proxy Agent workstations using
# database ONLY.

```

```

APP(LMU_UTILITY),
    KEY(BIND),
    ASCIIIZ(d:\LMU2);

```

```

#####
# THE FOLLOWING PARAMETERS APPLY TO "MANAGED SYSTEMS".      #
#####

```

```

# Identifies the frequency in minutes that the heartbeat
# function will send a message to the managing system.
#
# NOTE: The hexnum value must be specified as 4 hexadecimal
#       digits, e.g. (000A) to indicate 10 minutes.
#
# If '0000' is specified only the initial and terminal
# heartbeats are sent.

```

```

APP(LMU_UTILITY),
    KEY(PULSE_RATE),
    HNUM(0005);

```

```
#####
# THE FOLLOWING PARAMETERS APPLY TO "MANAGING SYSTEMS". #
#####
```

```
# Identifies the file to contain
# the node description change log.
```

```
APP(LMU_UTILITY),
    KEY(CHANGE_LOG),
    ASCIIIZ(d:\LMU2\CHANGE.LOG);
```

```
# Identifies the location to which transferred
# files are to written.
```

```
APP(LMU_UTILITY),
    KEY(FILE_PATH),
    ASCIIIZ(d:\LMU2);
```

```
#####
# THE FOLLOWING PARAMETERS APPLY TO "FAULT MANAGER" #
# WORKSTATIONS. #
#####
```

```
# Identifies the Fault Manager's input user table.
# For example C:\LMU2\AUEUSER.TAB
```

```
APP(LMU_UTILITY),
    KEY(FAULT_TABLE),
    ASCIIIZ(d:\LMU2\AUEUSER.TAB);
```

```
# Alerts can be forwarded to a specific adapter address if desired.
# This key is optional and if not specified the default LAN management
# functional address of 'C00000002000' is used.
```

```
APP(LMU_UTILITY),
    KEY(FM_FORWARDING_ADDR),
    ASCIIIZ(C00000002000);
```

```
# Identifies the computer names and/or internetwork addresses
# of the GUI workstations to the FAULT MANAGER.
```

```
#
# Note: The character values for this field must be specified as
# character fields separated by a comma.
# Ex. (LMUGUI,000000A1:100012345678)
```

```
APP(LMU_UTILITY),
    KEY(GRAPHICAL_USER_INTERFACE),
    ASCIIIZ(00000009:400000033342);
```

```
# Identifies the computer names and/or internetwork addresses
# of the SNMP Proxy Agent workstations to the FAULT MANAGER.
```

```
#
# Note: The character values for this field must be specified as
# character fields separated by a comma.
```

```

# Ex. (LMUSNMPD,000000A1:100012345678)

APP(LMU_UTILITY),
  KEY(SNMP_PROXY_AGENT),
  ASCIIZ(lmusnmpd,00000009:400000033342);

#####
# THE FOLLOWING PARAMETERS APPLY TO "SCHEDULER" #
# WORKSTATIONS. #
#####

# Identifies the path and file name of the Schedule log file
# For example C:\LMU2\SCHEDULE.LOG

APP(LMU_UTILITY),
  KEY(SCHEDULE_LOG),
  ASCIIZ(d:\LMU2\SCHEDULE.LOG);

# Identifies the path and file name of the Schedule file
# For example C:\LMU2\SCHEDULE.TIM

APP(LMU_UTILITY),
  KEY(SCHEDULE_FILE),
  ASCIIZ(d:\LMU2\SCHEDULE.TIM);

# Identifies the path and file name of the Schedule group file
# For example C:\LMU2\SCHEDULE.GRP

APP(LMU_UTILITY),
  KEY(SCHEDULE_GROUP_FILE),
  ASCIIZ(d:\LMU2\SCHEDULE.GRP);

# Identifies the frequency in minutes that the schedule
# file will be checked for changes.
# For example 60

APP(LMU_UTILITY),
  KEY(SCHEDULE_READ),
  ASCIIZ(60);

#####
# THE FOLLOWING PARAMETERS APPLY TO "ADMINISTRATOR" #
# WORKSTATIONS RUNNING THE GRAPHICAL USER INTERFACE (GUI). #
#####

# Indicates additional managing systems to be queried
# at GUI startup.
#
# Note: The character values for this field must be specified as
# character fields separated by a comma.
# For example: (LmuMgr,HelpDesk,Ops1).

#APP(LMU_UTILITY),
# KEY(GUI_ADDITIONAL_MANAGING_SYSTEMS),
# ASCIIZ(computername or internetnetwork address,...);

```

```

# Indicates the type of view to be displayed at GUI startup.
#
# For additional information see GUI documentation.

APP(LMU_UTILITY),
    KEY(GUI_INITIAL_DISPLAY),
    ASCIIZ(A);

# Indicates which symbol is associated with the thirteen types of
# view objects.
#
# NOTE: The hexnum value for this field must be specified
# as 26 hexadecimal digits, e.g. (04030A0806020709050B01120E).
# For additional information see GUI documentation.

APP(LMU_UTILITY),
    KEY(GUI_NODE_SYMBOLS),
    HNUM(04030A0806020709050B01120E);

# Indicates the text color and background color to be used
# when commands are submitted via the GUI.
#
# Note: The character values for this field must be specified
# as two 2-digit numbers separated by a comma, e.g. (34,47)
# to indicate white text on a black background.
# For additional information see GUI documentation.

APP(LMU_UTILITY),
    KEY(GUI_COLORS),
    ASCIIZ(34,47);

# Indicates the name and the nominal point size, in tenths, of the
# image font used to display all text in the GUI window.
#
# Note: The character values for this field must be specified as a
# character field and a 3-digit number separated by a comma,
# e.g. (Helv,100) to indicate Helvetica 10 point.
# For additional information see GUI documentation.

#APP(LMU_UTILITY),
#    KEY(GUI_FONTS),
#    ASCIIZ(System Proportional,120);

# Identifies the location of the file to contain
# command sequences store by the GUI.

APP(LMU_UTILITY),
    KEY(GUI_COMMANDS_TABLE),
    ASCIIZ(d:\LMU2\LMUGUI.TAB);

# Specifies which pattern is used to indicate that a node
# has received alerts or that a collection has subordinate

```

```

# nodes that have received alerts.
#
# NOTE: The hexnum value for this field must be specified
# as 2 hexadecimal digits, e.g. (0C) to indicate medium
# density, diagonal hash marks.
# For additional information see GUI documentation.

APP(LMU_UTILITY),
    KEY(GUI_PATTERN),
    HNUM(0C);

# Indicates if the view is to be refreshed when a resource is
# added due to the arrival of an event for an unknown workstation
# that matches the type of resources being displayed.
# Coding N or n indicates that an automatic refresh is not done.
#
# For additional information see GUI documentation.

APP(LMU_UTILITY),
    KEY(GUI_AUTO_REFRESH),
    ASCIIZ(Y);

# Indicates the height and width ratios that will be used as the
# aspect ratio for the ellipse used to display the workstations.
#
# Note: The character values for this field must be specified as
# two 3-digit numbers separated by a comma, e.g. (480,640) to
# indicate an ellipse that approximates the height to width ratio
# of a standard file monitor in 640 X 480 mode.
# Note: specifying (001,001) will result in a circle.
# For additional information see GUI documentation.

APP(LMU_UTILITY),
    KEY(GUI_COORDINATES),
    ASCIIZ(001,001);

# Indicates the resource layout limit to be used when displaying
# the GUI views.
#
# Note: The character value for this field must be specified as
# a 3-digit number. For example: (020) to indicate that up to
# 20 resources will be displayed as an ellipse, while 21 or more
# will be displayed in rows and columns.
# For additional information see the GUI documentation.

APP(LMU_UTILITY),
    KEY(GUI_RESOURCE_LAYOUT_LIMIT),
    ASCIIZ(020);

#####
# THE FOLLOWING PARAMETERS APPLY TO "SNMP PROXY AGENT" #
# WORKSTATIONS. #
#####

# Indicates additional managing systems to be queried
# at SNMP Proxy Agent startup.

```



```

#
# Note: The character values for this field must be specified as
# character fields separated by a comma.
# For example: (LmuMgr,HelpDesk,Ops1).

#APP(LMU_UTILITY),
#   KEY(PROXY_ADDITIONAL_MANAGING_SYSTEMS),
#   ASCIIZ(computername or internetwork address,...);

#####
# THE FOLLOWING PARAMETERS APPLY TO "LAN NETVIEW" (LMULNV) #
# WORKSTATIONS. #
#####

# Identifies the LMU SNMP Proxy Agents to be queried at LMULNV
# startup. Specify the IP address (or host name) along with
# a community name for each proxy agent. The community name
# defaults to "public" if not specified.
#
# For example: ([LmuProxy,public],[9.179.7.66,rtp],[9.179.7.50,]).

#APP(LMU_UTILITY),
#   KEY(SNMP_PROXY_INFORMATION),
#   ASCIIZ([hostname,community],...);

#####
# THE FOLLOWING PARAMETERS APPLY TO THE APPWATCH UTILITY. #
#####

# Identifies the path and file name of the application watch table.
# For example C:\LMU2\APPWATCH.SMP

APP(LMU_UTILITY),
    KEY(APPWATCH_TABLE),
    ASCIIZ(d:\LMU2\APPWATCH.SMP);

```

A.2 USERVPD.CFG File

```

1) Assigned_user           [Suzuki, Roberto Shiguo   ]
2) User Serial #          [123456]
3) User department #      [123]
4) User Internal Phone #  [123-4567]
5) User External Phone #  [919-123-4567]
6) Building                [anyone]
7) Floor                   [lowest]
8) Location Office #      [somewhere]
9) Location Internal Phone # [321-7654]
10) Location External Phone # [919-321-7654]
11) Owning_Manager        [Boss      ]
12) Owning_Department     [XYZ]
13) T/R Port ID           [XXXX]
14) Power Outlet          [XXXXXXX]
15) Equipment
    Format: {Machine_Type,Model,Serial_Number,Date_Installed}
-----
[Start of equipment
  {IBM-8580,001,23-1234567,09-01-1992}   System Unit
  {IBM-8514,001,00-1097175,09-01-1992}   Display

```

{IBM-8513,001,23-CLV46,09-01-1992}	Display
{IBM-1391401,,4655517,09-01-1992}	Keyboard
{IBM-90X6778,,1306518,09-01-1992}	Mouse
{IBM-4216,031,41-8886A,09-01-1992}	Printer
{IBM-6180,,B1506,09-01-1992}	Plotter
End of equipment]	

A.3 LMU.INI File

```
[LMU_UTILITY]
MANAGING_SYSTEM=00000009:40000033342
MANAGING_SYSTEM_WITH_DATABASE=00000009:40000033342
FAULT_MANAGER=00000009:40000033342
PULSE_RATE=5
MESSAGE_LOG=d:\LMU2\LMU.LOG
```

A.4 LMUBIND.CTL File

The following property and value identify the LMU Managing System.

```
property(MANAGING_SYSTEM)    value(00000009:40000033342)
```

The following property and value identify the LMU Managing System which also has the database containing the LMU data and tables.

```
property(M_WITH_DATABASE)    value(00000009:40000033342)
```

The following property and value identify the internet address of the LMU fault manager machine.

```
property(FAULT_MANAGER)      value(00000009:40000033342)
```

The following property and value identify the volume and path and name of where the message log for LMU will be written.

```
property(MESSAGE_LOG)        value(SYS:\LMU2\LMU.LOG)
```

The following property and value identify the pulse rate (minutes) interval the client is expected to maintain.

```
property(PULSE_RATE)         value(00010)
```

Index

Numerics

- 8250 Intelligent Hub
 - does not use proxy agents 2
- 8260 Intelligent Hub Program Management Family

A

- agent
 - proxy 4
 - LMU 4
 - OS/2 4
- AIX
 - in management workstation console 1

C

- configuration
 - AIX LMU/6000 48
 - DOS/Windows station 223
 - Fault Manager station 224
 - IHMP/6000 142
 - LAN Network Manager 80, 81
 - defining proxy agents 81
 - LMU/2 49
 - for DOS stations 54
 - for NetWare servers 56
 - for OS/2 stations 49
 - for Windows stations 55
 - RMONitor for AIX 107
 - policies, defining 114
 - RMONitor Agent for OS/2 111
 - RMONitor for AIX 107
 - trap information 113
 - Router and Bridge Manager/6000 154
 - USERVPD.CFG file 235

D

- Database Manager 2/2
 - installation and configuration 30
- DOS
 - proxy agents 2
- DOS workstation
 - installation 47
- DOS/Windows

E

- environment, IP networks 23

F

- file
 - LMU.CTL 229
 - LMU.INI 236

- file (*continued*)
 - LMUBIND.CTL 236
 - USERVPD.CFG 235

I

- IBM LAN Network Manager for AIX
 - configuration 80
 - LNM for AIX 81
 - description 75—99
 - functions
 - AIX NetView/6000 integration 75
 - configuration information 76
 - fault information 76
 - FDDI segment management 76
 - graphical user interface 75
 - integration with hub management applications 76
 - performance information 76
 - resource monitoring 76
 - SNMP token-ring management 76
 - token-ring segment management 75
 - installation 76
 - IBM LAN Network Manager for AIX 77
 - OS/2 proxy agent 77
 - operations 89
 - overview 75
 - starting LAN Network Manager 85
 - starting LNM for AIX 86
 - starting OS/2 LNM proxy agent 89
- IHMP (Intelligent Hub Management Program)
- IHMP Family (Intelligent Hub Management Program Family)
- IHMP Family for the IBM 8260
- IHMP/6000 (Intelligent Hub Management Program/6000)
 - configuration 142
 - description 139
 - installation 141
 - overview 139
 - startup 144
- installation
 - AIX LMU/6000 45
 - AIX Trouble Ticket/6000 167
 - Database Manager 2/2 30
 - IHMP/6000 141
 - LAN Network Manager 76, 77
 - LNM for AIX 77
 - OS/2 proxy agent 77
 - LMU/2, for DOS stations 47
 - LMU/2, for NetWare servers 47
 - LMU/2, for OS/2 stations 46
 - LMU/2, for Windows stations 47
 - RABM/6000 153
 - RISC System/6000 software 40

installation (*continued*)
 RMON 102
 RMONitor Agent for OS/2 103
 RMONitor for AIX 102
 TCP/IP for OS/2 30
integration
 database 21
 Map 8
 product overview 1–42
 scenarios 205, 228
 status propagation 19

L

LAN Network Manager
 operations 89
 starting 85
LMU/6000
 description 43–73
 functions 44
 installation 45
 network view 4
 operation 59
 overview 43
 prerequisites 44
 starting the program 64
 startup 57
 submaps 59
 using the program 68
LMU.CTL file 229
LMU.INI file 236
LMUBIND.CTL file 236

N

NetView/6000
NetWare
 servers, configuration 56
 servers, installation 47
NetWare Server 4

O

OS/2
 in management workstation console 1
 proxy agents 2
OS/2 workstation
 installation 46
overview
 AIX LMU/6000 1
 AIX NetView/6000 Network View 1
 IBM LAN Network Manager for AIX 1

P

policies
 defining 114
 types 114
 agent 114
 collection 114

R

RABM/6000 (Router and Bridge Manager/6000)
 description 153–163
RISC System/6000
 software installation 40
RMONitor Agent for OS/2
 configuration 111
RMONitor for AIX
 configuration 107
 description 101–138
 installation 102
 starting RMONitor 122
rules
 RMONitor for AIX and RMONitor Agent for OS/2 114
 agent rules 114
 collection rules 115
 threshold rules 115

T

TCP/IP for OS/2
 installation 30
trap information
 configuring 113
 defining 114
Trouble Ticket/6000
 description 165–204

U

USERVPD.CFG file 235

W

workstation

AIX NetView/6000 LAN Integration**Publication No. GG24-4332-00**

Your feedback is very important to help us maintain the quality of ITSO Bulletins. **Please fill out this questionnaire and return it using one of the following methods:**

- Mail it to the address on the back (postage paid in U.S. only)
- Give it to an IBM marketing representative for mailing
- Fax it to: Your International Access Code + 1 914 432 8246
- Send a note to REDBOOK@VNET.IBM.COM

Please rate on a scale of 1 to 5 the subjects below.
(1 = very good, 2 = good, 3 = average, 4 = poor, 5 = very poor)

Overall Satisfaction	_____		
Organization of the book	_____	Grammar/punctuation/spelling	_____
Accuracy of the information	_____	Ease of reading and understanding	_____
Relevance of the information	_____	Ease of finding information	_____
Completeness of the information	_____	Level of technical detail	_____
Value of illustrations	_____	Print quality	_____

Please answer the following questions:

- a) If you are an employee of IBM or its subsidiaries:
- | | | |
|--|----------|---------|
| Do you provide billable services for 20% or more of your time? | Yes_____ | No_____ |
| Are you in a Services Organization? | Yes_____ | No_____ |
- b) Are you working in the USA? Yes_____ No_____
- c) Was the Bulletin published in time for your needs? Yes_____ No_____
- d) Did this Bulletin meet your needs? Yes_____ No_____

If no, please explain:

What other topics would you like to see in this Bulletin?

What other Technical Bulletins would you like to see published?

Comments/Suggestions: (THANK YOU FOR YOUR FEEDBACK!)

Name

Address

Company or Organization

Phone No.



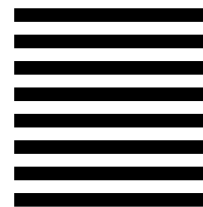
Fold and Tape

Please do not staple

Fold and Tape



NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES



BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM International Technical Support Organization
Department 545, Building 657
P.O. BOX 12195
RESEARCH TRIANGLE PARK NC
USA 27709-2195



Fold and Tape

Please do not staple

Fold and Tape



Printed in U.S.A.

GG24-4332-00

