Integrating NetWare Management into NetView for AIX

October 1995

IBM

International Technical Support Organization

Raleigh Center

IBM
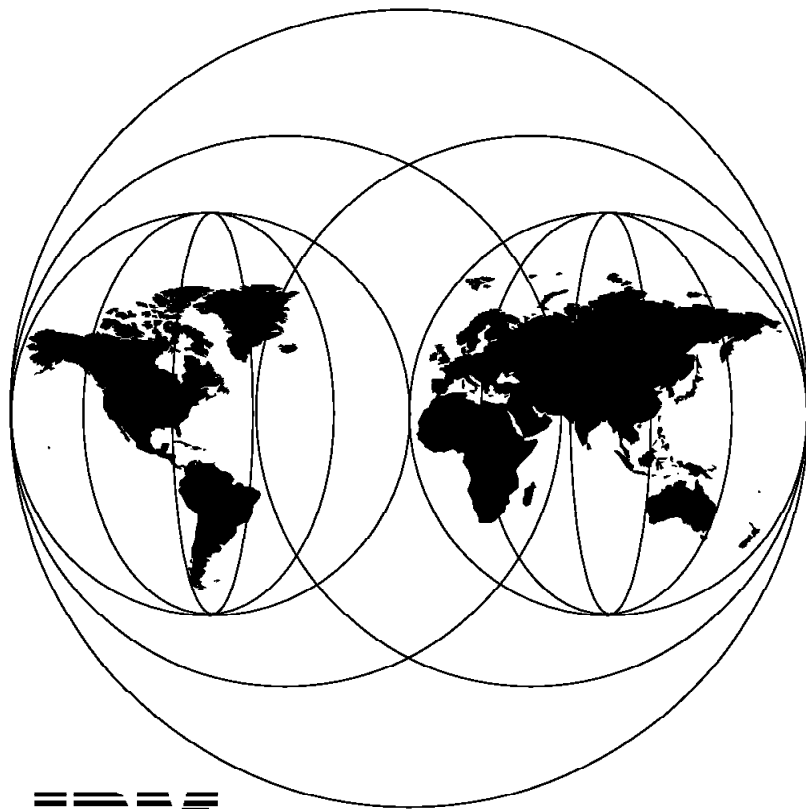
International Technical Support Organization

Integrating NetWare Management into NetView for AIX

October 1995

┌─ **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 (October 1995)

Abstract

This document is unique in its detailed coverage of NetView for AIX and its interactions with the Novell NetWare environment. It focuses on how to start managing a NetWare network using NetView for AIX. The version of code used in this book enabled topology information to flow between the NMS server and NetView for AIX's topology database. It also shows how to take advantage of LMU/6000 and LMU for OS/2 to begin managing the NetWare LANs.

This document was written for technical professionals who have already installed NetView for AIX and NetWare 4.01, but are managing the two environments independently. Some knowledge of NetView for AIX and NetWare is assumed.

(298 pages)

Contents

Figures

Tables

Special Notices

This publication is intended to help technical support personnel manage Novell NetWare networks from the NetView for AIX management platform. The information in this publication is not intended as the specification of any programming interfaces that are provided by NetView for AIX or Novell NetWare Management System. See the PUBLICATIONS section of the IBM Programming Announcement for NetView for AIX 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, 500 Columbus Avenue, Thornwood, NY 10594 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 are trademarks of the International Business Machines Corporation in the United States and/or other countries:

AIX	DATABASE 2
DB2/2	IBM
Micro Channel	NetView
OS/2	RISC System/6000
RMONitor	RS/6000
400	

The following terms are trademarks of other companies:

Windows is a trademark of Microsoft Corporation.

PC Direct is a trademark of Ziff Communications Company and is used by IBM Corporation under license.

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

C-bus is a trademark of Corollary, Inc.

AppleTalk	Apple Computer, Incorporated
Intel Corporation	
IPX, LANalyzer, NetWare, NetWire, SCSI	Novell, Incorporated
NDIS	3Com Corporation
NFS	Sun Microsystems Incorporated

Other trademarks are trademarks of their respective companies.

Preface

This document is intended to explain the functional capabilities of NetView for AIX's Openmon feature and Novell's NetWare Management System. These capabilities are illustrated by examples and scenarios. The document focuses on the setup of the environments, which is the most difficult part of the management processes.

This document is intended for use by persons who are involved with the installation of distributed systems management using IBM's NetView for AIX and Novell's Netware Management System.

How This Document Is Organized

The document is organized as follows:

- Chapter 1, "Overview of the Environment"

  This chapter provides an overview of the environment that we used to show how to use all of the functions that relate to managing NetWare from NetView for AIX. It describes what the components are, and how they fit into the framework for systems management.

- Chapter 2, "Installation"

  This chapter describes the installation process for all of the systems management pieces of NetView for AIX that relate to Openmon management, as well as the NetWare-related installations. In addition, other OS/2 and DOS products are described from an installation perspective.

- Chapter 3, "Clients"

  This chapter describes the functions of the agents that are used in the systems management processes.

- Chapter 4, "NetWare Tools"

  This chapter describes how to configure and use the Netware Management System (NMS) functions.

- Chapter 5, "Integrating Novell NMS Topology into NetView for AIX"

  This chapter describes how to set up the communications between the NetWare Management System and NetView for AIX.

- Chapter 6, "Activating an LMU Client on a Remote Workstation"

  This chapter describes a scenario where the LMU function is activated on a remote client workstation.

- Chapter 7, "Automated Response to an NMA Alarm/Trap"

  This chapter describes a scenario where automation is set up to create a trouble ticket on AIX when a trap is received from the NetWare environment.

- Chapter 8, "Using LMU for AIX to Help Manage NetWare Servers and Clients"

  This chapter shows how to manage the NetWare console from NetView for AIX and how to send commands using LMU.

- Appendix A, "DOS and NetWare Files"

This appendix provides sample configuration files for the DOS, DOS/Windows, and NetWare environment.

- Appendix B, "OS/2 System Files"

  This appendix provides sample configuration files for OS/2.

Related Publications

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

- *NetView for AIX Installation and Configuration*, SC31-6237
- *NetView for AIX Administrator's Guide*, SC31-7192
- *Trouble Ticket for AIX Version 3 Release 2 User's Guide*, SC31-7160-01
- *LAN NetView Management Utilities for OS/2 Installation and Configuration Version 1.1*, SC30-3637-01
- *LAN NetView Management Utilities for OS/2 User's Guide Version 1.1*, SC30-3555-04
- *Novell NetWare 3.12 Concepts*
- *Novell NetWare 3.12 Installation and Upgrade*
- *Novell NetWare 3.12 Workstation Basics and Installation*
- *Novell NetWare 3.12 Workstation for DOS and Windows*
- *Novell NetWare 3.12 Workstation for OS/2*
- *Novell Netware 3.12 System Administration*
- *Novell NetWare 3.12 Utilities Reference*
- *Novell NetWare 3.12 TCP/IP Transport Supervisor's Guide*
- *ManageWise 1.0 Setup Guide*
- *ManageWise 1.0 NMS Software: Getting Started*
- *ManageWise 1.0 NMS Software: Managing NetWare Servers*
- *ManageWise 1.0 LANDesk Manager Tools*

International Technical Support Organization Publications

- *NetWare Client for OS/2 Installation and Configuration*, GG24-3891-01
- *AIX NetView/6000 LAN Integration*, GG24-4332

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

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

To get a catalog of ITSO technical publications (known as redbooks), VNET users may type:

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

A listing of all redbooks, sorted by category, may also be found on MKTTOOLS as ITSOCAT TXT. This package is updated monthly.

How to Order ITSO Technical Publications

IBM employees in the USA may order ITSO books 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 MasterCard are accepted. Outside the USA, customers should contact their local IBM office. Guidance may be obtained by sending a PROFS note to BOOKSHOP at DKIBMVM1 or E-mail to bookshop@dk.ibm.com.

Customers may order hardcopy ITSO books individually or in customized sets, called BOFs, which relate to specific functions of interest. IBM employees and customers may also order ITSO books in online format on CD-ROM collections, which contain books on a variety of products.

ITSO Redbooks on the World Wide Web (WWW)

Internet users may find information about redbooks on the ITSO World Wide Web home page. To access the ITSO Web pages, point your Web browser (such as WebExplorer from the OS/2 3.0 Warp BonusPak) to the following:

```
http://www.redbooks.ibm.com/redbooks
```

IBM employees may access LIST3820s of redbooks as well. Point your web browser to the IBM Redbooks home page:

```
http://w3.itsc.pok.ibm.com/redbooks/redbooks.html
```

Acknowledgments

This project was designed and managed by:

Barry D. Nusbaum
International Technical Support Organization, Raleigh Center

The authors of this document are:

Caroline Truong
IBM France

Debbie Sparg
IBM South Africa

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:

Fergus Stewart
International Technical Support Organization, Raleigh Center

Chapter 1. Overview of the Environment

This chapter provides an overview of the physical and logical layout of the ITSO environment, as well as a topology view of the two separate logical networks. We show how to enable the new Openmon functions in NetView for AIX and the new NetWare NetExplorer functions, and then how to merge the management of the two networks.

We also define terms that are used in AIX, as well as in the Novell environment. In addition, this chapter provides an overview of the components that were involved in this residency.

Since we use multiple levels of code, the environment shown in Figure 1 is only a representative of the environments that were used for the scenarios in this book. We use AIX V3.2.5 as well as AIX V4.1.3, and NetView for AIX V3.1 and V4.1. For our NetWare servers, we use V4.01 and V4.1. There are other products with multiple releases, but these are the most important ones for our scenarios.
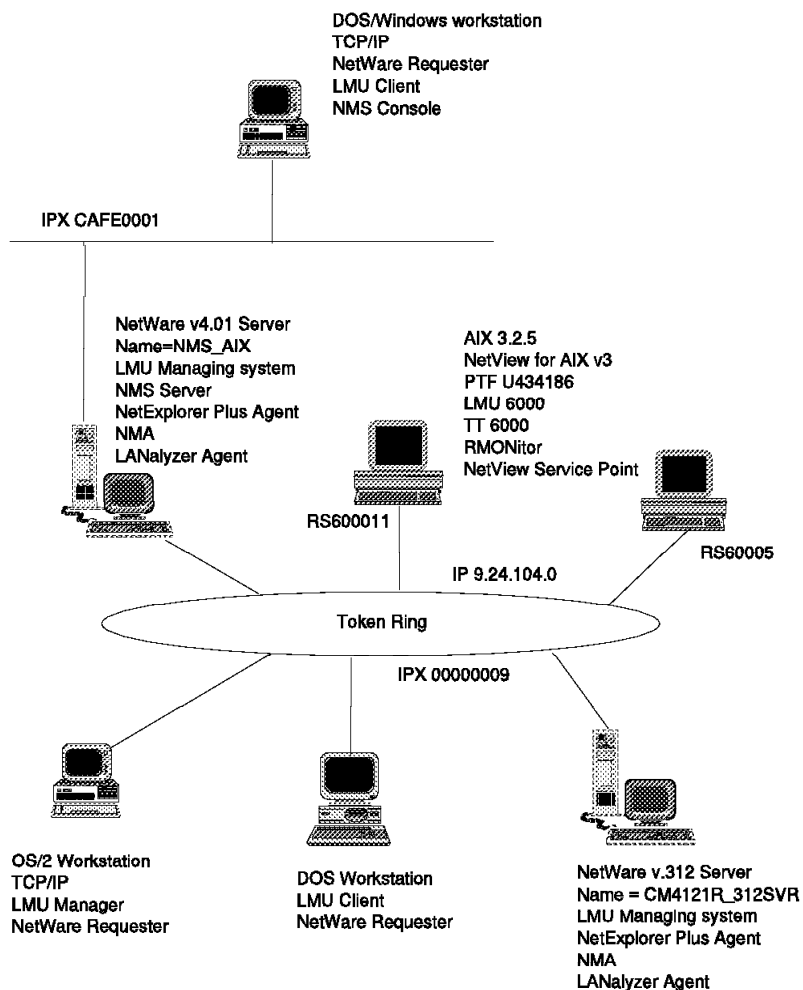
Figure 1. Residency Environment Schema

1.1 NetView for AIX

NetView for AIX is an open management platform for multi-vendor, heterogeneous networks. It was originally a manager of TCP/IP networks using the SNMP protocol. Enhancements now provide support for non-IP network topologies, based on the IBM generic topology model. In this project we investigate the integration of the IPX topology with NetView for AIX. This is provided by the new Openmon function of NetView for AIX (PTF U438561) and NMS Export Services for NMS 2.0.

Openmon enables the user to create an application to interact with an agent that represents a specific non-IP topology (in our case IPX). The application stores the information obtained from the agent in the Generic Topology Manager (gtmd) database. The data can be viewed from the NetView for AIX graphical interface and appears as standard topology submaps. The NetView for AIX help pages describe the Openmon function, as follows:

Purpose
To load non-IP topology information from an Openmon topology
agent into the NetView for AIX program.

Description
The Openmon function enables you to create an application to
interact with an agent that represents a specific non-IP
topology. The application stores the information obtained from
the agent in the Generic Topology Manager (gtmd) database. The
data can be viewed from the NetView for AIX graphical interface
and will be displayed as standard topology submaps.

The following terms are used in this description:
Openmon topology agent   An agent that discovers a non-IP
                                topology and passes data to an
                                Openmon topology application
Openmon topology application   An application, created by the
                                Openmon function, that receives
                                topology data from an Openmon
                                topology agent and stores the
                                data in gtmd
Openmon   A NetView for AIX function that
                                enables the user to create and
                                configure an Openmon topology
                                application.
Ordinarily, you will create one Openmon topology application to
interact with each separate agent.

Configuring an Openmon Topology Application
The Openmon configuration program, openmonconf, can be used to
set up and configure an Openmon topology application to interact
with an Openmon topology agent. You can execute the Openmon
configuration program by selecting Administer..Openmon
Application..Start Openmon Configuration Program from the NetView
for AIX main menu bar.

Warning: Make sure that the Openmon topology delete program is
not running while an Openmon application is running and loading
topology information into NetView for AIX. The Openmon topology
delete program might delete objects unexpectedly.
Use the Openmon configuration program to perform the following
tasks:
o   Initially set up the files and perform the necessary steps to
     create a new Openmon topology application to interact with a
     topology agent:
     -   Specify a name for the application.
     -   Set up the configuration file for the application.
     -   Set up the local registration file and register the
         application with NetView for AIX.
     -   Start up the application process to interface with a
         topology agent (if needed). Or the application can be
         started at a later time.
o   Dynamic update of a configuration file for an Openmon
     topology application:
     -   Select a configuration file to be updated.
     -   Change the value(s) of the configuration file.
     -   Start the application process if it is not already
         running. Or if the application process is running,
         notify it that the configuration file has been changed.
For more information about the Openmon Configuration Program
dialog box, see the help panel accessible from that dialog box.

Figure 2. NetView for AIX Openmon Help Part 1 of 2

```
Related Functions

Deleting the Discovered Topology
The Openmon topology delete program, openmondel, can be used to
delete the non-IP topology from NetView for AIX.  The openmondel
program can delete all topology starting at a root object and all
the objects below the root object, or delete one part of the
topology starting at a network segment object.  See the help
panel for Using the Openmon Application for the steps to delete
topology data.

Replacing the Discovered Topology
If you need to replace the information that has been stored for a
particular topology, you should first delete the existing
topology information using the topology delete program, and then
execute the appropriate Openmon topology application to re-load
the topology information.

Controlling an Openmon Topology Application
When an Openmon topology application is started, it will create
an object icon under the root object named applicationRoot and
the parent submap named nvApplications.  You can view the
application object by opening the applicationRoot submap from the
Root map, and opening the nvApplications submap.

After an Openmon topology application has been properly
configured, you can control it either through the NetView for AIX
menu or by using the commands ovstart, ovstop, and ovstatus.  You
can perform the following actions on an openmon topology
application:
o   Start the application by using the ovstart appname command or
    by selecting the application's icon and then selecting
    Tools..Start/Query/Stop Daemon Process..Start daemon from the
    main menu.
o   Stop a daemon by using the command ovstop appname command or
    by selecting the application's icon and then selecting
    Tools..Start/Query/Stop Daemon Process..Stop daemon from the
    main menu.
o   Check the status of an Openmon topology application by using
    the ovstatus appname command or by selecting the
    application's icon and then selecting Tools..Start/Query/Stop
    Daemon Process..Query daemon from the main menu.
```

Figure 3. NetView for AIX Openmon Help Part 2 of 2

1.2 LMU for AIX and LMU for OS/2

LAN Management Utilities for AIX (LMU for AIX), using an SNMP Proxy agent
called LMUSNMPD that is part of LMU for OS/2, provides a topology view and
management of both IPX and NetBIOS networks. For the purpose of this project
we only discuss the management of IPX networks. The reasons we include LMU
for AIX in this project are:

- At this time, the integration between NetView for AIX and NMS only provides
  the NetWare topology. We used LMU for AIX to get more information about
  the IPX resources and to send commands to these resources.
- We compared the IPX topology information received from NMS with that
  received from LMU for AIX.

1.3 Trouble Ticket for AIX

Trouble Ticket for AIX provides complete problem management which includes automatic assignment, escalation, service level agreements, notifications and more. It also has a systems inventory function. In this scenario we look at how management of the IPX resources can be integrated with Trouble Ticket for AIX.

1.4 Event Configuration

It is possible to configure NMA to send traps about servers it is managing to NetView for AIX. We show how to do this and how to configure the traps/events in NetView for AIX.

1.5 RMONitor for AIX

RMONitor for AIX is used for performance monitoring of token-ring and Ethernet segments. We will look at the integration of RMONitor for AIX with Novell's RMON agent LANalyzer. We installed PTF U434878, which provides support for the LANalyzer product.

1.6 NetWare (3.12, 4.x) Server and Clients

NetWare V3.12 and NetWare V4.x represent the most popular versions of NetWare Operating System products and are critical resources to manage in a network.

NetWare's native protocol is IPX/SPX. NetWare OSs are multiprotocol platforms. They achieve this using the Novell ODI (open data-link interface).

NetWare 4.x or 3.12 workstations use a multiprotocol environment in two different ways:

- Novell ODI (open data-link interface)
  ODI is the most common used in NetWare environment. It's a complete Novell interface and it's more flexible (Load and Unload the module from memory, for example is really useful).

  The three components of ODI are:
  – MLID (Multiple Link Interface Driver), which is provided by the LAN Adapter Manufacturer
  – LSL (Link Support Layer), the Novell interface for ODI providing the link between the MLID driver and the protocol stack
  – Protocol Stack, which is an OSI level 3 protocol stack such as IPX, IP or Appletalk
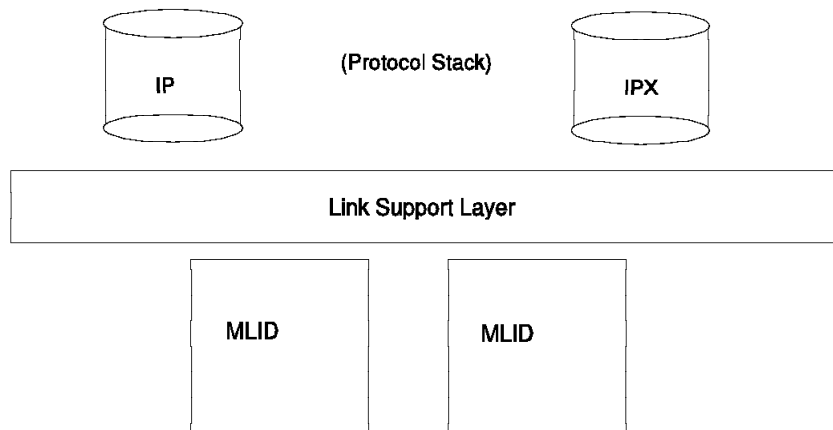
Figure 4. Open Data-Link Interface (ODI)

- NDIS
  NDIS is usually used in a NetWare native environment to provide NetBEUI or NetBIOS services more easily in conjunction with any communication product, such as IBM communication products.

Both solutions provide IPX/SPX and TCP/IP (and other protocols) support on the same network adapter to communicate simultaneously with NetWare servers and UNIX servers.

ODI and NDIS drivers are usually provided with every LAN Adapter board from any manufacturer.

We cover both of them in the installation sections of this book.

NetWare servers can be managed three different ways:

- Novell NetWare Management System (NMS)
- ManageWise (NMS & Intel LANDesk)
- IBM LAN NetView Management Utilities (LMU)

They can now be integrated into NetView for AIX. Integration of these products is covered in this book.

1.7 NetWare Management System (NMS)

NMS is a Novell product that provides management of NetWare servers, hubs and routers, as well as monitoring and analyzing networks.

It runs in a Microsoft Windows-based operating environment.

NMS supports token-ring or Ethernet networks running IPX or IP protocols.

The NetWare Management Agent software is installed on each NetWare Server you want to manage.

Novell developed a new function called Export Services which enables you to retrieve the NMS discovered network topology from the NMS Database and transmit it to other network management systems, like NetView for AIX. This new function represents real integration of NetWare server management with NetView for AIX.

1.8 NetExplorer

NMS has two components:

- NMS Console, which contains the NetExplorer Manager Software
- NMS Server, which runs with the NetExplorer Agent Software

The NetExplorer Agent discovers network devices and places them in a file so they can be forwarded to the NetExplorer Manager that is executing on the same machine as the NetWare Console.

1.9 NetWare Management Agent (NMA)

The Novell NetWare Management Agent Software is not an NMS component. It is packaged separately, by server license, and is completely integrated into the NMS platform. If you have ManageWise, you get NMA integrated into the package.

The NetWare Management Agent software installed on all servers makes it possible for NMS to display real time server performance, configuration and alarm data.

1.10 LANalyzer

Novell LANalyzer is another product that can be installed on the NMS platform; it is packaged separately. If you have ManageWise, you get LANalyzer integrated into the package.

LANalyzer has two components:

- The LANalyzer Agent Software running on servers (one on each segment)
- The LANalyzer Options of the NMS Console Manager

The NetWare LANalyzer Agents discover devices, provide statistics, and detect events on each segment on which they are installed.

In addition, if requested by the NMS console/LANalyzer option, they will also capture packets.

The LANalyzer Agent is now supported by IBM RMONitor for AIX with PTF U434878, which provides an integration with NetView for AIX.

1.11 Alerts/Traps

NMA can forward alerts/traps to NetView for AIX. We show how this is done and how events are configured in NetView for AIX.

NetWare LANalyzer is running as an RMON agent and can forward alerts/traps to NetView for AIX. We show how this is done in NetView for AIX.

Chapter 2. Installation

This chapter documents the installation of NetView for AIX and NetWare functions that are necessary to provide management capability on the AIX platform. The customization of the following products is shown before we integrate them:

- NetView for AIX PTF for Openmon
- RMONitor PTF
- IPX on all platforms
- TCP/IP on all platforms
- NMS 2.0
- NetExplorer
- NetWare Management Agent
- LANalyzer
- LMU on all platforms

2.1 Installing PTF U438561 for Openmon Function on NetView for AIX

PTF U438561 provides the Openmon function under NetView for AIX. Openmon is a function which enables you to create an application that interacts with an agent representing a specific non-IP topology. In our case, the agent is NMS Export Services representing the NMS topology (that is, the IPX topology). Your application stores the information it obtains from the agent in the Generic Topology Manager (GTM) database. This means that the non-IP topology that you have imported can be viewed from the NetView for AIX graphical interface and appears as standard topology submaps.

In addition, using NetView for AIX APIs and the gtmdump command, you can view or change the GTM database. The options for the gtmdump command are as follows:

```
Use gtmdump as described below:
gtmdump -h  or
gtmdump [-g <filename>]  or
gtmdump [-o <filename>] [-d <filename>] [-p <filename>]
gtmdump without options provides a gtmd database dump in stdout.

-h option provides a brief gtmdump help.

-g option specifies an output file for dumping gtmd database.

-o option specifies an output file that will print data in a
   readable format.

-d (debug) option specifies an output file that will print data in
   a format that could be used by NetView for AIX Team to
   reproduce the customer topology.

-p generates a program using nvot api basic routines to recreate
    the same topology in gtmd; this is a debug option also and our
    intention is to generate code for testing the basic routines,
    so we will neither provide support on this option nor guarantee
    the integrity of the code generated.

either -o, -d or -p options should be used to get the data that is
arriving in gtmd just after gtmd processed it.
```

Figure 5. gtmdump Options in NetView for AIX

To install PTF U438561, use SMIT or smitty. From the SMIT main menu:

- Choose **Software Installation and Maintenance**.
- Choose **Install / Update Software**.
- Choose **Install / Update Selectable Software (Custom Install)**.
- Choose **Install Subsystems (Selective Fixes)**.
- For the INPUT device, enter the device or directory that you are installing from.
- The options we used for our installation were:
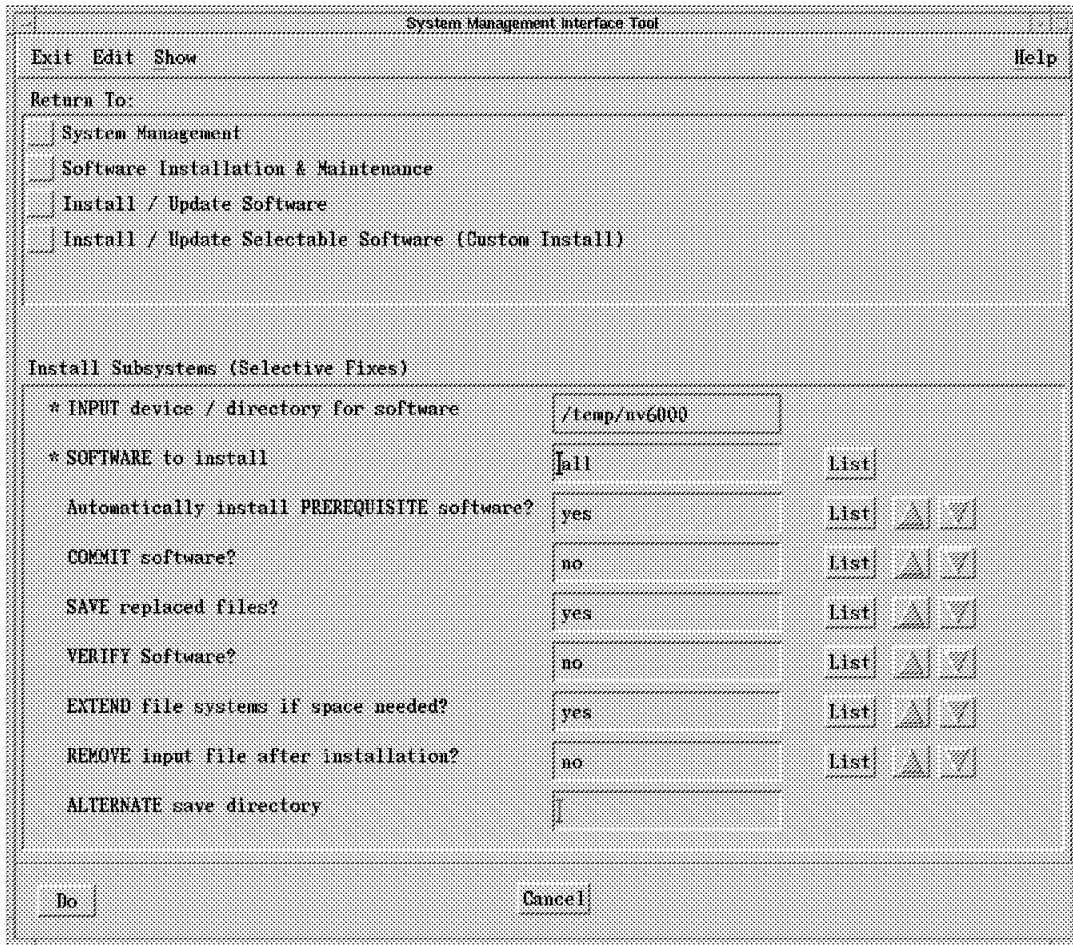
Figure 6. Installation Options

- The items we chose to install were:

```
┌─────────────────────────────────────────────────────────────────────────────┐
│                            Multi-select List                                 │
├─────────────────────────────────────────────────────────────────────────────┤
│  Select one or more items from the list.                                     │
│                                                                              │
│  SOFTWARE to install                                                         │
│                                                                              │
│  ┌─────────────────────────────────────────────────────────────────────┐    │
│  │ #───────────────────────────────────────────────────────────────     │    │
│  │ # Subsystems                                                         │    │
│  │ #───────────────────────────────────────────────────────────────     │    │
│  │ 3.1.0.0  nv6000                                          SS/ALL       │    │
│  │    3.1.0.0  nv6000.base.obj                              SS/ALL       │    │
│  │        NetView for AIX Base                              U434186      │    │
│  │    3.1.0.0  nv6000.database.obj                          SS/ALL       │    │
│  │        NetView for AIX Database                          U434186      │    │
│  │    3.1.0.0  nv6000.features.obj                          SS/ALL       │    │
│  │        NetView for AIX Features                          U434186      │    │
│  │                                                                       │    │
│  │                                                                       │    │
│  └─────────────────────────────────────────────────────────────────────┘    │
│                                                                              │
│  ┌──────────┐      ┌────────────┐      ┌──────────┐        ┌──────────┐       │
│  │   OK     │      │ Select All │      │  Cancel  │        │   Help   │       │
│  └──────────┘      └────────────┘      └──────────┘        └──────────┘       │
│                    ┌────────────┐      ┌────────────┐                         │
│                    │    Find    │      │ Find Next  │                         │
│                    └────────────┘      └────────────┘                         │
└─────────────────────────────────────────────────────────────────────────────┘
```
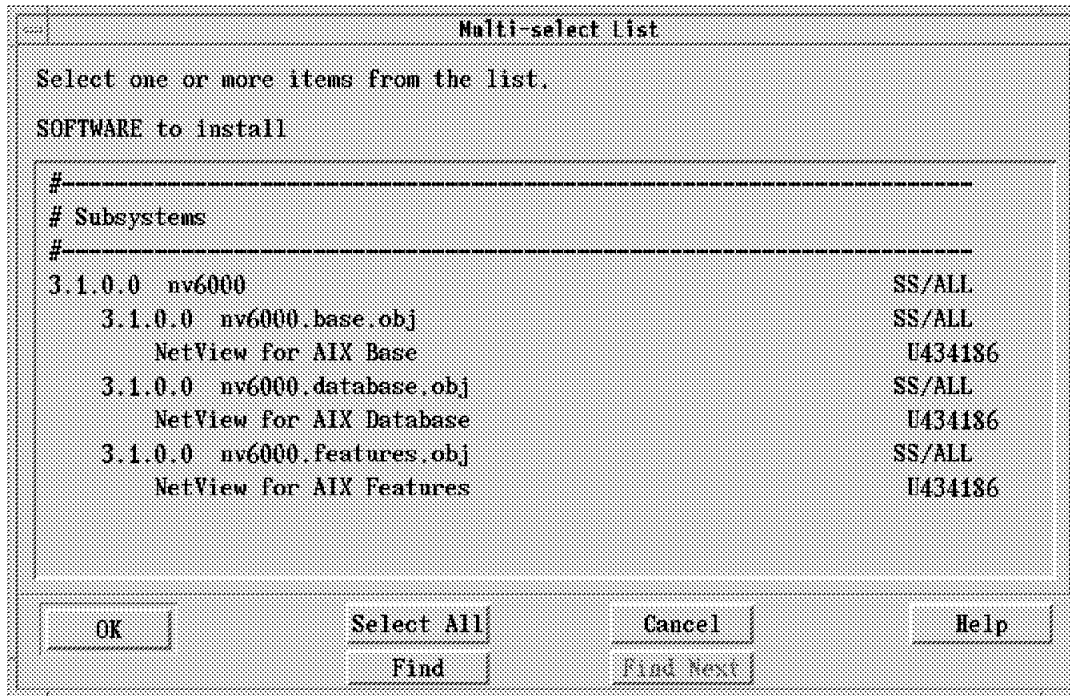
Figure 7. Installing NetView for AIX PTF, U438561

2.2 RMONitor PTF, U434878

PTF U434878 provides support for Novell's Ethernet LANalyzer product. LANalyzer does not yet fully support token-ring.

To install PTF U434878, use SMIT. From the SMIT main menu:

- Choose **Software Installation and Maintenance**.
- Choose **Install / Update Software**.
- Choose **Install / Update Selectable Software (Custom Install)**.
- Choose **Install Subsystems (Selective Fixes)**.
- For the INPUT device, enter the device or directory you are installing from.
- The options we use for our installation are:

Exit Edit Show   Help

Return To:

  System Management

  Software Installation & Maintenance

  Install / Update Software

  Install / Update Selectable Software (Custom Install)

Install Subsystems (Selective Fixes)

  * INPUT device / directory for software   /temp/rmonptfs

  * SOFTWARE to install   all   List

    Automatically install PREREQUISITE software?   yes   List ▲ ▼

    COMMIT software?   no   List ▲ ▼

    SAVE replaced files?   yes   List ▲ ▼

    VERIFY Software?   no   List ▲ ▼

    EXTEND file systems if space needed?   yes   List ▲ ▼

    REMOVE input file after installation?   no   List ▲ ▼

    ALTERNATE save directory

  Do   Cancel

Figure 8. Installation Options

- The items we chose to install were:

Multi-select List

Select one or more items from the list.

SOFTWARE to install

```
#------------------------------------------------------------------
# Subsystems
#------------------------------------------------------------------
1.1.0.0  RMONitor                                          SS/ALL
    1.1.0.0  RMONitor.base.obj                             SS/ALL
        RMONitor base product                             U434878
    1.1.0.0  RMONitor.dyna.obj                             SS/ALL
        RMONitor DynaText on-line book feature            U434878
```

  OK   Select All   Cancel   Help
                  Find   Find Next
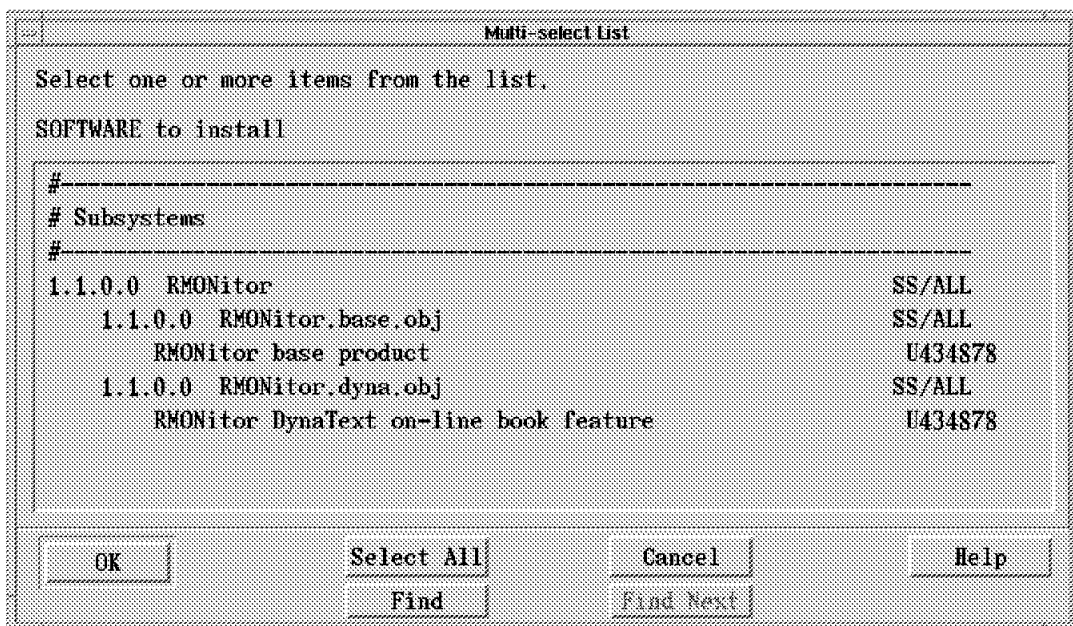
Figure 9. Installing RMONitor PTF U434878

2.2.1 Installing NetWare Server V3.12 under DOS

We install the NetWare 3.12 Server on a 386 processor under DOS 6.3. Our machine has 140 MB of hard disk space and 16 MB of RAM. We allocate a DOS partition of 20 MB, leaving the rest for the NetWare server.

2.2.2 Memory Considerations

In a NetWare V3.x environment you have to consider several things before installing and configuring your NetWare server.

The algorithm for the RAM needed on the NetWare v3.x server is:

```
RAM = (volume size in MB * 0.023) / block size
      ─────────────────────────────────────────

                   Per Volume
```

RAM is the minimum memory needed for the disk cache. This algorithm is for volume without a Name Space. If you are using any Name Spaces, replace the 0.023 value with 0.032 for the volume using a Name Space.

```
Minimum Memory =     RAM      +    2 MB     +   Memory to load NLMs
                  ───────────     ─────────     ──────────────────────
                  Memory for       Memory          Memory
                  the Disk Cache   for the OS   needed to load all the NLM
```

In addition, to exactly determine the memory you will need on the server, you have to consider that the minimum RAM available for the cache must be greater than or equal to 20% of the total memory.

To run the server in the most efficient configuration, the RAM available for the disk cache must be around 60%. This number assumes that you are running the appropriate NLMs the system needs and *doesn't* include the NLMs memory used.

The steps we follow to install the server are:

1. Insert the *Install* diskette in drive A:; change to drive A: and type:

   ```
   INSTALL.EXE
   ```
2. Choose **Install new NetWare V3.12** from the Select an Installation Option menu.
3. Name the File Server: CM4121R_312SVR.

   This name should be unique, from 47 to 298 alphanumeric characters, and contain no period or spaces.
4. Assign an IPX internal network number: C4121.

   This number should be unique (a hexadecimal number with one to eight digits).
5. Press Enter to copy the server boot files to the DOS partition.

   The server boot files include SERVER.EXE (the NetWare operating system), INSTALL.NLM, name spaces, and LAN drivers. We accept the default source path of A: and the default destination path of C:\SERVER.312.

   During the copy process, insert the NetWare diskettes you are prompted for into the source drive and press Enter. Once all the files are copied, the following language screen appears:

```
    Press Enter to view choices

    Country Code:        001    (United States)

    Code Page:           437    (United States English)

    Keyboard Mapping:    None
```

6. Enter your Country Code, Code Page, and Keyboard Mapping settings and press F10.

   For a list of settings for each field, highlight a field and press Enter.

   The following screen then appears:

```
    Select the format you desire and press Enter

    DOS Filename Format  (recommended)
    NetWare Filename Format
```

7. Selecting NetWare Filename Format leaves previously saved DOS files with non-standard DOS characters as they are.

   Selecting DOS Filename Formats replaces all non-standard DOS characters with standard DOS characters.

   Since our system was a new installation with no user files yet saved, we chose the NetWare Filename Format.

8. You are then asked if you want to specify any special startup commands. We selected **no**.
   This would be used mainly for changing the default setting of SET AUTO REGISTER MEMORY to OFF, which allows you to load disk drivers that cannot be loaded in the memory area above 16 MB.

9. When the copy process is complete, an optional step follows to add SERVER.EXE to your AUTOEXEC.BAT file. We chose not to do this since we chose to start the server manually.

10. Insert the Install diskette into the disk drive and press Enter. The INSTALL utility automatically executes SERVER.EXE.

    You will see the following message:

```
CM4121R_312SVR:
Loading
System_Console
NetWare 3.12  ( 5 user )
Internal Network Number:   000C4121
```

When the system is loaded you get the server prompt:

```
LOAD DISK DRIVER LOADABLE MODULES
```

After you have created a bootable disk partition for the server, you must load the disk drivers.

Load the disk drivers for the controller board in your file server B by typing the following and pressing Enter: LOAD disk-driver

For *disk-driver*, choose a driver from one of those shown in Table 1. We had a micro-channel PS2 and therefore chose the PS2ESDI driver.

Table 1. Disk Drive Determination

Type of Architecture	Controller Type	Add-On Board	Disk Driver
Industry Standard Architecture (ISA)	AT, MFM, RLL, ARLL	Built in	ISADISK
		Third-party secondary adapter	ISADISK
	ESDI		ISADISK /B
	IDE		IDE
	Novell SCSI	DCB	DCB
Micro Channel	ESDI	Built in	PS2ESDI
	MFM	Built in	PS2MFM
	IBM SCSI	IBM SCSI	PS2OPT
		Built in	PS2OPT
Extended Industry Standard Architecture (EISA)	AT class	Built in	ISADISK
		See vendor	ISADISK
	EISA vendor proprietary	Built in	See vendor
		See vendor	See vendor

2.2.3 Create NetWare Disk Partition Tables

Once the disk drives were loaded, we used the INSTALL.NLM to create a NetWare partition on the hard disk.

1. Type:

   `LOAD INSTALL`

2. Choose **Disk Options** from the Installation Options menu.
3. Choose **Partition Tables** from the Available Disk Options menu.
4. If you have more than one disk, choose the disk you need to partition from those listed on the Available Disk Drives menu.
5. Choose **Create NetWare Partition** from the Partition Options menu.

   NetWare allows only one NetWare partition per physical disk; so if you have more than one free partition on your disk, select a free area for the NetWare partition. NetWare will allocate 98% of the space as a data area and 2% for the Hot Fix redirection area. You will be given an option to accept or decrease the size of the NetWare partition.

2.2.4 Create Volume SYS:

Your NetWare partition must have a SYS: volume for storing the SYSTEM, PUBLIC, LOGIN, and MAIL directories.

1. To create the SYS: volume, choose **Volume Options** from the Installation Options menu.
2. Press the Insert key on the **Volumes** panel.
3. If you have more than one hard disk, choose one to place the first volume on the Free Space Available for Volume Segments panel. NetWare automatically enters volume SYS: as the first volume on the New Volume Information screen.

Its default size will be the entire partition. If you want to create more than one volume, enter the size of volume SYS: on the Initial Segment Size screen. The space not allocated for SYS: will then be available for additional volumes.

4. Press the Escape key and answer Yes to the Create Volume? prompt.

   Refer to the *Novell NetWare Installation and Upgrade Guide* for additional information and recommendations on creating volumes.

2.2.5 Mount Volumes

After creating volume SYS: you will need to mount it.

1. Choose **volume SYS:** from the volumes list.
2. Use the down arrow key to highlight the status field, press Enter and choose **Mount Volume**.
3. Press Escape to return to the Installation Options menu.

2.2.6 Copy System and Public Files

You now need to load the NetWare operating system and utility files into the file server's SYS:PUBLIC and SYS:SYSTEM directories.

1. From the Installation Options menu choose **Copy SYSTEM and PUBLIC Files**.
2. Insert the System_2 diskette and press Enter.
3. Follow the prompts for the other diskettes.

2.2.7 Load LAN Drivers and Frame Types

The next step is to load the LAN drivers and frame types. Choose LAN drivers for the cabling system and network boards you use. We chose the NTR2000 driver for token-ring support.

Type the following and press Enter:

```
LOAD LAN-driver
```

The final step is to bind the protocol to the LAN driver. Type the following:

```
BIND IPX To LAN_driver
```

You will be prompted to assign the network address. Each LAN driver must be assigned the network address that identifies the cabling system it uses to communicate with similar LAN drivers on the network. Please note that this network address is not the same as the internal IPX network number which we assigned previously to the file server. In our lab environment all NetWare file servers use network address 00000009, so we used this as our network address. The address should be a hexadecimal number from one to eight digits.

For more information on internal network numbers, see Chapter 3 of Network Numbering in the *NetWare 3.12 Concepts Guide.*

2.2.8 Create File Server Boot Files

NetWare 3.12 is now installed, but you still need to create the STARTUP.NCF and AUTOEXEC.NCF files, which are necessary to boot the file server.

The STARTUP.NCF file contains commands to load disk drivers and name space support for your file server. This file is executed before SERVER.EXE and is stored on the disk you boot from (in our case the hard disk). Once this file has loaded the disk drivers and name space support and mounted volume SYS:, it passes control over to AUTOEXEC.NCF to complete the boot process.

1. From the Available System Options menu, choose **Create STARTUP.NCF**.
2. Enter the path for STARTUP.NCF. Our path was:
   C:\SERVER.312\STARTUP.NCF
3. Press Enter.

   Here is our sample STARTUP.NCF file:

```
LOAD PS2ESDI slot=8
```

4. Press Escape to save the file.

The AUTOEXEC.NCF file contains the commands to complete the boot process after SERVER.EXE and STARTUP.NCF execute. This file is saved in and runs from SYS:SYSTEM. You should place most of your commands here. Some examples of things you would put in AUTOEXEC.NCF are:

- The name of the file server.
- Assign the server's internal network number.
- Load LAN drivers for the server and assign the network address.
- Bind LAN drivers to the server's registered protocol.
- Mount volumes.

1. From the Available System Options menu, choose the **Create AUTOEXEC.NCF** file.

   The operating system gathers information you have previously entered at the console prompt for the file. A screen, similar to the following, appears, showing the commands that are automatically placed in AUTOEXEC.NCF.

```
file server name CM4121R_312SVR
ipx internal net C4121
load NTR2000 slot=3 frame=TOKEN-RING name=TOKENIPX
bind IPX to TOKENIPX net=00000009
mount all
```

2. Press Escape to save the file.

For detailed information on setting up the network, which involves determining directory structure, adding users, groups, etc., refer to the *NetWare 3.12 Installation and Upgrade Guide*.

The following diagram illustrates the simple directory structure we set up:

```
                ┌─── LOGIN

                ├─── MAIL

SYS ────────────┼─── SYSTEM

                ├─── PUBLIC
                                  ┌─── SPARG
                └─── HOME ────────┼─── TRUONG

                                  └─── BARRY
```
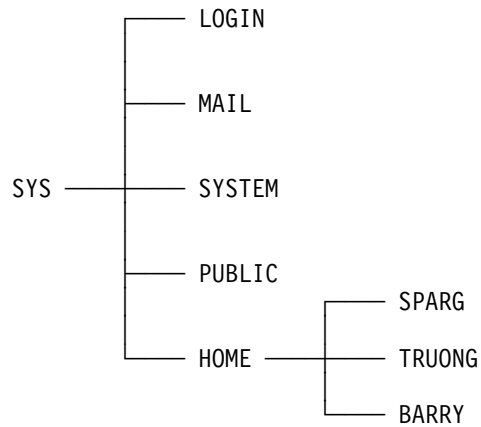
SYSCON is a utility that may be used to control accounting, file server, group, and user information. As supervisor, you can also control the network activities of the workgroup managers. The tasks you can do are organized according to the options in SYSCON's Available Options menu:
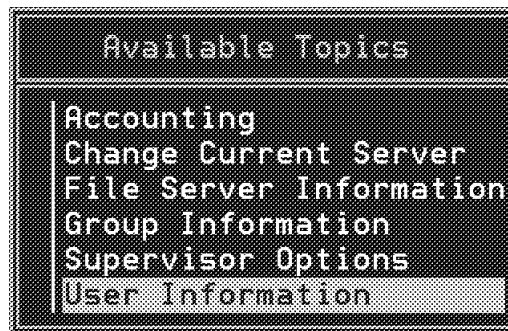
Figure 10. SYSCON Available Topics Menu

ADDING A NEW USER

1. Type SYSCON and choose **User Information** from the Available Topics menu.

Figure 11. List of User Names

2. To create a user, press Insert. The User Name entry box appears. Enter the user's name. The user name can be up to 47 characters long.
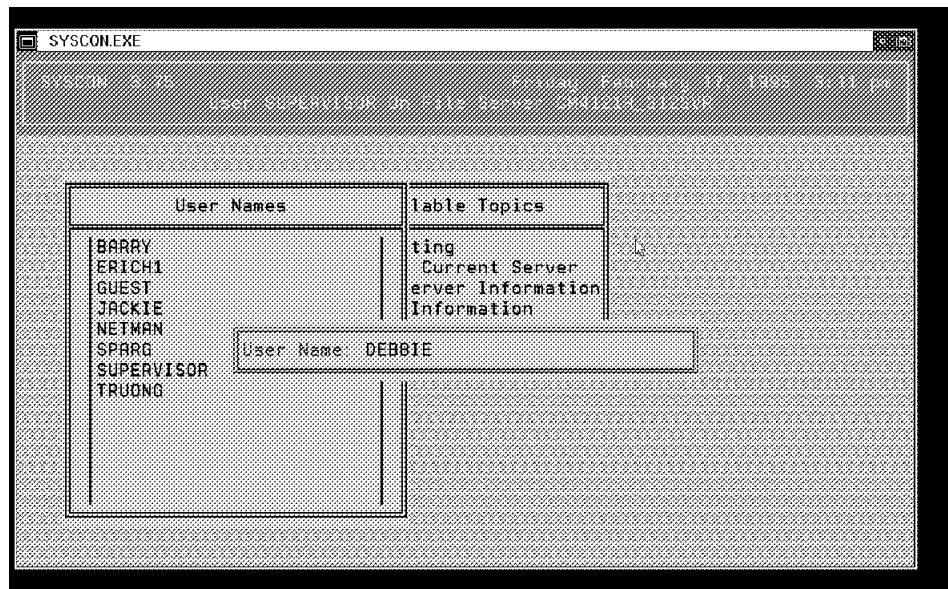
Figure 12. Enter User Name

3. You are prompted for the user's home directory. You can accept the default directory that is shown, or you can specify a different directory.

Figure 13. Path to Create User's Home Directory

4. If you choose a directory that doesn't already exist, it is created for you.
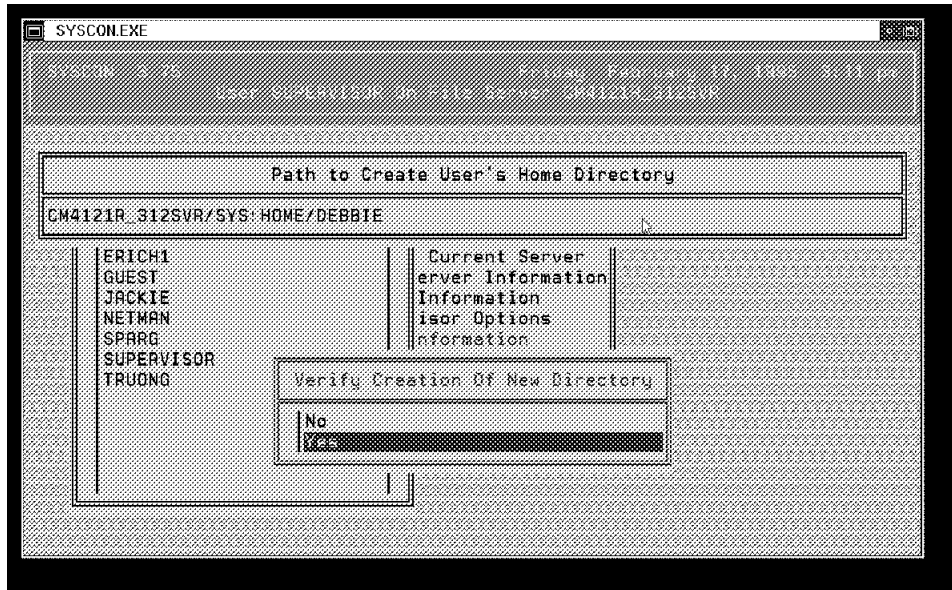
Figure 14. Verify Creation of New Directory

5. After creating the new directory, you will see that the new user has been added to the list of user names.

Figure 15. List of User Names

2.3 Installing NetWare Server V4.01 under DOS

This chapter does not describe all of the NetWare V4.01 server installation
procedure, but it covers the important steps to understand and use the NetWare
V4.01 environment compared to NetWare V3.12, in the NMS/NetView for AIX
management platform.

2.3.1.1 Prerequisite

To install the NetWare V4.01 server, check the needed prerequisites as follows.
For any NetWare V4.x version, check the specific prerequisites.

- Memory considerations:

   The algorithm for the RAM needed on the NetWare V4.01 server is:

   ```
   RAM = (volume size in MB * 0.023) / block size
         _____

                      Per Volume
   ```

   RAM is the minimum memory needed for the disk cache. This algorithm is for
   volume without Name Space; if you are using any Name Space, replace the
   0.023 value with 0.032 for the volume using a Name Space.

   ```
   Minimum Memory =      RAM      +    2,5 MB  +   NDS    +    Memory to load NLMs

                    _____   _____  _____    _____
                      Memory for       Memory    Minimum             Memory
                     the Disk Cache   for the OS  Memory      needed to load all the NLM
   ```

   Minimum Memory is the minimum memory you need to run the NetWare V4.01
   server without a problem.

   In addition, to exactly determine the memory you will need on the server, you
   have to consider that the minimum RAM available for the cache must be
   greater than or equal to 20% of the total memory.

To run the server in the most efficient configuration, the RAM available for the disk cache must be around 60% This value assumes that you are running the appropriate NLMs the system needs and doesn't include the NLMs memory used.

As with NetWare V3.x, the more RAM you have the better the server will run.

2.3.2 Bindery Emulation

The most important difference between NetWare V3.x and NetWare V4.x is the NetWare Directory Services (NDS) implementation.

NDS replaced the Bindery services used in NetWare V3.12.

NetWare's Bindery is a database that contains objects for servers, users and groups, and the properties that are associated with these objects. Some of the properties are right's trustees. The values of the properties are also stored in the database. An example of this would be a password. In NetWare V3.12 OS version, the Bindery is divided into three files:

```
SYS:\SYSTEM\NET$OBJ.SYS
SYS:\SYSTEM\NET$PROP.SYS
SYS:\SYSTEM\NET$VAL.SYS
```

Those files have *Hidden* and *System* attributes. When you back up your server check the complete backup of those files, since a large part of your NetWare server configuration is dependent upon these files.

In a NetWare V3.x environment, each NetWare server is independent and each has its own Bindery. In NetWare V4.x, the concept of NDS will replace that. The NDS concept is based on an object-oriented approach and uses a structure similar to X500.

With NDS, each NetWare network resource is considered as an object.

All objects are independent of their physical place and the NDS database is not completely replicated on each server. Each server contains a part of the total NDS database.

The NDS is structured like a tree where the root is the entire structure or domain (for example, a company) and each leaf is an organization (for example, a department or a branch office). In this context, the NDS implementation is not simple, and it must be planned correctly before installing all the physical network resources.

All the NetWare servers you will install, NetWare V2.2, V3.x or V4.x, will be a part of the NDS tree. They will be in a container, which can be an organization unit, or directly, an organization.

In any case, the container where you will install the NetWare NMS server, which runs NetExplorer, and the NMA Servers, should contain the Bindery Emulation object.

The Bindery Emulation object can only exist one time in only one container in your NDS Tree.

It is the only way to have compatibility with NetWare V2.2 or V3.x OS versions and to have compatibility with most NetWare add-on products such as NMS, NMA and NetWare LANalyzer.

Until NMS, NMA and LANalyzer are completely integrated into NDS, you will have to install the Bindery Emulation and set up all of the NetWare servers that will use NMS, NMA or LANalyzer servers in the same container.

To install Bindery Emulation, create an NDS object *Bindery Emulation* in the container you select for the Bindery Context and where you will install all of the NetWare NMS/NMA/LANalyzer servers.
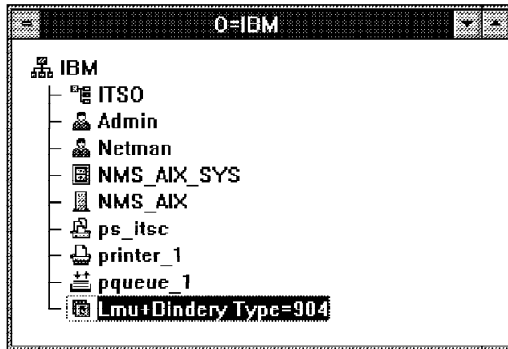
Figure 16. NWADMIN, Bindery Emulation Object Organization Container

Set the Bindery Context in the SYS:\SYSTEM\AUTOEXEC.NCF file as follows:

```
Set Bindery Context = <Organization_name>
```

The <Organization_name> is the name of the Bindery Emulation Container.
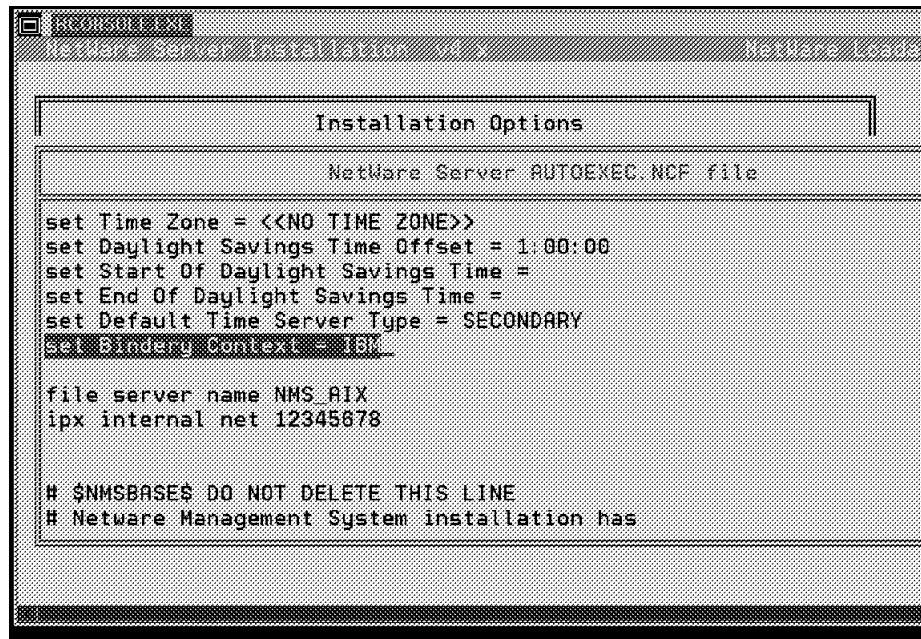
Figure 17. Bindery Emulation Setting in the SYS:SYSTEM\AUTOEXEC.NCF File

> **Note**
>
> To get more information about the Bindery Emulation Implementation, refer to the *NetWare Application Notes from June 1993*.

2.3.3 Installing NetWare DOS/Windows Requester

NetWare DOS/Windows Requester needs the ODI interface to run correctly. In our environment, our DOS/Windows workstations communicate with all the NetWare servers installed on the network and the two RS/6000 running NetView for AIX.

Both IPX/SPX and TCP/IP stacks must be installed and you have many options to select, since there are different types of drivers for IPX and TCP/IP.

2.3.3.1 Installing NetWare DOS/Windows Requester with IPX and IP on ODI

To install the NetWare DOS/Windows Requester, perform the following steps:

1. Insert the WSDOS_1 diskette in drive A:; change to drive A: and type:

   `INSTALL.BAT`

2. Enter the client directory name for the client installation (the default is C:\NWCLIENT).

3. Enter Y(Yes) if you allow the modification of your CONFIG.SYS and AUTOEXEC.BAT files by the installation program.

   The installation process requires `LASTDRIVE=Z` to be placed in CONFIG.SYS and `CALL STARTNET.BAT` in the AUTOEXEC.BAT file.

   STARTNET.BAT is in the client directory (the default is C:\NWCLIENT) and is the batch file that starts all of the NetWare client stacks.

4. You have an option to select the NetWare drivers and DLLs for Windows as defaults or to specify your own.

   If you respond Y(Yes) in this step, then you have to specify your MS-Windows subdirectory.

   If MS-Windows is not installed and you want to use it, stop the NetWare client installation program (press Esc) and proceed to the MS-Windows installation before restarting the NetWare client installation program.

5. Next, you have to install your ODI LAN Driver.

   Press Enter for this option and then insert your WSDRV_2 diskette into drive A:.

   In the list, select your LAN driver and press Enter. If your LAN driver doesn't appear in the list, then insert the options diskette for your LAN adapter.

   After verifying the driver, check the hardware adapter configuration and press Esc to install it.

   If you want to configure a specific MAC address for your workstation, select the **Node Address** option and enter the address you want.

   This logical MAC address definition is used when you want to describe your workstation and to be sure that the address corresponds to a specific location of the workstation.

6. Press Enter to install the NetWare DOS/Windows Requester software.
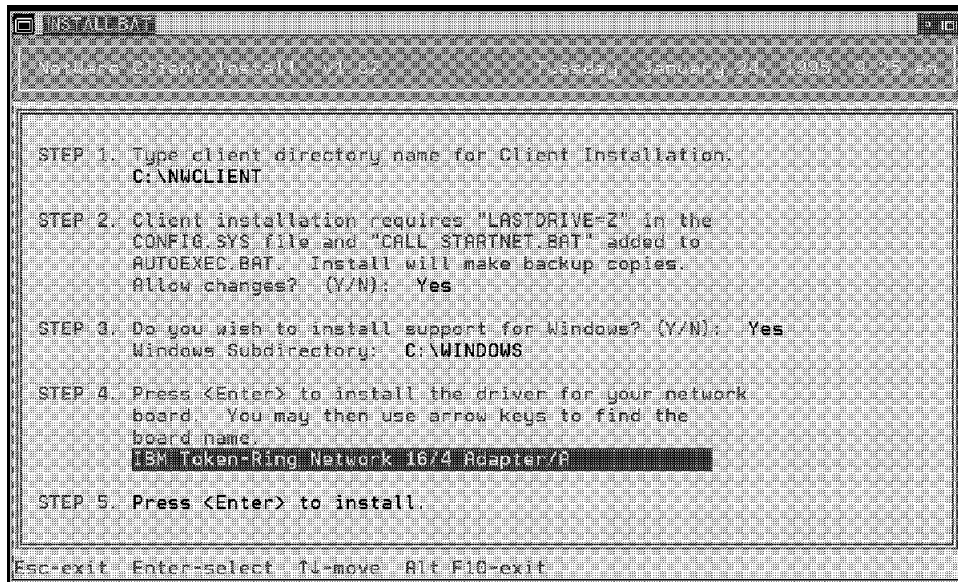
Figure 18. NetWare Requester Installation Program

After installing the NetWare Requester Software, your files might look something like the following:

- **CONFIG.SYS**

```
DEVICE=C:\DOS\HIMEM.SYS
DOS=HIGH
DEVICE=C:\DOS\SERVER.EXE
FILES= 80
BUFFERS= 40
DEVICE=C:\WINDOWS\SMARTDRV.EXE /DOUBLE_BUFFER
STACKS=9,256
LASTDRIVE=Z
```

- **AUTOEXEC.BAT**

```
C:\WINDOWS\SMARTDRV.EXE
@ECHO OFF
PROMPT $p$g

SET TZ=EST5EDT
SET path=C:\WINDOWS;C:\DOS
SET TEMP=C:\DOS
C:\DOS\MOUSE.COM
rem C:\DOS\DOSSHELL.EXE
@Call C:\NWCLIENT\STARTNET
```

- **STARTNET.BAT**

```
@ECHO OFF
C:
CD NWCLIENT
SET NWLANGUAGE=ENGLISH
LSL
TOKEN.COM(The IBM Token-ring Driver for ODI)
ROUTE IPXODI
VLM
CD \
```

> **Note**
>
> If you are using a token-ring driver, you have to place the ROUTE command in your STARTNET.BAT file ROUTE.COM.

- **NET.CFG**

  NET.CFG must reside in the same directory that you start STARTNET.BAT from.

```
Link Support
    Buffers 8 4162
    MemPool 8392

Link Driver TOKEN
    Frame Token-Ring_SNAP
    Frame TOKEN-RING
    Protocol IPX E0 TOKEN-RING
    PORT A20
    MAX FRAME SIZE 4208
    NODE ADDRESS 400052005143
    SLOT 3

NetWare DOS Requester
    PREFERRED SERVER = NMS_AIX
    FIRST NETWORK DRIVE = F

Protocol TCPIP
    PATH SCRIPT     C:\NET\SCRIPT
    PATH PROFILE    C:\NET\PROFILE
    PATH LWP_CFG    C:\NET\HSTACC
    PATH TCP_CFG    C:\NET\TCP
    ip_router       9.24.104.1
    ip_netmask      255.255.255.0
    ip_address      9.24.104.112

Protocol IPX
    Bind #2
```

2.3.3.2 Installing NetWare DOS/Windows Requester with IPX on ODI and TCP/IP on NDIS

To install the NetWare DOS/Windows Requester, perform the following steps:

- Insert the WSDOS_1 diskette in drive A:; change to drive A: and type:

  `INSTALL.BAT`

- Enter the client directory name where the client directory will be created (the default is C:\NWCLIENT).
- Enter Y(Yes) if you allow the modification of your CONFIG.SYS and AUTOEXEC.BAT files.

  Installation will require `LASTDRIVE=Z` in the CONFIG.SYS and `CALL STARTNET.BAT` in the AUTOEXEC.BAT.

  STARTNET.BAT is in the client directory (the default is C:\NWCLIENT) and it is the batch file that starts all of the NetWare client stacks.

- Next you have the choice to install the NetWare drivers and the DLLs for Windows.

If you respond Y(Yes) in this step, then you have to specify your MS-Windows subdirectory.

If MS-Windows is not installed and you want to use it, stop the NetWare client installation program (press Esc) and proceed to the MS-Windows installation before restarting the NetWare client installation program.

- You then have to install your LAN Driver.

  Press Enter on this option and then insert your WSDRV_2 diskette into drive A:.

  In the list, select **ODI Module for the IBM LAN Support Program** and press Enter.
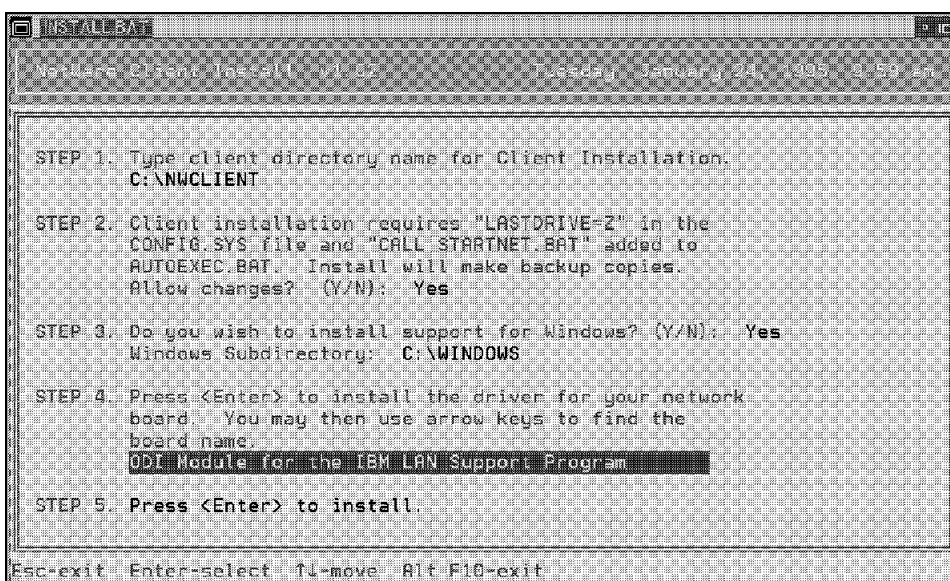
Figure 19. NetWare Requester Installation Program

Attention

If the LAN Support Program is not installed, stop the NetWare Requester installation program and install your LAN support program first.

Check the adapter configuration and press Esc to install it.
- Press Enter on the last line to install the NetWare DOS/Windows Requester software.

After installing the NetWare Requester software, check your system and configuration files. They should look similar to the following files:

- **CONFIG.SYS**

```
DEVICE=C:\WINDOWS\SMARTDRV.EXE /DOUBLE_BUFFER
device=C:\DOS\HIMEM.SYS
device=c:\dos\emm386.exe noems ram x=a000-b0ff i=b100-b7ff
device=c:\dos\ramboost.exe
dos=high

DEVICE=C:\DOS\SETVER.EXE
FILES=40
BUFFERS=50
```

```
STACKS=9,256
DEVICE = C:\DOS\ANSI.SYS
DEVICE = C:\TCPDOS\BIN\PROTMAN.DOS /I:C:\TCPDOS\ETC
DEVICE = C:\TCPDOS\BIN\IBMTOK.DOS
DEVICE=C:\LSP\DXMA0MOD.SYS 001
DEVICE=C:\LSP\DXME0MOD.SYS
DEVICE=C:\LSP\DXMT0MOD.SYS  O=N
REM Consider removing drivers below this comment
DEVICE = C:\TCPDOS\BIN\DOSTCP.SYS
```
LASTDRIVE=Z

- **AUTOEXEC.BAT**

```
C:\lsp\NETBIND
C:\WINDOWS\SMARTDRV.EXE
SET ETC=C:\TCPDOS\ETC
@ECHO OFF
PROMPT $p$g
path=C:\WINDOWS;c:\dos;C:\TCPDOS\BIN;
PATH C:\NWCLIENT\;%PATH%
SET TEMP=C:\DOS
REM BDN C:\DOS\DOSSHELL.EXE
CALL TCPSTART
```
@CALL C:\NWCLIENT\STARTNET

- **STARTNET.BAT**

```
SET NWLANGUAGE=ENGLISH
C:\NWCLIENT\LSL
```
C:\NWCLIENT\LANSUP.COM (The LANSUP driver for ODI)
C:\NWCLIENT\ROUTE C:\NWCLIENT\IPXODI
```
C:\NWCLIENT\VLM
```

> ┌─ **Note** ───
>
> If you are using a token-ring driver, you have to place the ROUTE
> command in your STARTNET.BAT file.
> └──

- **NET.CFG**

NET.CFG must reside in the directory where you start the STARTNET.BAT procedure.

```
Link Support
    BUFFERS 8 1920

Link Driver LANSUP
    LINK STATIONS 1
    MAX FRAME SIZE 4208
    FRAME TOKEN-RING
    PROTOCOL IPX E0 TOKEN-RING

NetWare DOS Requester
    FIRST NETWORK DRIVE = F
    NETWARE PROTOCOL = NDS BIND
    PREFERRED SERVER = CM4121R_312SVR

Protocol IPX
    Bind #1
```

2.3.4 Installing NetWare OS/2 Requester on a Workstation

The NetWare client for OS/2 kit provides support for the following network protocols:

- IPX
- SPX
- Named Pipes
- NetBIOS Emulation

On our OS/2 workstations we needed the following programs to run simultaneously:

- LAN Server Requester
- NetWare Requester
- TCP/IP
- LMU

Therefore, we needed multiprotocol support on our token-ring adapter for the following protocols:

- 802.2
- NetBIOS
- NetWare Requester support
- TCP/IP

We had a choice of token-ring drivers available to achieve this multiprotocol support.

1. ODINSUP
2. LANSUP
3. ODI2NDI

The Open Data-Link Interface (ODI) is Novell's LAN Transport Architecture. ODI was jointly developed by Novell and Apple to fulfill customer's requirements in multiprotocol, networked environments.

IBM's LAN transport strategy is based on Network Driver Interface Specification (NDIS) which is an industry standard jointly developed by 3COM and Microsoft Corporation. NDIS allows different network protocols to operate over the same interface at the same time.

1. ODINSUP

    ODINSUP is a special network protocol driver written to the ODI specification. It provides an interface that allows NDIS network protocol drivers to have access to a LAN adapter through the ODI network interface driver. It may be used in a DOS or OS/2 workstation. ODINSUP is recommended if you have more than one ODI-aware network protocol and only one NDIS-aware network protocol. However, there are disadvantages:

    - This environment is *not* officially supported by IBM.

    - Some problems have been reported using ODINSUP with IBM's TCP/IP for OS/2.

    - You must manually edit CONFIG.SYS and PROTOCOL.INI.

    We chose not to use ODINSUP because of these disadvantages.

2. LANSUP

LANSUP is Novell's method of enabling ODI-aware protocols to use the IEEE 802.2 interface. LANSUP provides an interface that allows IPX/SPX to access the LAN through the IEEE 802.2 interface. This interface may also be used by other network protocols (for example TCP/IP). This interface provides coexistence between the network protocol drivers written to the ODI specification and those written to NDIS, such as NetBIOS.

3. ODI2NDI

   To run the NetWare Client for OS/2 over the NDIS interface, IBM developed a special driver: ODI2NDI, or ODI to NDIS. The ODI2NDI driver provides an interface to the Open Data-Link interface driver from Novell so that these drivers can use the NDIS interface and are able to coexist on the same workstation.

   The ODI2NDI driver is included in IBM's Network Transport Services/2 (NTS/2).

We could find no real advantage/disadvantage for choosing LANSUP over ODI2NDI or vice versa. So, we decided to install both on different OS/2 workstations. On our LMU managing station we used ODI2NDI, and on another NetWare Requester for OS/2 station we used LANSUP. We documented both installations in the following two sections.

2.3.4.1 Installing NetWare Requester for OS/2 with the ODI2NDI Driver

ODI2NDI is a driver from IBM that allows IPX to use IBM's NDIS transport. It is provided with IBM's NTS/2 product.

To configure your machine to use ODI2NDI, perform the following steps. We assume that OS/2 2.11 is already installed on your machine.

1. Install NTS/2 using LAPS by choosing to bind NetBIOS and IEEE 802.2 for the network driver you have installed, as illustrated in Figure 20 on page 32. However, do not choose to add the NetWare Requester protocol support to your network adapter just yet. Save and exit LAPS.
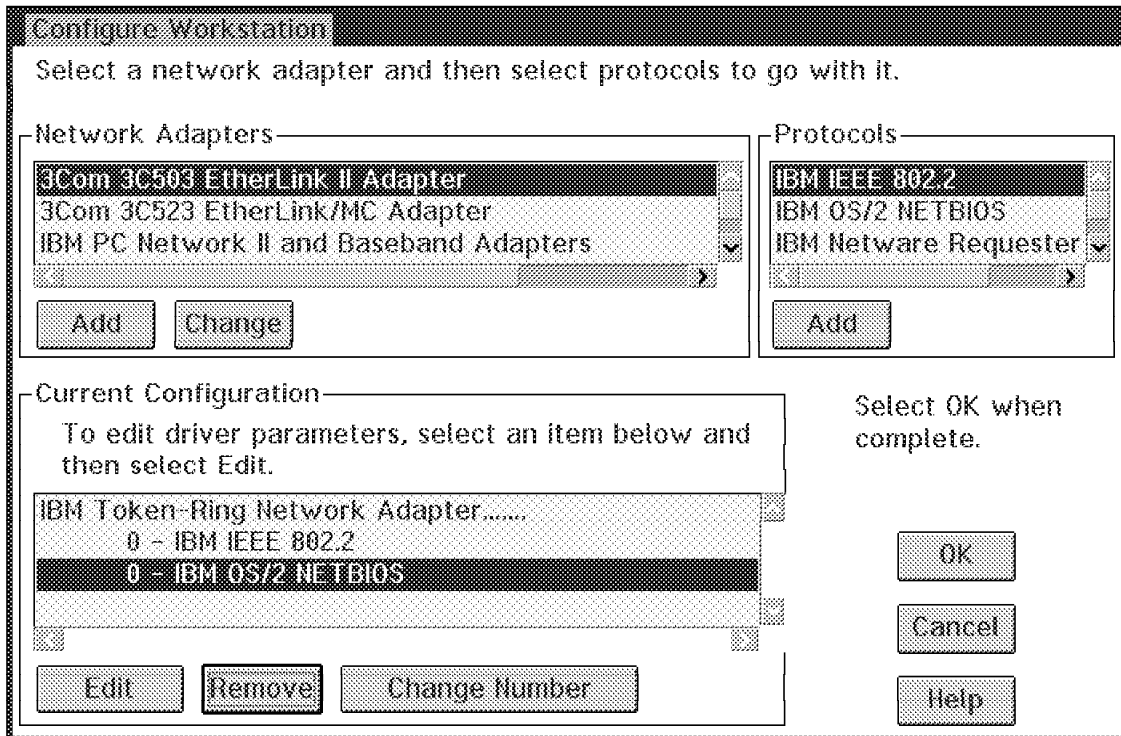
Figure 20. Add Protocol Drivers

2. At this stage you may install those products that require the NDIS transport. On our machine we installed LAN Requester, CM/2, DB2/2, TCP/IP for OS/2 V2.0, and LMU for OS/2 V1.1.
3. Install and configure your environment as you would for a pure NDIS environment.
4. Install the NetWare client code as per the following instructions:

   Before you start, you will need the following diskettes:
   - WSOS2_1
   - WSOS2_2
   - WSDRV_1

   a. Insert the diskette marked WSOS2_1 into the A: drive and type:

   ```
   install
   ```

   b. Highlight the language you wish to use for your installation (the choice includes German, English, Spanish, French and Italian) and click on **OK**. We chose English.
   c. From the window entitled NetWare Workstation for OS/2 Installation Utility, select **Installation**, and then select **Requester on Workstation** from the pull-down menu.
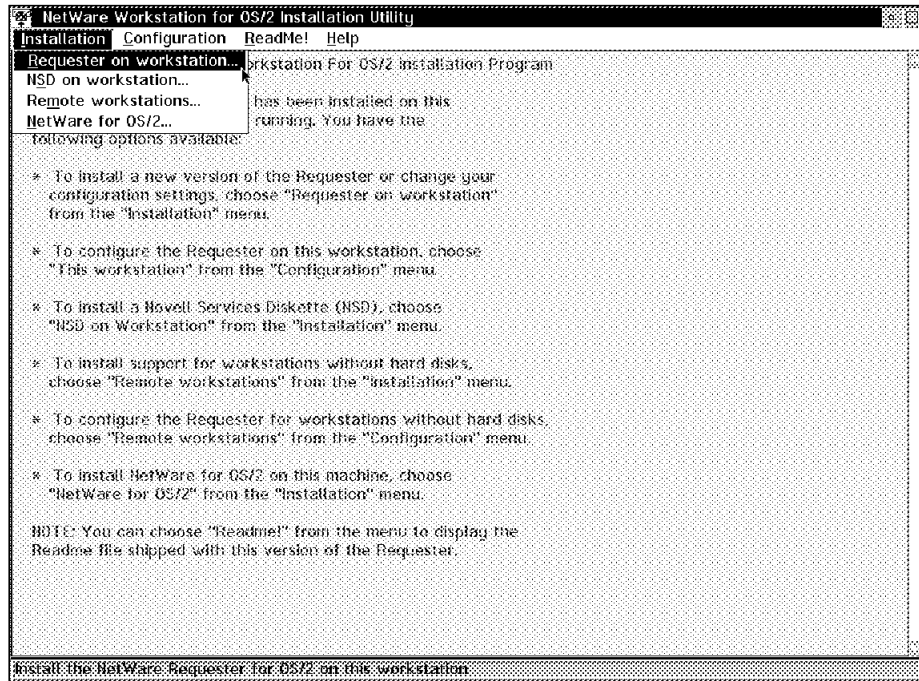
Figure 21. NetWare Workstation for OS/2 Installation Utility

    d. Enter the target directory for the requester files and a source drive for the installation, and then select **OK**.
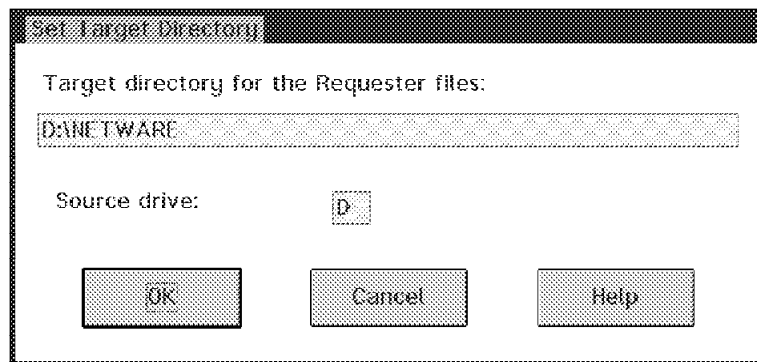
Figure 22. Set Target Directory

    e. You are then required to specify the type of installation you wish to proceed with. For an initial installation, you should generally choose to edit CONFIG.SYS and copy all files. You might take one of the other choices only if you are updating configuration after an initial installation.

    f. You are then asked to choose the ODI LAN driver. To select a driver, click on the scroll bar to the right of the entry field. You are then prompted to insert the WSDRV_1 diskette and select **OK**. It is not so important which driver is chosen, as this information is changed by the LAPs configuration utility. Do not reboot after installing the NetWare client code.

5. After installing the NetWare client code, exit out of the installation utility. Before rebooting, execute the LAPS installation utility. Choose the **Configure** option,

then the **Configure LAN Transports** option and add NetWare Requester
support to your adapter as shown in Figure 23 on page 34.
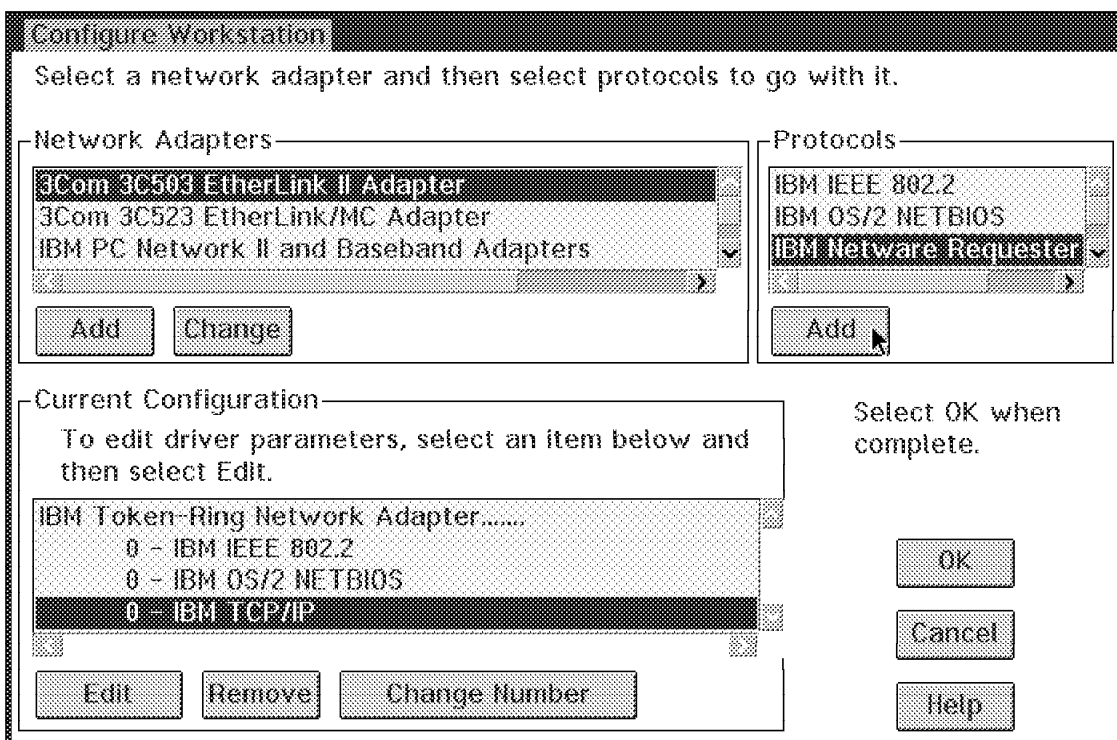
Figure 23. Add NetWare Support

6. You may use either a locally administered address (LAA), or the burnt-in
address of the adapter, but you must specify that address in the IBM NetWare
Requester support to reflect this.

To obtain the burnt-in address, examine the LANTRAN.LOG file, which is in the
C:\IBMCOM directory.

If you specify an address for another protocol (NetBIOS or 802.2) and the
address does not correspond to the address you entered for the NetWare
Requester, IPX will not be enabled in your environment. Figure 24 on page 35
illustrates how to specify this address.

```
┌─────────────────────────────────────────────────────────────────────┐
│▓Parameters for IBM Netware Requester Support▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓│
│                                                                       │
│  Edit the parameters as needed.  Except for parameters preceded by "*",│
│  changes affect all instances of the driver.                          │
│                                                                       │
│  ┌──────────────────────────────────────────────────────────────┐▓  │
│  │                                                                │   │
│  │  *Network adapter address              │T400052005144       │  │   │
│  │                                                                │   │
│  │  *TOKEN-RING frame header support      │yes                 │  │   │
│  │                                                                │   │
│  │  *TOKEN-RING_SNAP frame header support │no                  │  │   │
│  │                                                                │   │
│  │  *ETHERNET_802.3 frame header support  │no                  │  │   │
│  │                                                                │   │
│  │  *ETHERNET_802.2 frame header support  │no                  │  │   │
│  │                                                                │   │
│  │  *ETHERNET_II frame header support     │no                  │  │   │
│  │                                                                │   │
│  │  *ETHERNET_SNAP frame header support   │no                  │  │   │
│  │                                                                │   │
│  │  ODI2NDI trace level                   │0                   │  │   │
│  │                                                              ▓ │   │
│  ▓                                                            ▓   │   │
│  └──────────────────────────────────────────────────────────────┘   │
│                                                                       │
│  ┌──────────┐  ┌──────────┐  ┌──────────┐  ┌──────────┐             │
│  │   OK     │  │  Cancel  │  │  Range   │  │   Help   │             │
│  └──────────┘  └──────────┘  └──────────┘  └──────────┘             │
└─────────────────────────────────────────────────────────────────────┘
```

Figure 24. Specifying the Network Address

After adding the IBM NetWare Requester, highlight the protocol driver in the Current Configuration panel, and choose **Edit**.

7. Save and exit LAPS.
8. You do not need to configure NET.CFG; however, you may do so if you want to make some changes to the default environment (for example, specifying a preferred server).
9. You must now reboot your machine for the changes to take effect.

Check your CONFIG.SYS and PROTOCOL.INI files. Our files are listed in Appendix B.

2.3.4.2 Installing NetWare Requester for OS/2 with the LANSUP Driver

LANSUP is a driver from Novell that allows IPX to use IBM's NDIS driver. It is provided with all NetWare OS products (NetWare V3.12 and V4.x). The LANSUP driver lets the NetWare Requester use the NDIS network driver; then the NDIS driver controls the board. Assuming that OS/2 2.11 is already installed on your machine, to configure your machine to use LANSUP, perform the following steps:

1. Insert the diskette WSOS2_1 into a disk drive.
2. Choose the **Drive A** icon on the desktop.
3. Select the **Drive A** icon from the Drive A Tree-View.

4. Select the **INSTALL.EXE** icon to load the installation program.
5. Select **Requester on workstation...** from the Installation menu.

Figure 25. NetWare Workstation for OS/2 Installation Utility

6. Select **Edit CONFIG.SYS and all configuration files**.

   The installation program will modify your CONFIG.SYS file and create the NET.CFG file.
7. We recommend that you install the SPX protocol stack and the DOS/Windows support.
8. Insert your WSDRV_1 diskette in the selected drive and select the **LANSUP** driver.
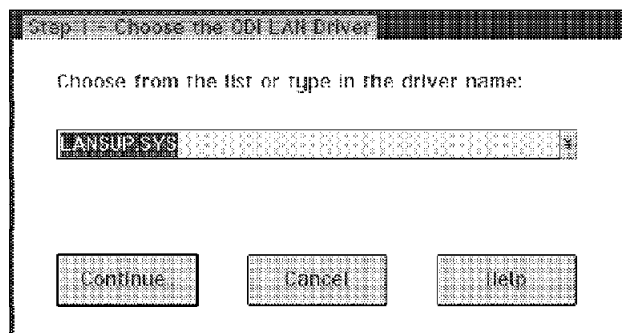
Figure 26. LANSUP Driver Selection

9. Follow the instructions on your screen until you get back to the NetWare Workstation for OS/2 Installation Utility main menu.
10. Next, select the **Configuration** option in the menu bar and the **This Workstation** option.
11. Edit the NET.CFG file
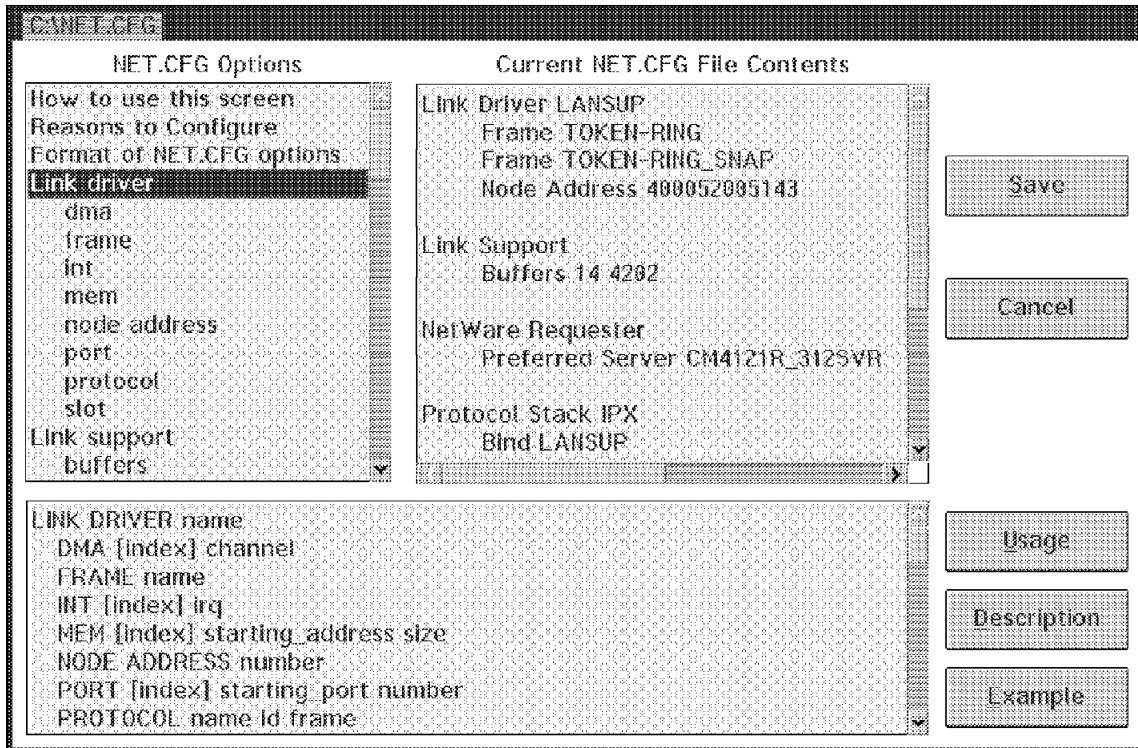
Figure 27. Edit the NET.CFG File for This Workstation

12. Check or enter the following:

```
Link Driver LANSUP
      Frame TOKEN-RING
      Frame TOKEN-RING_SNAP
      Node Address 400052005143 (set your logical MAC address)
Link Support
      Buffers 14 4202
NetWare Requester
      Preferred Server CM4121R_312SVR
Protocol Stack IPX
      Bind LANSUP
Protocol Stack SPX
      Sessions 6
Protocol ROUTE
```

13. Save and exit out of the installation program.
14. You *must* now *reboot* your machine for the changes to take effect.

After installing the NetWare Requester for OS/2, check your system and configuration files:

• **CONFIG.SYS**

```
IFS=C:\OS2\HPFS.IFS  /CACHE:2048 /CRECL:32 /AUTOCHECK
PROTSHELL=C:\OS2\PMSHELL.EXE
SET USER_INI=C:\OS2\OS2.INI
SET SYSTEM_INI=C:\OS2\OS2SYS.INI
SET OS2_SHELL=C:\OS2\CMD.EXE
SET AUTOSTART=PROGRAMS,TASKLIST,FOLDERS,CONNECTIONS
SET RUNWORKPLACE=C:\OS2\PMSHELL.EXE
SET COMSPEC=C:\OS2\CMD.EXE
LIBPATH=.;C:\USERDLLS;C:\OS2\DLL;C:\IBMLAN\NETLIB;C:\MUGLIB\DLL;
C:\IBMCM\DLL;C:\OS2\APPS\DLL;C:\CMLIB\DLL;C:\OS2\MDOS;
C:\;\\WTRDC\LANDLLS;C:\NETWARE;
SET PATH=C:\CMDS;C:\OS2UTILS;C:\OS2;C:\IBMLAN\NETPROG;C:\MUGLIB;
C:\CMLIB;C:\OS2\SYSTEM;C:\OS2\APPS;C:\OS2\MDOS\WINOS2;C:\OS2\INSTALL
C:\OS2\MDOS;C:\;C:\NETWARE;L:\OS2;P:\OS2;L:\NLS;P:\NLS;
SET DPATH=C:\OS2UTILS;C:\OS2;C:\IBMLAN\NETPROG;C:\IBMLAN;C:\MUGLIB;
C:\IBMCOM;C:\CMLIB;C:\OS2\SYSTEM;C:\OS2\APPS;C:\OS2\MDOS\WINOS2;C:\ILL;
C:\OS2\BITMAP;C:\OS2\MDOS;C:\;C:\NETWARE;L:\OS2;P:\OS2;L:\LS;P:\NLS;
SET PROMPT=$e½7mOS2$e½0m $P$G
SET HELP=C:\OS2\HELP;C:\HELPLIB;C:\OS2\HELP\TUTORIAL;C:\CMLIB;
SET BOOKSHELF=C:\IBMLAN\BOOK;C:\OS2\BOOK;C:\INFLIB;C:\CMLIB\BOOK;
SET EPMPATH=C:\EBOOKIE2;C:\OS2\APPS;
SET GLOSSARY=C:\OS2\HELP\GLOSS;
SET CMPATH=C:\CMLIB
SET IPF_KEYS=SBCS
SET KEYS=ON

rem ** ** ** ** ** ** ** ** ** **
PRIORITY_DISK_IO=YES
FILES=40
BUFFERS=60
IOPL=YES
MAXWAIT=3
MEMMAN=SWAP,PROTECT
SWAPPATH=D:\ 2048 12288
BREAK=OFF
THREADS=1024
PRINTMONBUFSIZE=134,134,134
COUNTRY=001,C:\OS2\SYSTEM\COUNTRY.SYS
rem ** ** ** ** ** ** ** ** ** **

PROTECTONLY=NO
SHELL=C:\OS2\MDOS\COMMAND.COM C:\OS2\MDOS
FCBS=16,8
RMSIZE=640
DOS=LOW,NOUMB

rem ** ** ** ** ** ** ** ** ** **
BASEDEV=PRINT02.SYS
BASEDEV=IBM2FLPY.ADD
BASEDEV=IBM2SCSI.ADD /LED
BASEDEV=OS2DASD.DMD
BASEDEV=XGA.SYS
rem ** ** ** ** ** ** ** ** ** **

DEVICE=C:\OS2\TESTCFG.SYS
DEVICE=C:\OS2\DOS.SYS
DEVICE=C:\OS2\PMDD.SYS
DEVICE=C:\OS2\POINTDD.SYS
```

```
DEVICE=C:\OS2\MOUSE.SYS
DEVICE=C:\OS2\COM.SYS
DEVICE=C:\OS2\XGARING0.SYS
DEVICE=C:\OS2\EPWDD.SYS
DEVICE=C:\OS2\LOG.SYS

rem ** ** ** ** ** ** ** ** ** **
DEVICE=C:\OS2\MDOS\VEMM.SYS
DEVICE=C:\OS2\MDOS\VXMS.SYS /UMB
DEVICE=C:\OS2\MDOS\VDPMI.SYS
DEVICE=C:\OS2\MDOS\VDPX.SYS
DEVICE=C:\OS2\MDOS\VCDROM.SYS
DEVICE=C:\OS2\MDOS\VWIN.SYS
DEVICE=C:\OS2\MDOS\VMOUSE.SYS
DEVICE=C:\OS2\MDOS\VCOM.SYS
DEVICE=C:\OS2\MDOS\VVGA.SYS
DEVICE=C:\OS2\MDOS\VXGA.SYS
rem ** ** ** ** ** ** ** ** ** **

CODEPAGE=850,437
DEVINFO=KBD,US,C:\OS2\KEYBOARD.DCP
DEVINFO=SCR,VGA,C:\OS2\VIOTBL.DCP
SET VIDEO_DEVICES=VIO_XGA
SET VIO_XGA=DEVICE(BVHVGA,BVHXGA)

rem ** ** ** ** ** ** ** ** ** **
DEVICE=C:\IBMCOM\PROTOCOL\LANPDD.OS2
DEVICE=C:\IBMCOM\PROTOCOL\LANVDD.OS2
DEVICE=C:\IBMCOM\LANMSGDD.OS2 /I:C:\IBMCOM
DEVICE=C:\IBMCOM\PROTMAN.OS2 /I:C:\IBMCOM
DEVICE=C:\IBMCOM\PROTOCOL\INET.SYS
DEVICE=C:\IBMCOM\PROTOCOL\IFNDIS.SYS
DEVICE=C:\IBMCOM\PROTOCOL\NETBEUI.OS2
DEVICE=C:\IBMCOM\PROTOCOL\NETBIOS.OS2
DEVICE=C:\IBMCOM\PROTOCOL\LANDD.OS2
DEVICE=C:\IBMCOM\PROTOCOL\LANDLLDD.OS2
```
DEVICE=C:\IBMCOM\MACS\IBMTOK.OS2 <u>(NDIS TOKEN Driver)</u>
```
rem ** ** ** ** ** ** ** ** ** **

DEVICE=C:\IBMLAN\NETPROG\RDRHELP.200
```

REM --- NetWare Requester statements BEGIN ---

SET NWLANGUAGE=ENGLISH
DEVICE=C:\NETWARE\LSL.SYS
RUN=C:\NETWARE\DDAEMON.EXE

REM -- ODI-Driver Files BEGIN --
DEVICE=C:\NETWARE\LANSUP.SYS   <u>(LANSUP Driver)</u>
DEVICE=C:\NETWARE\ROUTE.SYS
REM -- ODI-Driver Files END --

DEVICE=C:\NETWARE\IPX.SYS
DEVICE=C:\NETWARE\SPX.SYS
RUN=C:\NETWARE\SPDAEMON.EXE
rem DEVICE=C:\NETWARE\NMPIPE.SYS
rem DEVICE=C:\NETWARE\NPSERVER.SYS
rem RUN=C:\NETWARE\NPDAEMON.EXE

```
DEVICE=C:\NETWARE\NWREQ.SYS
IFS=C:\NETWARE\NWIFS.IFS
RUN=C:\NETWARE\NWDAEMON.EXE
rem DEVICE=C:\NETWARE\NETBIOS.SYS
rem RUN=C:\NETWARE\NBDAEMON.EXE
DEVICE=C:\NETWARE\VIPX.SYS
DEVICE=C:\NETWARE\VSHELL.SYS PRIVATE

REM --- NetWare Requester statements END ---

IFS=C:\IBMLAN\NETPROG\NETWKSTA.200 /I:C:\IBMLAN /N
DEVICE=C:\IBMLAN\NETPROG\VNETAPI.OS2

rem ** ** ** ** ** ** ** ** ** **
DEVICE=C:\CMLIB\ACSLANDD.SYS
DEVICE=C:\CMLIB\CMKFMDE.SYS
rem ** ** ** ** ** ** ** ** ** **

RUN=C:\IBMCOM\PROTOCOL\NETBIND.EXE
RUN=C:\IBMCOM\LANMSGEX.EXE
RUN=C:\IBMCOM\PROTOCOL\LANDLL.EXE
RUN=C:\IBMLAN\NETPROG\LSDAEMON.EXE
RUN=C:\IBMLAN\NETPROG\VNRMINIT.EXE
RUN=C:\OS2\EPWDDR3.EXE
RUN=C:\OS2\EPW.EXE
RUN=C:\OS2\SYSTEM\LOGDAEM.EXE
RUN=C:\OS2\EPWROUT.EXE 1
```

- **PROTOCOL.INI**

  The PROTOCOL.INI file must reside in the C:\IBMCOM directory.

  ```
  [PROT_MAN]

      DRIVERNAME = PROTMAN$

  [LANDD_NIF]

      Bindings = IBMTOK_NIF
      NetAddress = "T400052005143"
      Etherand_Type = "D"
      System_Key = 0x0
      Open_Options = 0x2000
      Trace = 0x0
      Links = 16
      Max_Saps = 5
      Max_G_Saps = 0
      Users = 5
      TI_Tick_G1 = 255
      T1_Tick_G1 = 15
      T2_Tick_G1 = 3
      TI_Tick_G2 = 255
      T1_Tick_G2 = 25
      T2_Tick_G2 = 10
      IPackets = 250
      UIPackets = 100
      MaxTransmits = 6
      MinTransmits = 2
      TCBS = 64
  ```

```
        GDTS = 30
        Elements = 800
        DriverName = LANDD$

[IBMLXCFG]

    LANDD_NIF = LANDD.NIF
    NETBEUI_NIF = NETBEUI.NIF
    TCPIP_NIF = TCPIP.NIF
    IBMTOK_NIF = IBMTOK.NIF

[NETBEUI_NIF]

    Bindings = IBMTOK_NIF
    Etherand_Type = "D"
    SessionS = 64
    NCBS = 128
    Names = 32
    Selectors = 5
    UseMaxDataGram = "NO"
    AdaptRate = 1000
    WindowErrors = 0
    TI = 30000
    T1 = 500
    T2 = 400
    MaxIn = 1
    MaxOut = 1
    NetBIOSTimeout = 500
    NetBIOSRetries = 8
    NameCache = 0
    PiggyBackACKS = 1
    DataGramPackets = 2
    Packets = 350
    Pipeline = 5
    MaxTransmits = 6
    MinTransmits = 2
    DLCRetries = 5
    DriverName = netbeui$

[TCPIP_NIF]

    Bindings = IBMTOK_NIF
    DriverName = TCPIP$

[IBMTOK_NIF]

    Adapter = "PRIMARY"
    MaxTransmits = 12
    RecvBufs = 20
    RecvBufSize = 2040
    XmitBufs = 2
    XmitBufSize = 4208
    DriverName = IBMTOK$
```

- **NET.CFG**

  The NET.CFG file must reside in the C:\ directory.

```
Link Driver LANSUP
        Frame TOKEN-RING
        Frame TOKEN-RING_SNAP
        Node Address 400052005143

Link Support
        Buffers 14 4202

NetWare Requester
        Preferred Server CM4121R_312SVR

Protocol Stack IPX
        Bind LANSUP

Protocol Stack SPX
        Sessions 6
```

2.4 Installing TCP/IP Stacks on all Platforms

We installed TCP/IP on the following:

- OS/2
- DOS/Windows
- NetWare

2.4.1 TCP/IP for OS/2

During this residency we used OS/2 V2.11 and OS/2 TCP/IP V2.0 with all the latest
CSDs installed. It is important that all of them be installed before you use TCP/IP.

The component levels we installed are:

```
TCP/IP  BASE  for OS/2 2.0 and 2.1
Version 2.00    Component ID 562208600
Current CSD level: UN64092
Prior   CSD level: UN56401

X-WINDOWS for TCP/IP on OS/2 2.0 and 2.1 (PMX)
Version 2.00    Component ID 562208600
Current CSD level: UN60006
Prior   CSD level: UN52841

DOSBOX  for TCP/IP on OS/2  2.0 and 2.1 (DNS)
Version 2.00    Component ID 562208600
Current CSD level: UN00000
Prior   CSD level: UN00000

NFS for TCP/IP on OS/2 2.0 and 2.1
Version 2.00    Component ID 562208600
Current CSD level: UN57064
Prior   CSD level: UN52836
```

Example screens follow for configuring TCP/IP on our nvclient workstation.

```
┌──────────────────────────────────────────────────────────────────────────┐
│ ☒  TCP/IP Configuration                                               □   │
│  ┌──────────────────────────────────────────────────────────┐──────┐      │
│  │                                                          │ Network │    │
│  │       Configure   Network   Interface   Parameters      └─────────┤    │
│  │  ☑ Enable LAN Adapter 0                                 │ Routing  │   │
│  │   IP Address  9.24.104.68       Subnet Mask  255.255.255.0 ────────┤   │
│  │   Broadcast                     Destination             │ Autostart │  │
│  │   Address    9.24.104.255       Address                 └──────────┤  │
│  │                                                          │  SLIP    │  │
│  │             Routing Metric Count  0                      └──────────┤  │
│  │                                                          │ Services │  │
│  │        Maximum Transmission Unit  1500                   └──────────┤  │
│  │                                                          │  SNMP    │  │
│  │   Current ifconfig State      (note:  Default state is all│ NFS     │  │
│  │                                                          └──────────┤  │
│  │  allrs    ▨ Single route broadcast   -trailers  ▨ Trailer│ PMX     │  │
│  │  arp      ▨ Disable use of ARP       -802.3     ▨ Enable 802.3     │  │
│  │  icmpred  ▨ Disable ICMP redirects   -canonical ▨ Canonical addresses │
│  │  snap     ▨ Disable extended SNAP support                          │  │
│  │  bridge   ▨ Disable routing field support                          │  │
│  │  ┌──────────┐  ┌───────────┐  ┌──────────┐                         │  │
│  │  │  Undo    │  │ Defaults  │  │  Help    │      Page 1 of 8         │  │
│  │  └──────────┘  └───────────┘  └──────────┘                         │  │
│  └──────────────────────────────────────────────────────────────────────┘│
└──────────────────────────────────────────────────────────────────────────┘
```

Figure 28. Configure Network Interface Parameters

You will need to get the IP-address and the subnet mask from your TCP/IP administrator. A common mistake for the first time installer is to forget to click on the box to enable the LAN Adapter.
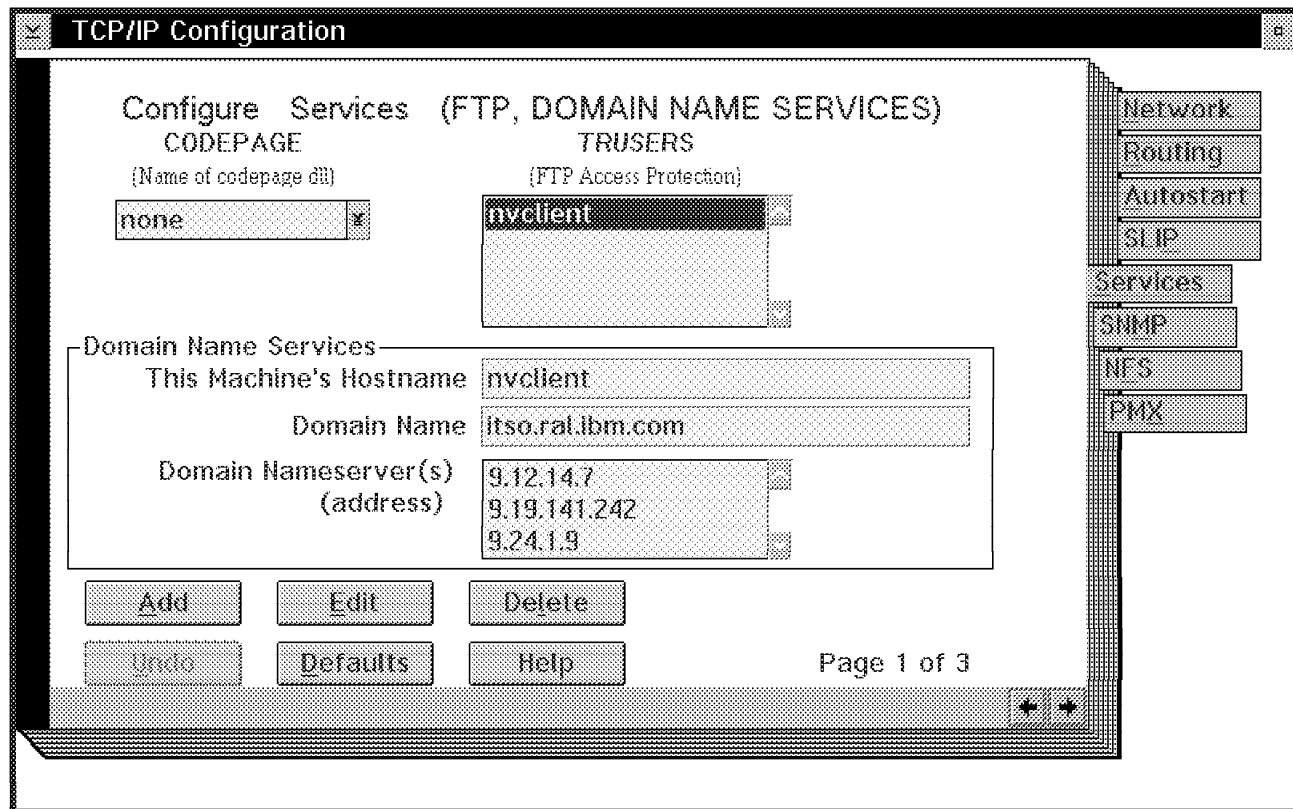
Figure 29. Configure Services (FTP, DOMAIN NAME SERVICES)

We configured our hostname and the domain name. We obtained this information from our TCP/IP administrator. We had several Nameservers in our environment, and used them all in this configuration. We also set up an FTP client. While this was not necessary for the scenarios, it was helpful for the project to move files around. Since the hostname is a parameter that will get placed in CONFIG.SYS, we need to reboot the machine after the customization for the changes to take effect.
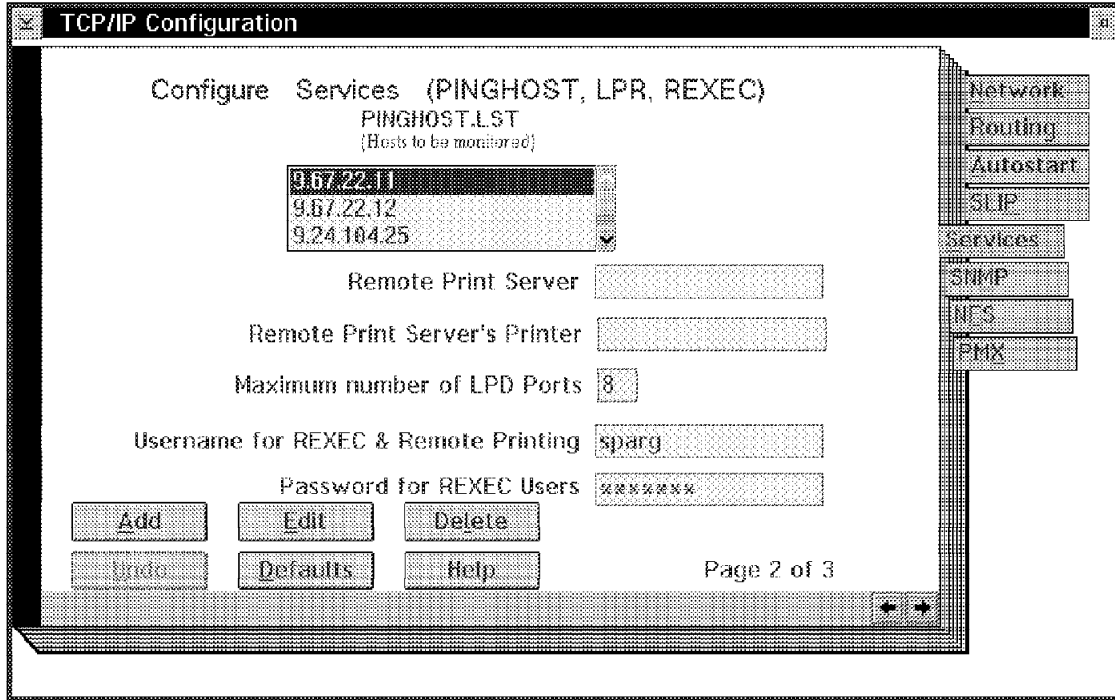
Figure 30. Configure Services (PINGHOST, LPR, REXEC)

The most important parameters in Figure 30 are the REXEC parameters for our scenarios. This gives us the capability to execute remote commands using either REXX or the facilities of LMU and LMU for AIX.
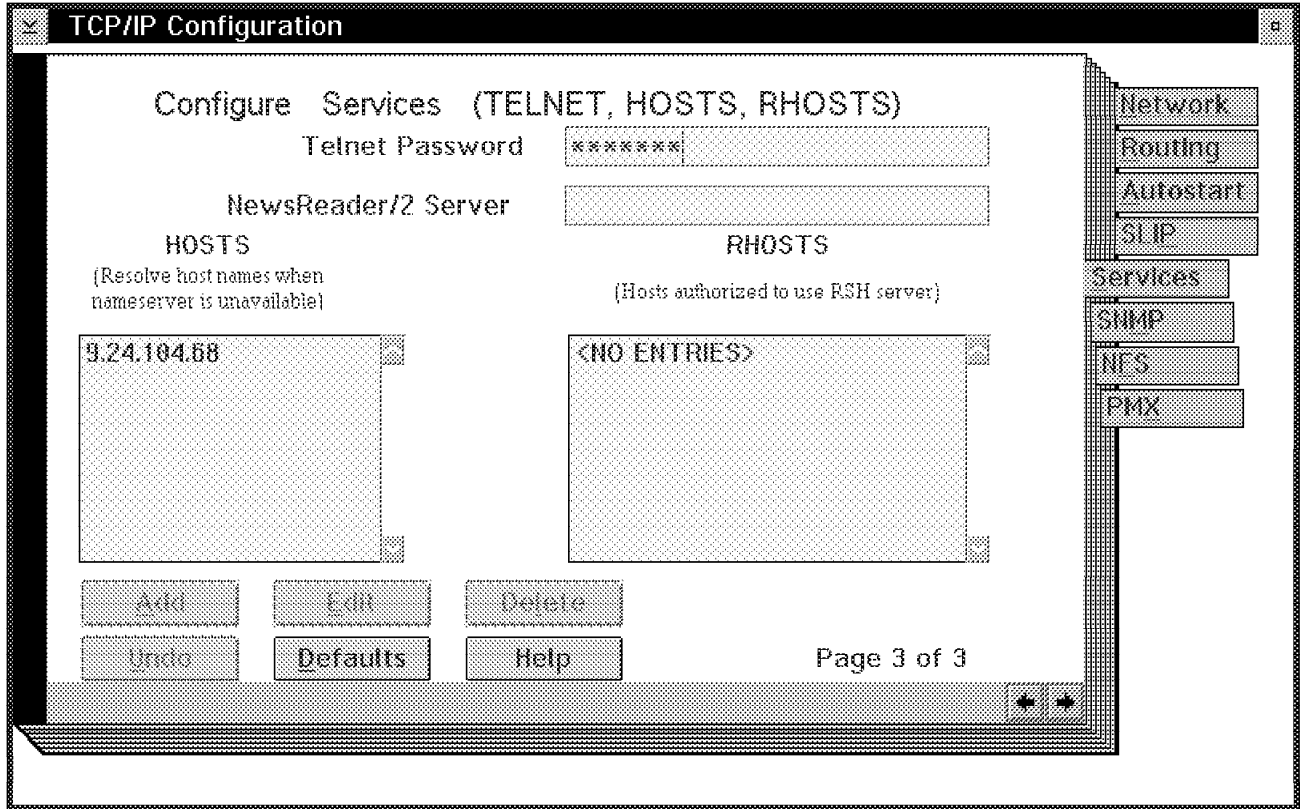
Figure 31. Configure Services (TELNET, HOSTS, RHOSTS)

While none of the scenarios require Telnet, we used Telnet to log on to each machine to make some changes. It is quite helpful to have this configured.
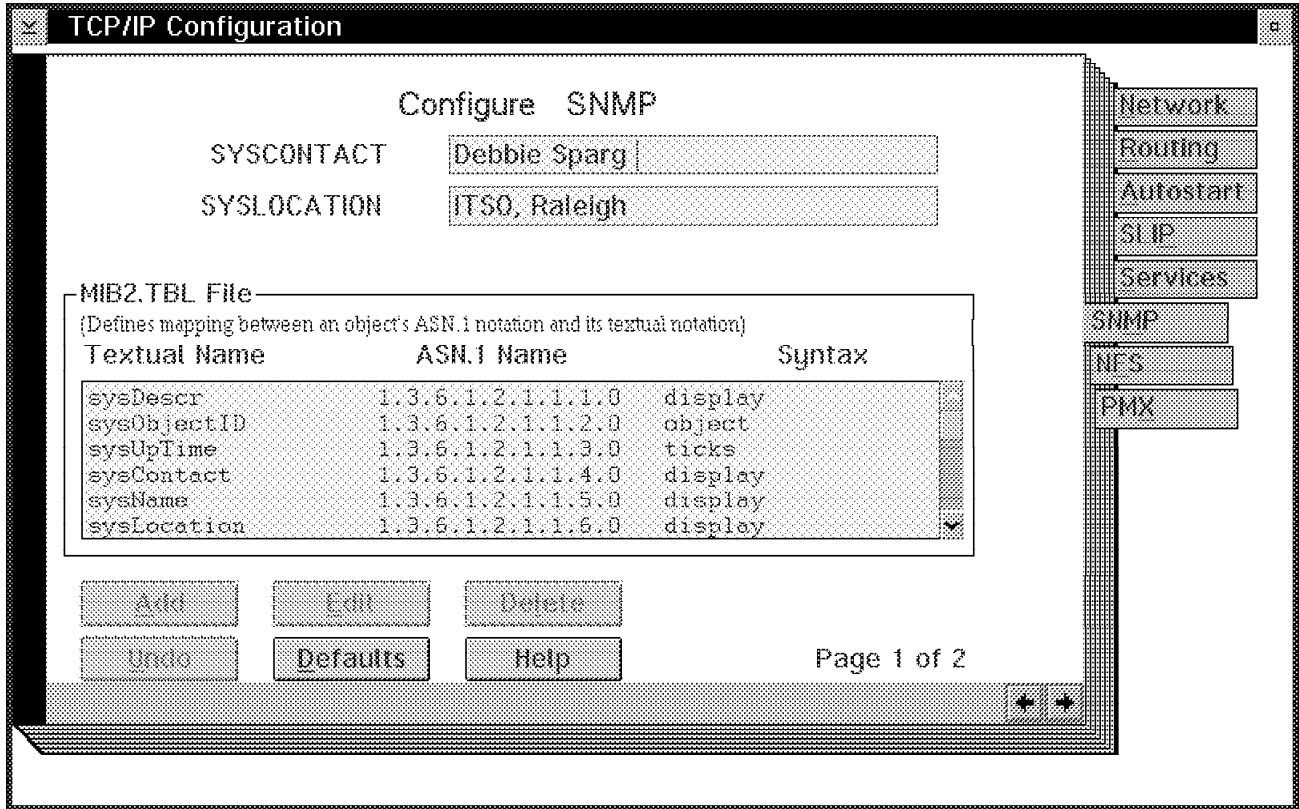
Figure 32. Configure SNMP

Since we will be communicating with NetView for AIX, which is an SNMP manager, we need to update the appropriate fields. This information is helpful for a NetView for AIX helpdesk person, or someone using an MIB browser when there are problems with this machine. We did not update the MIB.TBL file for this project.
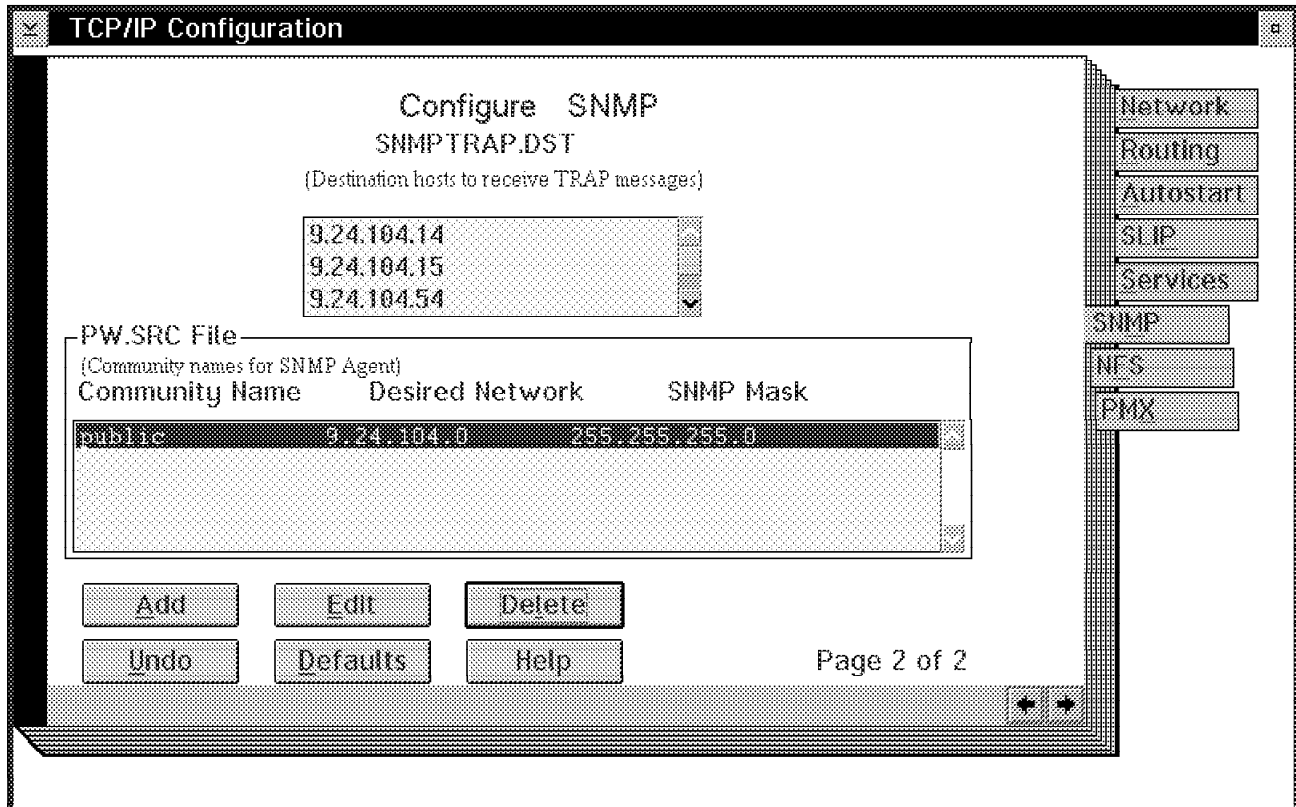
Figure 33. Configure SNMP

We sent our traps (using SNMPTRAP.DST) to several SNMP managers. Since we were using a default community name of public, it is not necessary to run the TCP/IP make_pw EXEC; but, you should be aware that if you are not using defaults, you need to use this EXEC.

The following is a copy of our TCP/IP startup procedure that is located in /TCPIP/BIN/TCPSTART.CMD. Note that you should not make any changes to this file since each time you use the TCP/IP folder it will rewrite this file. You can use TCPEXIT.CMD to start other applications after TCP/IP has been started.

```
@echo off

echo CONFIGURING TCP/IP .....
IF EXIST D:\TCPIP\BIN\B4TCP.CMD CALL D:\TCPIP\BIN\B4TCP.CMD
IF EXIST D:\TCPIP\BIN\SETUP.CMD CALL D:\TCPIP\BIN\SETUP.CMD
echo ..... FINISHED CONFIGURING TCP/IP


echo STARTING THE TCP/IP PROCESSES .....
start /min inetd
echo      ..... INET Daemon Started
 start telnetd
echo      ..... TELNET Daemon Started
REM start ftpd
REM echo     ..... FTP Daemon Started
REM start tftpd
REM echo     ..... TFTP Daemon Started
```

```
REM start rexecd
REM echo      ..... REXEC Daemon Started
REM start rshd
REM echo      ..... RSH Daemon Started
REM start lpd
REM echo      ..... LP Daemon Started
start /min xinit.cmd -nocopyright -iconify
echo      ..... X System Server Started
REM start talkd
REM echo      ..... TALK Daemon Started
start /min portmap
echo      ..... Portmapper Started
start /min nfsd
echo      ..... Network File System Server Started
REM start routed -q
REM echo      ..... ROUTED Started
nfsstart.exe
echo      ..... Network File System Client Started
REM start sendmail -bd -q30m
REM echo      ..... SENDMAIL Started
REM start nr2
REM echo      ..... NR2 Started
REM start lamail
REM echo      ..... LAMAIL Started
REM detach lprportd
REM echo      ..... LPRPORTD Started
start /min snmpd
echo      ..... SNMP Daemon Started
echo ..... FINISHED STARTING THE TCP/IP PROCESSES
IF EXIST D:\TCPIP\BIN\TCPEXIT.CMD CALL D:\TCPIP\BIN\TCPEXIT.CMD
echo .....  EXITING TCPSTART.CMD  .....
```

The following is our CONFIG.SYS and PROTOCOL.INI files:

CONFIG.SYS

```
IFS=C:\OS2\HPFS.IFS  /CACHE:2048 /CRECL:32 /AUTOCHECK:CD
PROTSHELL=C:\OS2\PMSHELL.EXE
SET USER_INI=C:\OS2\OS2.INI
SET SYSTEM_INI=C:\OS2\OS2SYS.INI
SET OS2_SHELL=C:\OS2\CMD.EXE
SET AUTOSTART=PROGRAMS,TASKLIST,FOLDERS,CONNECTIONS
SET RUNWORKPLACE=C:\OS2\PMSHELL.EXE
SET COMSPEC=C:\OS2\CMD.EXE
LIBPATH=C:\IBMCOM\DLL;D:\SQLLIB\DLL;.;C:\USERDLLS;C:\OS2\DLL;
C:\IBMLAN\NETLIB;C:\MUGLIB\DLL;C:\OS2\APPS\DLL;C:\CMLIB\DLL;C:\OS2\MDOS;
C:\;\\WTRDC\LANDLLS;
D:\TCPIP\DLL;D:\LMU2;D:\NETWARE;
SET PATH=D:\SQLLIB;C:\CMDS;C:\OS2UTILS;C:\OS2;C:\IBMLAN\NETPROG;
C:\MUGLIB;C:\CMLIB;C:\OS2\SYSTEM;C:\OS2\APPS;C:\OS2\MDOS\WINOS2;
C:\OS2\INSTALL;C:\OS2\MDOS;C:\;
D:\TCPIP\BIN;D:\LMU2;D:\NETWARE;L:\O 2;
P:\OS2;L:\NLS;P:\NLS;
SET DPATH=C:\IBMCOM;D:\SQLLIB;C:\OS2UTILS;C:\OS2;C:\IBMLAN\NETPROG;C:\IBMLAN;
C:\MUGLIB;C:\CMLIB;C:\OS2\SYSTEM;C:\OS2\APPS;C:\OS2\MDOS\WINOS2;
C:\OS2\INSTALL;C:\OS2\BITMAP;C:\OS2\MDOS;D:\LMU2;C:\;D:\NETWARE;L:\OS2;P:\OS2;
L:\NLS;P:\NLS;
SET PROMPT=$e[7mOS2$e[0m $P$G
```

```
SET HELP=D:\SQLLIB;C:\OS2\HELP;C:\HELPLIB;C:\OS2\HELP\TUTORIAL;C:\CMLIB;
D:\TCPIP\HELP;D\LMU2;D:\LMU2;
SET BOOKSHELF=C:\IBMLAN\BOOK;C:\OS2\BOOK;C:\INFLIB;C:\CMLIB\BOOK;
D:\TCPIP\DOC;D\LMU2;D:\LMU2;
SET EPMPATH=C:\EBOOKIE2;C:\OS2\APPS;
SET GLOSSARY=C:\OS2\HELP\GLOSS;
SET CMPATH=C:\CMLIB
SET IPF_KEYS=SBCS
SET KEYS=ON
rem ** ** ** ** ** ** ** ** ** **
PRIORITY_DISK_IO=YES
FILES=40
BUFFERS=60
IOPL=YES
MAXWAIT=3
MEMMAN=SWAP,PROTECT
SWAPPATH=D:\ 2048 12288
BREAK=OFF
THREADS=1024
PRINTMONBUFSIZE=134,134,134
COUNTRY=001,C:\OS2\SYSTEM\COUNTRY.SYS
rem ** ** ** ** ** ** ** ** ** **
PROTECTONLY=NO
SHELL=C:\OS2\MDOS\COMMAND.COM C:\OS2\MDOS
FCBS=16,8
RMSIZE=640
DOS=LOW,NOUMB
rem ** ** ** ** ** ** ** ** ** **
BASEDEV=PRINT02.SYS
BASEDEV=IBM2FLPY.ADD
BASEDEV=IBM2SCSI.ADD /LED
BASEDEV=OS2DASD.DMD
BASEDEV=XGA.SYS
rem ** ** ** ** ** ** ** ** ** **
DEVICE=C:\IBMCOM\PROTOCOL\LANPDD.OS2
DEVICE=C:\IBMCOM\PROTOCOL\LANVDD.OS2
DEVICE=C:\OS2\TESTCFG.SYS
DEVICE=C:\OS2\DOS.SYS
DEVICE=C:\OS2\PMDD.SYS
DEVICE=C:\OS2\POINTDD.SYS
DEVICE=C:\OS2\MOUSE.SYS
DEVICE=C:\OS2\COM.SYS
DEVICE=C:\OS2\XGARING0.SYS
DEVICE=C:\OS2\EPWDD.SYS
DEVICE=C:\OS2\LOG.SYS
rem ** ** ** ** ** ** ** ** ** **
DEVICE=C:\OS2\MDOS\VEMM.SYS
DEVICE=C:\OS2\MDOS\VXMS.SYS /UMB
DEVICE=C:\OS2\MDOS\VDPMI.SYS
DEVICE=C:\OS2\MDOS\VDPX.SYS
DEVICE=C:\OS2\MDOS\VCDROM.SYS
DEVICE=C:\OS2\MDOS\VWIN.SYS
DEVICE=C:\OS2\MDOS\VMOUSE.SYS
DEVICE=C:\OS2\MDOS\VCOM.SYS
DEVICE=C:\OS2\MDOS\VVGA.SYS
DEVICE=C:\OS2\MDOS\VXGA.SYS
rem ** ** ** ** ** ** ** ** ** **
CODEPAGE=850,437
```

```
DEVINFO=KBD,US,C:\OS2\KEYBOARD.DCP
DEVINFO=SCR,VGA,C:\OS2\VIOTBL.DCP
SET VIDEO_DEVICES=VIO_XGA
SET VIO_XGA=DEVICE(BVHVGA,BVHXGA)
rem ** ** ** ** ** ** ** ** ** **
DEVICE=C:\IBMCOM\LANMSGDD.OS2 /I:C:\IBMCOM
DEVICE=C:\IBMCOM\PROTMAN.OS2 /I:C:\IBMCOM
DEVICE=C:\IBMCOM\PROTOCOL\NETBEUI.OS2
DEVICE=C:\IBMCOM\PROTOCOL\NETBIOS.OS2
DEVICE=C:\IBMCOM\PROTOCOL\LANDD.OS2
DEVICE=C:\IBMCOM\PROTOCOL\LANDLLDD.OS2
DEVICE=C:\IBMCOM\MACS\IBMTOK.OS2
rem ** ** ** ** ** ** ** ** ** **
DEVICE=C:\IBMLAN\NETPROG\RDRHELP.200
REM --- NetWare Requester statements BEGIN ---
SET NWLANGUAGE=ENGLISH
DEVICE=D:\NETWARE\LSL.SYS
RUN=D:\NETWARE\DDAEMON.EXE
DEVICE=C:\IBMCOM\PROTOCOL\ODI2NDI.OS2
REM -- ODI-Driver Files BEGIN --
DEVICE=D:\NETWARE\ROUTE.SYS
REM -- ODI-Driver Files END --
DEVICE=D:\NETWARE\IPX.SYS
DEVICE=D:\NETWARE\SPX.SYS
RUN=D:\NETWARE\SPDAEMON.EXE
DEVICE=D:\NETWARE\NMPIPE.SYS
DEVICE=D:\NETWARE\NPSERVER.SYS
RUN=D:\NETWARE\NPDAEMON.EXE
DEVICE=D:\NETWARE\NWREQ.SYS
IFS=D:\NETWARE\NWIFS.IFS
RUN=D:\NETWARE\NWDAEMON.EXE
DEVICE=D:\NETWARE\NETBIOS.SYS
RUN=D:\NETWARE\NBDAEMON.EXE
DEVICE=D:\NETWARE\VIPX.SYS
DEVICE=D:\NETWARE\VSHELL.SYS PRIVATE
REM --- NetWare Requester statements END ---
IFS=C:\IBMLAN\NETPROG\NETWKSTA.200 /I:C:\IBMLAN /N
DEVICE=C:\IBMLAN\NETPROG\VNETAPI.OS2
rem ** ** ** ** ** ** ** ** ** **
DEVICE=C:\CMLIB\ACSLANDD.SYS
DEVICE=C:\CMLIB\CMKFMDE.SYS
rem ** ** ** ** ** ** ** ** ** **
RUN=C:\IBMCOM\PROTOCOL\NETBIND.EXE
RUN=C:\IBMCOM\LANMSGEX.EXE
RUN=C:\IBMCOM\PROTOCOL\LANDLL.EXE
RUN=C:\IBMLAN\NETPROG\LSDAEMON.EXE
RUN=C:\IBMLAN\NETPROG\VNRMINIT.EXE
RUN=C:\OS2\EPWDDR3.EXE
RUN=C:\OS2\EPW.EXE
RUN=C:\OS2\SYSTEM\LOGDAEM.EXE
RUN=C:\OS2\EPWROUT.EXE 1
DEVICE=C:\IBMCOM\PROTOCOL\INET.SYS
DEVICE=C:\IBMCOM\PROTOCOL\IFNDIS.SYS
SET ETC=D:\TCPIP\ETC
SET TMP=D:\TCPIP\TMP
SET READIBM=D:\TCPIP\DOC;D:\LMU2;
SET HOSTNAME=nvclient
RUN=D:\TCPIP\BIN\CNTRL.EXE
```

```
IFS=D:\TCPIP\BIN\NFS200.IFS
SET DISPLAY=nvclient:0
SET XFILES=D:\TCPIP\X11
SET TZ=est5edt
SET NFS.PERMISSION.BITS=700
SET NFS.PERMISSION.DBITS=700
SET USER=sparg
SET PASSWD=xxxxxxx
SET TELNET.PASSWORD.ID=xxxxxxx
SET SYSCONTACT=Debbie Sparg
SET SYSLOCATION=ITSO, Raleigh
SET INCLUDE=D:\SQLLIB;
SET LIB=D:\SQLLIB;
DEVICE=D:\LMU2\LMUIPL.SYS
SET BOOKMGR=D:\LMU2;
SET QRWDR=D:
SET QRWINST=D:\SQLLIB
```

PROTOCOL.INI

```
[PROT_MAN]

    DRIVERNAME = PROTMAN$


[IBMLXCFG]

    landd_nif = landd.nif
    netbeui_nif = netbeui.nif
    odi2ndi_nif = odi2ndi.nif
    tcpip_nif = tcpip.nif
    IBMTOK_nif = ibmtok.nif


[landd_nif]

    DriverName = LANDD$
    Bindings = IBMTOK_nif
    NETADDRESS = "T400052005144"
    ETHERAND_TYPE = "I"
    SYSTEM_KEY = 0x0
    OPEN_OPTIONS = 0x2000
    TRACE = 0x0
    LINKS = 32
    MAX_SAPS = 30
    MAX_G_SAPS = 0
    USERS = 5
    TI_TICK_G1 = 255
    T1_TICK_G1 = 15
    T2_TICK_G1 = 3
    TI_TICK_G2 = 255
    T1_TICK_G2 = 25
    T2_TICK_G2 = 10
    IPACKETS = 250
    UIPACKETS = 100
    MAXTRANSMITS = 6
    MINTRANSMITS = 2
    TCBS = 64
    GDTS = 30
    ELEMENTS = 800
```

```
[netbeui_nif]

   DriverName = netbeui$
   Bindings = IBMTOK_nif
   NETADDRESS = "T400052005144"
   ETHERAND_TYPE = "I"
   USEADDRREV = "YES"
   OS2TRACEMASK = 0x0
   SESSIONS = 100
   NCBS = 100
   NAMES = 60
   SELECTORS = 5
   USEMAXDATAGRAM = "NO"
   ADAPTRATE = 1000
   WINDOWERRORS = 0
   MAXDATARCV = 4168
   TI = 30000
   T1 = 500
   T2 = 200
   MAXIN = 1
   MAXOUT = 1
   NETBIOSTIMEOUT = 500
   NETBIOSRETRIES = 8
   NAMECACHE = 0
   PIGGYBACKACKS = 1
   DATAGRAMPACKETS = 2
   PACKETS = 350
   LOOPPACKETS = 1
   PIPELINE = 5
   MAXTRANSMITS = 6
   MINTRANSMITS = 2
   DLCRETRIES = 5
   FCPRIORITY = 5
   NETFLAGS = 0x0

[odi2ndi_nif]

   DriverName = odi2ndi$
   Bindings = IBMTOK_nif
   NETADDRESS = "T400052005144"
   TOKEN-RING = "yes"
   TOKEN-RING_SNAP = "no"
   ETHERNET_802.3 = "no"
   ETHERNET_802.2 = "no"
   ETHERNET_II = "no"
   ETHERNET_SNAP = "no"
   TRACE = 0x0

[tcpip_nif]

   DriverName = TCPIP$
   Bindings = IBMTOK_nif

[IBMTOK_nif]

   DriverName = IBMTOK$
   ADAPTER = "PRIMARY"
   MAXTRANSMITS = 6
```

```
                    RECVBUFS = 2
                    RECVBUFSIZE = 256
                    XMITBUFS = 1
```

2.4.2 TCP/IP on DOS/Windows Workstation

We installed TCP/IP on all of the DOS/Windows workstations we used.

2.4.2.1 Installing the Novell TCP/IP Stack on DOS/Windows

The Novell TCP/IP stack is packaged with the NMS product or LAN
WorkPlace/LAN WorkGroup products. You have to use Version 4.12 or later.
In this case, we recommend that you install an ODI driver.

After installing your NetWare DOS/Windows LAN Requester, proceed as follows:

1. Boot your workstation under DOS.
2. Insert the TCP/IP Transport for DOS in the A: drive and type:

   ```
   INSTALL.BAT
   ```

3. Confirm that you have the information required for installing this component.
4. Provide the IP address, subnet mask and router IP address information.
5. Click on **Yes** when you are prompted about inserting the IP information into
   your NET.CFG file.

After installing the NetWare TCP/IP stack, check the following configuration and
system files before starting it.

- **AUTOEXEC.BAT**

  ```
  C:\WINDOWS\SMARTDRV.EXE
  @ECHO OFF
  PROMPT $p$g

  SET TZ=EST5EDT
  SET path=C:\WINDOWS;C:\DOS
  SET TEMP=C:\DOS
  C:\DOS\MOUSE.COM
  rem C:\DOS\DOSSHELL.EXE
  @Call C:\NWCLIENT\STARTNET
  Call C:\NET\BIN\TCPIP
  ```

  ┌─ **Recommendation** ───┐
  │   │
  │ Remove the CALL \NET\BIN\TCPIP line in your AUTOEXEC.BAT file and   │
  │ place it in the STARTNET.BAT file as follows.   │
  │   │
  │ When you want to remove a stack from your PC memory, such as VLM or │
  │ ROUTE or IPX, it's easier to have the right order.   │
  │   │
  └──┘

- **STARTNET.BAT**

  ```
  @ECHO OFF
  C:
  CD NWCLIENT
  SET NWLANGUAGE=ENGLISH
  LSL
  TOKEN.COM(The IBM Token-Ring Driver for ODI)
  ROUTE
  IPXODI
  VLM
  ```

```
CD \
```

> **Note**
>
> If you are using a token-ring driver, you have to place the ROUTE
> command in your STARTNET.BAT file.

- **NET.CFG**

  The NET.CFG file must reside in the directory that you start the
  STARTNET.BAT procedure from.

  ```
  Link Support
      Buffers 8 4162
      MemPool 8392

  Link Driver TOKEN
      Frame Token-Ring_SNAP
      Frame TOKEN-RING
      Protocol IPX E0 TOKEN-RING
      PORT A20
      MAX FRAME SIZE 4208
      NODE ADDRESS 400052005143
      SLOT 3

  NetWare DOS Requester
      PREFERRED SERVER = NMS_AIX
      FIRST NETWORK DRIVE = F

  Protocol TCPIP
      PATH SCRIPT     C:\NET\SCRIPT
      PATH PROFILE    C:\NET\PROFILE
      PATH LWP_CFG    C:\NET\HSTACC
      PATH TCP_CFG    C:\NET\TCP
      ip_router       9.24.104.1
      ip_netmask      255.255.255.0
      ip_address      9.24.104.112

  Protocol IPX
      Bind #2
  ```

2.4.2.2 Installing the IBM TCP/IP Stack on DOS/Windows

The IBM TCP/IP stack is packaged with the IBM TCP/IP for DOS/Windows product.

In this case, we recommend that you install a LANSUP driver.

The installation of TCP/IP for DOS/Windows is not documented here since it is
fairly straightforward. We used DOS TCP/IP V2.1.1 and also V2.1.4 successfully.
We installed TCP/IP after our Windows V3.1 installation. We now check all the
configuration and system files:

- **CONFIG.SYS**

  ```
  DEVICE=C:\WINDOWS\SMARTDRV.EXE /DOUBLE_BUFFER
  device=C:\DOS\HIMEM.SYS
  device=c:\dos\emm386.exe noems ram x=a000-b0ff
  device=c:\dos\ramboost.exe load
  dos=high
  ```

```
DEVICE=C:\DOS\SETVER.EXE
FILES=40
BUFFERS=50
STACKS=9,256
DEVICE = C:\DOS\ANSI.SYS
DEVICE = C:\TCPDOS\BIN\PROTMAN.DOS /I:C:\TCPDOS\ETC
DEVICE = C:\TCPDOS\BIN\IBMTOK.DOS
DEVICE=C:\LSP\DXMA0MOD.SYS 001
DEVICE=C:\LSP\DXME0MOD.SYS
DEVICE=C:\LSP\DXMT0MOD.SYS  O=N
REM Consider removing drivers below this comment
DEVICE = C:\TCPDOS\BIN\DOSTCP.SYS

LASTDRIVE=Z
```

- **AUTOEXEC.BAT**

```
C:\lsp\NETBIND
C:\WINDOWS\SMARTDRV.EXE
SET ETC=C:\TCPDOS\ETC
@ECHO OFF
PROMPT $p$g
path=C:\WINDOWS;c:\dos;C:\TCPDOS\BIN;
PATH C:\NWCLIENT\;%PATH%
SET TEMP=C:\DOS
REM BDN C:\DOS\DOSSHELL.EXE
CALL TCPSTART
@CALL C:\NWCLIENT\STARTNET
```

- **STARTNET.BAT**

```
SET NWLANGUAGE=ENGLISH
C:\NWCLIENT\LSL
C:\NWCLIENT\LANSUP.COM  (The LANSUP driver for ODI)
C:\NWCLIENT\ROUTE
C:\NWCLIENT\IPXODI
C:\NWCLIENT\VLM
```

> ┌─ **If you are using a token-ring driver** ─────────────────────┐
>
> You have to place the ROUTE command in your STARTNET.BAT file.
>
> └──┘

- **NET.CFG**

The NET.CFG file must reside in the directory before you start the STARTNET.BAT procedure.

```
Link Support
    BUFFERS 8 1920

Link Driver LANSUP
    LINK STATIONS 1
    MAX FRAME SIZE 4208
    FRAME TOKEN-RING
    PROTOCOL IPX E0 TOKEN-RING

NetWare DOS Requester
    FIRST NETWORK DRIVE = F
    NETWARE PROTOCOL = NDS BIND
    PREFERRED SERVER = CM4121R_312SVR
```

```
                Protocol IPX
                   Bind #1
```

- **PROTOCOL.INI**

  ```
  [PROTMAN]
  DriverName=PROTMAN$

  [TCPIP_V21]
  DriverName=DOSNDIS$
  Bindings=IBMTOK,,,

  [DXME0_MOD]    (For LAN Support Program)
  DriverName=DXME0$
  Bindings=IBMTOK

  [IBMTOK]
  ; IBM Token Ring
  ; IBMTOK.DOS
      DriverName = IBMTOK$
      netaddress="400052005190"
  ```

- **TCPSTART.BAT**

  ```
  :=----------------------------------------------------------------------------=:
  :=- TCPSTART batch file                                                      -=:
  :=- begins by determining that the necessary environment variables are set  -=:
  :=----------------------------------------------------------------------------=:
  @echo off
  IF %ETC%.==. GOTO ETCHELP
  INETCHK
  IF ERRORLEVEL 1 GOTO INET_DOWN
  GOTO INET_UP
  :INET_DOWN
  :=----------------------------------------------------------------------------=:
  :=- install the Protocol Stack                                              -=;
  :=----------------------------------------------------------------------------=:
     IF %INET%.==. inet
     IF NOT %INET%.==. inet -d %INET%
     if errorlevel 1 GOTO done
  :=----------------------------------------------------------------------------=:
  :=- Assign our IP address and set NETMASK and default ROUTE                 -=:
  :=----------------------------------------------------------------------------=:
  c:\tcpdos\bin\route -fnq
  arp -dan
  lh ifconfig nd0 9.24.104.54 netmask 255.255.255.0 up
  REM slipdial
  c:\tcpdos\bin\route add -hopcount 1 -mtu 1496 default 9.24.104.1
  PING -c1 9.24.104.1>nul
  REM ftpd -b
  REM if errorlevel 0 echo ..... FTP Daemon Started
  REM lpd -b
  REM if errorlevel 0 echo ..... LP Daemon Started
  lh dosnfs
  REM routed -b
  REM if errorlevel 0 echo ..... ROUTED Started
     echo.
     echo TCP/IP is enabled.
  ```

```
:=------------------------------------------------------------------------------=:
REM  USER CUSTOMIZATION SECTION
REM
REM  WARNING:  Do not remove the lines, 'REM  Begin_User_Customization'
REM            and 'REM  End_User_Customization' because these are used
REM            to protect any user-added commands from being deleted by
REM            the CUSTOM program
REM
REM  Begin_User_Customization
REM  End_User_Customization
   goto DONE
:=------------------------------------------------------------------------------=:
:INET_UP
   ECHO TCP/IP is already up!
   goto DONE
:=------------------------------------------------------------------------------=:
:=- Provide any needed HELP                                                   -=:
:=------------------------------------------------------------------------------=:
:
   ECHO You MUST set the • [1;33;40m ETC • [0;37;40m variable
   ECHO before attempting to start TCPPLUS█
:DONE
```

2.4.3 TCP/IP on NetWare Servers

We installed TCP/IP on all NetWare V3.12, V4.01 and V4.1 servers that we used.

TCP/IP Components and Memory Requirements

```
        Module              Memory              Usage

        TCPIP.NLM           180 KB              Required
        SNMP.NLM             35 KB              Required
        TCPCON.NLM          100 KB              Optional *
        SNMPLOG.NLM           8 KB              Optional *
        IPTUNNEL.LAN          4 KB              Optional *
        IPCONFIG.NLM          5 KB              Transient **
        PING.NLM             16 KB              Optional *


        * Consumes memory only when running
        ** Occupies memory only for a few seconds when running
```

The two components you really need are TCPIP.NLM and SNMP.NLM as well as the PING utility to test the connection.

2.4.3.1 Installing the Novell TCP/IP Stack on the NetWare Server

The Novell TCP/IP stack is packaged with the NetWare operating systems V3.12 and V4.x. You can enter all the TCP/IP configuration information on the command line to test it, and if need be, correct it in the AUTOEXEC.NCF file.

Proceed as follows:

1. On the NetWare OS console, enter the following command:
   Load <Driver_name> FRAME=Token-Ring_Snap* NAME=TokenIP

   where Driver_name is the driver name you installed.

   The frames used by TCP/IP are:

```
TOKEN-RING_SNAP
```

(if you are using a token-ring adapter)

```
ETHERNET_SNAP
ETHERNET_II
ETHERNET_802.3
ETHERNET_802.2
```

(if you are using an Ethernet Adapter, depending upon your network configuration)

2. Next, load the TCP/IP stacks on the server with the following command:

   `:Load TCPIP`

   The SNMP.NLM file is automatically loaded when you load TCPIP. If there are any optional parameters that you want for SNMP, you will have to load the SNMP.NLM file before TCPIP. This was done in the NMS installation process.

3. Bind the IP protocol stack to the LAN driver using the correct frame type:

   `:Bind IP to TokenIP addr=9.24.104.54 mask=255.255.255.0`

   where `addr` is your IP address, `mask` is the subnet mask you use and `TokenIP` is the LAN driver name for the correct frame type.

4. Now, to test the connectivity, load the PING utility:

   `:Load PING <addr>`

   where `addr` is the IP address that you want to ping. If you want to ping multiple addresses, you can use the escape key and add additional addresses.
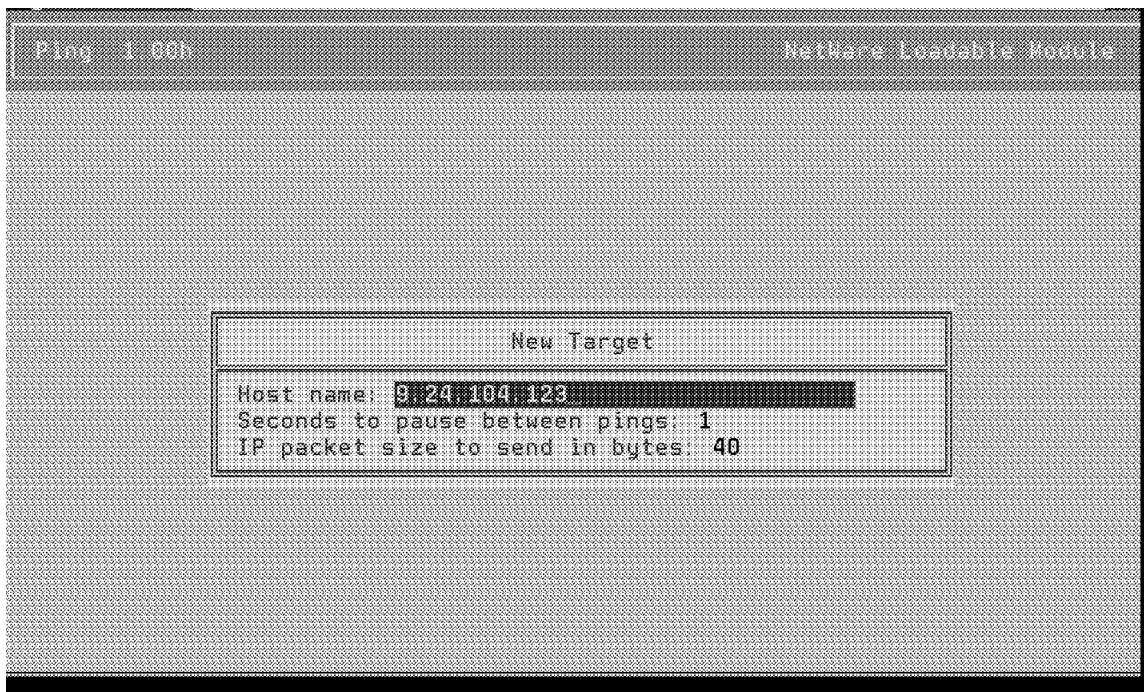
Figure 34. PING.NLM Screen

5. If everything works, then save this configuration in your AUTOEXEC.NCF file and restart the NetWare server.

   - Load the install utility:

     `:Load INSTALL`

- Select **Product Options** if you are using a NetWare V3.12 server, or **NCF Files Options** if you are using a NetWare V4.x server.
- Next, select the **Edit AUTOEXEC.NCF file** option and press Enter.
- Enter the following lines.

    These lines could be entered on the NetWare console command line and saved in the AUTOEXEC.NCF as shown in Figure 35.

    ```
    :Load <LAN_Driver_name> Frame=<Frame_type> Name=<Logical_name>
    :Bind IP to <Logical_name> Addr=<IP_address> Mask=<Subnet_Mask>
    ```

    LAN_Driver_name is the ODI Driver for your LAN adapter board.

    Frame_type is the specific frame type used for IP.
    – TOKEN-RING_SNAP if you are using a token-ring board
    – ETHERNET_II or ETHERNET_SNAP or ETHERNET_802.2 if you are using an Ethernet board

    Logical_name is a name used to bind the protocol to the ODI LAN driver with the correct frame.

    IP_address is the IP address of your NetWare server.

    Subnet_mask is the IP subnet mask used on your network.

    Attention

    If you are using token-ring, do not forget to load the ROUTE.NLM file a second time for the IP protocol LAN adapter (even if it is the same ODI LAN adapter driver used in a re-enterant mode).

```
NetWare Server Installation  v4.x                      NetWare Loadable Module

                        Installation Options

                    NetWare Server AUTOEXEC.NCF file

Load SNMP verbose Control=public Trap=public

Load TCPIP Forward=Yes
Load SNMPLOG

load TOKEN SLOT=3 NODE=400052005190M FRAME=Token-Ring MSB   NAME=TOKEN_1T_EN
load ROUTE board=1
bind IPX to TOKEN_1T_EN-RING net=9

Load TOKEN SLOT=3 FRAME=Token-Ring_Snap NAME=TOKEN_IP
Load ROUTE board=2
Bind IP to TOKEN_IP addr=9.24.104.54 mask=255.255.255.0


Save File <F10>
Help <F1>           Previous screen <Esc>          Abort INSTALL <Alt><F10>
```

Figure 35. Edit AUTOEXEC.NCF

Press Escape to Quit and Save.

6. Stop your server and restart it to load and verify your modifications.

```
:Down
```

```
                   :Exit

                   C:>Server
```

After installing the NetWare TCP/IP stack, check the following configuration and system files before starting it:

- **AUTOEXEC.NCF**

```
set Time Zone = <<NO TIME ZONE>>
set Daylight Savings Time Offset = 1:00:00
set Start Of Daylight Savings Time =
set End Of Daylight Savings Time =
set Default Time Server Type = SECONDARY
set Bindery Context = IBM

file server name NMS_AIX
ipx internal net 12345678

Load TCPIP Trap=9.24.104.123 Forward=Yes
Load SNMPLOG

Load IBMETHR SLOT=7 FRAME=Ethernet_802.3 NAME=Ether_IPX
bind IPX to Ether_IPX net=CAFE0001

Load IBMETHR SLOT=7 FRAME=Ethernet_II NAME=Ether_IP
Bind IP to Ether_IP addr=9.24.104.114 mask=255.255.255.0

load TOKEN SLOT=3 NODE=400052005190M FRAME=Token-Ring MSB  NAME=TOKEN_1T_EN-RING
load ROUTE board=2
bind IPX to TOKEN_1T_EN-RING net=9

load TOKEN SLOT=3 FRAME=Token-Ring_Snap NAME=TOKEN_IP
Load ROUTE board=3
Bind IP to TOKEN_IP addr=9.24.104.54 mask=255.255.255.0

load remote
load rspx

Mount ALL

Load Install
rem Load TCPCON
Load Monitor /p
```

2.5 Installing NMS Components

NMS is composed of many complementary components (listed below). It is important to describe them, their prerequisites, and how they must be installed.

2.5.1 NMS Family Components

The NMS configuration that we used on our platform is:

- NetWare Management System software V2.0c

  This includes the patch NMS002.EXE (NMS V2.0c update).
- NMS Export Service V1.0

  NMS Update is contained in the NMSXP1.EXE patch (available on Net   Wire).

- NetWare Management Agents V1.5 and V1.6

  NMA is not packaged with NMS and is not required, but we needed it for NetWare system management, and it's an NMS option.

  > **Attention**
  >
  > NMA V1.5 runs on NetWare V3.11 and V4.01 servers.
  >
  > NMA V1.6, the latest release, only runs with NetWare V3.12 and NetWare V4.02 and V4.1.
  >
  > *Don't* use it with NetWare V3.11 or V4.01.

- NetWare LANalyzer V1.0

  LANalyzer is not packaged with NMS and is not required; but we used it for network management, and it's an NMS option.

2.5.1.1 Checklist for NMS Installation

The NMS console requires the following hardware:

- 80386- or 80486-based IBM PC or compatible
- VGA or SVGA graphics adapter and monitor
- 12 MB RAM, including 540 KB free (of the lower 640 KB) before starting MS-Windows
- 10 to 50 MB of free disk space for NMS DATA, depending on the size of your network:
  - Small (up to 100 nodes): 10 MB
  - Medium (up to 1 000 nodes): 30 MB
  - Large (up to 10 000 nodes): 50 MB
- 30 MB additional free disk space for the following:
  - 20 MB for NMS software
  - 10 MB for the NMS Tutorial and NetWare help

Software:

- MS-DOS 5.0 or later, DR DOS 6.0 or later, or Novell DOS 7.0.
- We used DOS 6.3 and 7.0.
- MS Windows V3.1 running in enhanced mode.
- The DOS program SHARE.EXE must be loaded and running.

Network:

- MS Windows 3.1 network option enabled for NetWare
- NetWare Requester for DOS/Windows installed

NMS Server Configuration Requirements (NetExplorer Server)

- NetWare V3.12 or V4.01 running 8 MB RAM dedicated to run NetExplorer (in addition to 8 MB RAM required on the server; 16 MB RAM total)
- 20 MB available disk space

NetExplorer Plus Servers Configuration Requirements

- NetWare V3.12 or V4.01

2.5.2 Installing NMS Software

The NMS installation program is very flexible and you can install all of the components in a single session or install the NMS Console Software at one time and the server-based software on the second pass.

For an initial installation, we recommend that you install all the NMS components in one pass.

```
┌─ Attention ─────────────────────────────────────────────────────────┐
│                                                                      │
│  Before starting, check all your requirements and verify that you    │
│  have all the NetWare server connections, supervisor access, and     │
│  passwords on all servers on which you have to install the NMS        │
│  components.                                                          │
│                                                                      │
└──────────────────────────────────────────────────────────────────────┘
```

NMS is installed on the machine that has the NetWare DOS Requester station where you intend to have the NMS console function.

1. Boot the DOS/Windows workstation.
2. Check that the SHARE.EXE is loaded and running.
3. Check that the NetWare Requester is loaded and running.

   To display the contents of the memory, enter the MEM /C command on the command line. You should see a screen similar to the following:

```
Modules using memory below 1Mb:

   name         Total      =    Conventional   +   Upper Memory
   --------   ----------------    ----------------    ----------------
   IBMDOS     20,445   (20K)      20,445   (20K)            0   (0K)
   HIMEM       1,072    (1K)       1,072    (1K)            0   (0K)
   SMARTDRV   30,768   (30K)      30,768   (30K)            0   (0K)
   COMMAND     2,928    (3K)       2,928    (3K)            0   (0K)
   SHARE       6,272    (6K)       6,272    (6K)            0   (0K)
   MOUSE      17,280   (17K)      17,280   (17K)            0   (0K)
   LSL        47,856   (47K)      47,856   (47K)            0   (0K)
   TOKEN       9,600    (9K)       9,600    (9K)            0   (0K)
   ROUTE       1,040    (1K)       1,040    (1K)            0   (0K)
   ROUTE       1,040    (1K)       1,040    (1K)            0   (0K)
   IPXODI     16,320   (16K)      16,320   (16K)            0   (0K)
   TCPIP      24,496   (24K)      24,496   (24K)            0   (0K)
   VLM        60,512   (59K)      60,512   (59K)            0   (0K)
   FREE      414,688  (405K)     414,688  (405K)            0   (0K)

Memory summary:

   Type of Memory       Total   =     Used    +      Free
   ----------------   ----------    ----------    ----------
   Conventional         655,360       240,672       414,688
   Upper                      0             0             0
   Reserved             393,216       393,216             0
   Extended (XMS)    32,505,856     2,209,792    30,296,064
   ----------------   ----------    ----------    ----------
   Total memory      33,554,432     2,843,680    30,710,752

   Total under 1Mb      655,360       240,672       414,688

   Largest executable program size      414,080    (404K)
   Largest free upper memory block            0      (0K)
   PC DOS is resident in the high memory area.
```

4. Start MS Windows with the WIN command.
5. Insert the NetWare Management System Setup diskette into drive A:.

6. From the MS Windows Program Manager, select the **File** and **Run** menu options.
7. In the run dialog box, type:

   `A:\SETUP`
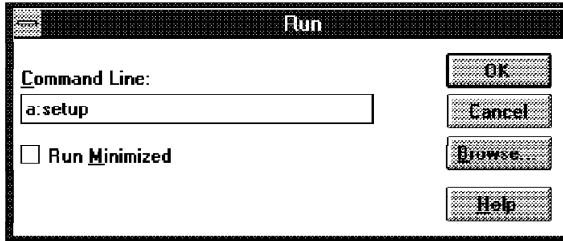
Figure 36. MS-Windows Dialog Box

8. The first installation screen gives you the option to install the NMS Tutorial or the NMS software.

   Choose **NMS software** and click on the **OK** button.
9. The next screen lists all of the NMS components that you can install.

   For a first installation, we recommend that you select all the components, except TCP/IP if it is already installed, and click on the **OK** button.

   > **Note**
   >
   > You must install the NMS Console software before you install the TCP/IP update software.
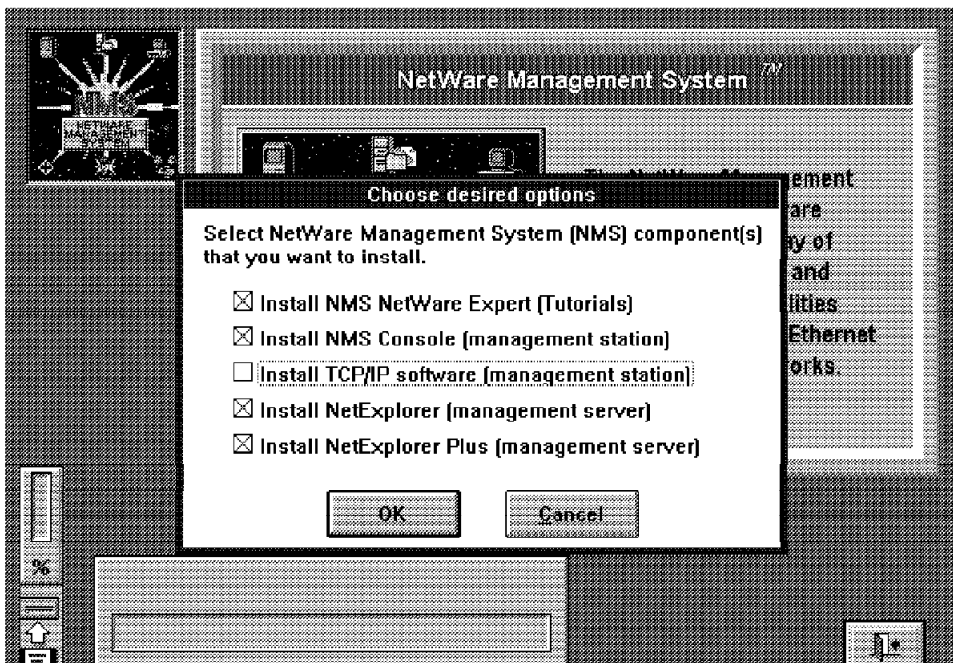
Figure 37. NMS Installation Program

If you did not choose to install all the NMS component software, you can install some of them later, following the same process, by choosing the components you want.

10. Complete the registration information and click on the **OK** button.

11. Select the approximate size of your network and click on the **OK** button.

> **Note**
>
> The installation program will check the available space to determine the approximate disk space required by NMS.
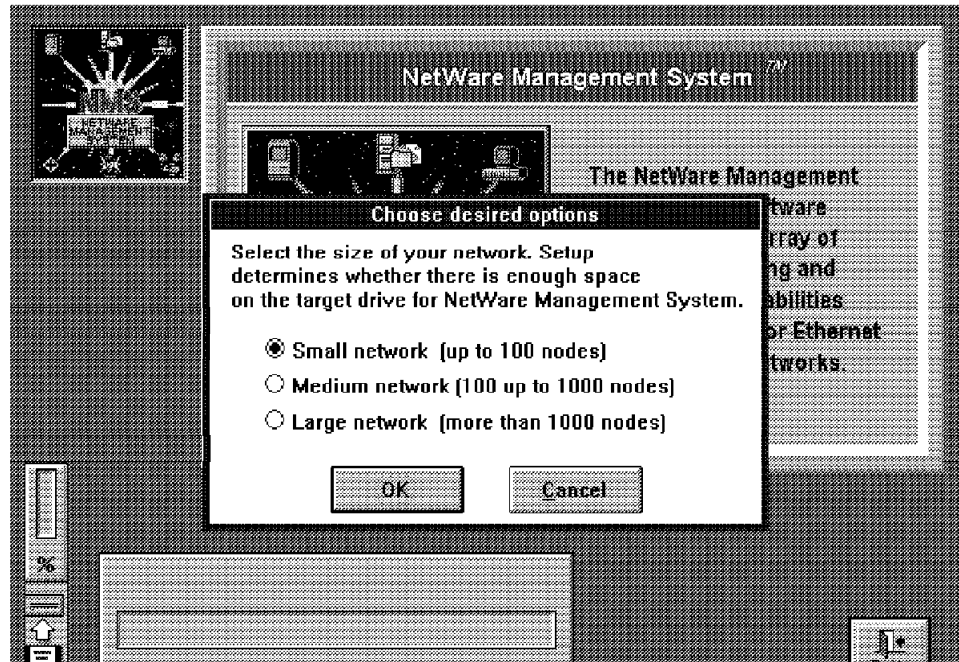
Figure 38. NMS Installation Program

You might need more or less disk space depending on how you customize NMS, the level of alarm activity on your network, and the frequency of your database maintenance.

After checking, it informs you of your remaining disk space.

12. Click on the **OK** button to modify the configuration files:

- CONFIG.SYS

- NET.CFG

- AUTOEXEC.BAT

- SYSTEM.INI

- WIN.INI

13. Insert all 11 diskettes as you are prompted for them.

14. You can now install the NetExplorer Agent server and NetExplorer Plus Agents servers software, or, if you choose to install the NMS Console only, skip the next step and go to step 19.

15. From the list that the setup presents, select the single NetWare server on which you want to install the NetExplorer software (NMS server) and click on the **Install** button.
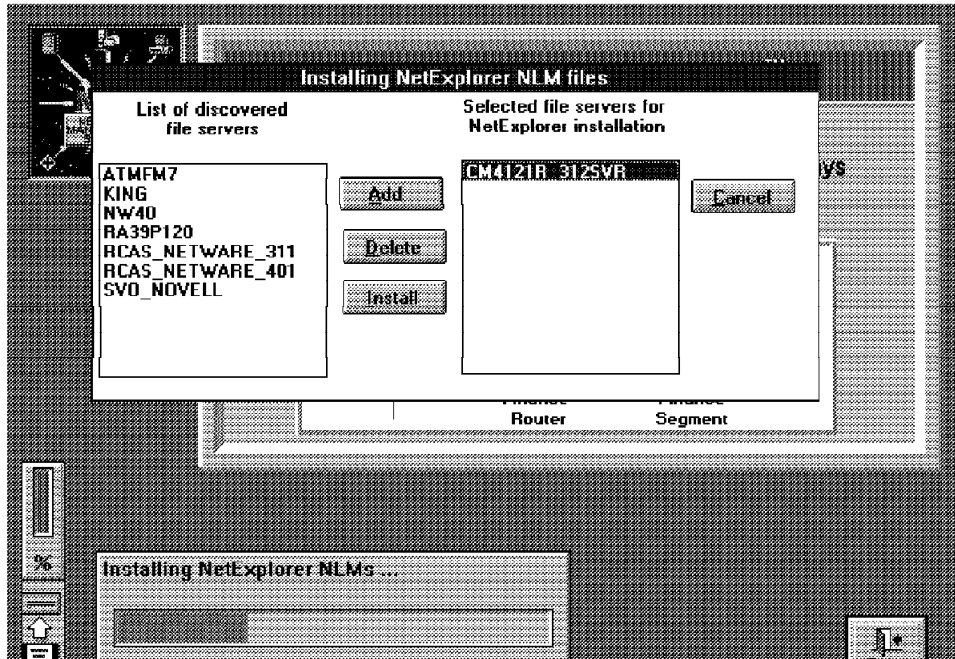
Figure 39. NMS Installation Panel

16. Enter a user name with supervisor rights (the default is supervisor) and its password for the server you selected.

    Click on the **Install** button.

    > **Important**
    >
    > If you choose a NetWare 4.01 server, the selected NetWare server must be in the *Bindery Context* of your NDS.
    >
    > Enter the ADMIN user name and its password. Be careful, if ADMIN is not under /Root, you must specify the complete NDS path.

    Setup logs in, using the specified user name, and transfers files over the network to the selected server. The setup program prepares the SYS:\SYSTEM\NETXPLOR.NCF and SYS:\SYSTEM\NMSBASE.NCF files and updates the AUTOEXEC.NCF with a commented reference to load the NETXPLOR.NCF.

17. From the list that setup presents, select all of the servers on which you want to install the NetExplorer *Plus* software and click on the **Install** button.
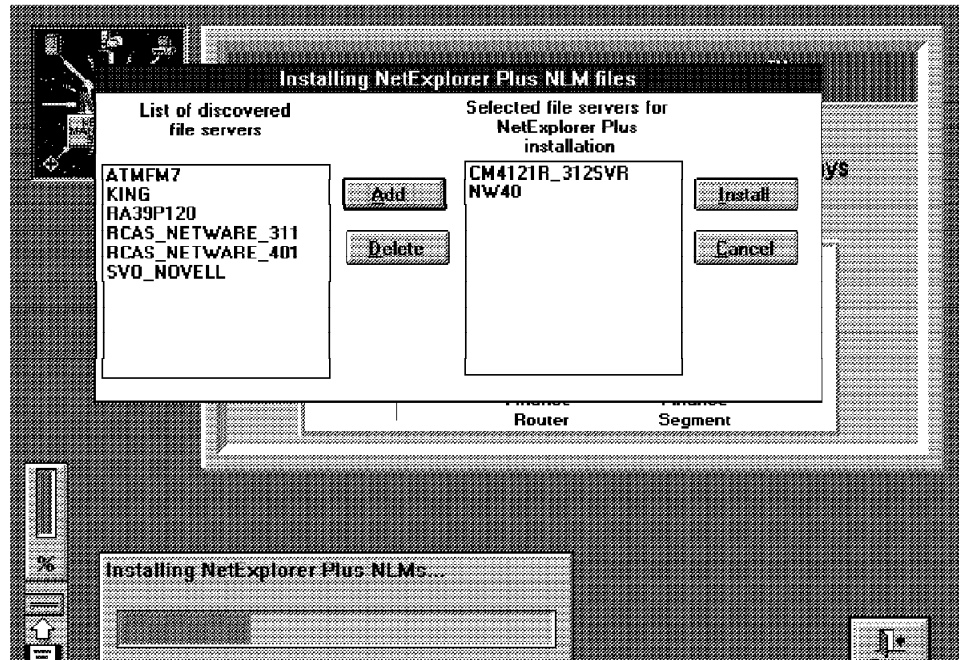
Figure 40. NMS Installation Panel

18. Enter a user name with supervisor rights and its password for each server you selected.

    Click on the **Install** button.

    Note

    If you choose a NetWare 4.01 server, the selected NetWare server must be in the *Bindery Context* of your NDS.

    Enter the ADMIN user name and its password. Be careful, if ADMIN is not under /Root, you must specify the complete NDS path.

    Setup logs in, using the specified user name, and transfers files over the network to that selected server.

    The setup program prepares SYS:\SYSTEM\NMSBASE.NCF file and updates the AUTOEXEC.NCF with a commented reference to load the .NCF file and NXPPLUS.NLM.
19. Exit the setup program and return to Windows.

    Check the NMS Configuration *before* you start all the components.

To have more information about the NMS installation or the NMS components description, load the NMS expert documentation from the NMS console window.
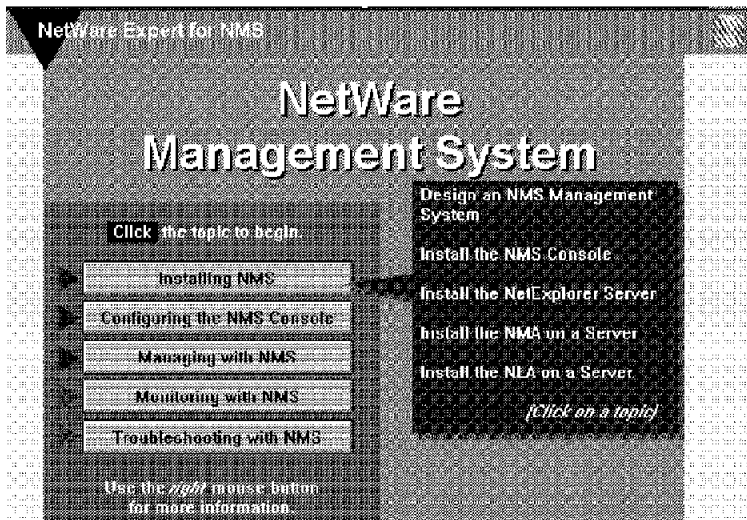
Figure 41. NMS Expert

2.5.3 Installing the NMS Updates

NMS002.EXE contains NMS 2.0 Rev C, which is the latest maintenance patch for the NetWare Management System. It is recommended for all NMS sites because it includes both fixes and new features for the NMS console, installation, and NetExplorer server. It supersedes NMS001.EXE and NMS202.EXE.

Before installing the NMS update, check and make sure of the following:

- NMS must be installed on your NMS console PC.
- You must have a minimum of 10 MB of free disk space on the disk drive where the NMS 2.0 software resides.

To install NMS 2.0 Rev C, you have to decompress the NMS002.EXE file:

```
NMS002.EXE      1461927     1-17-95     7:30p
```

It's a self-extracting file that includes the following:

```
Files Included      Size      Date       Time
  NMS002.TXT        29747    12-19-94     6.09p
    SETUP.BMP       22812    12-06-94     2:00a
    SETUP.EXE      276480    12-06-94     2:00a
    SETUP.INS       25267    12-06-94     2:00a
    SETUP.PKG         770    12-06-94     2:00a
  NMSPATCH.1       286819    12-06-94     2:00a
  NMSPATCH.2       863218    12-06-94     2:00a
 INS0762.LIB        18010    12-06-94     2:00a
 INSTALL.INS        83358    12-06-94     2:00a
 NMSSTAR.BMP         5998    12-06-94     2:00a
```

To install the NMS update software on the NMS Console, complete the following steps:

1. Start MS-Windows with the WIN command.

2. Insert the NetWare Management System Setup diskette into the A: drive.

3. From the MicroSoft Windows Program Manager, run the SETUP.EXE program
   found in the directory which you self-extracted NMS002.EXE (the NMS 2.0 Rev
   C files). In our case we ran:

   `D:\NMSPATCH\SETUP`

Figure 42. MS-Windows Dialog Box

4. Select the **Console Update** check box, the **Server Update** check box, or both,
   then click on **OK**.

   If you selected only the NMS Console Update, setup continues to completion.
   Skip to Step 7. Otherwise, Setup presents a list of servers to choose for
   updating. Continue with Step 5.

5. Select one NetExplorer server to update.

6. Enter the username and password when setup prompts you.

   The user must have supervisor equivalent privileges. The setup process
   continues to completion.

7. If you successfully updated the NMS Console software, exit Windows, then
   start Windows again. This ensures that the console software is loaded
   properly.

8. If you updated a server, restart the server.

   If you want to update another server, run the setup again. You do not need to
   restart MS Windows each time you update an additional server.

2.5.3.1 Installing the NMSXP1 Update

NMSXP1.EXE contains NMS Export Service 1.0. NMS Export Service enables you
to retrieve discovery information from the NMS database and transmit it to other
network management consoles. It has been tested to work with the IBM NetView
for AIX system. Before installing the NMS update, check the following:

* NMS must be installed on your NMS Console PC.
* You must have a minimum of 20 MB of free disk space on the disk drive where
  the NMS 2.0 software resides.

To install the Export Service, you have to decompress the NMSXP1.EXE file:

```
NMSXP1.EXE      434841    12-12-94      6:50a
```

It's a self-extracting file that contains the following:

```
Files Included      Size      Date      Time
  NMSXP1.TXT       7970    11-15-94    10:33a
    SETUP.Z       79881    11-08-94     1:00a
  SETUP.EXE      273920    11-08-94     1:00a
  SETUP.INS       17774    11-08-94     1:00a
```

```
    SETUP.PKG         192    11-08-94     1:00a
    TCPIP.EXE       43652    08-02-94     2:39p
   VTCPIP.386       10721    04-04-94     4:20a
 N_NTSID.DLL         4960    11-08-94     1:00a
  WINSOCK.DLL       35120    07-20-94    10:57a
 NOVASYNC.EXE        4672    07-20-94    10:57a
 N_NMSVER.DLL        5344    11-08-94     1:00a
 WLIBSOCK.DLL       47846    04-04-94     4:20a
  INS0762.LIB        2957    11-08-94     1:00a
```

Continue installing the NMS Export Service update using the following two steps:

1. Setting up the NMS Export Service Environment

   a. Verify that Novell TCP/IP is installed on the NMS Console.

      From DOS, type `TCPIP` to verify that TCP/IP loads or is already loaded.

      If you have not installed Novell TCP/IP, install the TCP/IP transport included with NetWare Client in NMS.

   b. Make a backup copy of all the files listed below:
      VTCPIP.386
      NOVASYNC.EXE
      TCPIP.EXE
      WINSOCK.DLL
      WLIBSOCK.DLL

   c. From the directory containing the NMSXP1 update files, copy VTCPIP.386 to C:\WINDOWS\SYSTEM.

   d. Copy the following TCP/IP files over all of the existing copies in the C:\NET\BIN directory:
      NOVASYNC.EXE
      TCPIP.EXE
      WINSOCK.DLL
      WLIBSOCK.DLL

2. Installing NMS Export Service

   During the installation, NMS Export Service setup adds four icons to your existing Novell-NMS program group:
   • Export Readme File
   • Export Scanner
   • Export Communication
   • Export Configuration.

   The NMS Export Service files will be copied to your existing NMS directory. NMS Export Service includes NMSXPORT.INI, which will be copied to the Windows directory. It contains information that is configurable through NMS Export Configuration.

   To install NMS Export Service, perform the following steps:
   a. Load the new TCP/IP transport, which you updated in the set up environment step.
   b. Start MS-Windows with the WIN command.
   c. From the MS-Windows Program Manager, select the **File** and **Run** options.
   d. In the Run Dialog Box, type: `C:\SETUP`
      Here drive:path is the path to the extracted NMSXP1.EXE file you downloaded.
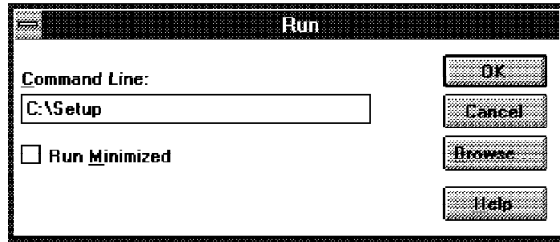
Figure 43. MS-Windows Dialog Box

This starts the NMS Export Service setup application. Setup will display a
dialogue box advising you that the setup application is initializing. Setup
will check your system path for WINSOCK.DLL. If the setup cannot find
WINSOCK.DLL, it will display a dialogue box informing you of this and quit.
If this happens, ensure that WINSOCK.DLL is in your path and run the
setup again. If an NMS application is running, setup will attempt to close it.
If the application cannot be shut down, the setup will prompt you that it
cannot continue and quit. Close the application manually, then run the
setup again.

e. Click on **OK** in the dialogue box that advises you that Novell NMS Export
Service will be installed in your NMS directory.

Setup begins decompressing all the NMS Export Service files to your
NMS\BIN directory.

When all the files are decompressed, the NMS Export Configuration
dialogue box is displayed.

f. Enter the configuration information.

If you want an explanation of any of the available fields, click the **Help**
button.

> **Note**
>
> If you need to make configuration changes later, you can run NMS
> Export Configuration from the NMS program group window.

g. Click on the **Readme** button to see details about NMS Export Service.
NMS Export Communication is launched automatically. You will see the
NMS Export Communication icon at the bottom of your screen. This icon
automatically appears every time you start MS Windows.

2.5.4 Installing NetExplorer Software on the NMS Server

Installing NetExplorer software on the NMS Server is usually done in the first NMS
installation, but if you didn't install it with the server or if you want to change the
previously specified NMS server name, proceed as follows:

Install the NetExplorer software on the NMS server and complete the following
steps.

1. Start MS-Windows with the WIN command.

2. Insert the NetWare Management System Setup diskette into the A: drive.

3. From the MS-Windows Program Manager, select the **File** and **Run** options.

4. In the Run Dialog Box, type: A:\SETUP.
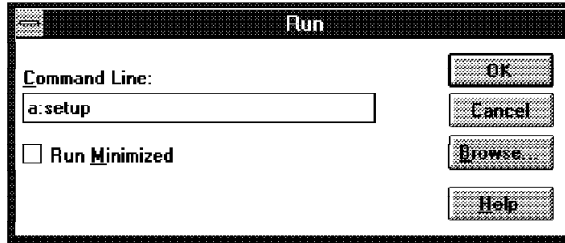
Figure 44. MS-Windows Dialog Box

5. From the NMS components list, only select **Install NetExplorer (management server)**.
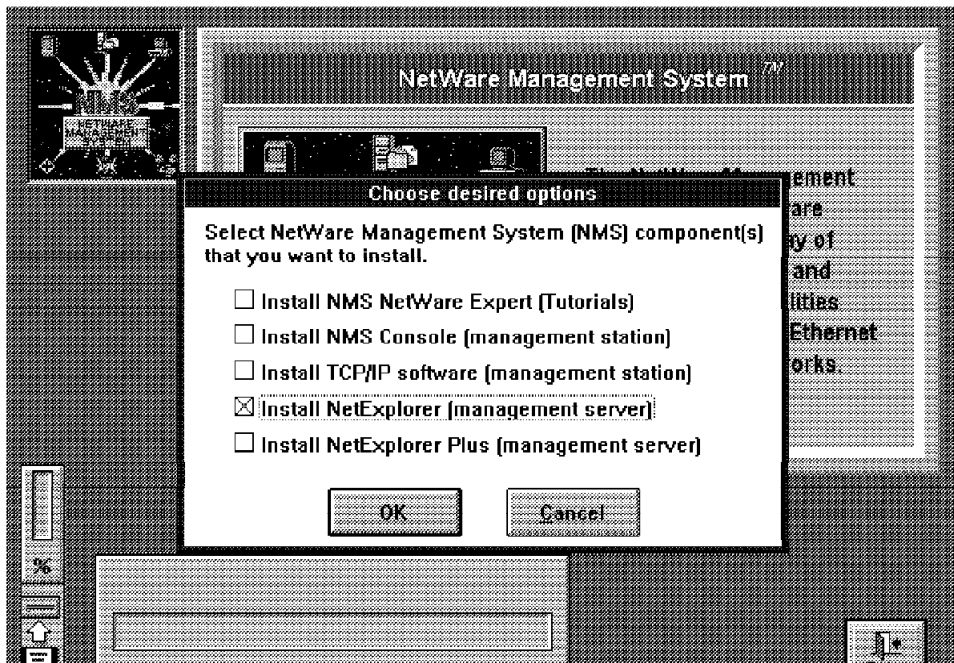
Figure 45. NMS Installation Program

6. In the list of discovered file servers:

   a. If it's the first installation, select the NMS server in the list and click on **Add**.

   b. If you have to modify the NMS Server, select it in the right list and click on **Delete**.

   Then select the new NMS Server you want in the list of discovered file servers and click on **Add**.
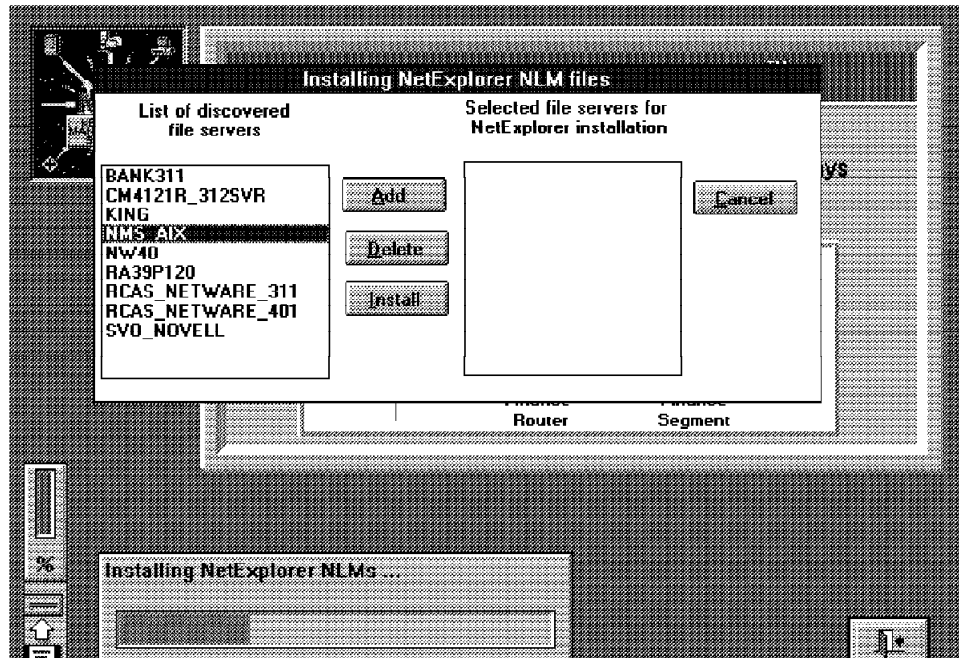
Figure 46. NMS NetExplorer Software Installation

When the NMS server is selected (in the right list), click on the **Install** button.

7. Enter a username with the Supervisor rights (the default is supervisor) and its password for the server selected.

   Click on the **Install** button.

   If you choose a NetWare 4.01 or V4.1 server, the selected NetWare server must be in the *Bindery Context* of your NDS.

   Enter the ADMIN username and its password. Be careful; if ADMIN is not under [Root], you must specify the complete NDS path.

   Setup logs in, using the specified username, and transfers files over the network to the selected server. The setup program prepares the SYS:\SYSTEM\NETXPLOR.NCF and SYS:\SYSTEM\NMSBASE.NCF files and updates the AUTOEXEC.NCF with a commented reference to load NETXPLOR.NCF.

8. Exit the Installation program to Windows.

Check the NetExplorer Installation Files, and remove the comment for NETXPLOR.NCF.

- **AUTOEXEC.NCF**

```
set Time Zone = <<NO TIME ZONE>>
set Daylight Savings Time Offset = 1:00:00
set Start Of Daylight Savings Time =
set End Of Daylight Savings Time =
set Default Time Server Type = SECONDARY
set Bindery Context = IBM

file server name NMS_AIX
ipx internal net 12345678
```

```
# $NMSBASE$ DO NOT DELETE THIS LINE
# Netware Management System installation has
# created the following NMSBASE.NCF file.
# Review the load sequence of NLMs in NMSBASE.NCF.
# Make sure that the NLM loaded by NMSBASE.NCF
# do not conflict with your existing setup.
# Uncomment the following line after review....
# NMSBASE.NCF *

* Uncomment the line to take effect after rebooting the server.

# Load the SNMP Agent Software
Load SNMP verbose Control= Trap=  *

* Modify this line with the following parameters:
Control is the Read/Write community name used by SNMP
Trap is the community name for sending Trap

Load TCPIP Forward=Yes
Load SNMPLOG

Load 3c523 SLOT=7 FRAME=Ethernet_802.3 NAME=Ether_IPX
bind IPX to Ether_IPX net=CAFE0001

Load 3c523 SLOT=7 FRAME=Ethernet_II NAME=Ether_IP
Bind IP to Ether_IP addr=9.24.104.114 mask=255.255.255.0

load TOKEN SLOT=3 NODE=400052005190M FRAME=Token-Ring MSB NAME=TOKEN
load ROUTE board=2
bind IPX to TOKEN_1T_EN-RING net=9

load TOKEN SLOT=3 FRAME=Token-Ring_Snap NAME=TOKEN_IP
Load ROUTE board=3
Bind IP to TOKEN_IP addr=9.24.104.54 mask=255.255.255.0

# $NETXPLOR$ DO NOT DELETE THIS LINE
# NetWare Management System installation has
# created the following NETXPLOR.NCF file.
# Review the load sequence of NLMs in NETXPLOR.NCF.
# Make sure that the NLM loaded by NETXPLOR.NCF
# do not conflict with your existing setup.
# Uncomment the following line after review....
# NETXPLOR.NCF  *

* Uncomment the line to take effect after rebooting the server.

Load remote
Load rspx

Mount ALL

Load Install
Load TCPCON
Load Monitor /p
```

NMSBASE.NCF

```
#-------------------------------------------------------
#                 Novell NetWare Management System
#                         Version 2.0
#
#-------------------------------------------------------
# NMSBASE.NCF: NetWare Management System Base NCF file
#-------------------------------------------------------
# Description: This NCF file loads all the NetWare 4.0
```

```
#               system components that are required by:
#
#               $VERSION LOG
#               $VERSION NMS 2.0 NetExplorer NLMs
#
#               You must load the NLMs in the top part of
#               your AUTOEXEC.NCF before you load any protocol
#               stacks (for example, load tcpip) or any network
#               adapter drivers (for example, load ne2000).
#------------------------------------------------------------

# Step-1: Review the following NetWare system parameters
#         for the IPX network discovery NLM files.
#         Note that these are MINIMUM VALUES. If your NetWare
#         system requires larger values edit the following
#         lines to set the parameters to required values.
#
#$ENVIRONMENTAL VARIABLES
#
SET MAXIMUM PACKET RECEIVE BUFFERS=500
SET UPGRADE LOW PRIORITY THREADS = ON

# Step-2: Load the following NetWare system software
#         Do not change the order in which the NLM files
#         are loaded.

LOAD SYS:\SYSTEM\STREAMS
LOAD SYS:\SYSTEM\CLIB
LOAD SYS:\SYSTEM\SPXS
LOAD SYS:\SYSTEM\IPXS
LOAD SYS:\SYSTEM\TLI
LOAD SYS:\SYSTEM\MATHLIBC
```

- **NETXPLOR.NCF**

```
#------------------------------------------------------------
#             Novell NetWare Management System
#                       Version 2.0
#------------------------------------------------------------
# NETXPLOR.NCF: NetExplorer NCF File
#
# WARNING:   You should not modify this file unless you need to change
#            one of the configuration parameters documented below.
#            Other changes to this file are not recommended.
#------------------------------------------------------------
# MODULE DEPENDENCIES
#
# NETXPLOR.NLM  -   STREAMS.NLM SPXS.NLM IPXS.NLM CLIB.NLM TLI.NLM
#                   MATHLIBC.NLM.
# NXPIP.NLM     -   STREAMS.NLM SPXS.NLM IPXS.NLM CLIB.NLM TLI.NLM
#                   MATHLIBC.NLM TCPIP.NLM and SNMP.NLM.
# NXPIPX.NLM    -   STREAMS.NLM SPXS.NLM IPXS.NLM CLIB.NLM TLI.NLM
#                   MATHLIBC.NLM NXPMEM.NLM and SNMP.NLM.
# NXPLANZ.NLM   -   STREAMS.NLM SPXS.NLM IPXS.NLM CLIB.NLM TLI.NLM
#                   MATHLIBC.NLM NXPMEM.NLM TCPIP.NLM and SNMP.NLM.
#
# LOAD ORDER
#
# The order in which the NetExplorer modules are loaded is critical. You
# must follow the same order as listed in this file. Loading NXPIP.NLM
# and NXPLANZ.NLM are optional. For best results, load NXPIP.NLM if your
# internet uses IP, and load NXPLANZ.NLM if you are running NetWare LANalyzer
# Agents or LANtern network monitors.
#
# Load Parameter Description
```

```
#
# LOAD SYS:\NMDISK\NETXPLOR /B count
#
# NETXPLOR.NLM module is a repository for topology data. It receives data
# from the discovery modules (NXPIP, NXPIPX, and NXPLANZ) and
# transmits this data to the NetExplorer Manager on request. This module
# must be loaded before any of the other discovery  modules are loaded.
#
# /B count      This optional parameter specifies the maximum number of
#               backups of NETXPLOR.DAT (the NetExplorer data file) that
#               NETXPLOR.NLM can store at any time. The backup copies
#               are stored in SYS:\NMDISK\DATSAV directory. The range
#               is between 0 and 999 inclusive. A 0 indicates no backup
#               copies of NETXPLOR.DAT are made; consequently, repeated
#               execution of the discovery modules overwrites the
#               previous NETXPLOR.DAT file.
#
#               Default: 0 copies if /B option is not used.
#
# LOAD SYS:\NMDISK\NXPIP /C filename /B /S xxx.x.x.x
#
# NXPIP.NLM module discovers the topology of IP networks. This module
# requires TCPIP.NLM and SNMP.NLM to be loaded.
#
# /C filename   This parameter allows you to specify a file containing
#               a list of SNMP community strings to be used for
#               communicating with IP devices. This file should be
#               placed in the SYS:\NMDISK directory. Each community string
#               must be specified as a separate line in the file.
#               The following is a sample of the community file:
#               _____
#               | public
#               | administrator
#
#               The default is no community file - NXPIP uses the
#               community name "public".
#
# /B            This parameter uses a RIP broadcast to discover the local router
#
# /S xxx.x.x.x  This parameter specifies the IP address of the router that will
#               be used to discover other IP routers.
#
# NOTE:         NXPIP.NLM can be forced to discover only specific networks.
#               This is done by specifying the network addresses of the
#               networks that need to be discovered in the SYS:\NMDISK\NXPIP.INI
#               file. If the file does not exist, the entire IP network, as
#               defined by the class of the IP network number will be discovered
#               For example, if the server's IP address is 133.33.65.100,
#               NXPIP discovers networks with network address 133.33.xx.xx.
#               The following is a sample of the NXPIP.INI file:
#               _____
#               | 11.0.0.0
#               | 130.57.0.0
#               | 200.5.7.0
#
# LOAD SYS:\NMDISK\NXPIPX
#
# NXPIPX.NLM module discovers the topology of IPX networks. The file
# SYS:\NMDISK\NXPIPX.INI specifies the initialization parameters
# associated with this module.
#
# LOAD SYS:\NMDISK\NXPLANZ /N /O /C filename
#
# NXPLANZ.NLM module discovers NetWare LANalyzer agents and LANtern
```

```
# network monitors. This module requires TCPIP.NLM and SNMP.NLM to be loaded.
#
# /N            This parameter disables station discovery. This option, when
#               used discovers only NetWare LANalyzer Agent servers or
#               LANtern network monitors.
#
#               Default: Station discovery is enabled.
#
# /O            This parameter runs NXPLANZ discovery once and
#               then terminates.
#
#               Default: NXPLANZ discovery is continuous.
#
# /C filename   This parameter allows you to specify a file containing a list
#               of SNMP community strings to be used for communicating with
#               NetWare LANalyzer Agents. This file should be placed in the
#               SYS:\NMDISK directory. Each community string must be specified
#               as a separate line in the file. The following is a sample of
#               the community file:
#               _____
#               | public
#               | administrator
#
#               The default is no community file - NXPLANZ uses the
#               community name "public".
#
# NOTE:         To discover NetWare LANalyzer Agents via IP (on networks that
#               do not route IPX), you must enter the IP address of the agent
#               in the file SYS:\NMDISK\NLA.ADR. Also, you must enter the IP
#               address of all LANtern network monitors in this file. You may
#               also enter the internal IPX network number of NetWare LANalyzer
#               Agents in this file only if your internetwork contains SAP
#               filtering and you are not running NXPIPX. The prototype file
#               is as follows:
#               _____
#               | #
#               | # SYS:\NMDISK\NLA.ADR
#               | #
#               | # '#' identifies a comment
#               | # Each line describes a single NetWare LANalyzer
#               | # Agent or LANtern network monitor and is as
#               | # follows:
#               | # <IP Address | IPX Network Number>,[<Name>',<S|L>
#               | # where:
#               | # IP Address - the IP node address of the agent
#               | # IPX Number - the internal network number of a
#               | #              a NetWare LANalyzer Agent server
#               | # Name - an optional name of the agent
#               | # S - Server, a NetWare LANalyzer Agent
#               | # L - LANtern, a LANtern network monitor
#               | #
#               | 127.1.2.3,LANtern-XYZ,L
#               | 127.4.5.6,SERVER-JUPITER,S
#               | 12345678,SERVER-VENUS,S
#               | 11111111,,S
#               |_____
#-----------------------------------------------------------

SEARCH ADD SYS:\NMDISK

LOAD SYS:\NMDISK\NETXPLOR

LOAD SYS:\NMDISK\NXPIP
```

```
LOAD SYS:\NMDISK\NXPIPX

LOAD SYS:\NMDISK\NXPLANZ
```

2.5.5 Installing NetExplorer Plus Software on all Servers

The NetExplorer Plus software must be installed on all NetWare servers to provide additional information such as:

- Connection number
- Connection name

It is also considered as a collection point of bindery services for the NetExplorer server which uses SAPs to gather information.

The NetExplorer Plus software installation is usually done in the first NMS installation, but, if you waited or if you have to add some servers in the NetExplorer Plus server list, proceed as follows:

1. Start MS-Windows with the WIN command.

2. Insert the NetWare Management System Setup diskette into drive A:.

3. From the MS-Windows Program Manager, select the **File** and **Run** options.

4. In the Run Dialog Box, type: `A:\SETUP`
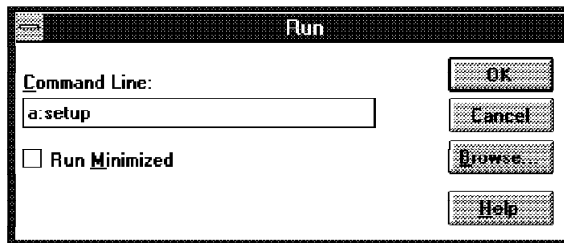
Figure 47. MS-Windows Dialog Box

5. From the NMS components list, select only **Install NetExplorer Plus (management server)**.
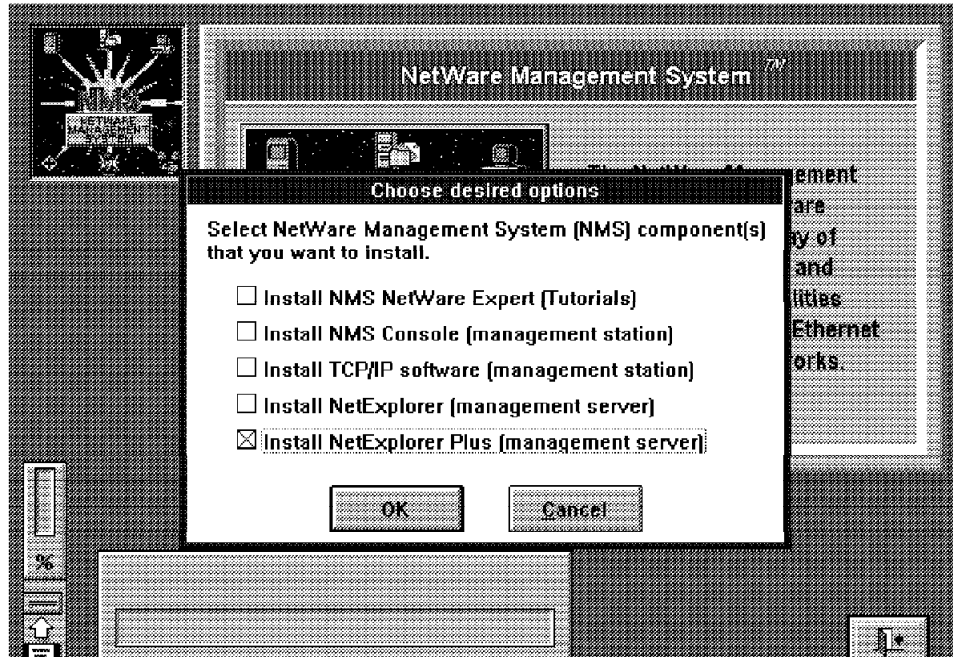
Figure 48. NMS Installation Program

6. In the list of discovered file servers:

   a. If it's the first installation, select all the NetWare servers you want installed with the NetExplorer Plus agent, and click on **Add**.

   b. If you want to add a NetExplorer agent, select the previously NetExplorer Plus agents in the right list and click on the **Delete** button.

      Then, select the new NetExplorer Plus Agents in the list of discovered servers and click on **Add**.
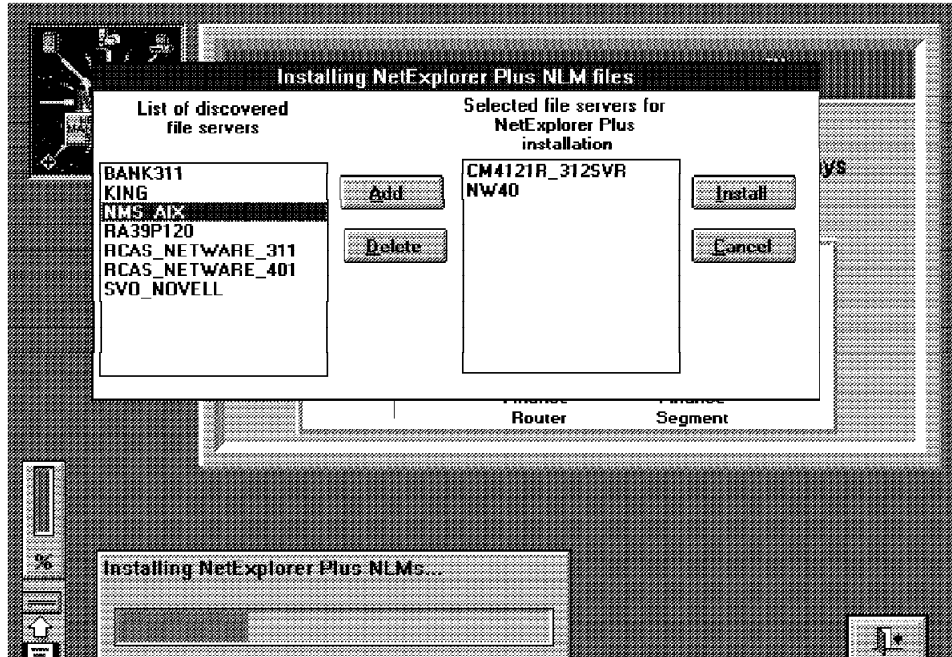
Figure 49. NMS NetExplorer Plus Software Installation

When the NetExplorer Plus agents are selected (in the right list), click on the
Install button.

7. Enter a username with supervisor rights (the default is supervisor) and its
password for the server selected.

Click on the **Install** button.

Note

If you choose a NetWare 4.x server, the selected NetWare server must be
in the *Bindery Context* of your NDS.

Enter the ADMIN username and its password. Be careful; if ADMIN is not
under [Root], you must specify the complete NDS path.

Setup logs in, using the specified username, and transfers files over the
network to the selected server. The setup program prepares the
SYS:\SYSTEM\NMSBASE.NCF file and updates the AUTOEXEC.NCF with a
commented reference to load the .NCF file and NXPPLUS.NLM.

8. Exit the Installation program to Windows.

Check the NetExplorer Plus installation files and remove the comment lines as
follows:

• **AUTOEXEC.NCF**

```
set Time Zone = <<NO TIME ZONE>>
set Daylight Savings Time Offset = 1:00:00
set Start Of Daylight Savings Time =
set End Of Daylight Savings Time =
set Default Time Server Type = SECONDARY
set Bindery Context = IBM
```

```
file server name NMS_AIX
ipx internal net 12345678

# $NMSBASE$ DO NOT DELETE THIS LINE
# Netware Management System installation has
# created the following NMSBASE.NCF file.
# Review the load sequence of NLMs in NMSBASE.NCF.
# Make sure that the NLM loaded by NMSBASE.NCF
# do not conflict with your existing setup.
# Uncomment the following line after review....
NMSBASE.NCF

# Load the SNMP Agent Software
Load SNMP verbose Control=public Trap=public

# Load NetExplorer Plus
Load SYS:SYSTEM\NXPPLUS

Load TCPIP Forward=Yes
Load SNMPLOG

Load 3c523 SLOT=7 FRAME=Ethernet_802.3 NAME=Ether_IPX
bind IPX to Ether_IPX net=CAFE0001

Load 3c523 SLOT=7 FRAME=Ethernet_II NAME=Ether_IP
Bind IP to Ether_IP addr=9.24.104.114 mask=255.255.255.0

Load TOKEN SLOT=3 NODE=400052005190M FRAME=Token-Ring MSB NAME=TOKEN_1_EN-RING
load ROUTE board=2
bind IPX to TOKEN_1T_EN-RING net=9

load TOKEN SLOT=3 FRAME=Token-Ring_Snap NAME=TOKEN_IP
Load ROUTE board=3
Bind IP to TOKEN_IP addr=9.24.104.54 mask=255.255.255.0

# $NETXPLOR$ DO NOT DELETE THIS LINE
# Netware Management System installation has
# created the following NETXPLOR.NCF file.
# Review the load sequence of NLMs in NETXPLOR.NCF.
# Make sure that the NLM loaded by NETXPLOR.NCF
# do not conflict with your existing setup.
# Uncomment the following line after review....
NETXPLOR.NCF

load remote
load rspx

Mount ALL

Load Install
Load TCPCON
Load Monitor /p
```

- **NMSBASE.NCF**

```
              #----------------------------------------------------------------
              #                Novell NetWare Management System
              #                          Version 2.0
              #
              #----------------------------------------------------------------
              # NMSBASE.NCF: NetWare Management System Base NCF file
              #----------------------------------------------------------------
              # Description: This NCF file loads all the NetWare 4.0
              #              system components that are required by:
              #
              #              $VERSION LOG
              #              $VERSION NMS 2.0 NetExplorer NLMs
              #
              #              You must load the NLMs in the top part of
              #              your AUTOEXEC.NCF before you load any protocol
              #              stacks (for example, load tcpip) or any network
              #              adapter drivers (for example, load ne2000).
              #----------------------------------------------------------------

              # Step-1: Review the following NetWare system parameters
              #         for the IPX network discovery NLM files.
              #         Note that these are MINIMUM VALUES. If your NetWare
              #         system requires larger values edit the following
              #         lines to set the parameters to required values.
              #
              #$ENVIRONMENTAL VARIABLES
              #
              SET MAXIMUM PACKET RECEIVE BUFFERS=500
              SET UPGRADE LOW PRIORITY THREADS = ON

              # Step-2: Load the following NetWare system software
              #         Do not change the order in which the NLM files
              #         are loaded.

              LOAD SYS:\SYSTEM\STREAMS
              LOAD SYS:\SYSTEM\CLIB
              LOAD SYS:\SYSTEM\SPXS
              LOAD SYS:\SYSTEM\IPXS
              LOAD SYS:\SYSTEM\TLI
              LOAD SYS:\SYSTEM\MATHLIBC
```

2.6 NMA

The Intel machine from which you are installing the NetWare Management Agent
software should have at least 3 MB of free disk space on the hard disk drive where
you installed the NMS software. It's used for temporary copies of all server files. A
list of hardware requirements for all NetWare servers where NMA will be installed
follows:

- 1.5 MB RAM must be available for the NetWare Management Agent process (2
  MB are recommended).

  After loading the NMA software on the server, verify that you have at least 40%
  of available memory resources available for file caching.
- At least 2 MB of free disk space on the SYS: volume.

> ┌─ **Note** ───┐
>
> Do not install the NetWare Management Agent software before installing the
> NetExplorer and NetExplorer Plus software. Be sure that all the NMS
> components are installed and NMSBASE.NCF is configured.
>
> If you are using a NetWare 4.01 server, be sure that the NetWare 4.01 client
> software is installed; if not, you will get an error message.
>
> └──┘

To install the NMA software, complete the following steps:

1. Start MS-Windows with the WIN command.

2. Insert the NMA Setup diskette into the A: drive.

3. From the MS-Windows Program Manager, select the **File** and **Run** options.

4. In the Run Dialog Box, type: `A:\SETUP`
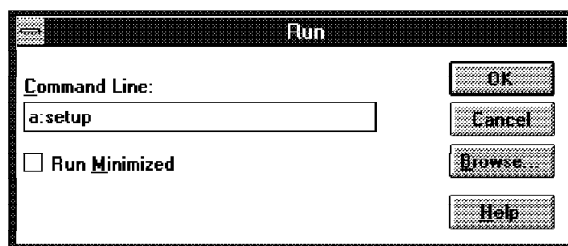
Figure 50. MS-Windows Dialog Box

   The setup program checks for free disk space in the NMS directory and copies
   the NetWare Management files to the hard disk.

5. The setup program prompts for the NETMAN password as in Figure 51 on
   page 84.
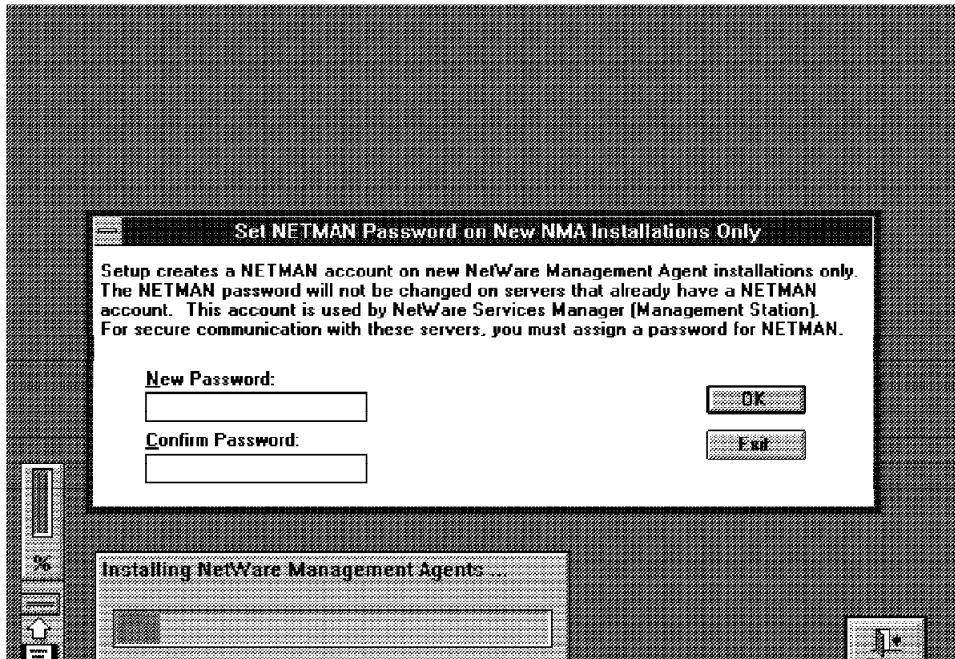
Figure 51. NMA Installation - NETMAN Password Registration

- If you are installing NMA on any new servers, enter your NETMAN account password, and then click on **OK**.
- If you are reinstalling NMA on servers, the setup program leaves the NETMAN password unchanged.

6. Click on **OK** when the setup program reminds you to register the NETMAN password with the NMS Console.

7. In the SLIST equivalent list that the setup program displays, select the name of each server on which you want to install the NMA software.
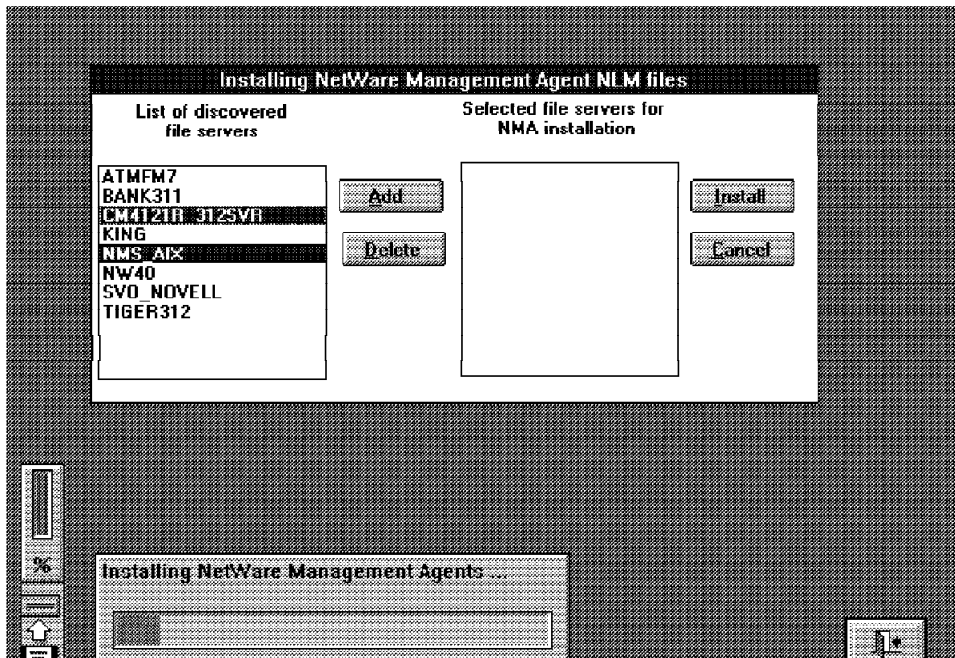
Figure 52. NMA Setup Program

When all the NMA servers are selected (in the right list), click on the **Install** button.

8. Enter a username with supervisor rights (the default is supervisor) and the password for each server selected. The supervisor password is used as the default for all servers, until the setup program finds a server for which it does not work.

   Click on the **Install** button.

   ┌─ **Note** ──┐
   │   │
   │ If you choose a NetWare 4.x server, the selected NetWare server must be │
   │ in the *Bindery Context* of your NDS.   │
   │   │
   │ Enter the ADMIN username and its password. Be careful; if ADMIN is not │
   │ under [Root], you must specify the complete NDS path.   │
   │   │
   └──┘

   Setup logs in using the specified username and transfers files over the network to the selected server. The setup program prepares the SYS:\SYSTEM\NMA.NCF and SYS:\SYSTEM\NMSBASE.NCF files and updates the AUTOEXEC.NCF with a commented reference to load NMA.NCF.

9. If you are prompted, check the incompatible files that you want the setup program to update.

   The setup program prompts you only if it finds more recent files; in this case, do not replace those files.

   It automatically replaces older files.

10. When the installation is completed on all the selected servers, the setup program displays a brief message and then displays the Write file that discusses NMA software.

11. Return to Windows.

On each server in which you installed the NetWare Management Agent software, verify that the .NCF files are correct and that they do not conflict with any other .NCF files used by your system. Check the NMA configuration files, and remove the comment marks as follows:

- **AUTOEXEC.NCF**

```
set Time Zone = <<NO TIME ZONE>>
set Daylight Savings Time Offset = 1:00:00
set Start Of Daylight Savings Time =
set End Of Daylight Savings Time =
set Default Time Server Type = SECONDARY
set Bindery Context = IBM

file server name NMS_AIX
ipx internal net 12345678

# $NMSBASE$ DO NOT DELETE THIS LINE
# Netware Management System installation has
# created the following NMSBASE.NCF file.
# Review the load sequence of NLMs in NMSBASE.NCF.
# Make sure that the NLM loaded by NMSBASE.NCF
# do not conflict with your existing setup.
# Uncomment the following line after review....
```

```
NMSBASE.NCF

# Load the SNMP Agent Software
Load SNMP verbose Control=public Trap=public

# Load NetExplorer Plus
Load SYS:SYSTEM\NXPPLUS

Load TCPIP Forward=Yes
Load SNMPLOG

Load 3c523 SLOT=7 FRAME=Ethernet_802.3 NAME=Ether_IPX
bind IPX to Ether_IPX net=CAFE0001

Load 3c523 SLOT=7 FRAME=Ethernet_II NAME=Ether_IP
Bind IP to Ether_IP addr=9.24.104.114 mask=255.255.255.0

load TOKEN SLOT=3 NODE=400052005190M FRAME=Token-Ring MSB NAME=TOKEN_1_EN-RING
load ROUTE board=2
bind IPX to TOKEN_1T_EN-RING net=9

load TOKEN SLOT=3 FRAME=Token-Ring_Snap NAME=TOKEN_IP
Load ROUTE board=3
Bind IP to TOKEN_IP addr=9.24.104.54 mask=255.255.255.0

# $NETXPLOR$ DO NOT DELETE THIS LINE
# NetWare Management System installation has
# created the following NETXPLOR.NCF file.
# Review the load sequence of NLMs in NETXPLOR.NCF.
# Make sure that the NLM loaded by NETXPLOR.NCF
# do not conflict with your existing setup.
# Uncomment the following line after review....
NETXPLOR.NCF

Load remote
Load rspx

Mount ALL

Load Install
Load TCPCON
Load Monitor /p

# $NMA$ DO NOT DELETE THIS LINE
# Netware Management System installation has
# created the following NMA.NCF file.
# Review the load sequence of NLMs in NMA.NCF.
# Make sure that the NLM loaded by NMA.NCF
# do not conflict with your existing setup.
# Uncomment the following line after review....
# NMA.NCF
*

* Uncomment the line to take effect after rebooting the server.
```

- **NMA.NCF**

```
#---------------------------------------------------------------
#                 Novell NetWare Services Manager
#                        Version 1.5
#---------------------------------------------------------------
# NMA.NCF: NetWare Management Agent NCF file
#---------------------------------------------------------------
# Description: This NCF file loads all the NetWare Management Agent
#              software for the NetWare 3.X. The following shows
#              the relationship between the the components loaded by this NCF
#              file. It also shows the dependencies of
#              these components on other system software.
#
#      RELATIVE
#      LOAD-ORDER  +----------------------------------+
#         1.       |   SOFTWARE  FROM  NMSBASE.NCF    |
#                  +----------------------------------+
#                               |      +--------------+
#         2.                    |      |   SNMP.NLM   |----+
#                               |      +--------------+    |
#                  +----------------------------------+    |
#         3.       |            NMAGENT2.NLM          |    |
#                  +----------------+---------+------+    |
#                  +--------------+ |         |      |    |
#         4.       | SIDEWIND.NLM | |         |      |    |
#                  +--------------+ |         |      |    |
#                  +--------------+ |         |      |    |
#         5.       | RATTLER.NLM  | |         |      |    |
#                  +--------------+ |         |      |    |
#                  +--------------+ |         |      |    |
#         6.       | SPAGENT.NLM  |--+        |      |    |
#                  +--------------+           |      |    |
#                                      +------+------+    |
#         7.                           |  NW2SNMP.NLM |----+
#                                      +--------------+    |
#                                      +--------------+    |
#         8.                           |  NWTRAP.NLM  |----+
#                                      +--------------+
#
#---------------------------------------------------------------

# Step-1: Load the NetWare Management Agent software.
LOAD SYS:\SYSTEM\NMAGENT
LOAD SYS:\SYSTEM\NMAGENT2
LOAD SYS:\SYSTEM\SIDEWIND /N
LOAD SYS:\SYSTEM\RATTLER
LOAD SYS:\SYSTEM\SPAGENT

# NOTE: RATTLER.NLM is not needed by the Microsoft Windows version
#       of NetWare Services Manager. However, it is needed by the
#       IBM OS/2 version of NetWare Services Manager.
UNLOAD RATTLER

# Step-2: Load the NetWare to SNMP trap translator software.
#         OPTION: If you want to change the default community name
#                 of traps from PUBLIC, use COMMUNITY=<CommunityName>
#                 option with NW2SNMP.NLM and /C=<CommunityName>
#                 option with NWTRAP.NLM.  For example:
#                 load SYS:\SYSTEM\NW2SNMP COMMUNITY=administrator
```

```
#                          load SYS:\SYSTEM\NWTRAP /C=administrator
#

LOAD SYS:\SYSTEM\NW2SNMP COMMUNITY=public GA=on
LOAD SYS:\SYSTEM\NWTRAP /C=public
```

2.7 NetWare LANalyzer

The NetWare LANalyzer Agent component of the NetWare Management System (NMS) product family adds additional functions to NMS. You have to install the LANalyzer Agent software on a server on each LAN segment you want to manage. The software is packaged separately and is used like an NMS option.

You will need to check the LANalyzer prerequisites before starting the installation. You will need the following:

1. A NetWare V3.12 or V4.x server running on each segment to manage.
2. A token-ring or Ethernet adapter in the server on which you plan to install the LANalyzer agent software. The LANalyzer agent needs a promiscuous mode driver for the network adapter board.

> **Note**
>
> Verify that your adapter is completely compatible with LANalyzer. Check NetWire or contact the board vendor for a certified promiscuous mode.

  The IBM Token-Ring Adapter/A and IBM Ethernet Adapter/A are not compatible. We used a 3COM Etherlink/MC Adapter with the promiscuous LAN drivers V4.0.
3. 2 MB of memory more on each server you want to install the LANalyzer software.
4. Sufficient disk space for code on each NetWare server with LANalyzer.
5. The NMS products have to be installed and running.

To install the LANalyzer software, complete the following steps:

1. On your NetWare operating system console, load the Install utility by typing:

   `:Load Install`

2. From the menu that it is displayed, select **Product Options** and press Enter.

3. Press the Insert key.

4. Insert the NetWare LANalyzer Agent Disk 1 (NLA_1) diskette into a floppy disk drive.

5. From the program prompt, enter the path of the installation program. In this case, it is the floppy drive.

6. Select all the adapter boards that you want to monitor (with the F5 key).

Figure 53. NetWare LANalyzer Installation
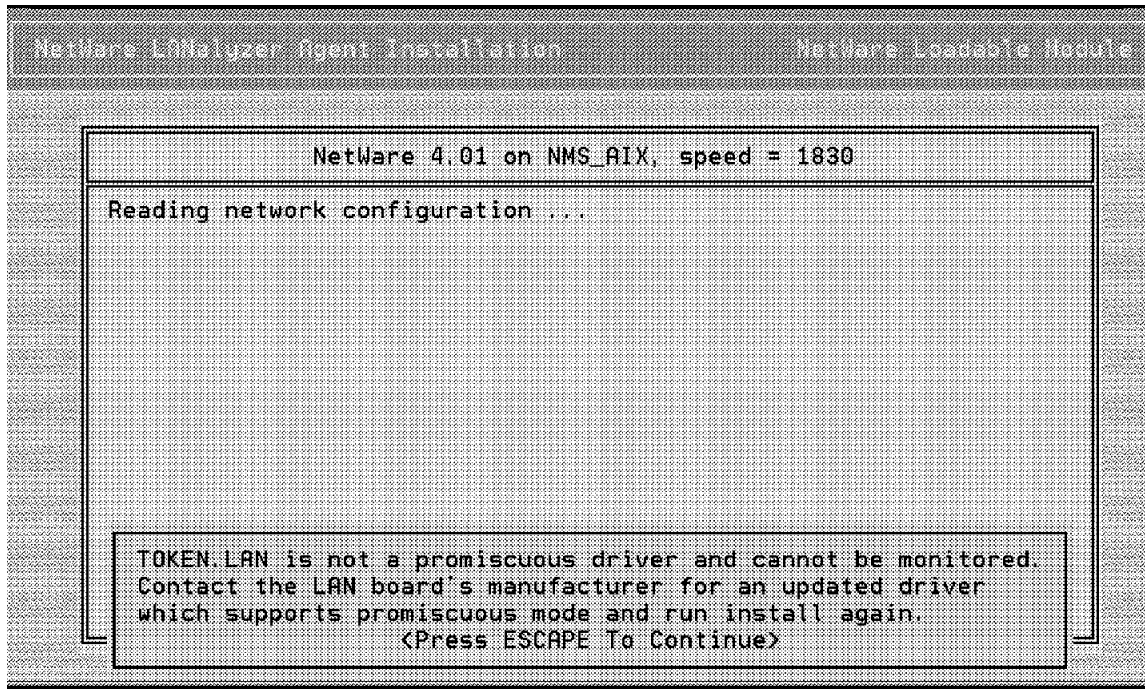
To use a driver that is not shipped with NetWare LANalyzer Agent, you must copy the driver to the DRIVERS directory on Disk1. If you try to install LANalyzer Agent using a driver that is not in that directory, you will receive the following message:

```
"Current <driver_name> is promiscuous capable but its updated driver was
not found"
```

Use installation disk 1 to solve this problem.
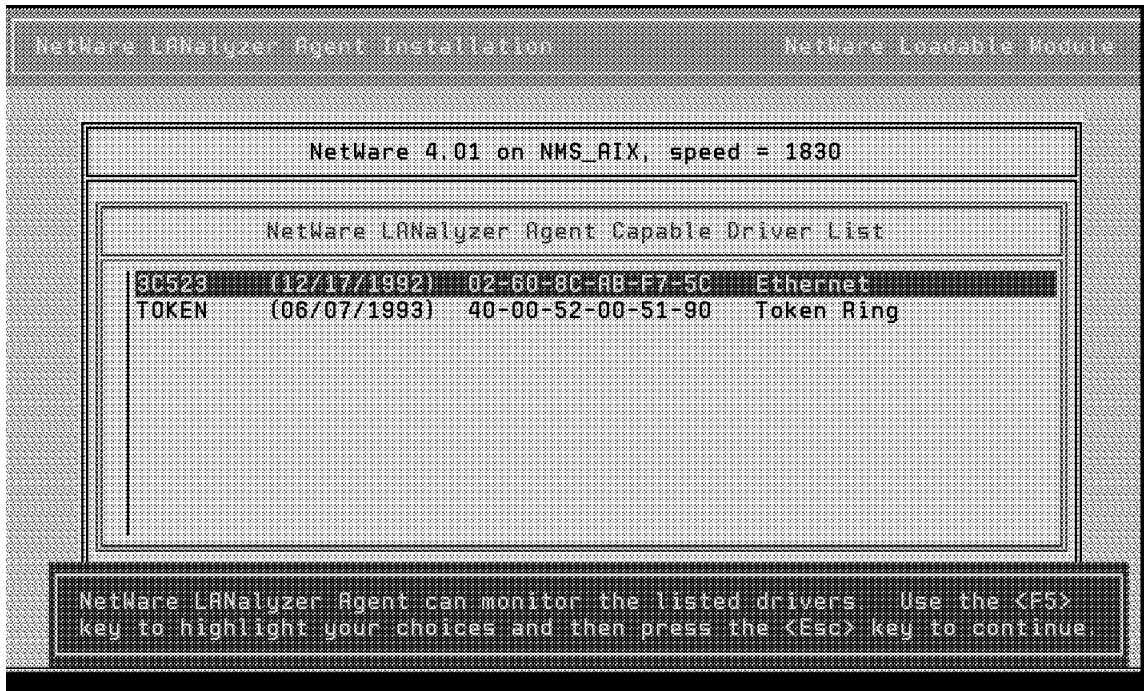
Figure 54. NetWare LANalyzer Installation Message

7. Continue the installation with the others diskettes.

On each server in which you installed the NetWare LANalyzer Agent software, verify that the .NCF files are correct and that they do not conflict with any other .NCF files used by your system. Check the LANalyzer configuration files, and remove the comment marks as follow:

- **AUTOEXEC.NCF**

```
set Time Zone = <<NO TIME ZONE>>
set Daylight Savings Time Offset = 1:00:00
set Start Of Daylight Savings Time =
set End Of Daylight Savings Time =
set Default Time Server Type = SECONDARY
set Bindery Context = IBM

file server name NMS_AIX
ipx internal net 12345678

# $NMSBASE$ DO NOT DELETE THIS LINE
# NetWare Management System installation has
# created the following NMSBASE.NCF file.
# Review the load sequence of NLMs in NMSBASE.NCF.
# Make sure that the NLM loaded by NMSBASE.NCF
# do not conflict with your existing setup.
# Uncomment the following line after review....
NMSBASE.NCF

# Load the SNMP Agent Software
Load SNMP verbose Control=public Trap=public

# Load NetExplorer Plus
Load SYS:SYSTEM\NXPPLUS
```

```
Load TCPIP Forward=Yes
Load SNMPLOG

Load 3c523 SLOT=7 FRAME=Ethernet_802.3 NAME=Ether_IPX
bind IPX to Ether_IPX net=CAFE0001

Load 3c523 SLOT=7 FRAME=Ethernet_II NAME=Ether_IP
Bind IP to Ether_IP addr=9.24.104.114 mask=255.255.255.0

load TOKEN SLOT=3 NODE=400052005190M FRAME=Token-Ring MSB NAME=TOKEN_1_EN-RING
load ROUTE board=2
bind IPX to TOKEN_1T_EN-RING net=9

load TOKEN SLOT=3 FRAME=Token-Ring_Snap NAME=TOKEN_IP
Load ROUTE board=3
Bind IP to TOKEN_IP addr=9.24.104.54 mask=255.255.255.0

# $NETXPLOR$ DO NOT DELETE THIS LINE
# Netware Management System installation has
# created the following NETXPLOR.NCF file.
# Review the load sequence of NLMs in NETXPLOR.NCF.
# Make sure that the NLM loaded by NETXPLOR.NCF
# do not conflict with your existing setup.
# Uncomment the following line after review....
NETXPLOR.NCF

Load remote
Load rspx

Mount ALL

Load Install
Load TCPCON
Load Monitor /p

# $NMA$ DO NOT DELETE THIS LINE
# NetWare Management System installation has
# created the following NMA.NCF file.
# Review the load sequence of NLMs in NMA.NCF.
# Make sure that the NLM loaded by NMA.NCF
# do not conflict with your existing setup.
# Uncomment the following line after review....
NMA.NCF

# $LANZ$ DO NOT DELETE THIS LINE
# NetWare LANalyzer Agent installation has created
# the following to load NetWare LANalyzer Agent.
# Uncomment the following 2 lines after review.

# SEARCH ADD SYS:LANZ
# LANZ.NCF  *

* Uncomment the line to take effect after rebooting the server
```

• **LANZ.NCF**

```
#-------------------------------------------------------------------------------
#
#                            NetWare LANalyzer Agent
#                                   Version 1.0
#
#-------------------------------------------------------------------------------
# LANZ.NCF: NetWare LANalyzer Agent Load File
#
# This NCF file is created by the NetWare LANalyzer Agent install program.
# It is used to load the NetWare Loadable Module files that make up NetWare
# LANalyzer Agent.
#
# WARNING:    You should not modify this file unless you need to change
#             one of the configuration parameters documented below.
#             Other changes to this file are not recommended.  Should you
#             damage this file, you must reinstall NetWare LANalyzer Agent.
#
# NOTE:       To change which network interfaces are monitored by
#             NetWare LANalyzer Agent, you must reinstall the product
#             and select which network interfaces you want NetWare
#             LANalyzer Agent to monitor.
#
#-------------------------------------------------------------------------------
# Load Parameter Descriptions
#
# load LANZMEM bound=KB age=HHH
#
# bound=KB    This is the upper limit on memory that can be allocated
#             dynamically by the NetWare LANalyzer Agent.
#
#             Increasing this number allows you to create larger packet
#             capture buffers and maintain data for inactive stations
#             for a longer period of time.
#
#             Decreasing this value reduces the amount of memory that
#             can be used by NetWare LANalyzer Agent.  This leaves more
#             memory for the other server tasks.
#
#             NetWare LANalyzer Agent automatically purges data for
#             inactive stations as the memory bound is approached.
#             This allows NetWare LANalyzer Agent to adjust to
#             the memory that is available to it dynamically.
#
#             If the bound is low, purging occurs frequently, saving
#             only data for stations that have been recently active on
#             the network.  If this happens, a message appears on the
#             system console indicating that not enough memory has been
#             allocated to NetWare LANalyzer Agent.
#
#             KB is the memory bound in kilobytes.
#
#             Initial value:                    set by the install program
#                                               based on memory usage
#
#             Minimum recommended value:        512
#
#             Maximum recommended value:        75% of free server memory
```

```
#                                                    when NLM files are loaded
#
#           Default value:                If bound=KB is not specified,
#                                          it defaults to 2048.
#
# age=HHH    NetWare LANalyzer Agent purges data for stations that have
#            not been active on the network recently. This parameter
#            controls how long data for inactive stations is maintained.
#
#            Memory that is used by the station table is not available
#            for other uses, such as capturing packets.  Reducing the
#            age value tends to increase the amount of memory
#            available for capturing packets.
#
#            If you cannot allocate capture buffers that are large,
#            you may need to reduce the age value.
#
#            HHH is the inactivity period, in hours, before station data
#            is purged.
#
#            Minimum recommended value:     1
#
#            Default value:                If age=HHH is not specified,
#                                          it defaults to 168  (1 week)
#
# load LANZDI level=1
#
# level=1    It indicates that the LANZDI will stop receiving packets
#            when CPU utilization gets high.
#
#            Default is OFF. LANZDI will continue to receive packets even
#            when CPU utilization gets high.
#
# load LANZSM topn=N
#
# topn=N     The number of concurrent top N station sorts that are
#            allowed by NetWare LANalyzer Agent.
#
#            Recommended value:             4
#            Minimum value:                 2
#            Maximum value:                 10
#
# load LANZCTL trapreg=1
#
# trapreg=1 Causes SNMP traps to be sent to management consoles
#            advertising themselves on the network as well as stations
#            listed in sys:\etc\traptarg.cfg.  Omitting this parameter
#            or setting it to 0 causes traps to be sent only to those
#            stations listed in sys:\etc\traptarg.cfg.
#
#-------------------------------------------------------------------------------
load lanzsu.nlm
load lanzmem.nlm bound = 13456
load lanzlib.nlm
load lanzdi.nlm
load lanzael.nlm
load lanzhis.nlm
load lanzfcb.nlm
```

```
                    load lanzsm.nlm  topn = 4
                    load lanztr.nlm
                    load lanzctl.nlm trapreg = 1
```

2.8 LMU for OS/2

This section briefly describes how we installed and configured LMU for OS/2 to integrate with LMU for AIX.

2.8.1 LMU for AIX Installation and Configuration

LMU for AIX V1.1.2 was installed using the smit installp procedure. No particular configuration changes were made. The installation procedure puts the LMU for AIX options into the NetView for AIX menus and the LMU for AIX daemons are started automatically when NetView for AIX is started. We also used LMU for AIX V1.1.3 with NetView for AIX V3.1 and with NetView for AIX V4.1 without any problems. From an AIX perspective, we used both AIX V3.2.5 and AIX V4.1.3.

2.8.2 LMU Installation and Configuration for OS/2

Here we describe the installation and configuration of both a managing and managed station under OS/2.

Insert the first diskette for LMU and type the following:

```
A:LMUINST ALL /TD
```

Press Enter and insert the other diskettes as they are requested.

- ALL specifies that the LMU/2 files and executables for all platforms are to be installed.
- /TD specifies that the target drive for the installation is D.

Note: All the configuration files mentioned in this section are in the \LMU2 directory.

We copied the sample file LMUCTL.SMP to LMU.CTL and made the following changes:

1. We substituted all *computername* or *internetwork address* references in the ASCIIZ entries to 00000009:400052005144. 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. Our MAC address was a locally administered address (LAA). If you have not defined an LAA, use the burned-in address of the adapter.
2. We modified all the drive references form C:\ to D:\ since we installed the LMU for OS/2 code on the D drive.

   The only exception was the following statement because this file must reside on the boot drive:

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

Here is a copy of our 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(00000009:400052005144);


     # 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(00000009:400052005144);


     # 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),
            ASCIIZ(00000009:400052005144);


    # Identifies the location of the file to contain
    # the messages issued by LMU.

    APP(LMU_UTILITY),
        KEY(MESSAGE_LOG),
        ASCIIZ(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),
        ASCIIZ(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(0001);

    # Identifies the type of command authorization being used.
    # Valid values are REJECT, ADMIN, USER, or NONE.

    APP(LMU_UTILITY),
        KEY(SECURITY),
        ASCIIZ(NONE);
```

```
##############################################################
#    THE FOLLOWING PARAMETERS APPLY TO "MANAGING SYSTEMS".      #
##############################################################

        # Identifies the file to contain
        # the node description change log.

        APP(LMU_UTILITY),
            KEY(CHANGE_LOG),
            ASCIIZ(D:\LMU2\CHANGE.LOG);


        # Identifies the location to which transferred
        # files are to written.

        APP(LMU_UTILITY),
            KEY(FILE_PATH),
            ASCIIZ(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),
            ASCIIZ(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),
            ASCIIZ(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),
            ASCIIZ(LMUGUI,00000009:400052005144);


        # 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,00000009:400052005144);


          # Indicates if the links between the various resources should
          # be displayed.
          #
          # The default is "N".

          APP(LMU_UTILITY),
               KEY(GUI_DISPLAY_LINKS),
               ASCIIZ(Y);

          # 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).

          APP(LMU_UTILITY),
               KEY(GUI_NODE_SYMBOLS),
               HNUM(04030A08060206020709050B01120E);

          # 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.

          APP(LMU_UTILITY),
               KEY(GUI_PATTERN),
               HNUM(0C);


          # 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.

          APP(LMU_UTILITY),
               KEY(GUI_COORDINATES),
               ASCIIZ(001,001);
```

```
################################################################
#   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.TAB);
```

2.8.3 User-Provided Configuration Files

The uservpd.dat file provides user-selected information to the QUERYVPD program. This configuration data will be sent to the LMU database during the customization process. We used a DB2/2 database. A sample file named uservpd.smp is provided, which can be edited and used as a base file. We copied this file to uservpd.cfg and ran the CVT_VPD utility against it to produce the uservpd.dat file. This utility is located in the \lmu2 directory, but the installation program updated the OS/2 PATH statement, so you won't need to specify the exact path.

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

We did not edit the sample file; it was sufficient for our purposes as it was.

Fault_Manager_Related File

We copied the sample file aueuser.smp to the aueuser.tab file. This is the table which defines the generic alerts which the fault manager uses. The sample table comes with the parameter -$g in the command field. This value indicates that the alerts received by this machine will be sent to the LMU GUI. We changed this value to -$b in all entries to indicate that alerts should be sent both to the LMU GUI and the LMU SNMP proxy agent called LMUSNMPD. LMUSNMPD, in turn, will send the trap to our SNMP manager (NetView for AIX).

This table is only read at the startup of AUERECVR (the process that actually performs actions against the alerts received). Whenever you make a change to this file, you must restart AUERECVR. Use the following commands to shutdown and then restart:

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

Our next step was to run the LMUCUST program, which reads in the LMU.CTL file and customizes LMU. We typed:

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

Note: LMUCUST.EXE is in the \LMU2 directory. Figure 55 on page 100 shows the output from this command.

```
IBM LAN NetView Management Utilities
5622-153 (C) Copyright IBM Corp. 1991, 1994. All rights reserved.

IBM LAN NetView Management Utilities Maintenance Level LM00215

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

LMUCUST: An LMU folder has been built.

LMUCUST: Your LMU.INI file is being backed up to D:\LMU2\LMU.BAK.
LMUCUST: LMU.INI built from D:\LMU2\LMU.CTL.

LMUCUST: Cannot locate line in STARTUP.CMD that starts SNMPD.
         In order to start the LMU proxy the server or requester must
         be running and SNMPD must be started.  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 55. Output from LMUCUST Utility

The LMUCUST utility updates the CONFIG.SYS file, creates the LMU.INI file and
creates an LMU folder for the administrator workstation. We did not add the
LMUSTART.CMD to STARTUP.CMD. Instead, we found it more useful to start
everything manually. For the station that maintains the LMU database, the
sequence in which the processes are started is very important.

Note: If your proxy agent is not running in the same station as the managing
station or if the community name to access the MIB variables in that machine is not
public, you must specify these values on the proxy agent entry inside the
LMUSTART.CMD file.

An example of the command is:

```
start "LMU SNMP Proxy Agent" /C d:\lmu2\lmusnmpd.exe /d nvclient ITSC
```

The parameters nvclient and ITSC must match your SNMP proxy agent station and
community name respectively.

2.8.4 LMU Installation and Configuration for NetWare Server

Since we had installed all the LMU programs and files on our OS/2 managing
workstation, we copied those files, needed by the NetWare Server, onto a diskette.
If we had the OS/2 NetWare Requester installed, we could just as easily mapped
the drive on the server and just copied the files to the server.

These files were:

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

From a NetWare Requester (our DOS client) we followed these steps:

- We logged on to our NetWare Server as *supervisor* and copied these files to the server's partition. We created an LMU2 directory on volume SYS: and copied the files to this directory.
- We copied the LMUBIND.SMP file to LMUBIND.CTL. The values we edited in are highlighted in the following listing:

LMUBIND.CTL

```
The following property and value identify the LMU Managing System.
property(MANAGING_SYSTEM)    value(00000009:400052005144)

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(00000009:400052005144)

The following property and value identify the internet address of the LMU
fault manager machine.
property(FAULT_MANAGER)      value(00000009:400052005144)

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 symbolic name of the
file server.
property(SYMBOLIC_NAME)      value(*)

The following property and value identify the pulse rate (minutes) interval
the client is expected to maintain.
property(PULSE_RATE)         value(0001)

The following property and value identify the type of security required
to execute commands on this workstation (REJECT, ADMIN, USER, or NONE).
property(SECURITY)           value(NONE)

The following property and value identify the default list of critical
NLM to be watched by NLMWATCH.
property(NLMWATCH_TABLE)     value(SYS:LMU2\NLMWATCH.SMP)
```

From the NetWare Server, we ran the following commands:

- `load SYS:LMU2\LMUBNDCS.NLM`

  This loads the bindery with the LMU control variables in the LMUBIND.CTL file.
- `load SYS:LMU2\LMUNLMCS.NLM`

  This appends the following lines to AUTOEXEC.BAT:

  `c:\qdosvpd +kc: +Q`

- `load SYS:LMU2\LMUNCFCS.NLM`

  This appends the following lines to AUTOEXEC.NCF:

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

  This has the effect of adding the LMU2 subdirectory to the search path, sending the user-provided data to the managing system maintaining the

database and loading the LMU client code to receive remote commands and
send heartbeats to the managing system.

-

    ```
    load SYS:LMU2\LMUVPDCS.NLM
    ```

    This copies QDOSVPD.COM and ADAPTERS.TBL to the DOS partition, into
    the same path as AUTOEXEC.BAT.
- Restart the machine.

2.8.5 LMU Installation and Configuration for DOS

We copied the files needed for a DOS client from our OS/2 managing station onto
a diskette. These files were:

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

On the DOS machine where we had NetWare Requester for DOS installed, we
copied these files into the boot directory C:.

We added the following statements to AUTOEXEC.BAT:

```
SET FAULT_MANAGER=00000009:400052005144
C:\LMUDOSHB 00000009:400052005144
```

The LMUDOSHB command is the function that sends a heartbeat to the LMU
managing system. The managing system is identified by using the network address.
In our case, that address was 00000009:400052005144. DOS is not a
multi-tasking operating system, therefore unlike OS/2 it cannot issue the heartbeat
periodically, which means LMU would not get status updates for DOS clients. You
may want to install a TSR program to run a resident that will issue the heartbeat at
given time intervals.

```
AUTOEXEC.BAT

@CALL C:\NWCLIENT\STARTNET
C:\WINDOWS\SMARTDRV.EXE
@ECHO OFF
PROMPT $p$g
PATH=C:\WINDOWS;C:\DOS
SET TEMP=C:\DOS
C:\DOS\MOUSE.COM
REM C:\DOS\DOSSHELL.EXE
SET FAULT_MANAGER=00000009:400052005144
C:\LMUDOSHB.COM 00000009:400052005144
```

If you want to get the configuration information about the DOS client, customize the
USERVPD.SMP file and create the USERVPD.DAT file. Details on this can be
found in the LAN NetView Management Utilities for OS/2 User's Guide. We simply
used the sample file as is and copied it to USERVPD.DAT. To send this information

to the managing system with the dcatabase, you must execute the QDOSVPD.COM program (this is the equivalent of QUERYVPD under OS/2).

```
qdosvpd /r00000009:400052005144
```

Where:

r sends it to the managing system with the dattabase.
00000009:400052005144 is its IPX network address.

2.8.6 Starting up LMU for OS/2 and LMU for AIX

The sequence in which processes are started is very important. Here is what we did.

1. The TCP/IP startup, tcpstart.cmd, is placed in startup.cmd. Therefore, TCP/IP and SNMP were started automatically when we rebooted our machine.
2. We logged onto our NetWare 3.12 Server as supervisor:

```
L:\OS2\login supervisor
```

3. We logged onto the local environment in order to access the DB2/2 database:

```
logon USERID /p:PASSWORD
```

   Note:

   Another method we sometimes used for logging onto the local environment was to select the **DATABASE 2 OS/2** icon on the desktop and start the Query Manager. With OS/2 Warp Connect and its integrated installation of the NetWare client, you just need to open the Novell folder and double-click on **NetWare tools** to get started.
4. From an OS/2 prompt we typed:

```
lmustart
```

   A sample of what lmustart.cmd looks like is:

```
@ECHO OFF
REM D:\LMU2\LMUCUST.EXE    Maintenance Level: LM00220
REM LMUCUST parameters: MANAGED MANAGING ADMINISTRATOR ALERTS
REM FAULT_MANAGER PROXY_DB LAN_MANAGER SCHEDULER VPD
START "LMU Fault Manager" /C /MIN D:\LMU2\AUECATCH.EXE 2
START "LMU Fault Automation Manager" /C /MIN D:\LMU2\AUERECVR.EXE
DETACH D:\LMU2\AUEPITCH.EXE
START "LMU Managing System" /C /MIN D:\LMU2\LMUSRV.EXE /A
D:\LMU2\LMUSLEEP.EXE 30
START D:\LMU2\LMUCLI.EXE
START /C /B /FS D:\LMU2\QUERYVPD.EXE /R
START "LMU Scheduler" /C /MIN D:\LMU2\LMUSTEP.EXE
START "LMU SNMP Proxy Agent" /C /MIN D:\LMU2\LMUSNMPD.EXE /D
```

Figure 56. LMUSTART.CMD

When you start LMU for the first time, you will see the following message:

```
LMU270I Creating database LMU2
```

On subsequent start ups, this message will not appear. The following screen shows our initial startup:

```
┌─────────────────────────────────────────────────────────────────┐
│ ▣  LMU Managing System                                        ▣ ▣│
│ IBM LAN NetView Management Utilities                             │
│ 5622-153 (C) Copyright IBM Corp. 1991, 1994. All rights reserved │
│                                                                  │
│ LMU0270I Creating database LMU2                                  │
│ LMU0060I Internetwork address = 00000009:400052005144           │
│ LMU0001I LMUSRV initialization complete; using database LMU2     │
│ LMU0092I Initial heartbeat received from 000C4121:000000000001   │
│ LMU0092I Initial heartbeat received from 12345678:000000000001   │
│ LMU0092I Initial heartbeat received from 00000009:400052005144   │
│                                                                  │
│                                                                  │
│                                                                  │
│                                                                  │
│                                                                  │
│                                                                  │
│                                                                  │
│                                                                  │
│                                                                  │
│                                                                  │
│                                                                  │
└─────────────────────────────────────────────────────────────────┘
```

Figure 57. LMU Managing System

00000009:400052005144 is the address of our OS/2 NetWare client.
000C4121:000000000001 is the address of our NetWare 3.12 server.
00000009:10005AAC3C45 is the address of our DOS NetWare client.

On starting the proxy agent, we saw the following messages in the proxy agent
window:

```
┌─────────────────────────────────────────────────────────────────┐
│ ▣  LMU SNMP Proxy Agent                                       ▣ ▣│
│ IBM LAN NetView Management Utilities                             │
│ 5622-153 (C) Copyright IBM Corp. 1991, 1994. All rights reserved │
│                                                                  │
│ LMU7500I LMUSNMPD initialization complete; using database LMU2   │
│                                                                  │
└─────────────────────────────────────────────────────────────────┘
```
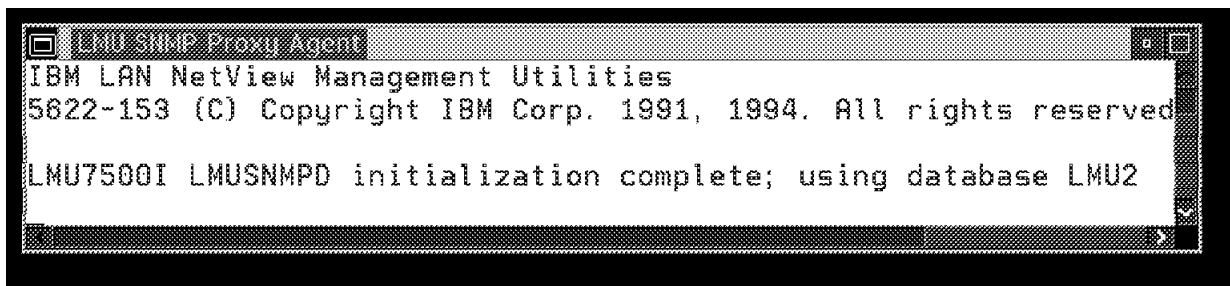
Figure 58. LMU SNMP Proxy Agent

In the snmpd window was the following message:

```
┌─────────────────────────────────────────────────────────────────┐
│ ▣  snmpd text                                                 ▣ ▣│
│ Accepted new SNMP-DPI sub-agent on fd 48, from 9.24.104.68       │
│                                                                  │
└─────────────────────────────────────────────────────────────────┘
```

Figure 59. snmpd

At this point our environment was up and running. In order to get the configuration data for our managed stations, we ran the QUERYVPD command for OS/2 and NetWare server stations and QDOSVPD for our DOS station.

Chapter 3. Clients

This chapter will describe the role of clients and agents in the processes used for viewing the IPX network, as well as trying to manage the network using tools like LMU.

- DOS/Windows Management Console
- LMU as a proxy agent for LMU for AIX
- LANalyzer as a RMON agent for RMONitor for AIX

3.1 The DOS/Windows Management Console

In this case the DOS/Windows client is very important because it is the NMS Console workstation from where you control and install all of the NetWare management agents.

The NMS DOS/Windows workstation has to run both IPX and TCP/IP stacks in order to be able to communicate with NetView for AIX and NMS agents, such as NetExplorer server, NMA servers and LANalyzer servers. The communication used between the NMS Console and the NetExplorer Server is IPX/SPX. The communication used between the NMS Console and the NetView for AIX is IP and SNMP.

In order for the NMS console function to be effective, we found it better to use it on a 486 processor. We did not have many performance problems using it on a 33 Mhz or 66 Mhz processor with 16 MB of memory. We felt it was more important to have a faster process for the GUI then for the NMS server.

NetWare NMS_AIX

Running:
IPX/SPX
TCP/IP

NetExplorer Server
NMA
LANalyzer
LMU Client

IP 9.24.104.54
IPX 00000009

IPX/SPX
SNMP

IPX/SPX

NetWare DOS/Windows
Client

Running:
IPX/SPX
TCP/IP

NMS Console EUI
NetExplorer Manager
LANalyzer
Export Communication
        Services
LMU CLient

IP 9.24.104.112
IPX 00000009
 or CAFE0001

NetWare OS/2 Requester

Running :
IPX/SPX
TCP/IP

LMU Manager

IP 9.24.104.68
IPX 00000009

TCP/IP

SNMP
(Topology)

TCP/IP
SNMP
(Traps)

RS60005

NetView for AIX
Openmon
LMU6000
RMONitor for AIX
TT 6000

IP 9.24.104.25

TCP/IP

Figure 60. Functions Schema

The NetWare DOS/Windows client we installed could be started on either Ethernet or token-ring networks. We used Ethernet for our LANalyzer agent. We installed IPX and IP on each client to communicate with the NetExplorer server and NetView for AIX.

- NMS Console Role

  The NMS Console runs the NMS Graphical User Interface. It also runs the NetExplorer Manager software which requests the NetExplorer server to dynamically receive, or schedule, information to build its topology database. The protocol used in this case is IPX/SPX.

  The NMS Console, is able to query all the NetWare management or LANalyzer agents servers to receive data about the NetWare operating system configuration, its utilization, and its performance. It is also able to receive all the traps or alerts generated by all NetWare management or LANalyzer agents.

  All of them are received through SNMP.
- NMS Export Services Role

  The NMS Export Services is an additional Novell option software which provides the NMS topology database export to other management consoles

such as NetView for AIX. This new function is running on the NMS console
and uses the TCP/IP protocol to communicate and transfer the database export
topology file.

3.2 The LMU SNMP Proxy Agent Role

LMU is a collection of software programs for the OS/2 environment that enable
management of NetBIOS (IBM LAN Server) and IPX (Novell NetWare) LANs. LMU
provides the capability to allow itself and the networks it manages to be managed
by higher level platforms such as NetView for OS/2, NetView for AIX and NetView
390. We will briefly describe how LMU, LMU for AIX and NetView for AIX work
together to provide management of the Novell NetWare environment.
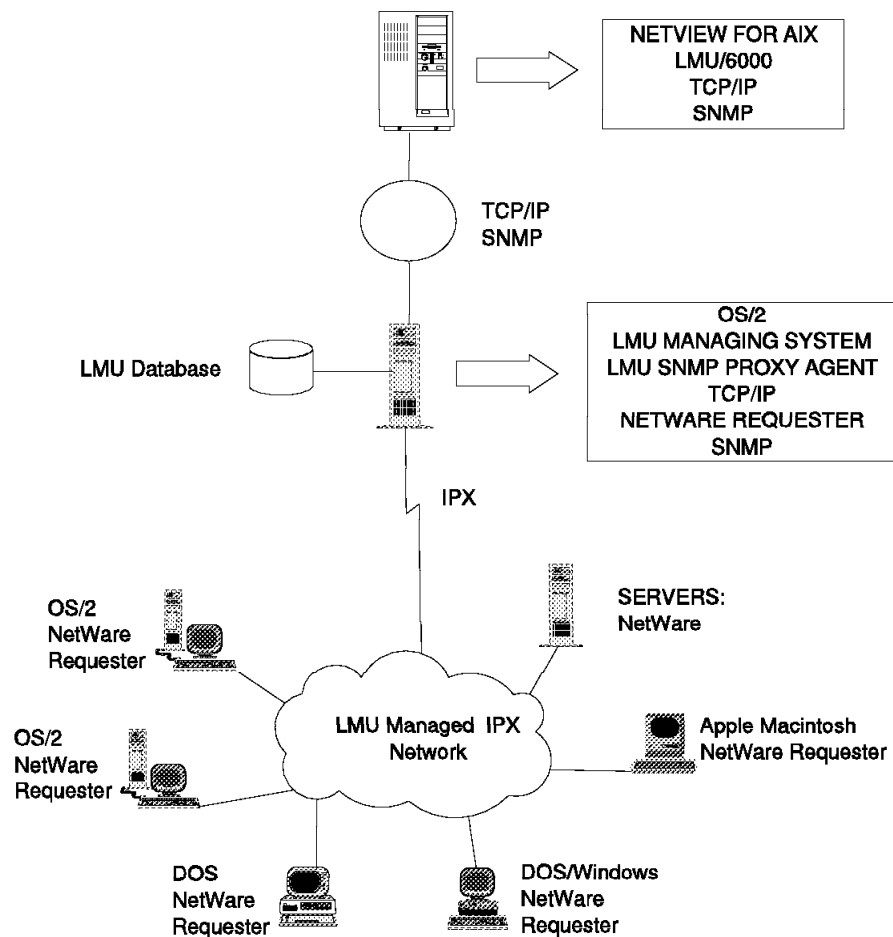
Figure 61. LMU Managed Environment

The reason that we included LMU in our project was because the current integration of NMS and NetView for AIX only gives us IPX topology information. To get status updates, query workstations for information and send commands to remote workstations for execution, we need LMU. The remote command execution is demonstrated in our scenarios.

3.2.1 LMU Components:

- **LMUCLI (Managed System)**

    – Sends heartbeats to the managed system
    – Monitors the network for commands sent from the administrator system and dispatches them to execute

- **LMUSRV (Managing System)**

    – Monitors the network for managed system heartbeats
    – May maintain the LMU database (DB2/2)
    – Maintains the status of managed systems
    – Sends status information to the LMUGUI and Proxy Agent

- **LMUGUI (Graphical User Interface)**

    – Administrator system that includes a graphical interface for displaying network status

- **LMUSNMPD (SNMP Proxy Agent)**

    – Acts as a gateway to forward information about managed system(s) from LMU managing system(s) to SNMP managers, for example NetView for AIX

3.2.2 LMU for AIX

LMU for AIX is an application which executes under NetView for AIX, which provides the following:

- A view of LMU Managed networks as standard topology submaps in NetView for AIX
- Retrieval of configuration, performance and fault management data from LMU managed stations
- Remote command execution on LMU managed stations

Any of the functions that can be set up and performed from an LMU for OS/2 workstation, can be set up to be done on LMU for AIX. The transport of the function to NetView for AIX's GUI is done by the LMU proxy agent.

LMU for AIX uses the SNMP protocol to communicate with the LMU SNMP Proxy Agent on an OS/2 workstation.

The communication from an LMU managing to an LMU managed station is over the IPX protocol; TCP/IP is not required on each managed station. LMU Client code (LMUCLI) is required on each managed station.

3.3 LANalyzer as a Proxy Agent for RMONitor for AIX

In Figure 62, we show the LAN configuration we used to implement LANalyzer and RMONitor for AIX. Since LANalyzer requires an Ethernet segment, we added an Ethernet card to our PS/2 and we used the built-in adapter on the RISC System/6000 Model 370.
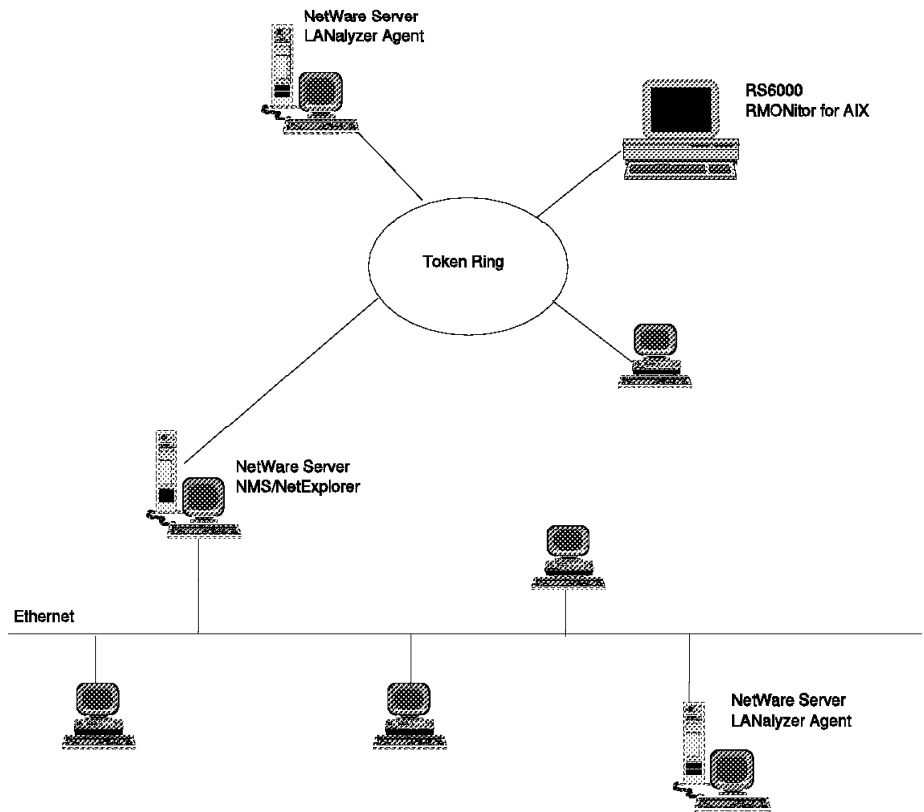
Figure 62. RMONitor for AIX and LANalyzer

3.3.1 RMONitor for AIX

RMONitor for AIX collects and monitors threshold 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 NetView for AIX user with complementary performance and operational and problem management functions.

RMONitor for AIX works in conjunction with RMON compliant agents, such as LANalyzer, to form a distributed management structure.

3.3.2 LANalyzer

NetWare LANalyzer agents discover devices, gather statistics and detect events on each segment on which they are installed. Upon request, they also capture data packets.

The NMS console may be used to view the information gathered by the NetWare LANalyzer agents. The NMS Console communicates with the NetWare LANalyzer agents over the LAN using the SNMP protocol.

Likewise, RMONitor for AIX can discover and communicate with NetWare LANalyzer Agents using the SNMP Protocol.

LANalyzer discovers devices by examining packets on the segment; therefore, it discovers only active devices. LANalyzer accumulates segment data, captures packets, stores short-term and long-term trend data and sends alarms.

Chapter 4. NetWare Tools

This chapter investigates, in detail, managing the Novell environment using the following tools:

- NetWare Management System (NMS) which includes:
  - The NMS SNMP MIB Browser
  - The NetExplorer Discovery
  - The NMS Export Services
- NetWare Management Agent (NMA)
- NetWare LANalyzer

4.1 NetWare Management System (NMS V2.0c) and Components
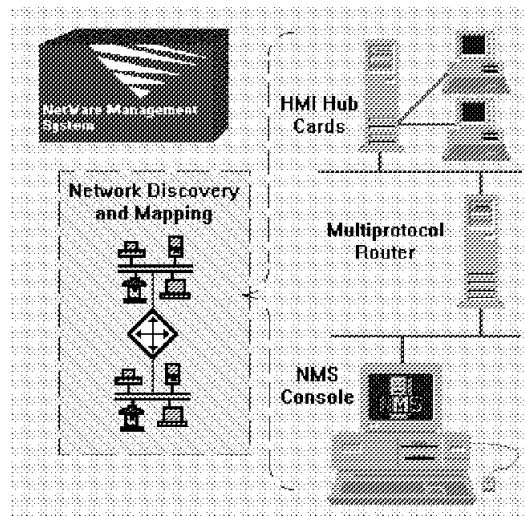
Figure 63. NetWare Management System Description

NMS provides systems management tools to provide the following functions:

- Graphical User Interface (GUI)
- Connectivity Maps for IP and IPX segments
- Topology database
- Remote console capability
- Resource discovery
- Management and monitoring of Hub cards compatible with the HMI specifications
- Management of routers
- Alarm management
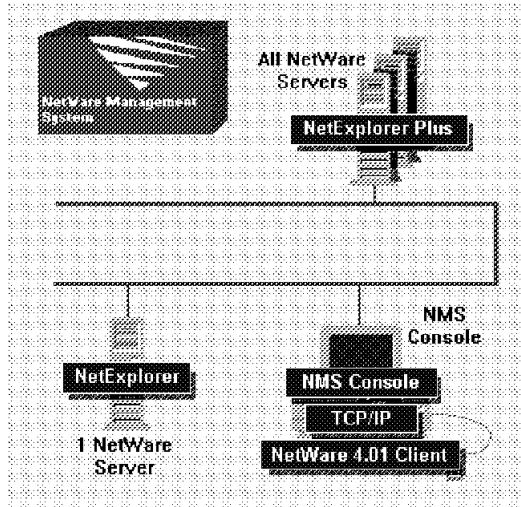
Figure 64. NetWare Management System Components

The NMS components are:

- NMS console - It is a DOS/Windows workstation from where you will install all the other NMS components. After the installation, the NMS console is your management console and where the following components are run:

  - NMS Graphical User Interface - This is where the user will interact with the server to manage the environment.
  - NetExplorer Manager - It collects discovery packets from the NetExplorer server (NMS server), updates the NMS database and generates discovery alarms.
  - NMS Database - This is where all topology and systems management information is stored.
  - The Alarm monitoring application - All unresolved alarms are kept in a database, and information can be added (notes), or they can be removed if they are resolved.
  - rconsole utility - rconsole is a utility which gives you NetWare server console capability from a remote workstation, which can be either DOS or OS/2.

- NetExplorer Agent software - This software should be installed on one server on the network. The NetExplorer software is the primary component of the NMS discovery process. It discovers network devices and places them in the NMS database on the NMS console station. NMS network maps are then created from this information.

  The NMS server contains the NetExplorer NLM known as NETEXPLOR.NLM. It also includes the NetExplorer discovery NLM software NXPIPX.NLM, for IPX discovery, NXPIP.NLM for IP discovery, and NXPLANZ.NLM for LANalyzer discovery. The discovery NLM software queries the following network devices for information about:

  - NetWare servers
  - IP Routers (IP stations are not discovered)
  - NetWare LANalyzer Agent servers
  - NetExplorer Plus servers
  - LANtern networks monitors

After gathering this information, it saves the information about the discovered objects in a local file (SYS:NMSDSK\NETXPLOR.DAT) and forwards it to NetExplorer Manager on the NMS Console.

- NetExplorer Plus Agent software - This software should be installed on all of your NetWare V3.x and V4.x servers. These agents respond to SNMP queries from the NXPIPX.NLM with the following information about any workstations that are logged into the server:

  - LAN type
  - User name
  - Address

- NetWare TCP/IP stack

  The NetWare TCP/IP stack for workstation is packaged with NMS software. The default install path from the NMS installation process usually has you install TCP/IP after you install the other NMS components. We installed all of the components at the same time, without any problems.

- Export Services - This software lets you get topology information that has been stored on the NMS database and transmit it to NetView for AIX.

4.1.1 NetExplorer Discovery System

The primary feature of NMS is the discovery of the network topology and display of that topology on the NMS Maps.

The NetExplorer is comprised of:

- The NMS console where the NetExplorer manager runs
- The NMS server where the NetExplorer agent runs
- The LANalyzer agent server

An NMS managed network must contain at least one NMS Server. The NMS server runs on a NetWare server where the NetExplorer NLM, known as NETXPLOR.NLM, is running.

The discovery NLM software can query the following types of devices on the network for information:

- NetWare servers
- IP Routers
- NetWare LANalyzer Agent servers
- NetExplorer Plus servers
- LANtern networks monitors

The discovery NLMs are:

- NXPIP.NLM   - IP Discovery
- NXPIPX.NLM   - IPX Discovery
- NXPLANZ.NLM   - LANalyzer Discovery

If you use the Control-Escape key sequence on the NetWare console, you will be able to jump between the various discovery processes and observe the process.

These NLM processes communicate through the NetExplorer Inter-Process Communication (IPC) NLM (NETXPLOR.NLM) at the NMS Console.

4.1.1.1 TCP/IP Discovery Process

The SNMP protocol is used to discover IP routers.

It queries the MIBs on the routers using SNMP and collects the following information:

- Router IP address
- Router Interface Types
- MAC address of each router
- Network adapter
- Number of hops to the NMS Console

4.1.1.2 IPX Discovery Process

This uses a variety of NetWare, SNMP and IPX functions such as SAP and IPX diagnostics to discover NetWare servers, IPX routers and IPX workstations. Through examination of the bindery, it learns the names of IPX devices that it is connected to and then queries the binderies of each of these devices to determine what they are attached to.

4.1.1.3 NetWare LANalyzer Agent Discovery Process

The NXPLANZ.NLM is installed on the NMS server. It queries all NetWare LANalyzer agents and LANtern monitors for information about all the devices that exist on their network segments, regardless of protocol. The NetWare LANalyzer agent monitors every packet on the network segment it is installed on, creating a list in local memory of all the physical addresses. The NetExplorer LANalyzer discovery software, NXPLANZ.NLM, uses SNMP to query all NetWare LANalyzer agent servers to read their discovery databases.

4.1.1.4 NetExplorer IPC

The NetExplorer IPC NLM uses IPC (Inter-Process Communication) to collect discovery data from the discovery NLM files and make it available to the NetExplorer manager on the NMS console.

4.1.1.5 NetExplorer Manager

The NetExplorer manager resides on the NMS management console and performs the following tasks:

- Extracts information from the NETXPLOR.DAT file
- Interprets information from the NETXPLOR.DAT file
- Checks to see whether the object has already been discovered
- Uses the rules list to determine any additional attributes of the discovered object
- Generates NetExplorer alarms and directs discovery information to the NMS database

It uses the SPX protocol to connect to the NMS server.

4.1.2 Configuring the NMS Console

It is not necessary to manually edit the NMS.INI file that is stored in the WINDOWS directory. There are many parameters in the file that you should be aware of. It is worth spending some time looking at the NMS.INI file online to become familiar with some of the ways that NMS is set up under Windows. Some fields that you should be aware of are:

- Root=\NMS - The path where NMS is stored

- Datapath=\nms\nmsdb - NMS database directory

- SapBroadcast =1 - Automatic registration for Alarms using SAPs

- Connectivity tests

    - ipxPingTimeout=2
    - ipxPingRetries=2
    - ipPingTimeout=2
    - ipPingRetries=2

- MIBPATH=\nms\bin\snmpmibs\current - Current MIBs being used

- SPX Slave Server=NMS_AIX - NetWare Server running NetExplorer agent

- NMS Debugging

    - DBFilelog=1 - To create a database log file
    - TraceFielLog=1 - To create error and trace debugging files

      NMS will create a table window which will display the debugging information. The table window is independent of all the NMS tasks and can be closed at any time without affecting the running NMS tasks. Set the following lines to 1 to enable this debug window.
    - DBAuxWinLog=0
    - ErrorWinLog=0
    - TraceWinLog=0

There are many more parameters in the NMS.INI file. These were just a few of the ones that you might want to change.
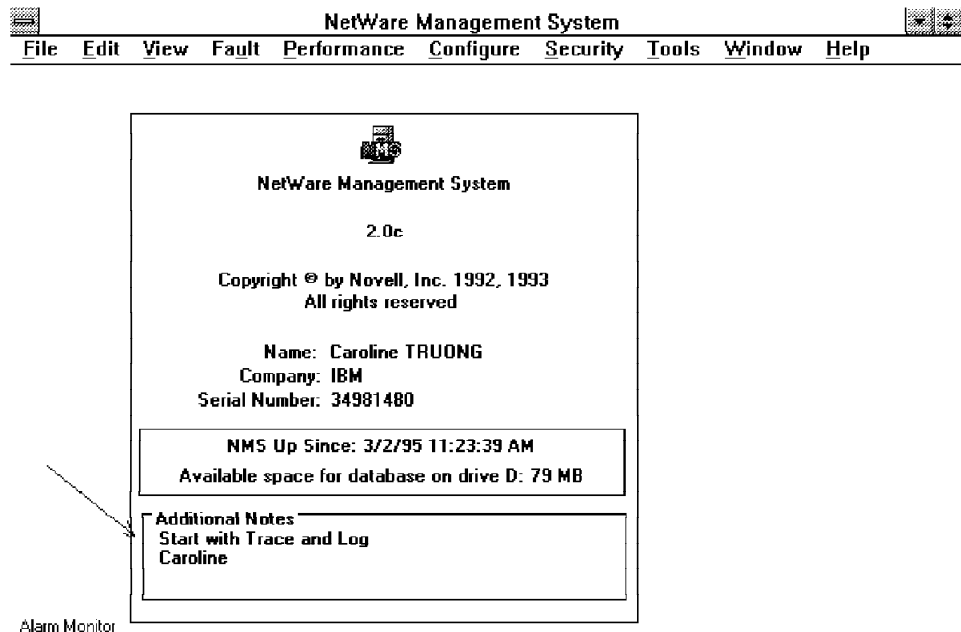
Figure 65. Starting NMS with a Customized Personal Message

You start the NMS console by double-clicking on the **NetWare Management** icon in the NetWare Management System window under the Program Manager in DOS/Windows.

When you first start the NMS console under DOS/Windows, you will get a screen similar to the one in Figure 65. You can customize some of the fields (for

example, name, company) by using the pull-down windows, Configure and Global
Preferences, as shown in Figure 66 on page 118.
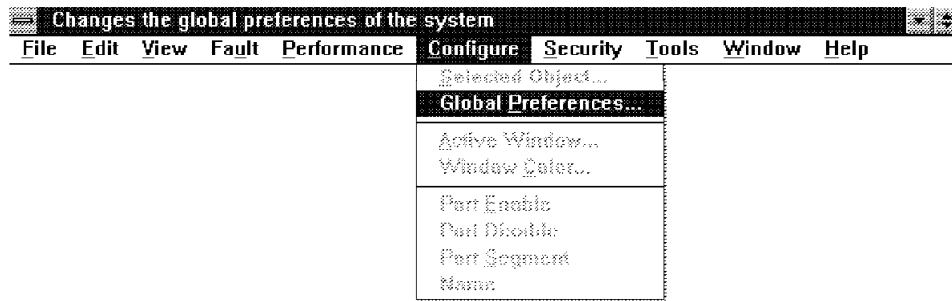
Figure 66. NMS User Interface, Configure Option

If you have not manually modified the NMS.INI file, you can change some of the parameters in the configuration menu shown in Figure 67. The options you should set are to check or modify the NMS database directory you want to use and enter an additional message which will be displayed when the NMS application starts.
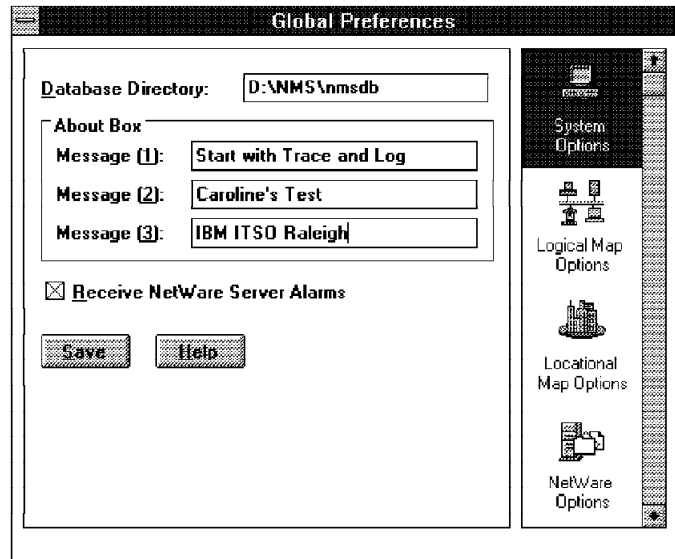
Figure 67. NMS User Interface, Global Preferences Option

If you use the slider bar along the right side of the window and go down it, you will come to the NetExplorer Options selection. The NetExplorer options are to check or set the NMS server name and to select the NetExplorer manager running mode. This determines if you will consolidate the IP and IPX segments.
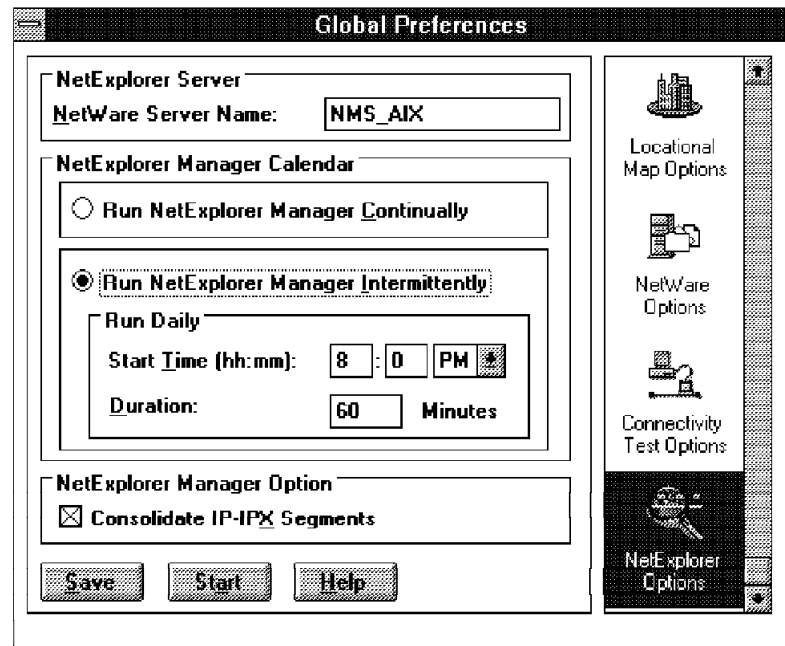
Figure 68. NetExplorer Manager Configuration

Select the **Security ... Console Login** option to set your initial password and to register your NETMAN password. During the installation of NMS, you were prompted to setup a password.
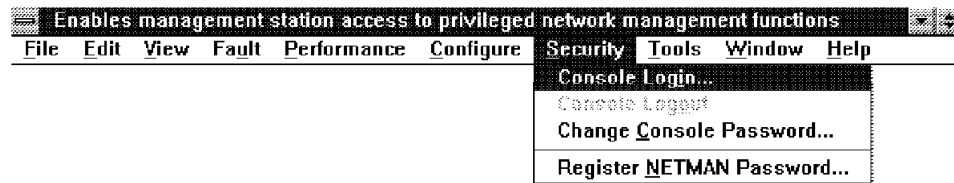
Figure 69. Setting NMS Console Password and Registering NETMAN Password
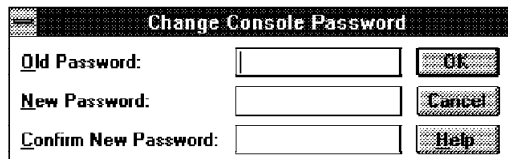
Figure 70. NMS Console User Interface, Change Console Password

4.1.2.1 Configuring the NMS Server/NetExplorer Agent

To configure the NMS server, edit the SYS:SYSTEM\NETXPLOR.NCF file.

You can do this as you are logged on to the server from the client or you can edit it from the server with:

```
load edit sys:system/netxplor.ncf
```

1. The /B count parameter for the NETXPLOR.NLM module specifies the maximum number of backups of NETXPLOR.DAT that NetExplorer can store at any one time.

   The backup files are stored in the SYS:\NMDISK\DATSAV directory:

   ```
   LOAD SYS:\NMDISK\NETXPLOR /B
   ```

   If you do not use the /B parameter, the default number of backups is 0.

2. If your network is running the IP protocol, you must remove the comment specification (#) from the LOAD NXPIP line in column one. You can force the

discovery with the equivalent of a seed file by specifying the network addresses of the networks that need to be discovered in the SYS:\NMDISK\NXPIP.INI file.

Use the /C <filename> parameter if want to specify a file containing a list of SNMP community strings to be used for communicating with IP devices: LOAD SYS:\NMDISK\NXPIP.NLM /C <filename>

Where filename should be placed in the SYS:\NMDISK directory.

An NXPIP.INI file could look like:

```
9.24.104.0
9.24.96.0
9.67.99.0
```

The file containing the community names would look like the following:

```
public
ITSC
ourname
secret
```

There is also an INI file for the IPX protocol located in SYS:\NMDISK\NXPIPX.INI. It is used when you load the NXPIPX.NLM module.

4.1.3 NMS Console User Interface

During the NetWare Management System installation, the Novell-NMS program group is created.
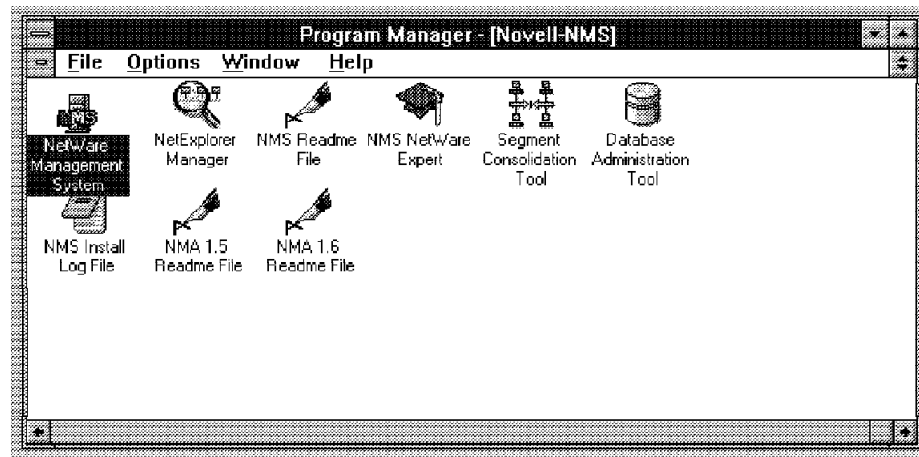
Figure 71. NMS Windows Screen

The contents of this group are:

- **NetWare Management System icon**

    This is the NMS main task. It starts the NMS user interface and two NMS background tasks:
    – Alarm Manager
    – SNMP Data Server
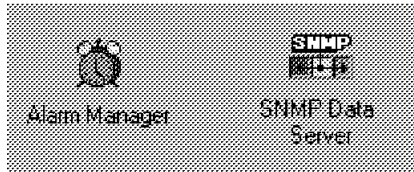
Figure 72. NMS Alarm Manager and SNMP Server Data Icons

- **NetExplorer Manager icon**

  The NetExplorer Manager collects network information from the NetExplorer agents and builds the database. It can be run continually or it can be scheduled to run at a specific time.

Figure 73. NetExplorer Manager Icon

- **NMS Readme File icon**

  This is a text file which you can view to get more information about your NMS version, configuration and utilization.
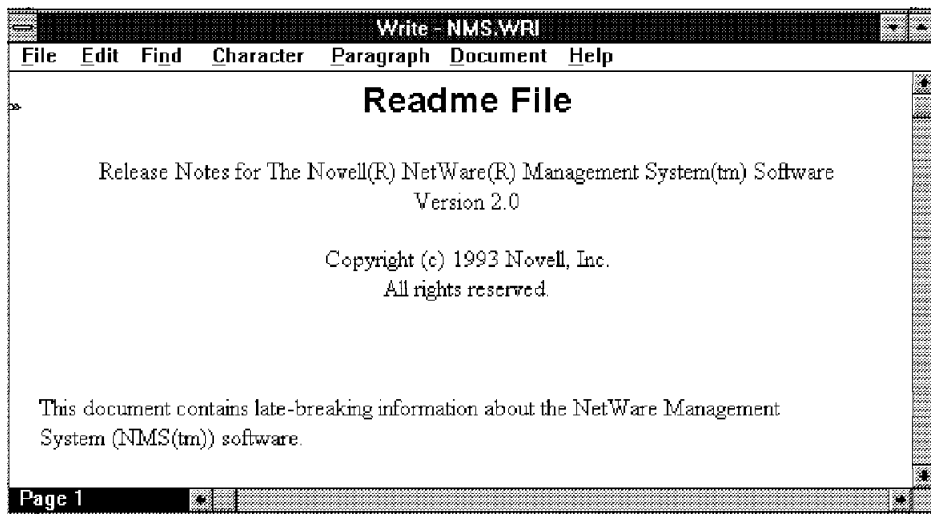
Figure 74. NMS Readme File

- **NMS NetWare Expert Tool icon**

  This is a utility that guides you through the NMS installation, helps you configure the NMS Console, and gets you started on monitoring network devices.

Figure 75. NMS NetWare Expert Tool Icon

- **Segment Consolidation Tool icon**

   This tool consolidates two segments into one.
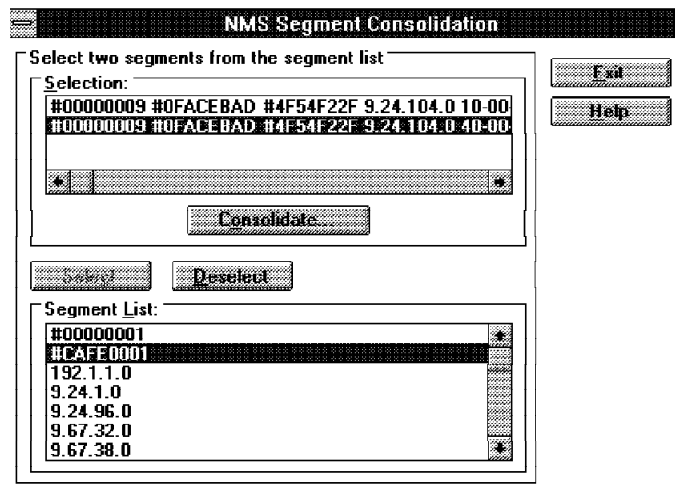
Figure 76. NMS Segment Consolidation Tool

- **Database Administration Tool icon**

   This tool helps you to maintain your database.
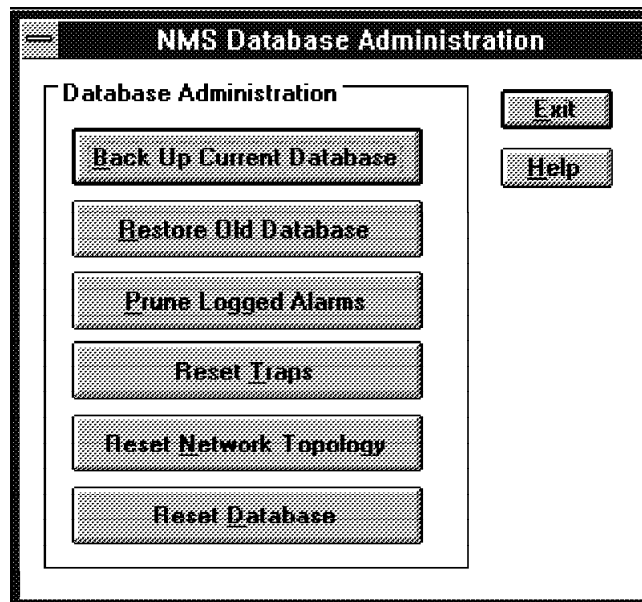
Figure 77. NMS Database Administration Tool

The NMS Database uses a Btrieve record Manager Database that contains information that describes the objects monitored by NMS. To have more information about the NMS Database structure and its relationship with the NMS Configuration options or alarm information, a schematic of the NMS Database structure is provided in the NMS package. You can find a copy of this manual in the directory \NMS\NMSDB. The file is a postscript file called: DBSCHEMA.PS.

- **NMS Install Log File icon**

  This file records information about the installation process.


```
Notepad - INSTALL.LOG

File   Edit   Search   Help

NMS 2.0 10/25/93 02:09:01
***********************************************************************
                        INSTALL LOG FILE
  If you are unable to successfully install NMS due to an
  installation error, consult the NMS documentation and your
  network administrator.  If the problem cannot be resolved,
  contact Novell technical support and present this file.


***********************************************************************
0 Initialize: S=A:\ T=C:\WINDOWS
0 setDialogStringOptions: S=A:\ T=C:\WINDOWS
0 DrawBitmap: S=A:\ T=C:\WINDOWS
0 QueryTutorial: S=A:\ T=C:\WINDOWS
**************** INSTALL OPTIONS ********************


   [ ] RUN TUTORIAL
   [X] INSTALL NMS


*****************************************************
0 SetDLLName: S=A:\ T=C:\WINDOWS
0 checkSystem: S=A:\ T=C:\WINDOWS
```

Figure 78. NMS Install Log File

4.1.3.1 Using NMS

This section shows the most frequently used functions that are part of the NMS Console.

- Network maps

  To see what the topology is for the automatically discovered map, select the **File...Open** and the **Internet** options from the pull-down menus.
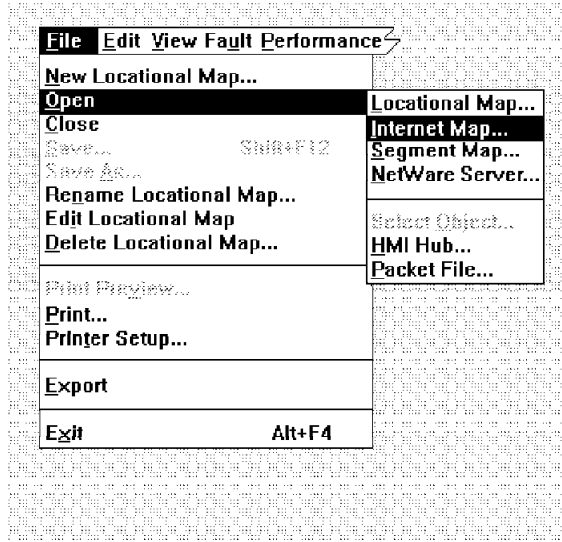
Figure 79. Pull-Down Menus to View NMS Maps

Figure 80 shows a high-level view of your network. It displays the Network segments, rings and the routers, NetWare servers, and your IP resources.
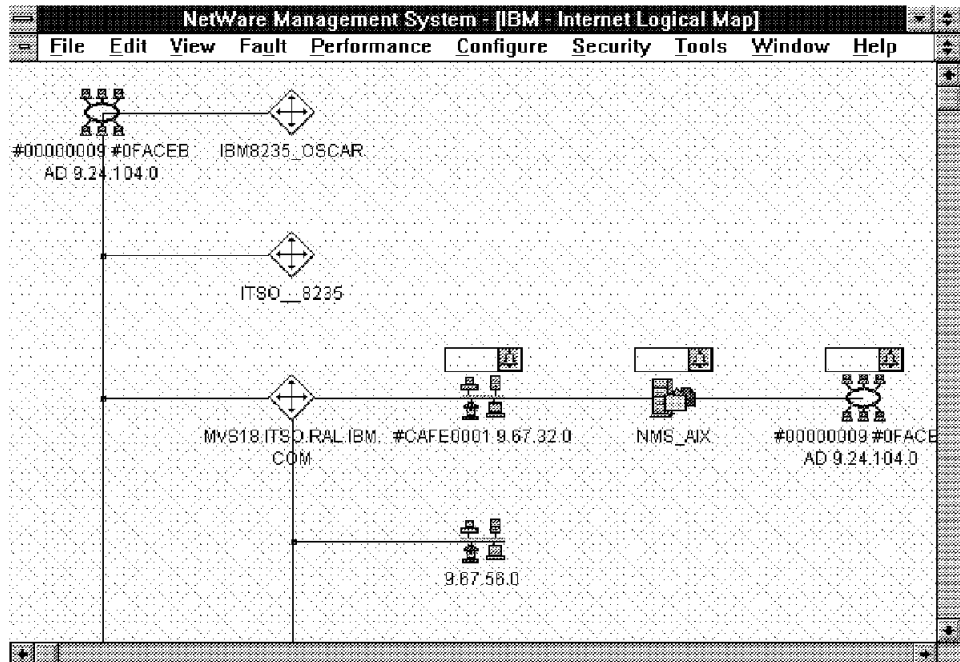
Figure 80. An NMS Internet Map

You can double-click on one of the network icons to go down another level. For example, if you select the 9.24.104.0 subnet, you can view the resources that are part of that subnet. If you select a NetWare server, you will get more information about that server.

In Figure 81 on page 126 we show the result of selecting the 9.24.104.0 subnet. Notice that we have the MAC addresses of some resources, the host-resolved names of some, and some NetWare servers that also have IP installed on them.
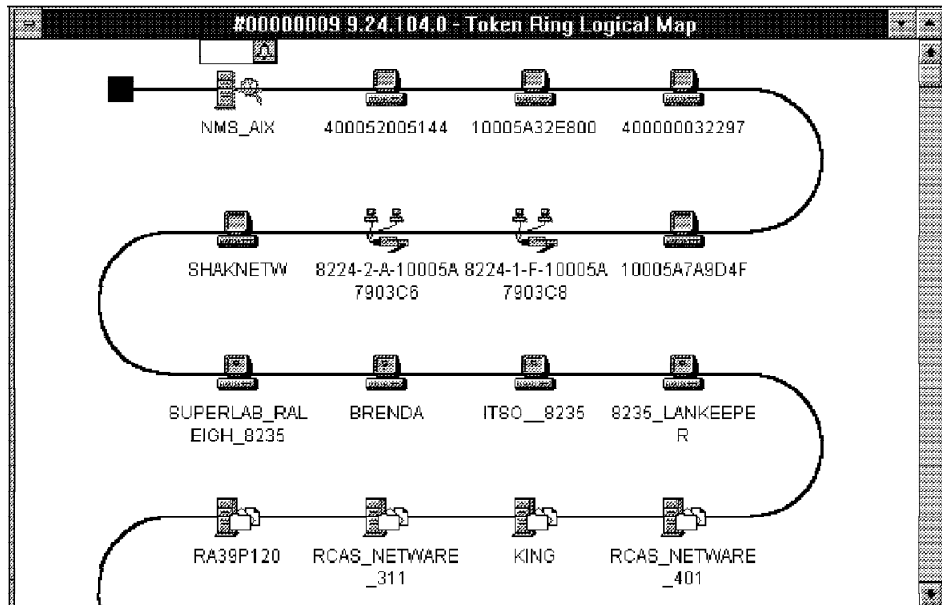
Figure 81. NMS Segment Map

If you double-click again on one of the resources in the map, you will get additional information about the object that you have selected. For example, in Figure 82 we selected the resource called BANK311.

Figure 82. NMS System Information

The Selected Object Configuration window has several fields that you can change or put initial information in about the selected object. If the selected node is an NMA agent server, then there will be another level of detail that you can view. You can get additional information about the NetWare server, as shown in Figure 83 on page 127.
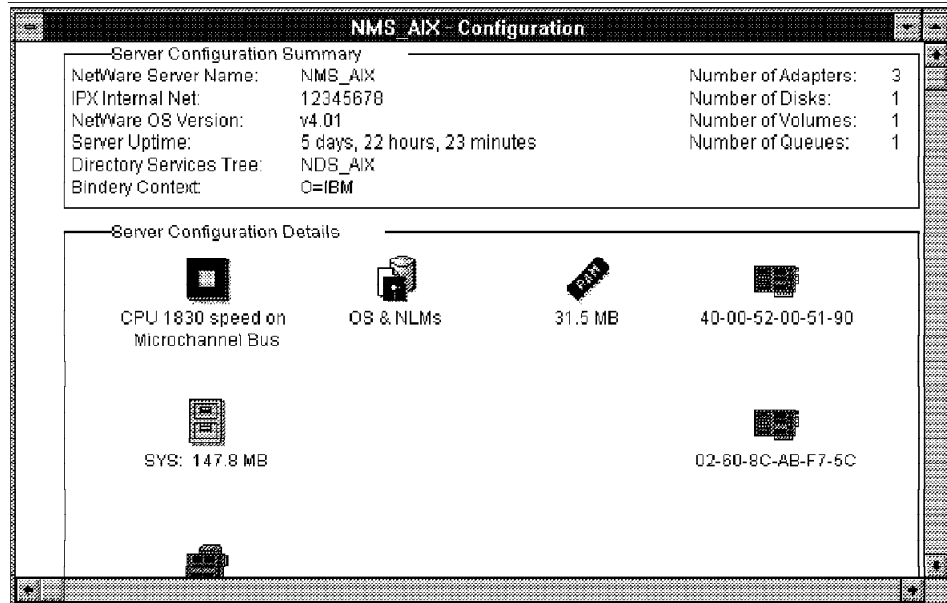
Figure 83. NetWare Server Information with NMA

Some of the additional information you can see from NMA are details about the hardware the server is running on (NLMs that are loaded) and the SYS volume information.

- Alarms

When the NMS console receives an alarm, meaning that some error condition has occurred, it puts an alarm icon on the top of the network and server icons on the map as shown in Figure 84.
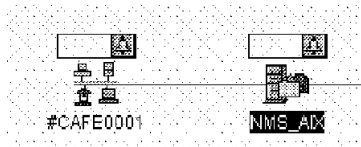
Figure 84. Internet Map, Alarm Icon

To display this alarm, select the node with the alarm icon and go to the Fault...Alarm Report options on the menu bar. You will get a window similar to the one that follows:

Figure 85. Alarm Report for NMS_AIX

In this panel, you will see all the alarms received for this specific node. To display all the alarms received since the NMS console started, explode the Alarm Monitor icon (displayed in the bottom of the main screen). The title bar for the Alarm Report shows which resources the alarms are for. Note that the Alarm Report and the Alarm Monitor windows are very wide, and you will need to scroll to the right to see additional information.

Figure 86. Alarm Monitor for All Resources

The top portion of the window in Figure 86 shows a graphical display which includes statistics about the percentage of alarms received by severity. You can change the alarms if you think that the severity that is set for it does not match your environment. To do that, select the **Fault...Alarm Disposition** options in the menu bar. There are also other fields that you can change, as shown in Figure 87 on page 129.
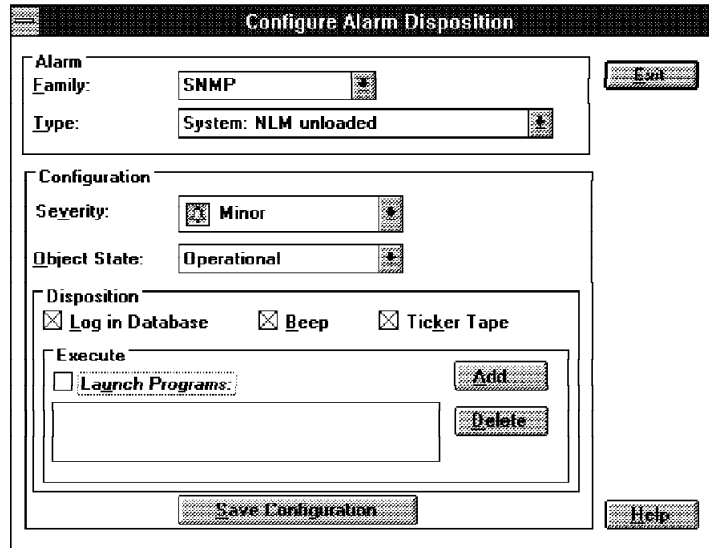
Figure 87. Configuring Alarm Dispositions

Then, select the alarm family which is the alarm you want to configure (the most important is the SNMP family), and then select the right alarm to modify.

- **Export function**

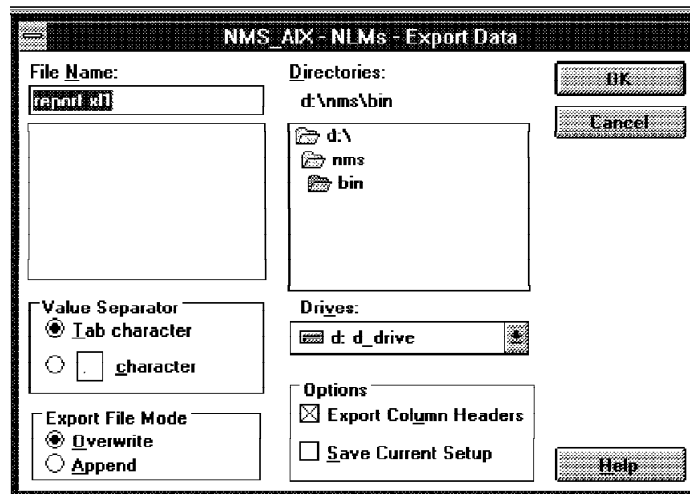Most of the NMS functions permit you to export the information to a file.

Figure 88. Exporting Data to a File

For example, you can display the NMA server information about the NetWare server you want, select the **NLM** icon, and then select the **File** and **Export** options from the main panel to export the data into a file.

- **rconsole tool**

The NMS Windows user interface provides a rconsole.exe function under MS-Windows to help you maintain and control the NetWare servers. The remote console function permits your NMS console (and your NetWare client) to perform any functions that can be done from the NetWare console. You will have to use some different function keys. For example, you will need to use

Alt+F2 instead of the Control+Escape key since the Escape key has other meanings in DOS/Windows. A sample window for the rconsole function follows.

Figure 89. NMS rconsole Tool

> **Note**
>
> To use rconsole on the server you want, check the following configuration in the SYS:SYSTEM\AUTOEXEC.NCF file. If you cannot access your server, enter those following lines on the console server command line to allow rconsole access:
>
> :Load REMOTE
> :Load RSPX

- **MIB Compiler and MIB Browser**

  In addition to SNMP managers, like NetView for AIX, providing MIB Browsers and MIB compilers, NMS provides one as well.

  You can copy the MIBs from the \NMS\SNMPMIBS\ALLMIBS directory into the \NMS\SNMPMIBS\CURRENT directory, and use the NMS compiler tool to integrate them. You can also copy the MIBs to NetView for AIX and use them there.
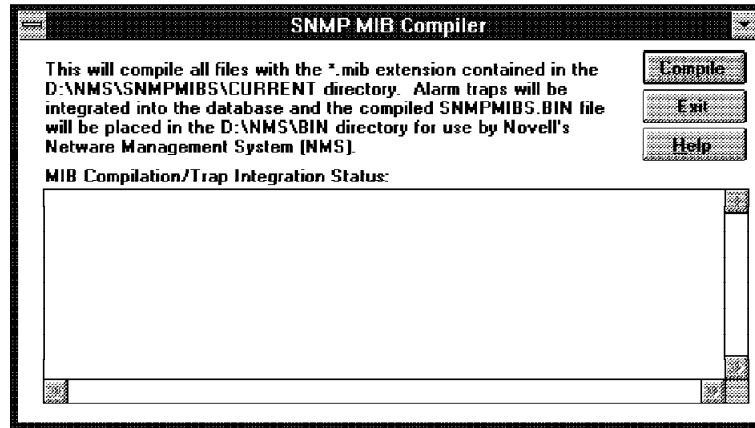
Figure 90. NMS MIB Compiler Tool

4.1.3.2 Troubleshooting and Maintaining NMS

There are some utility functions to help you maintain the NMS application. We used the following:

- NMS segment consolidation tool
- Trace and debugging functions

- **The NMS Segment Consolidation Tool**

    If you have installed all the NMS additional agents, such as NMA and LANalyzer, and you start the IP and IPX discovery, NMS may display your network in 2 or 3 different networks. If you want to modify that to have a better map, use the NMS Segment Consolidation Tool. Figure 91 and Figure 92 on page 132 provide an example of this.
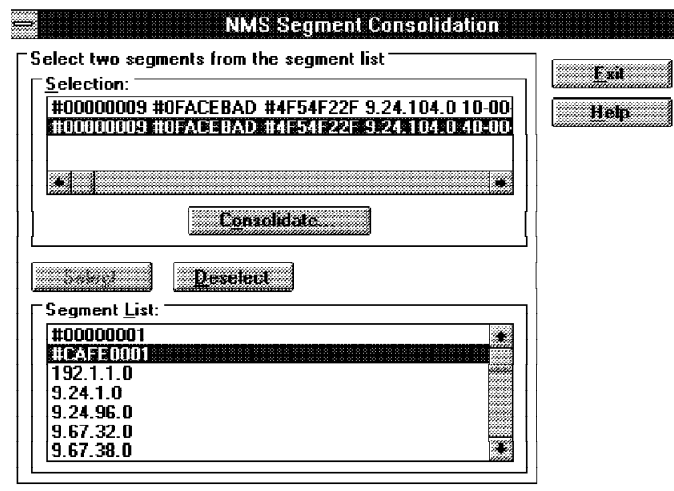

Figure 91. NMS Segment Configuration Tool

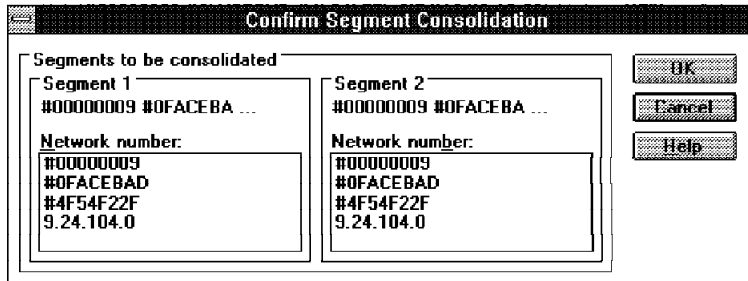   Select the two segments you want to consolidate and click on the **Consolidate** button.

Figure 92. NMS Segment Configuration Tool

> Then, confirm the consolidation and restart the NMS User Interface since the changes do not occur until you restart the NMS console. Check the changes in your map to set the new layout.

- **The NMS Database Administration Tool**

  > This tool offers interesting functions as shown in the following and in Figure 93.
  > - You can back up the current database and initialize it back to its starting state. You can also restore a previous database.
  > - Reset the network topology, but leave all the alarms and other configuration information in the database.
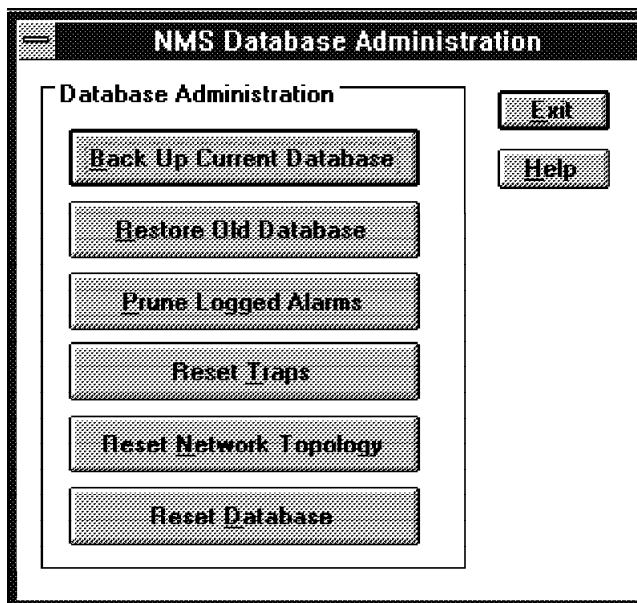 > - Reset the traps or prune the logged alarms.

Figure 93. NMS Database Administration Tool

- **The Trace and Debug functions**

  > To understand how network discovery and tracing works for the NMA and the NetExplorer functions, use the NMS trace and debug options as follows:

  > 1. Modify the NMS debug section in the NMS.INI file:

  >   Setting the first three options below to 1 turns the option on.

```
DBFileLog=1
ErrorFileLog=1
DebugFileLog=1
Pathname=D:\NMS\logfiles
DBFilesize=1000000
Numfiles=99
```

This will create an error and a trace file in the \NMS\logfiles directory. If you would prefer to have this information displayed dynamically in a window, modify the following parameters that are located in the *LOGGING TO DEBUG WINDOW* section of the NMS.INI file:

```
DBWinLog=1
ErrorWinLog=1
TraceWinLog=1
```

2. As with most changes, you will need to restart the NMS console.

A new window will show up, after a restart, similar to Figure 94.


```
                                    NMS Debug
KEY  DATE AND TIME            ERROR OR TRACE MESSAGE
180 [2/15/95 2:55:48 PM] ------------------------------------------------------
181 [2/15/95 2:55:48 PM] __LSM IF_INFO For: #00000009 #0FACEBAD #4F54F22F 9.2
182 [2/15/95 2:55:48 PM] __AGENT=NMS_AIX Server IPX IP
183 [2/15/95 2:55:48 PM] __T 802.5,statIdx=0      ,ifIndex=1      ,ifStatus=2
184 [2/15/95 2:55:48 PM] __        sHstIdx=0      ,lHstIdx=0      ,hsCtlIdx=0
185 [2/15/95 2:55:48 PM] __        mtCtlIdx=0
186 [2/15/95 2:55:48 PM] ------------------------------------------------------
187 [2/15/95 2:55:48 PM] ------------------------------------------------------
188 [2/15/95 2:55:48 PM] __LSM IF_INFO For: #CAFE0001
189 [2/15/95 2:55:48 PM] __AGENT=NMS_AIX Server IPX IP
190 [2/15/95 2:55:48 PM] __E 802.3,statIdx=1      ,ifIndex=3      ,ifStatus=1
191 [2/15/95 2:55:48 PM] __        sHstIdx=1      ,lHstIdx=2      ,hsCtlIdx=1
192 [2/15/95 2:55:48 PM] __        mtCtlIdx=0
193 [2/15/95 2:55:48 PM] ------------------------------------------------------
194 [2/15/95 2:55:49 PM] CONN_MONITOR: ** monitoring cycle finished **
195 [2/15/95 2:56:47 PM] RSMEX: ddeServerProc: received XTYP_WILDCONNECT
196 [2/15/95 2:56:47 PM] RSMEX: ddeServerProc: received XTYP_CONNECT_CONFIRM
197 [2/15/95 2:56:47 PM] RSMEX: ddeServerProc: received XTYP_DISCONNECT
198 [2/15/95 2:56:47 PM] RSMEX: ddeServerProc: received XTYP_CONNECT_CONFIRM
199 [2/15/95 2:56:47 PM] RSMEX: ddeServerProc: received XTYP_DISCONNECT
200 [2/15/95 2:56:49 PM] ============== Restart polling ================
201 [2/15/95 2:56:49 PM] ***Trying RMON: NMS_AIX***
202 [2/15/95 2:56:49 PM] MAC ADDR 400052005190, IF index 1
203 [2/15/95 2:56:49 PM] IF INX 1 is not monitored
204 [2/15/95 2:56:49 PM] MAC ADDR 02608cabf75c, IF index 3
205 [2/15/95 2:56:49 PM] IF INX 3 is monitored(statInx 1)
206 [2/15/95 2:56:49 PM]                        (shortHistInx 1)
207 [2/15/95 2:56:49 PM]                        (longHistInx 2)
208 [2/15/95 2:56:49 PM]                        (hostCtrlInx 1)
209 [2/15/95 2:56:49 PM] ***Trying RMON: CM4121R_312SVR***
210 [2/15/95 2:56:49 PM] MAC ADDR 10005a20e795, IF index 1
```

Figure 94. NMS Trace and Debug Window

3. Some of the \nms\logfiles entries are displayed in Figure 95 on page 134.

```
 0  [1/26/95 3:53:13 PM]   netexplorer
 1  [1/26/95 3:53:13 PM]   Shell export header version: 8
 2  [1/26/95 3:53:14 PM]   Shell exe version: 2.69
 3  [1/26/95 3:53:14 PM]   Loading DLL: D:\NMS\bin\n-snoopr.dll
 4  [1/26/95 3:53:14 PM]   LoadLibrary(D:\NMS\bin\n-snoopr.dll) hLib = 28310
 5  [1/26/95 3:53:14 PM]   RSMEX: ddeServerProc: received XTYP_REGISTER
 6  [1/26/95 3:53:14 PM]   AlarmMgr:  Received XTYP_REGISTER.  Requested an advise link
 7  [1/26/95 3:53:14 PM]   AlarmMgr:   Service name is 'Novell NetExplorer' and topic is
                                               'Novell Canonical Events'
 8  [1/26/95 3:53:14 PM]   Total rules from D:\NMS\olf\rmonserv.OLF = 1
 9  [1/26/95 3:53:14 PM]   Total rules from D:\NMS\olf\lantern.OLF = 1
10  [1/26/95 3:53:14 PM]   Total rules from D:\NMS\olf\n_mac.OLF = 2
11  [1/26/95 3:53:14 PM]   smCacheFARules() FArule=<S570>, FunctionName=<NLA>
12  [1/26/95 3:53:14 PM]   smCacheFARules() FArule=<S585>, FunctionName=<LANtern>
13  [1/26/95 3:53:14 PM]   smCacheFARules() FArule=<S4>, FunctionName=<NetWare Server>
14  [1/26/95 3:53:14 PM]   smCacheFARules() FArule=<A2>, FunctionName=<Ip Router>
15  [1/26/95 3:53:14 PM]   smCacheFARules() FArule=<A3>, FunctionName=<Ipx Router>
16  [1/26/95 3:53:14 PM]   smCacheFARules() FArule=<A4>, FunctionName=<Workstation>
17  [1/26/95 3:53:14 PM]   smCacheFARules() FArule=<S71+S7>, FunctionName=<Print Server>
18  [1/26/95 3:53:15 PM]   smCacheFARules() FArule=<S569>, FunctionName=<Hub>
19  [1/26/95 3:53:15 PM]   smCacheFARules() FArule=<V08001470FFFF>,
                                                   FunctionName=<Terminal Server>
20  [1/26/95 3:53:15 PM]   smCacheFARules() FArule=<V08001471FFFF>,
                                                   FunctionName=<RMonLantern>
                 .
                 .
                 .
2630  [1/26/95 3:55:26 PM]   alarmmanager
2631  [1/26/95 3:55:26 PM]   WM_DESTROY
2632  [1/26/95 3:55:26 PM]   FreeLibrary  D:\NMS\BIN\N-EVMGR.DLL
2633  [1/26/95 3:55:38 PM]   map
2634  [1/26/95 3:55:38 PM]   WM_CLOSE
2635  [1/26/95 3:55:39 PM]   End_TC_GET: Entry
2636  [1/26/95 3:55:39 PM]   End_TC_GET: OK
2637  [1/26/95 3:55:40 PM]   rmon_dap: db tables closed
2638  [1/26/95 3:55:40 PM]   rmon_sa2: CALLING saDeRegisterAlarms
2639  [1/26/95 3:55:40 PM]   RSMEX: ddeServerProc: received XTYP_UNREGISTER
2640  [1/26/95 3:55:40 PM]   LSM EISNMP TERMINATE HOOK
2641  [1/26/95 3:55:40 PM]   map
2642  [1/26/95 3:55:40 PM]   WM_DESTROY
2643  [1/26/95 3:55:40 PM]   FreeLibrary  D:\NMS\BIN\N-LOCMAP.DLL
```

Figure 95. Logfile Entries

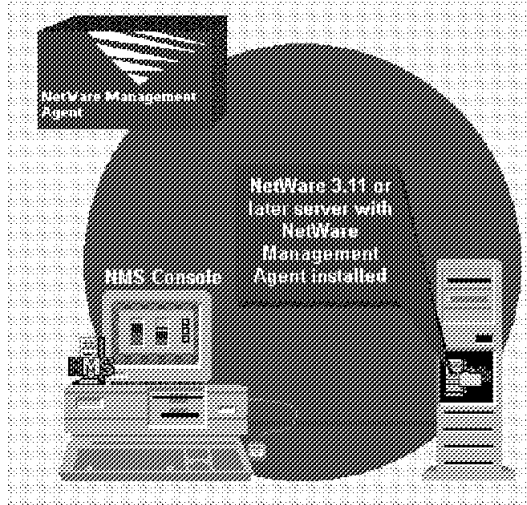## 4.2 NetWare Management Agent (NMA V1.5/V1.6)

Figure 96. NetWare Management Agent Description

The NetWare Management Agent (NMA) is used to gather NetWare operating system management information. It complements the NMS product, which is only used to discover the IPX topology and IP routers.

The types of system information that NMA provides is:

- A list of all the NLMs loaded on the server, with their version number and the amount of memory used. In addition, a description is provided.
- Dynamic display of CPU utilization on the server.
- Dynamic display of memory utilization as well as the memory allocated in the various pools.
- A list of all LAN and disk adapters installed on the server as well as the protocols they are using and their utilizations.
- A list of all volumes configured with their utilization percentage and size.
- A list of all hard disk configured with their type and size.

NMA must be installed on all NetWare V3.x and V4.x servers that you want to manage. NMA is completely integrated in NMS. NMA provides an icon for NetWare servers which have NMA running. If you double-click on those icons, the NMS application will display a new screen with all the NMA system information.

NMA components are:

- NMAGENT.NLM
- NMAGENT2.NLM
- SIDEWIND.NLM
- SPAGENT.NLM
- NW2SNMP.NLM
- NWTRAP.NLM

NW2SNMP.NLM and NWTRAP.NLM comprise the NetWare to SNMP Trap Translator software. Its function is to convert NetWare alarms to SNMP traps and send traps to NMS and Non-NMS management consoles.

4.2.1 NMA Configuration

After installing the NetWare Management Agent, you have to set up the SYS:SYSTEM\NMA.NCF file.

You can do that by editing this file from the NetWare server console as follows:

`Load EDIT SYS:SYSTEM\NMA.NCF`

This file is like a batch file for NetWare OS, so you can start it on the NetWare console command line, as follows:

`:NMA`

Then all of the NMA NLMs will be loaded as configured in the NMA.NCF.

4.2.1.1 Configuring the NMA.NCF

The NMA.NCF file loads all the NMA NLM components needed. NMA uses SNMP to send traps to any management console, such as NMS or NetView for AIX. It uses extensions of the SNMP NLM to send and translate specific NMA traps over the SNMP stack.

The two NLMs providing that function, called NetWare to SNMP trap translator software, are:

- NW2SNMP.NLM
- NWTRAP.NLM

In order to configure the NetWare to SNMP trap translator software, you need to set the following options:

- **NW2SNMP options**

  `LOAD SYS:SYSTEM\NW2SNMP COMMUNITY=<community name>`

  Here, community name is the community name you use for sending traps.

  - **COMMUNITY** option is used to specify a community Name for sending traps to the SNMP management console (the default is public).

    Use the COMMUNITY option, as follows, in the NMA.NCF file.
  - **GA** option is used with some NW2SNMP versions to enable generic agent alerts (the default is disabled). The generic alerts are the NMA generated alarms, which are non-trap/SNMP alerts. Those generic alerts are translated in trap/SNMP format by the NWTRAP NLM.

    `LOAD SYS:SYSTEM\NW2SNMP GA=<ON/OFF>`

    ON is the option to enable Generic Agent Alerts.

- **NWTRAP options**

  - **/C<community name>** to specify the correct community name you use for sending trap (the default is public).

    `LOAD NWTRAP /C<community name>`

    community name is the password specify.
  - **/S<n>** option is used to define the minimum severity level of alarms to be sent to your management station (as a filter) as follows (the default is all the traps).

    `LOAD NWTRAP /S<n>`

Here, n is the severity threshold level. n can take the values of 0 through 4.

The following is a table with the severity levels:

Severity	NetWare OS Severity Level	NWTRAP Severity Level
Informational	0	0
Warning	1	1
Recoverable	2	2
Critical	3	3
Fatal	4	4
Operation Aborted	5	4
Unrecoverable	6	4

> **Attention**
>
> If you do not set this parameter, all the traps will be sent and both your network and your management console will be flooded with traps and your work traffic could increase.

- **/T<n>** option is used to define the time interval to indicate the number of seconds that must elapse before a later event is not discarded (the default time is 10 seconds).

  LOAD NWTRAP /T<n>

  n can take any value between 0 and 232.

- **Sample NMA.NCF**

```
#------------------------------------------------------------------
#                 Novell NetWare Services Manager
#                          Version 1.5
#------------------------------------------------------------------
# NMA.NCF: NetWare Management Agent NCF file
#------------------------------------------------------------------
# Description: This NCF file loads all the NetWare Management Agent
#              software for the NetWare 3.X. The following shows
#              the relationship between the the components loaded by this NCF
#              file. It also shows the dependencies of
#              these components on other system software.
#
#       RELATIVE
#       LOAD-ORDER  +---------------------------------+
#           1.      |   SOFTWARE  FROM  NMSBASE.NCF   |
#                   +---------------------------------+
#                                 |      +--------------+
#           2.                    |      |  SNMP.NLM    |----+
#                                 |      +--------------+    |
```

```
#                +-----------------------------------+   |
#       3.       |           NMAGENT2.NLM            |   |
#                +----------------+---------+------+  |   |
#                +--------------+ |         |      |   |
#       4.       | SIDEWIND.NLM | |         |      |   |
#                +--------------+ |         |      |   |
#                +--------------+ |         |      |   |
#       5.       | RATTLER.NLM  | |         |      |   |
#                +--------------+ |         |      |   |
#                +--------------+ |         |      |   |
#       6.       | SPAGENT.NLM  |--+        |      |   |
#                +--------------+            |      |   |
#                                   +-------+------+  |
#       7.                          |  NW2SNMP.NLM |----+
#                                   +--------------+  |
#                                   +--------------+  |
#       8.                          |  NWTRAP.NLM  |----+
#                                   +--------------+
#
#-----------------------------------------------------------------

# Step-1: Load the NetWare Management Agent software.
LOAD SYS:\SYSTEM\NMAGENT
LOAD SYS:\SYSTEM\NMAGENT2
LOAD SYS:\SYSTEM\SIDEWIND /N
LOAD SYS:\SYSTEM\RATTLER
LOAD SYS:\SYSTEM\SPAGENT

# NOTE: RATTLER.NLM is not needed by the Microsoft Windows version
#       of NetWare Services Manager. However, it is needed by the
#       IBM OS/2 version of NetWare Services Manager.
UNLOAD RATTLER

# Step-2: Load the NetWare to SNMP trap translator software.
#         OPTION: If you want to change the default community name
#                 of traps from PUBLIC, use COMMUNITY=<CommunityName>
#                 option with NW2SNMP.NLM and /C=<CommunityName>
#                 option with NWTRAP.NLM.  For example:
#                 load SYS:\SYSTEM\NW2SNMP COMMUNITY=administrator
#                 load SYS:\SYSTEM\NWTRAP /C=administrator
#

LOAD SYS:\SYSTEM\NW2SNMP COMMUNITY=public
LOAD SYS:\SYSTEM\NWTRAP /C=public
```

4.2.1.2 Configuring AUTOEXEC.NCF

By default, NMA sends alarms to the NMS console management stations. NMS uses Service Advertising Protocols (SAPs) to identify itself to the NMA software installed on the NetWare servers.

To modify that, it is possible to configure the SNMP NLM load. In the AUTOEXEC.NCF, the TCP/IP NLM is loaded with the optional parameter:

```
trap=<IP address>
```

If you specify an IP address of a management console like NetView for AIX, all the traps are sent to that station.

If you want to send alarms to several management stations, you can create a TRAPTARG.CFG file as follows:

- Create the TRAPTARG.CFG in the SYS:\ETC\ directory on the NMA server.
- Enter all the IPX and IP addresses of the Management Console you want to use, as shown in the SYS:ETC\SAMPLE\TRAPARG.CFG.

  For example, here is our *SYS:\ETC\TRAPTARG.CFG*:

```
    9.24.104.112        # Our NMS Console
protocol udp
    9.24.104.123        # NetView for AIX on RS60005
    9.24.104.25         # NetView for AIX on RS600011
```

Note

To have more information about NMA V1.5 and V1.6 configuration, especially for NMA V1.6, print the \NMS\NMA15.WRI and \NMS\NMA16.WRI files.

4.2.1.3 Limiting Transmission SAP Packets from NMS Consoles

Each NMS console sends a SAP packet with the ID number 0x026A. The NW2SNMP.NLM file uses this packet to identify consoles that it should send traps to. This procedure can create excessive traffic on remote links. This is a particular problem for on-demand, dial-up connections, which can be kept up almost constantly by this process. To eliminate this problem, complete the following steps:

1. Follow the instructions in defining recipients for SNMP alarms to define the recipients of SNMP traps.
2. Configure the NMS Console not to send SAP packets.
3. Select **Configure > Global Preferences**. The system displays the first Global Preferences dialog page, System Options. It is identified by the highlighted icon on the right side of the dialog box.
4. Click on the **Receive NetWare Server Alarms** check box to de-select this option and save the changes.
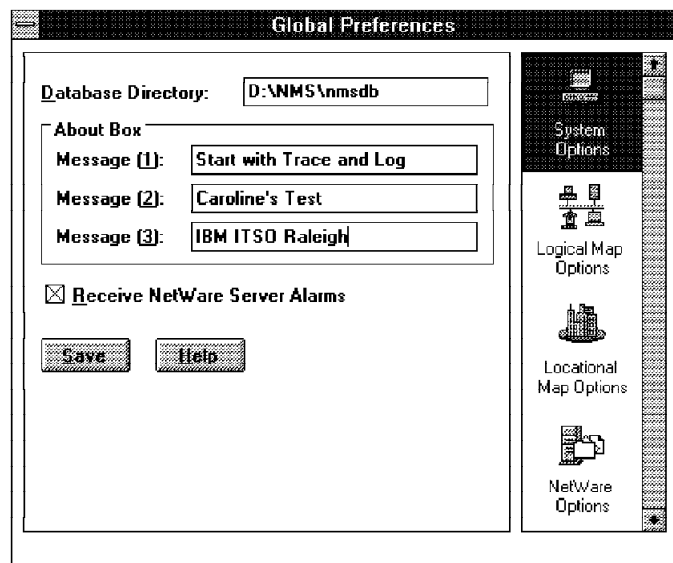
Figure 97. NMS Global Preferences

After these changes, the NMS Console no longer sends SAP packets.

Note

However, NMS might have already sent a SAP packet. In this case, the address of the console will be in the servers memory. To remove the servers address, you must either down the server or unload and reload SNMP.NLM.

4.2.2 How to Use NMA with NMS

NMA is completely integrated in NMS. It provides another icon for NetWare servers which have NMA running. It is the same NetWare server icon with a different color. To display the NMA information screen, double-click on the selected NMA server icon. The first time you want to access the NMA server, you have to enter the NETMAN password registered for this server.

The NETMAN registration procedure is usually done during the installation step. If not, proceed as follows:

- Start the NMS Windows application.
- Select the **Security** and **Register NETMAN Password** options.
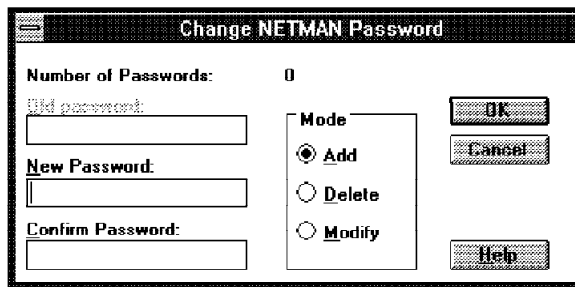
Figure 98. NMS Register NETMAN Password

Enter the NETMAN password for the server you want to access. If you do not have the same NETMAN account password on each NMA server, you have to register all the NETMAN account passwords into the NMS Console application. The NETMAN user is a special username used by NMA to request information from all NetWare NMA servers with the appropriate rights. In a NetWare V4.x architecture, the NETMAN user is created in the server and bindery emulation container.
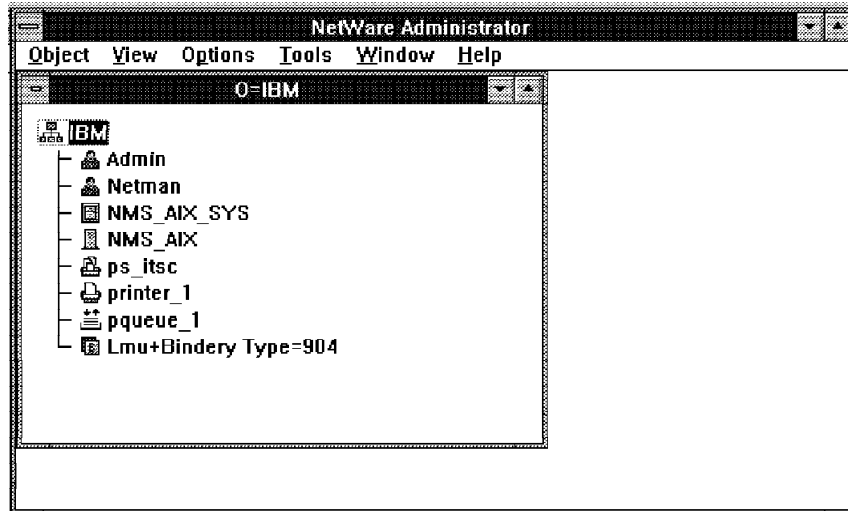
Figure 99. NetWare Administrator Tool for NetWare V4.x

NMA provides system information about the NetWare system resources. Examples of this would be:

- Monitoring the NetWare operating system and the NLM files

  A list of all the NLMs loaded on the server, the version number, the amount of memory used and a description of the NLM. The NLM table contains real-time information about the servers NLM files.

Figure 100. List of NLMs from NMA

- CPU speed and utilization

  NMA provides you with the relative CPU speed of the server. This is the same value that you obtain from NetWare when you start the NetWare server or by typing in the `:SPEED` command on the server.

Double-clicking on the **CPU** icon gives you a CPU utilization graph with a percent utilization for the servers CPU.
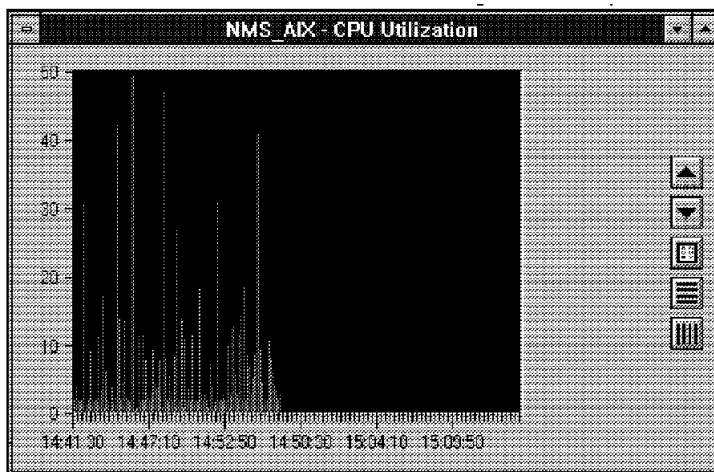

Figure 101. NMA CPU Utilization

- Monitoring memory usage

  Memory utilization is displayed as a pie chart and the values can be displayed as either percentages or absolute values.
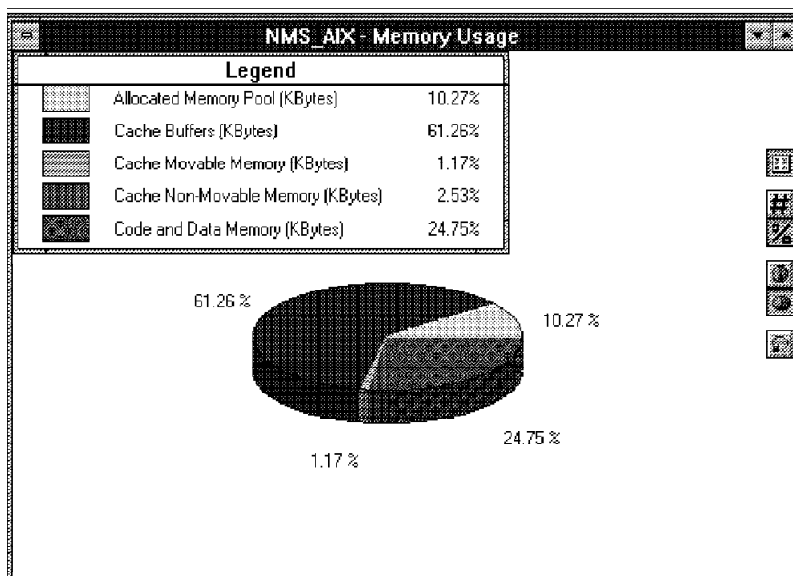

Figure 102. NMA Captured CPU Utilization

- Monitoring LAN (or disk) adapter boards

  This is the list of all adapters installed on the server with all of the protocol stacks that are loaded on the boards. In addition, the MAC addresses, frames and configuration information can be displayed, as in Figure 103 on page 143.
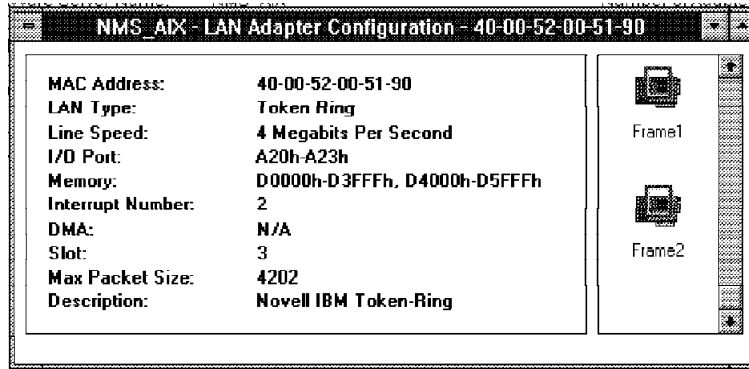
Figure 103. LAN Adapter Configuration from NMA

- Monitoring volume information

  This is the list of all volumes that are configured and their utilization and size.

Figure 104. Volume Utilization from NMA

- Monitoring server hard disk information

  This is the list of all hard disks configured, with their type, size and controllers.

Figure 105. Device Configuration and Utilization

- Monitoring server traffic

Using NMS, you can graph the traffic in and out of a server, showing the traffic by protocol type.
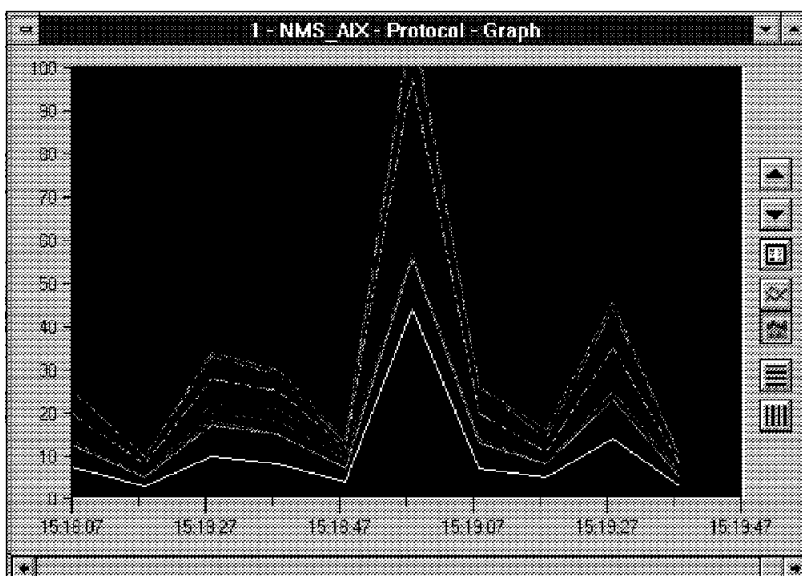
Figure 106. Server Traffic Graph Gathered from NMA

NMA must be installed on all the NetWare V3.x and V4.x servers that you want to manage.

4.3 NetWare LANalyzer Agent (LANalyzer V1.0)

Figure 107. NetWare LANalyzer Agent Description

The NetWare LANalyzer agent is used to provide physical network management, regardless of the protocol. It complements the NMS and the NMA products.

The NetWare LANalyzer agent should be installed on one NetWare V3.x or V4.x server per physical segment. It includes the NLM server software for the following functions:

- SNMP RMON monitoring of Ethernet and token-ring segments (trends and alarms)
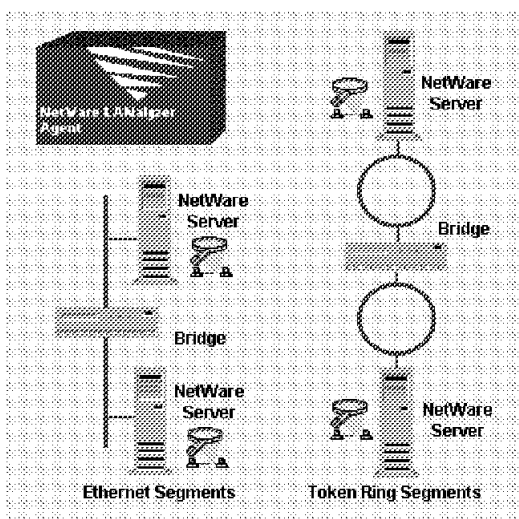- Remote capture and decoding of Ethernet and token-ring frames

These functions are integrated into the NMS Console software, but a NetWare server with the LANalyzer agent installed must exist on one NetWare server per segment.

The NLM components of the NetWare LANalyzer are:

- LANZSU.NLM
- LANZMEM.NLM
- LANZLIB.NLM
- LANZDI.NLM
- LANZAEL.NLM
- LANZHIS.NLM
- LANZFCB.NLM
- LANZSM.NLM
- LANZTR.NLM
- LANZCTL.NLM

4.3.1 LANalyzer Configuration

After installing the NetWare Management Agent, you have to check the SYS:SYSTEM\LANZ.NCF file. This file is a batch file for NetWare OS, so you can start it on the LANZ.

Usually, the default components are sufficient and some of them should be able to dynamically increase their size.

Configuring AUTOEXEC.NCF - By default, LANalyzer sends alarms to all the management stations specified in the SYS:\ETC\TRAPTARG.CFG file.

- Create the TRAPTARG.CFG in the SYS:\ETC\ directory on the LANalyzer server.
- Enter all the IPX and IP addresses of the management console you want to use (as shown in the SYS:ETC\SAMPLE\TRAPARG.CFG).

    For example, here is our TRAPARG.CFG:

    SYS:\ETC\TRAPTARG.CFG

    ```
        9.24.104.112        # Our NMS Console
    protocol udp
        9.24.104.123        # NetView for AIX on RS60005
        9.24.104.25         # NetView for AIX on RS600011
    ```

Edit the SYS:\SYSTEM\AUTOEXEC.NCF file on each NetWare LANalyzer agent server to remove the comment mark before the LANZ.CFG command.

4.3.2 How to Use LANalyzer Agent V1.0
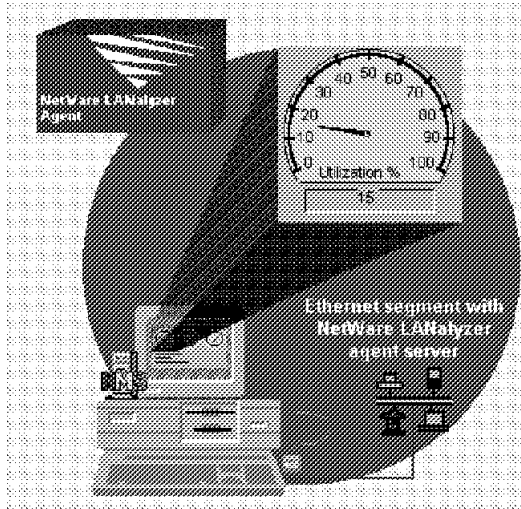
Figure 108. NetWare LANalyzer Agent

LANalyzer functions are completely integrated in NMS. They provide additional functions to manage segments and routers, and for NetView for AIX, it can feed the RMONitor for AIX application.

4.3.2.1 LANalyzer into NMS

To access LANalyzer monitoring functions, select a network icon on which NetWare LANalyzer is running and select the **Performance> segment** options in the menu bar of the NMS user interface.

1. NMS provides trend data for both Ethernet and token-ring segments through segment graphs. Graphs are accessed from the Network segment option.

Figure 109. Monitoring Segment

2. With one NetWare LANalyzer agent installed on each bridged Ethernet segment, you can monitor and set thresholds for the following Ethernet segment vital signs:
   - Packets/sec
   - Utilization %
   - Broadcasts/sec
   - Multicasts/sec
   - CRC errors/sec
   - Undersized packets/sec
   - Oversized packets/sec
   - Fragments/sec
   - Jabbers/sec

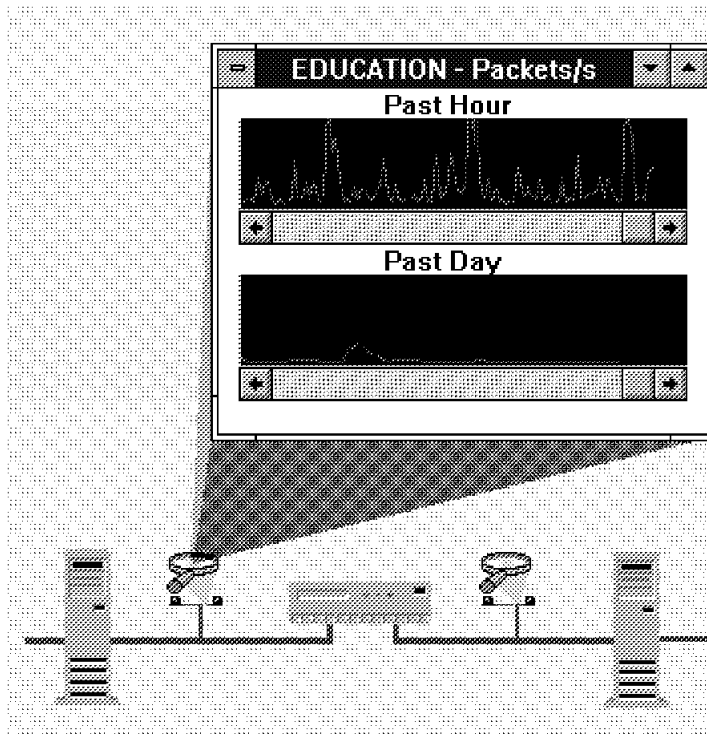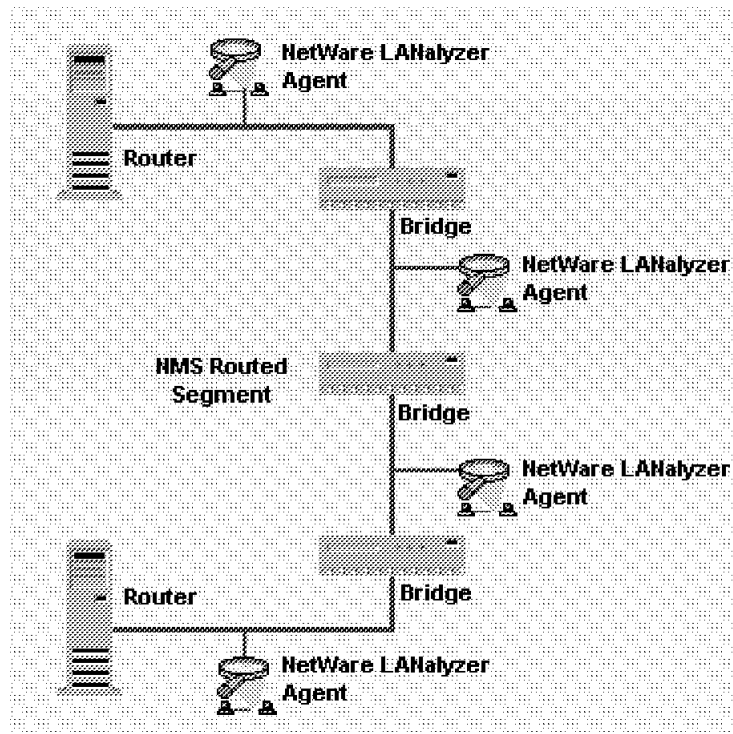*Figure 110. Monitoring Ethernet Segments*

3. With one NetWare LANalyzer agent installed on each bridged ring segment, you can monitor and set thresholds for the following token-ring segment vital signs:
   - Packets/sec
   - Utilization %
   - Beacons
   - Monitor contention
   - Line errors/sec
   - Burst errors/sec
   - Congestion errors/sec
   - Broadcasts/sec
   - Multicasts/sec
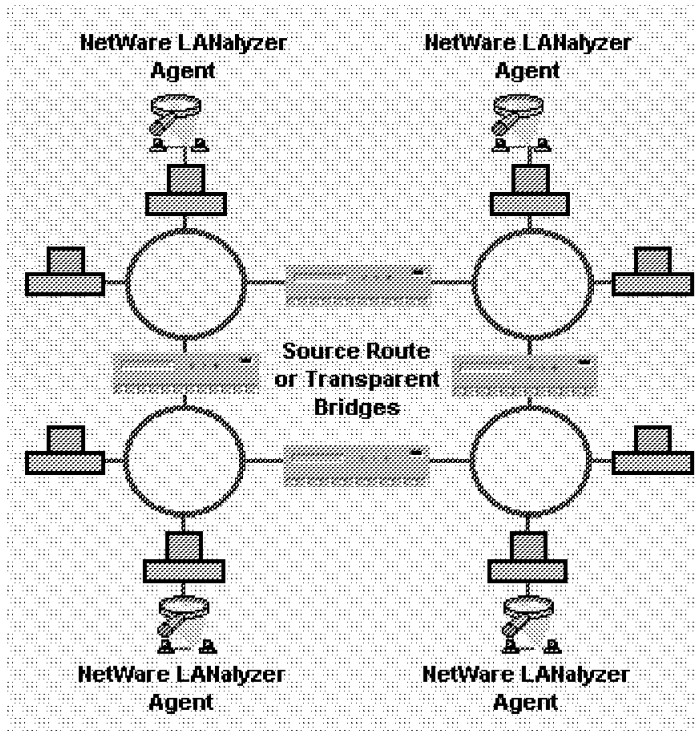
Figure 111. Monitoring Token-Ring Segments

4. The NetWare LANalyzer agent provides the capability to remotely capture and decode Ethernet and token-ring frames.

   Clicking on the **capture** icon, the monitored segment selected opens the Packet Capture Setup window, as shown in Figure 112.

Figure 112. Packet Capture Setup

Then you have to select the stations from which you want to capture packets. The default is any. You also need to specify the protocols you are interested in and the type of packets you want to capture.

Then click on **OK** when your setup has completed and the Capture Status screen appears.
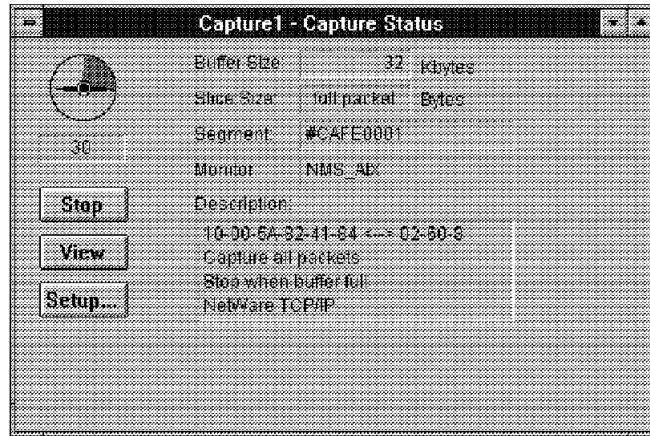
Figure 113. Capture Status

Figure 113 shows you the status of the capture packets procedure; you can **stop** it or **View** the contents of the capture buffer by clicking on the correct button.

If you select to view the packet, you will see a summary of the packet, as well as each byte in the packet, as shown in Figure 114.
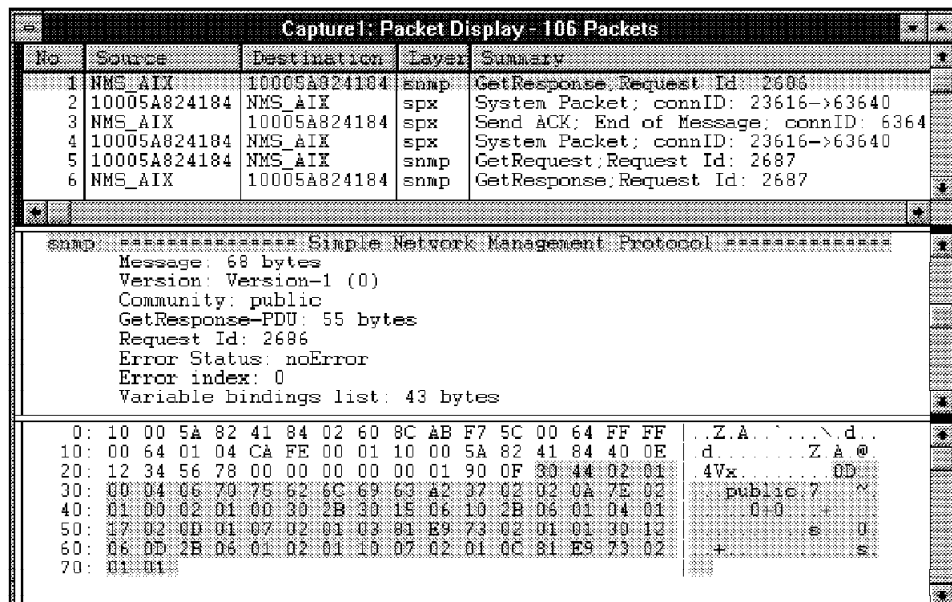
Figure 114. Packet Display

The top is the packet summary (one line for each packet), and the bottom is the decode of the packet.

5. Another function allows you to display the top 20 nodes using the selected segment.

In order to show this, select the **Performance > Segment > Stations** options from the menu bar.

Station	Util %	Pkts/s Out	Bytes/s Out	Errors/s	Pkts/s In	Bytes/s
NMS_AIX	1	5	1210	0	4	1(
10005A824184	1	5	1040	0	5	1:
RS60001	0	0	0	0	1	
6611A	1	1	81	0	1	
0180C2000000	0	0	0	0	1	
8224-2-10005A1	1	1	12	0	0	
RS60007	0	0	0	0	1	
0800202378C1	0	0	0	0	0	
02008C2E0040	0	0	0	0	0	
400008580321	1	1	12	0	0	
02008C2E9449	0	0	0	0	0	
AA0004000110	0	0	0	0	0	
8224-1-10005A1	1	1	12	0	0	
RS600010	1	1	19	0	0	
10005AC26899	0	0	0	0	0	
4000012A3172	0	0	0	0	0	
DEC_End_nodes	0	0	0	0	0	
BANK311	1	1	13	0	0	
08008F108FE9	0	0	0	0	0	
08005A910378	1	2	65	0	0	

Figure 115. Top 20 Stations

6. NMS LANalyzer provides a network dashboard for the segment selected.

   To see this displayed, select the **Performance > Segment > Dashboard** options from the menu bar.
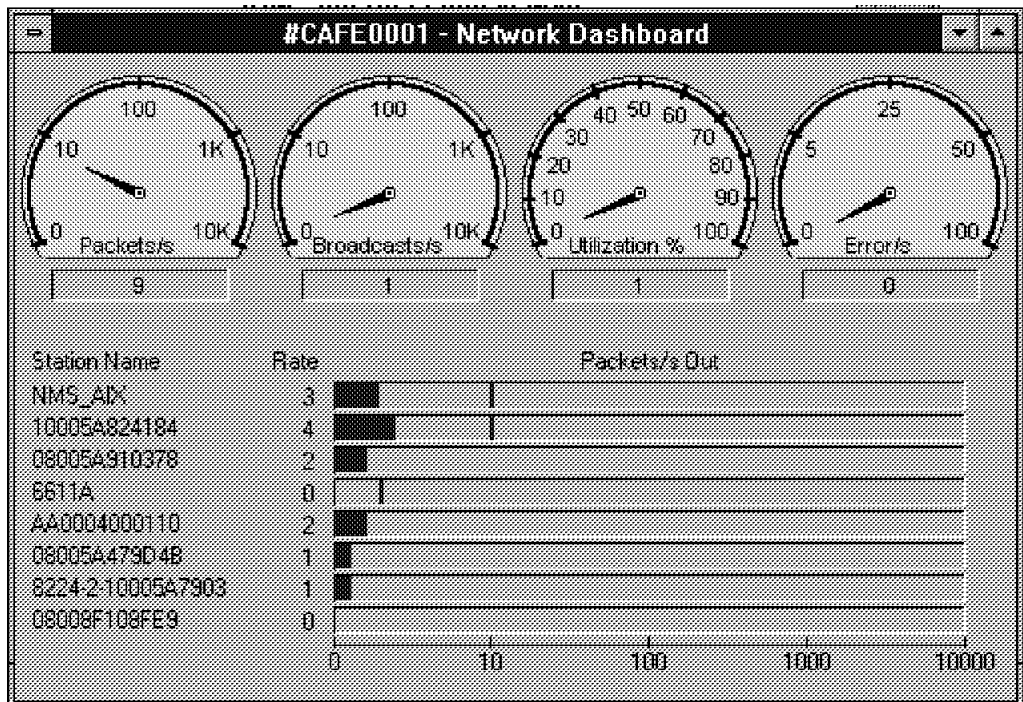
Figure 116. Network Dashboard

4.3.2.2 LANalyzer Information to NetView for AIX

From the NetView for AIX application, start the RMONitor for AIX application. Then, you should be able to see the LANalyzer managed segment, as shown in Figure 117.

Figure 117. RMONitor for AIX, Network Monitor

After selecting the displayed network, choose the **Selected > Agent Profile** option to see details about your LANalyzer agent monitor. You will find out what is supported from an RMONitor perspective when you display the agent profile. This window can not be updated by you. It is just a display showing the status of the agent.
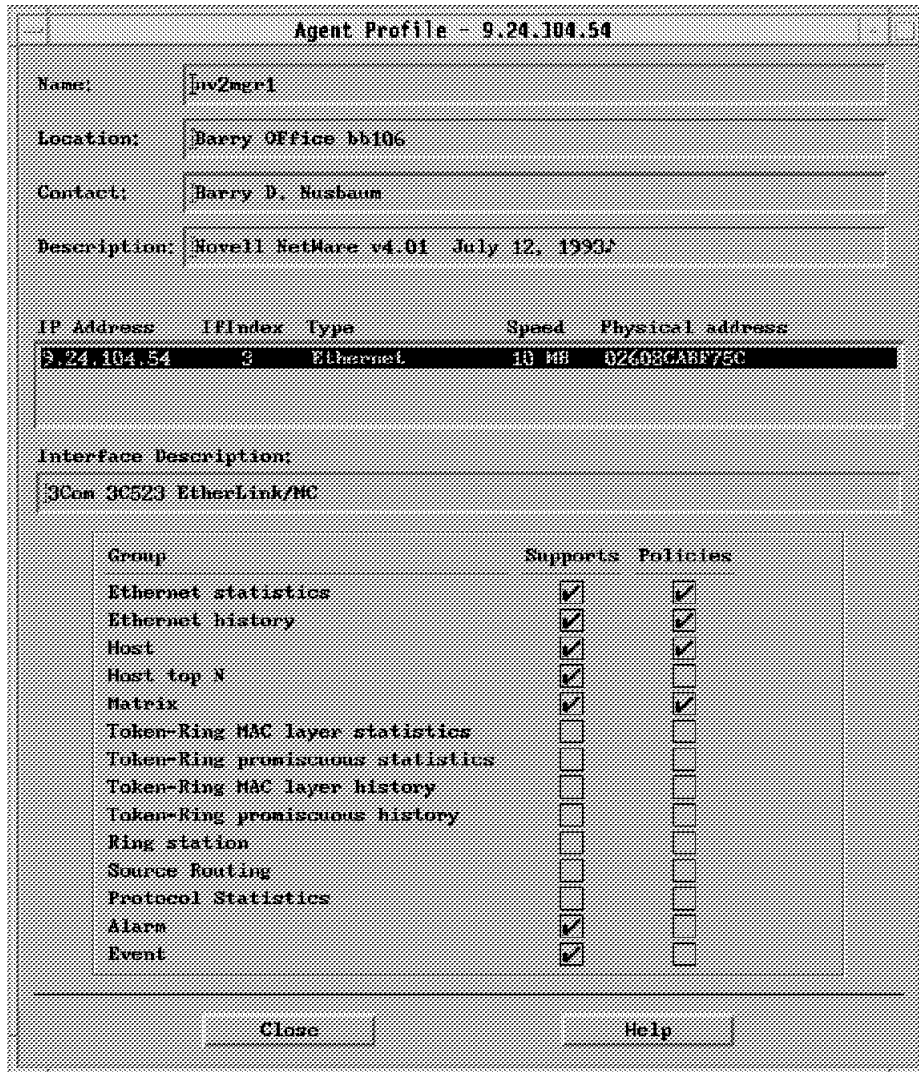
Figure 118. RMONitor for AIX, Agent Profile

To monitor the selected segment, choose the **Selected > Segment Monitor...** option from the main panel menu bar. This will give you the Ethernet monitored attributes as shown in Figure 119 on page 153.
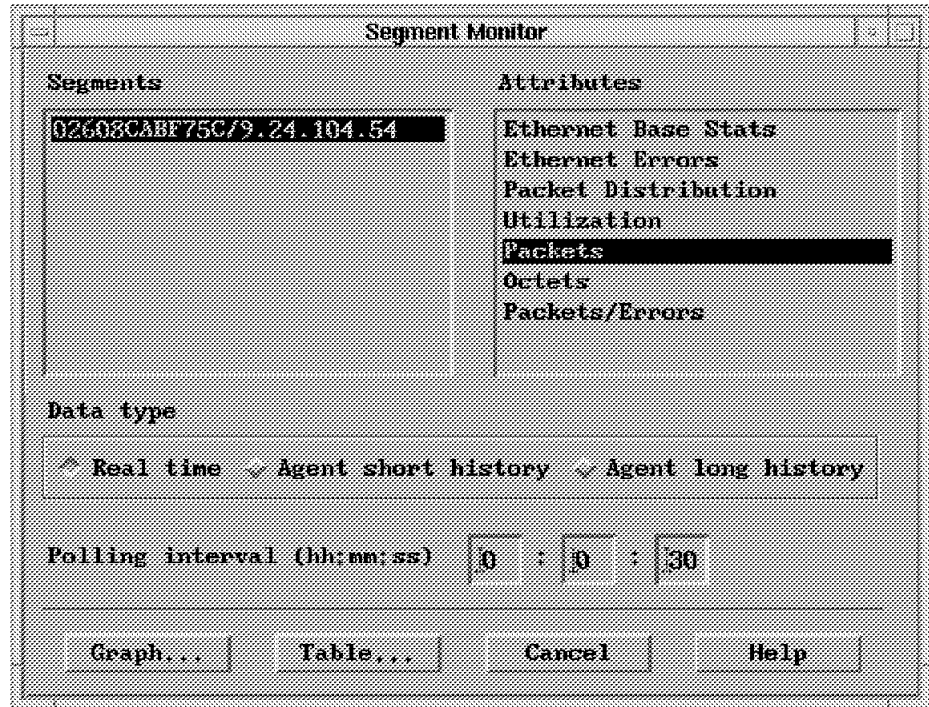
Figure 119. RMONitor for AIX, Segment Monitor

Select the attribute you want to monitor and the type of the display you prefer.

Figure 120. RMONitor for AIX, Ethernet Real-Time Packets
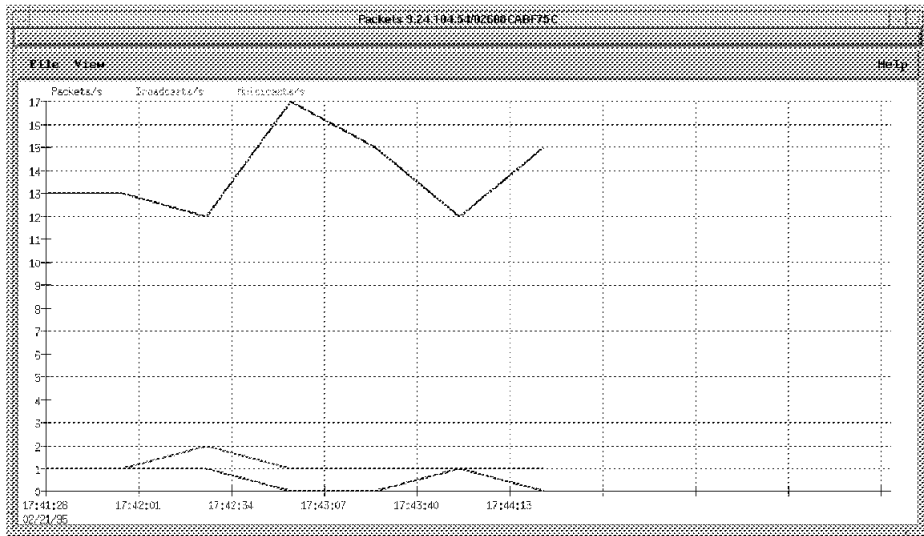
Figure 121. RMONitor for AIX, Packets Utilization Graph

Chapter 5. Integrating Novell NMS Topology into NetView for AIX

This chapter will describe how to configure and use Openmon under NetView for AIX and NMS Export Services to integrate the Novell NMS topology with NetView for AIX.

Together, the NetView for AIX V3.1 Openmon PTF, U438561, and the Novell NMS Export Services 1.0 enable you to integrate the NMS topology into NetView for AIX. This is the first step towards the real integration of NetWare Management into NetView for AIX. We used NetView for AIX V3.1 and also NetView for AIX V4.1. We were using AIX V4.1.3 when we used the NetView for AIX V4.1 system.

In addition to using NMS with NetView for AIX, we used ManageWise V1.0 and Export Services to communicate with NetView for AIX. The traps and topology information were only from the NMS part of ManageWise.

In Chapter 2, "Installation" on page 9, we described the installation of these products. Now we will show you how to configure and use these products to export the Novell NMS Topology to NetView for AIX.

5.1 Configuring and Starting NMS Export Services

The Novell NMS Console builds a database and map of network devices. For our project, we focused on the IP and IPX devices.

NMS Export Services:

- Retrieves discovery information from the NMS database and transmits it to other network management consoles
- Has been tested to work with IBM NetView for AIX
- Consists of Export Configuration, Export Scanner, and Export Communication utilities
  - The Export Configuration Utility provides an interface to set communication parameters for client connection and enables you to schedule database extraction from the NMS Console.
  - The Export Scanner Utility reads the NMS database and creates the export file. The Export Scanner 1.0 Utility exports the entire discovery database.
  - The Export Communication Utility waits for the connection from another network management console and sends the exported file when it receives the connection.

To configure and run the NMS Export application:

1. Start the MS-Windows and display the NMS-Group window as shown in Figure 122 on page 156.
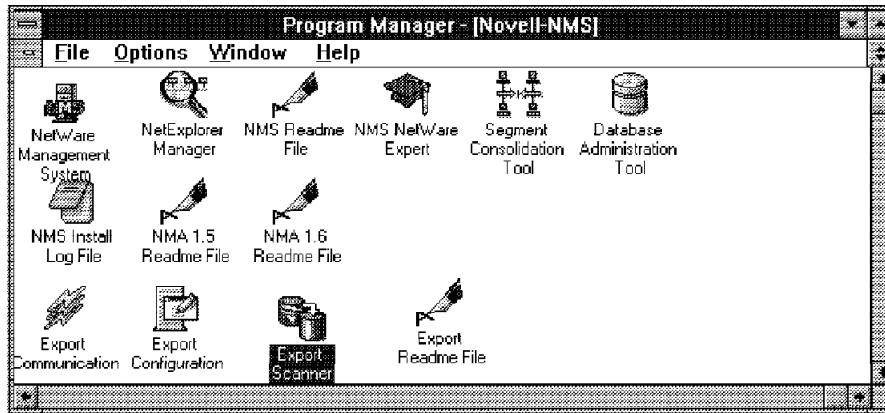
Figure 122. NMS Export Services

2. To configure the NMS Export Services, or check its parameters, double-click on the **NMS Export Configuration** icon.
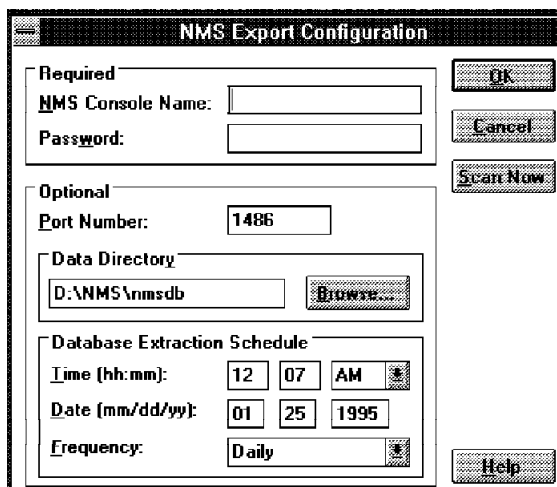
Figure 123. NMS Export Services Configuration

There are several fields that you will need to fill in. Some of them will need to match up with NetView for AIX values.

- The NMS Console Name field will end up as the label on one of the NetView for AIX submaps for displaying the NMS resources.
- Password is the community name used to communicate with the NetView for AIX Openmon application; so, you will need to specify the NetView for AIX's community name.
- Port Number must be the same number as you specified in the Openmon configuration as shown in Figure 127 on page 158.
- Data Directory is the directory where the export file will be created and from where the Communication Export Program will look for this file (NMSXPORT.XPT).
- The Data Extraction Schedule determines when the information in the NMS database should be exported to a file. You specify when you want this information to be exported and how often.

3. NMS Console Name will be the application, and an icon label will appear on your NetView for AIX Console.
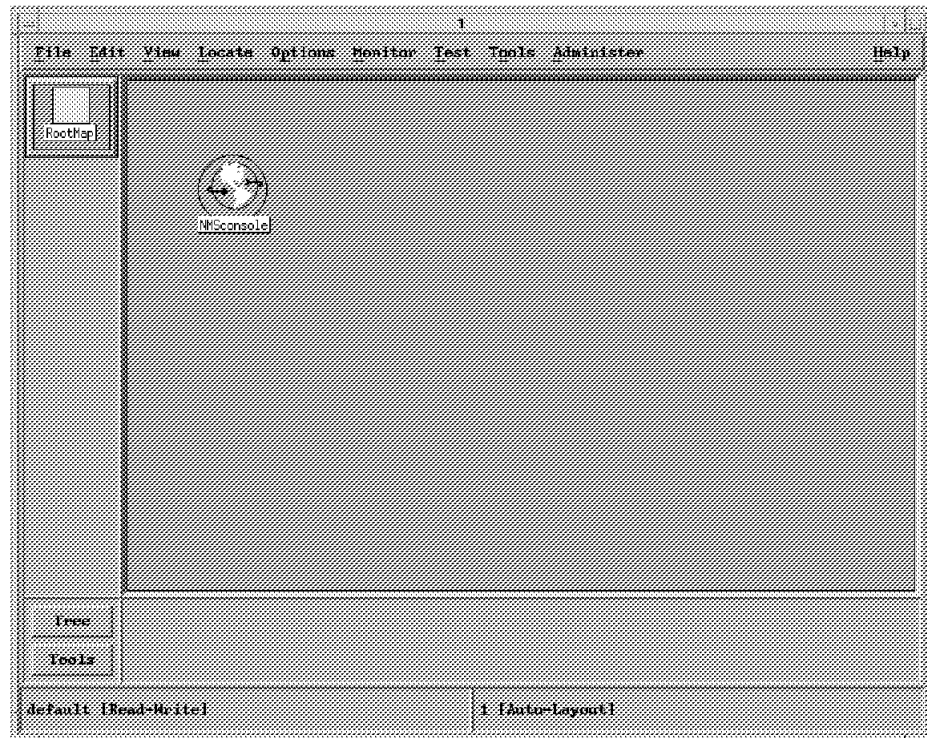
Figure 124. NetView for AIX Openmon Application NMS Console

 4. You can save the configuration or immediately start the export.
 5. Check that the Export Communication application is running; if not, start this
    application (an icon will be displayed).

Figure 125. NMS Export Communication Icon

 6. Double-click on the **NetWare Management System** icon to start the NMS
    console user interface.
 7. Answer Yes to load the NetExplorer Manager if a dialog box appears.
 8. Wait for the complete discovery of your network. It is possible that this process
    could take *several hours*.
 9. Double-click the **NMS Export Scanner** icon to start NMS Database Export file
    creation. When the NMS Export Scanner icon appears on the bottom of the
    screen, it has started processing. When it disappears from the screen it means
    it has finished processing.

Figure 126. NMS Export Scanner Icon

It creates a NMSXPORT.XPT file in the directory you specified during the installation and configuration step. \NMS\nmsdb is the default directory. While the file is readable, if you type it out or edit it, it is not very readable to use in another application.

5.2 Configuring and Starting an Openmon Application

The Openmon configuration program, openmonconf, can be used to set up and configure an Openmon topology application to interact with any Openmon topology agent. It can discover and load other network topologies into NetView for AIX. In our case, the topology agent was NMS Export Services. In the future, it could be any vendor's Openmon topology agent.

Execute the Openmon configuration program as follows:

From the NetView for AIX window, as shown in Figure 124 on page 157:
- Choose the **Administer** menu.
- Choose **Openmon Application**.
- Choose **Start Openmon Configuration Program**.

The screen shown in Figure 127 will appear.

Figure 127. Openmon Application Configuration

- Enter a name for your application and click on the **Add Application** button. The letters OM will be added at the beginning of the name to facilitate identification of Openmon topology applications (for example, when viewing the results of the ovstatus command). This change applies to the executable file and the lrf, but not to the application's configuration file.

- The Host parameter is the IP address or host name of the Openmon topology agent, that is, the NMS Console where NMS Export Services is executing.

- The Port number is the port on which the Openmon topology agent listens for requests from your application. This port number must match the port number you specified when configuring NMS Export Services. The default port number is 1486.

- The Community parameter is required for communication with the Openmon topology agent. This must match the Password parameter you specified when configuring NMS Export Services.

- The Update Interval is the interval, in minutes, at which your application should request updated information from the topology agent. The first interval begins when your application has finished storing the initial information in the GTM database. Enter 0 to disable update processing. Currently, NMS Export Services does not support the update function.

- The Update Sequence Number field is a counter which keeps track of topology resources. The Openmon application will use this to request updates from NMS Export Services in a future release of export services.

- In the Trace Option parameter, specify the following:

  - N if you want your application to write only error messages to its trace file.
  - Y if you want your application to write informational trace messages as well as error messages to its trace file.

  The trace file will be placed in the /usr/OV/log directory. It will be called filename.trace. So, for example, if your application is called test, the file will be OMtest.trace.

A sample piece of the trace file looks like the following:

```
Wed Aug 30 15:43:33 EDT 1995
*** OMnms21 started () ***
*****************************************************
OMnms21: host = (9.24.104.21)
OMnms21: port = (1486)
OMnms21: community = (public)
OMnms21: update interval = (0) minutes
OMnms21: update sequence = ()
OMnms21: trace = (y)
Setting up socket communication with topology agent
OMnms21: connected to host (9.24.104.21) port (1486)
*****************************************************
Wed Aug 30 15:43:33 EDT 1995
OMnms21: sending topology request to application
*****************************************************
Sending message to application $%Stopology load%Ppublic%E$
***current topo record=database reset (%Sdatabase reset%E)***
current topo record=(%Sbulk data%E)
*** END OF TOPO DATA RECORD RECEIVED ***
*-*-*-*-*-*-*-*-*-*-*-*-*--*-*-*-*-*-*-*-*-*-*-*-*-*
*-*-*-*-*-*-*-*-*-*-*-*-*--*-*-*-*-*-*-*-*-*-*-*-*-*
Wed Aug 30 15:43:34 EDT 1995
Processing topology bulk data file (/usr/OV/log/OMnms21.load)
*-*-*-*-*-*-*-*-*-*-*-*-*--*-*-*-*-*-*-*-*-*-*-*-*-*
*-*-*-*-*-*-*-*-*-*-*-*-*--*-*-*-*-*-*-*-*-*-*-*-*-*
*****************************************************
Wed Aug 30 15:45:03 EDT 1995
OMnms21: topology load processing completed
*****************************************************
OMnms21: host = (9.24.104.21)
OMnms21: port = (1486)
OMnms21: community = (public)
OMnms21: update interval = (0) minutes
OMnms21: update sequence = ()
OMnms21: trace = (y)
Wed Aug 30 15:45:03 EDT 1995
OMnms21: program terminating
```

After entering the required parameters, click on the **OK** button. A confirmation box will appear which asks if you would like to register your application with NetView for AIX.

Note

You must be superuser (root) under AIX to do this.
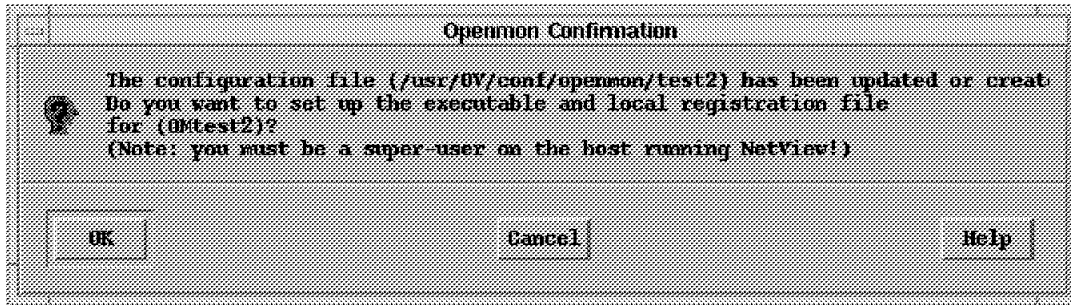
Figure 128. Openmon Confirmation

Click on the **OK** button and the Start Openmon Application window will appear.
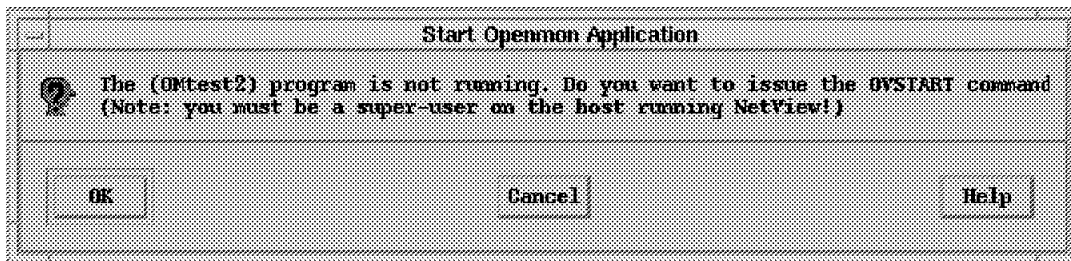
Figure 129. Start Openmon Application

Click on the **OK** button to start your application.

The Openmon configuration program creates a configuration file in /usr/OV/conf/openmon directory for your application. Here is the configuration file of the application we added:

```
host 9.24.104.21
port 1486
community public
updateinterval 0
trace y
```

5.3 Viewing the Novell NMS Topology

After starting your application, your Root map will contain 2 new root objects:

- applicationRoot
- Novell NMS

While your application is processing and loading the Novell NMS topology into the GTM database, both the applicationRoot and Novell NMS objects will be green.
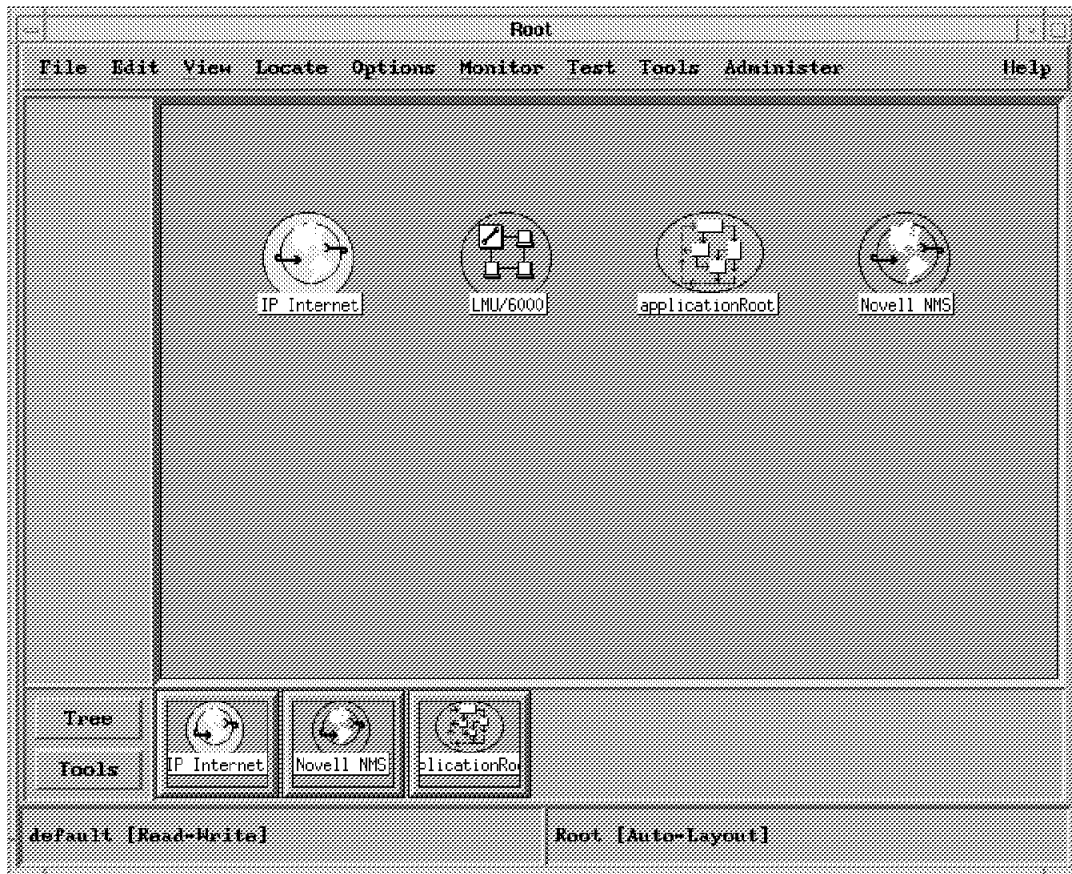
Figure 130. Root Map with applicationRoot and Novell NMS Submaps

Open the Novell NMS submap; then, open your application topology submap. In our case this submap was called NMSConsole, which was the name you configured in NMS Export Services window.
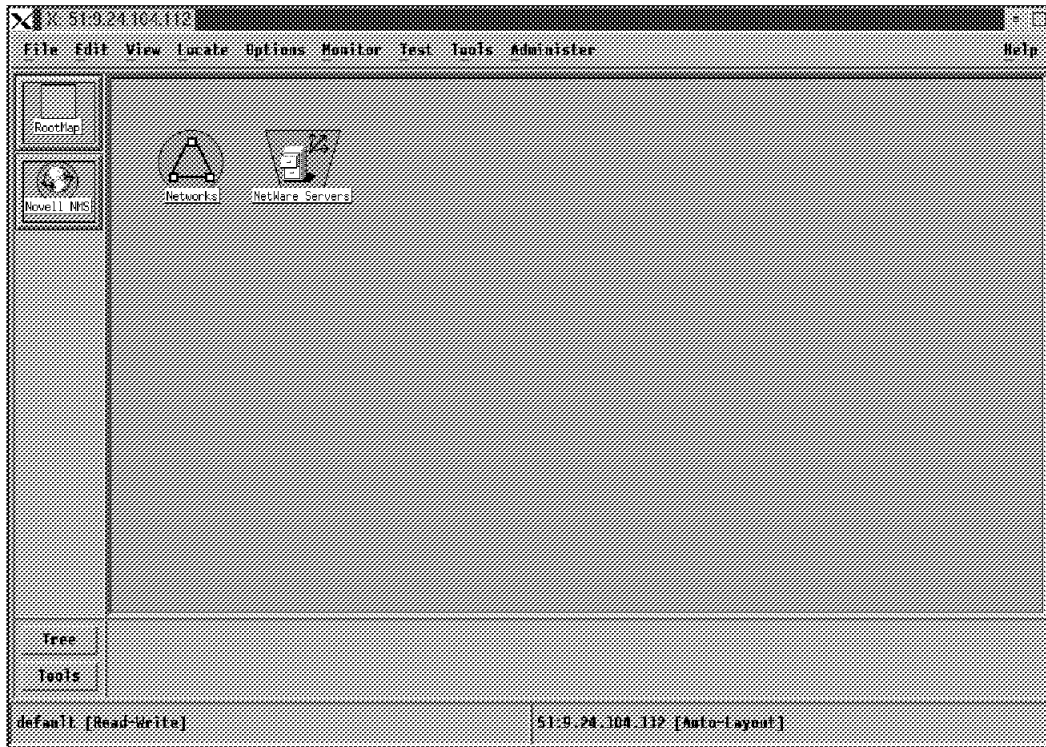
Figure 131. NMSConsole Submap

This submap will contain the following two objects:

- Networks submap
- Servers submap

Open the **Networks** submap.
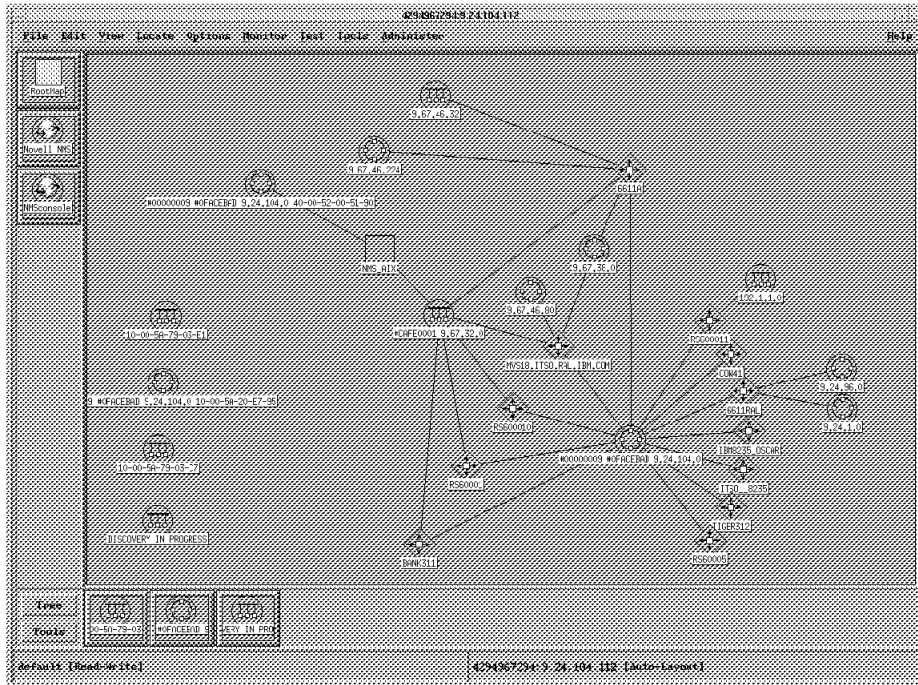
Figure 132. Novell NMS Network Level Submap

The NetWare topology discovered and loaded into NetView for AIX includes network segments, routers, hubs, servers and workstations.

From this NMS network map, select a NetWare server and the menu pull-down choice **Display Object Information**, as shown in Figure 133 on page 165.

Figure 133. OVW Object Information

This tool is a tool provided by the NetView for AIX V3 and V4. It gives the complete OVW Object information (as displayed).

From the Novell NMS submap, open the **Servers** submap. The Servers submap shows only NetWare servers.
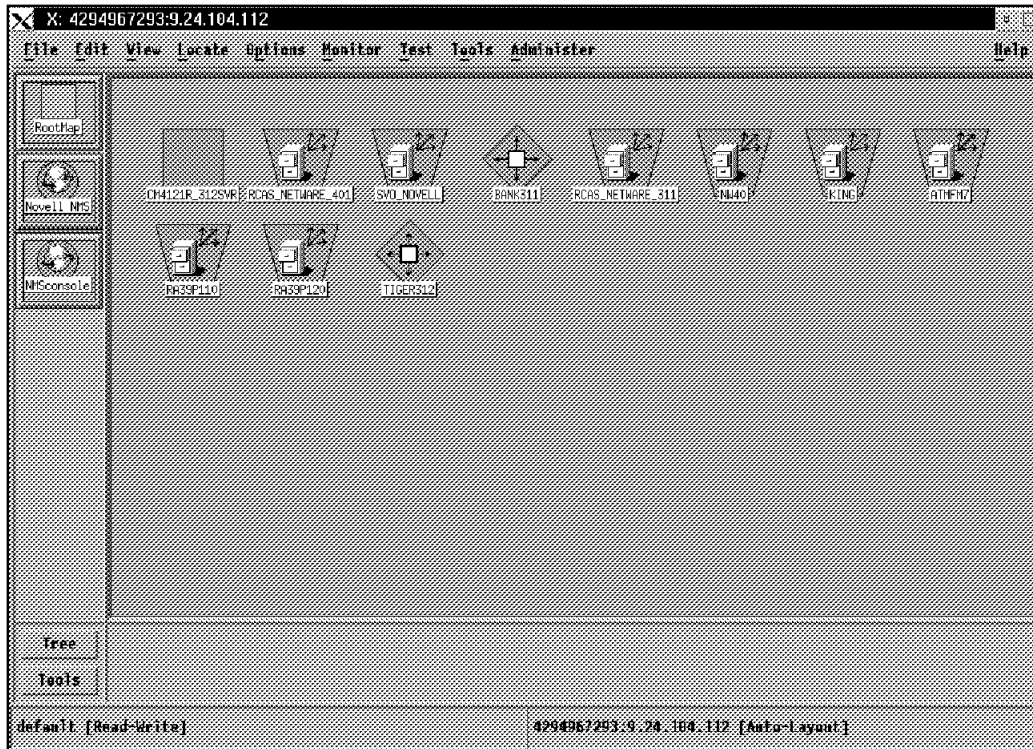
Figure 134. Novell NMS Network Level Submap

> **Note:** You will see that our NetWare 3.12 server is shown as a generic icon (a plain green box). This is because NetView for AIX does not yet have all the correct icons for the NMS discovered resources. There are different icons for a server with NMA installed and for the NetExplorer server. Our 3.12 server had NMA installed and this is why it had a generic icon. These and other icons will be added in the next release of Openmon which will correct this problem.

5.4 Correlation of Topologies

Correlation is provided at the workstation level between NetWare (IPX) and other network topologies (for example IP and LMU).

We opened the submap for object CM4121R_312SVR, which is our NetWare 3.12 server.
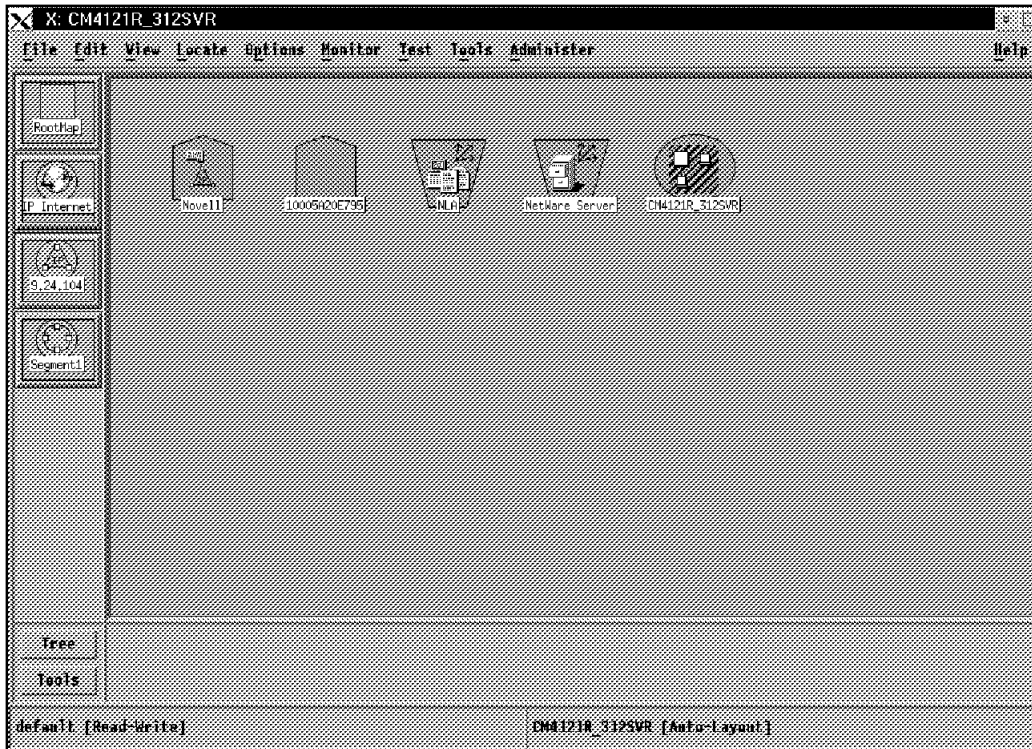
Figure 135. Our NetWare 3.12 Server Submap

As you can see, correlation is provided; we can see the IP interface, the IPX interface, the LANalyzer interface, the NetWare server and the LMU icon. The IP parent submaps are shown on the left side.

From the NMS network map or the NetWare Servers map, select a server and the **Protocol** option for this object to display protocol information, as follows:
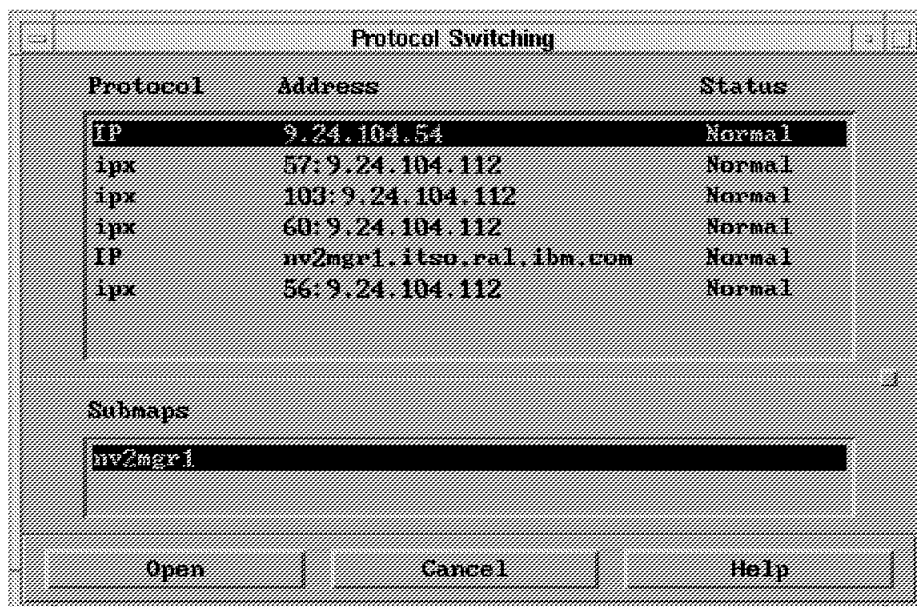
Figure 136. Protocol Switching for the Object

This displays all the loaded protocols with the address used and the status on each.

The Navigation Tree can be used to navigate from one topology to another.
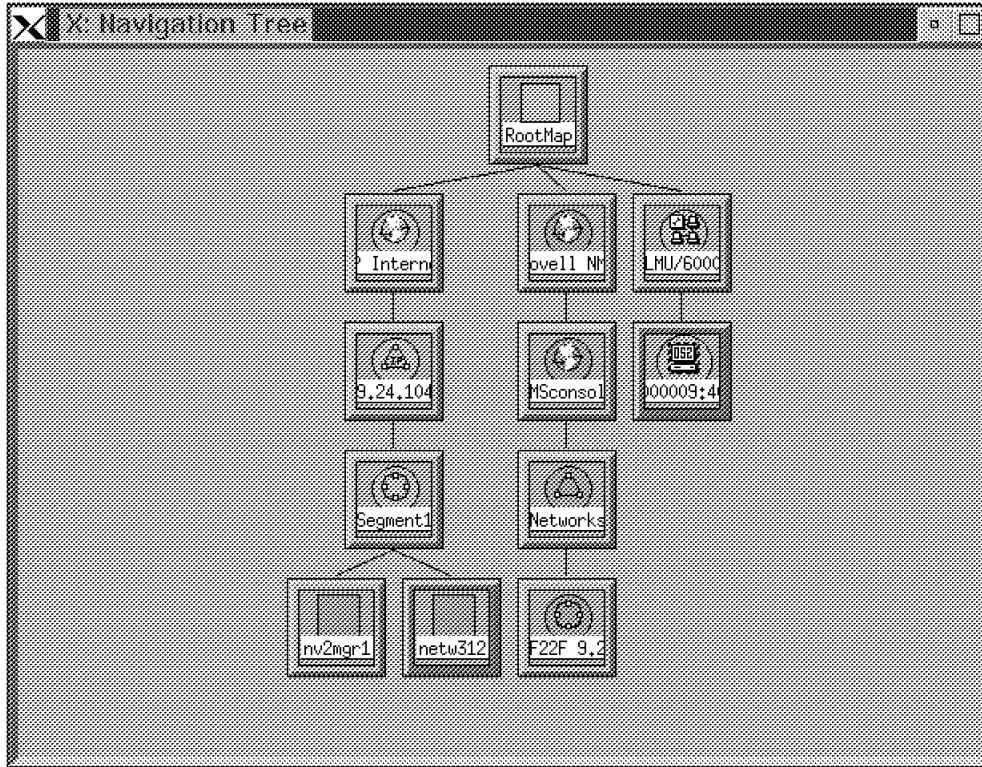
Figure 137. Navigation Tree

5.5 Viewing the Application Submaps

An icon is created for your application. You can view your application object by opening the applicationRoot submap from the Root map and opening the nvApplications submap.

Figure 138. applicationRoot Submap
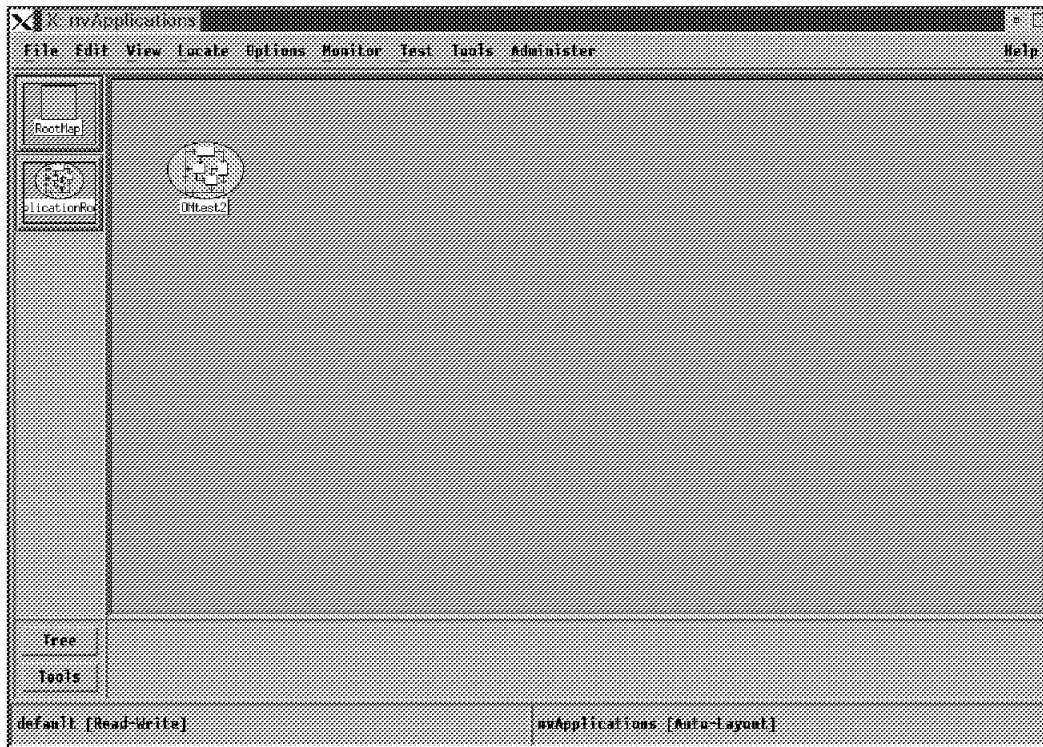
Figure 139. nvApplications Submap

The color of the object indicates the status of your Openmon application; that is, green indicates your application is running and blue indicates it is not.

It was decided to use blue rather than red to indicate a status of not running because red usually represents an error, which is not the case here.

If you click with the right mouse button on your application object, and choose **Start/Query/Stop Daemon Process**, you get a submenu which allows you to either start, query or stop your application.

For example, we queried our application when the object was blue and got the following results:
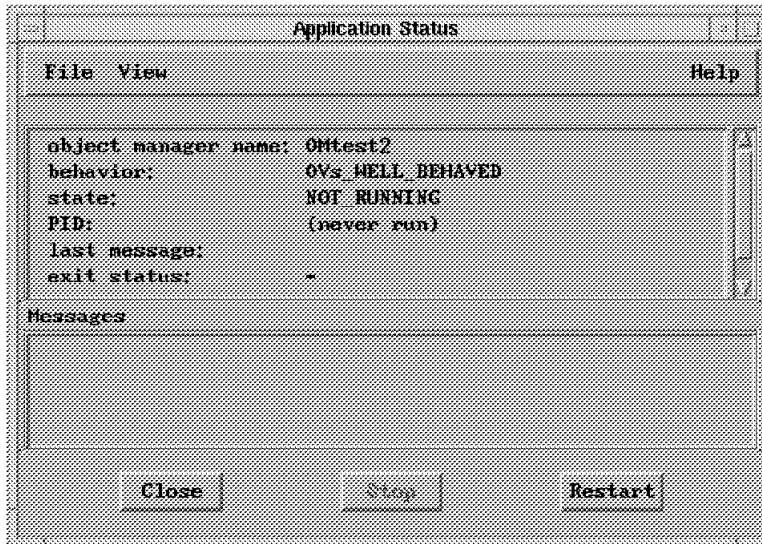
Figure 140. Application Status

5.6 Deleting the Discovered Topology

The Openmon Topology delete program, openmondel, can be used to delete the non-IP topology from NetView for AIX. The openmondel program can delete the following:

- An entire topology starting at a root object and all the objects below the root object
- One part of the topology starting at a network segment object

If you need to replace the topology information that has been stored for a particular topology, you have the following two options:

- Run your Openmon application to import the updated topology, which will simply overlay what you already have in the GTM database.
- Delete the existing topology information using the topology delete program, and then run your Openmon application to reload the new topology information.

We recommend you delete the existing topology first, before importing the new topology.

To delete an entire topology:

1. From the Administer pull-down menu choose **Openmon Application**.
2. Choose **Start NMS topology delete program** as shown in Figure 141 on page 172.

   This will start the topology delete program in the background.
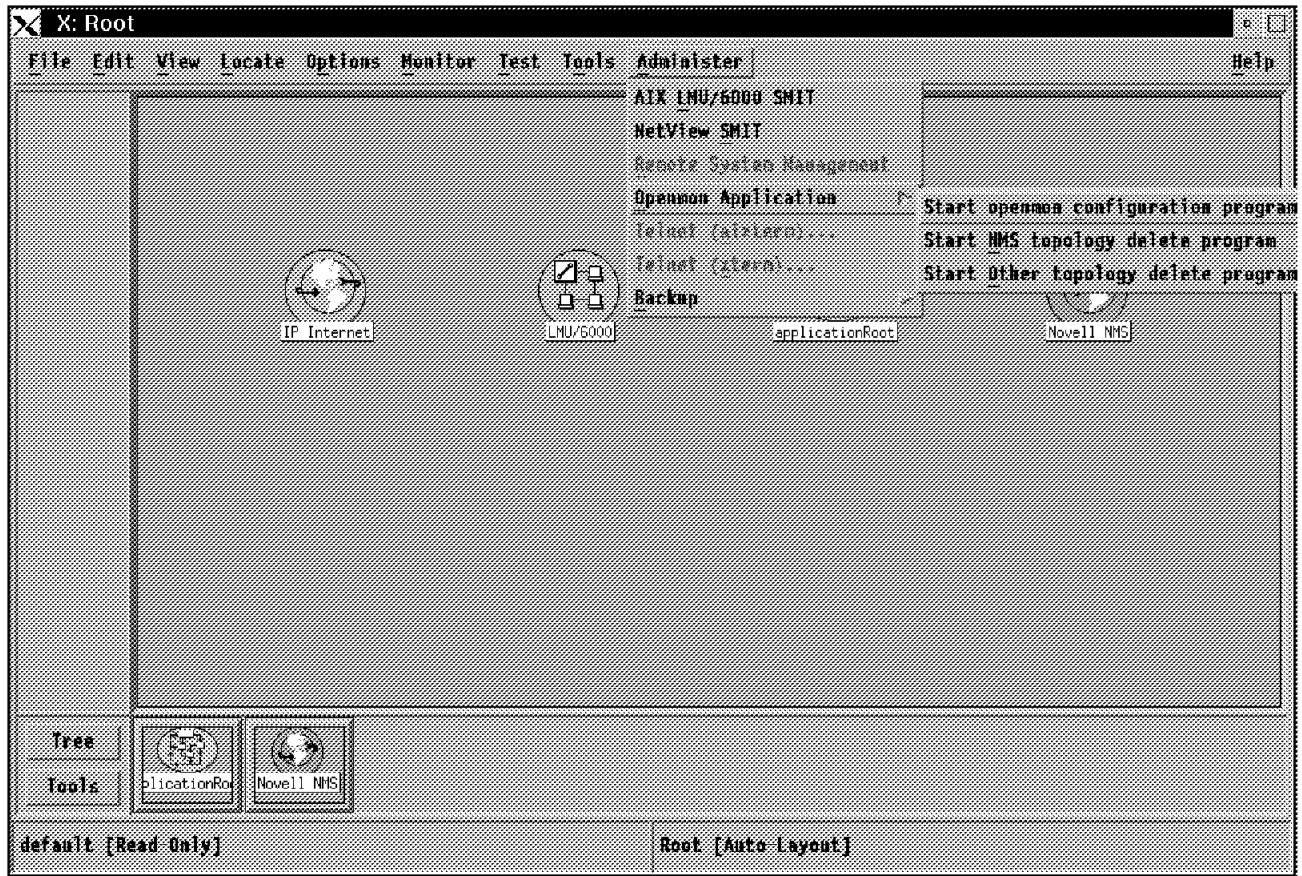
Figure 141. Start NMS Topology Delete Program

      3. Use the right mouse button to click on the **Novell NMS** object in the Root map.

      4. Choose **Edit..Delete..Object** from this submap.
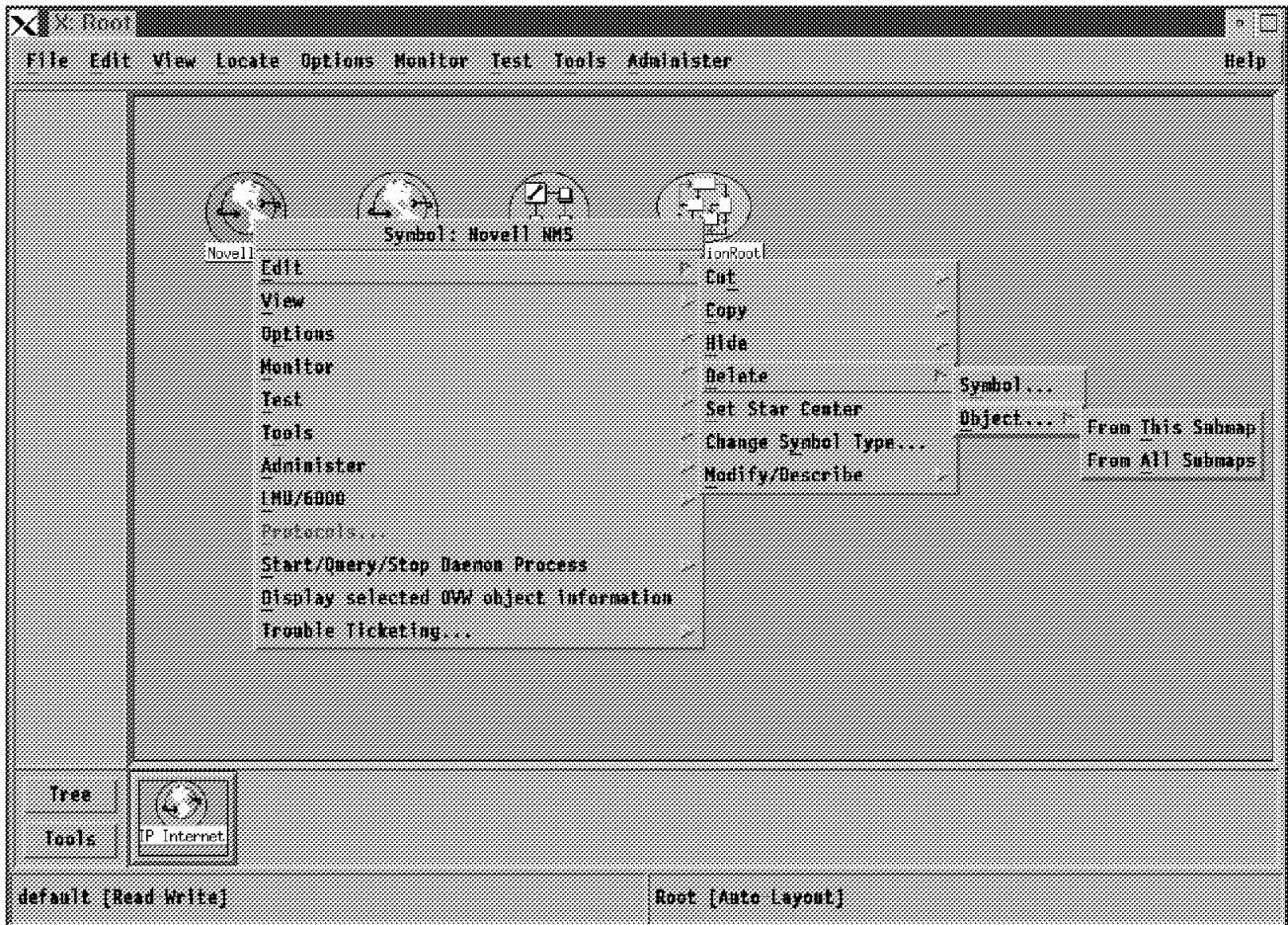
Figure 142. Deleting Novell NMS Topology

Note

The Novell NMS Topology information is stored in both the GTM and OVW database. The NetView for AIX delete function will only delete the objects from the OVW database and not the GTM database. If the Openmon topology program is running, it will ensure the object is deleted from the GTM database as well as the OVW database. This is why you start the Openmon topology delete program before using the NetView for AIX delete function (to keep the OVW and GTM databases synchronized).

To delete a segment and the objects below it, complete the following:

• Follow the same steps as above, but select the right mouse button on the object you want to delete rather than the *Novell NMS* object.

Chapter 6. Activating an LMU Client on a Remote Workstation

This chapter will describe a scenario that activates the LMU client on a remote IPX workstation that has been discovered through NetView for AIX's Openmon and the Novell NMS Export Services integration.

The products used are as follows:

- NetView for AIX V3.1 with Openmon PTF U438561 or V4.1
- Trouble Ticket for AIX V3R2
- LMU/6000 V1.1.2 or LMU for AIX V1.1.3
- LMU for OS/2 V1.1
- TCP/IP for OS/2 v2.0 or V3.0
- NetWare Requester for OS/2
- NetWare Server V3.12, V4.01 and V4.1
- NMS V2.0c and NMS Export Services V1.0

At the time of this project, the integration of NMS discovered IPX topology into NetView for AIX was limited. Only the topology information was available; no events were driven, and no status update information was available.

In this scenario, topics that will be covered include:

- Event configuration in NetView for AIX
- Automatic execution of shell scripts
- Incident filtering in Trouble Ticket for AIX
- Notification methods in Trouble Ticket for AIX

The following steps are shown in this scenario:

1. When Openmon discovers a new IPX resource and adds it to the GTM database, an event is generated.
2. Upon receipt of this event, a trouble ticket is created.
3. A shell script is driven which:
    - FTP's LMU startup.cmd from LMU managing station to AIX
    - FTP's LMU startup.cmd from AIX to discovered IPX station
    - Using the TCP/IP REXEC daemon, issues a remote LMU command, SHUTDOWN /b , to reboot the workstation
    - Sends an SNMP trap to NetView for AIX to inform it that the LMU client code has been activated on the remote IPX station

Figure 143 on page 176 illustrates the environment for our scenario.
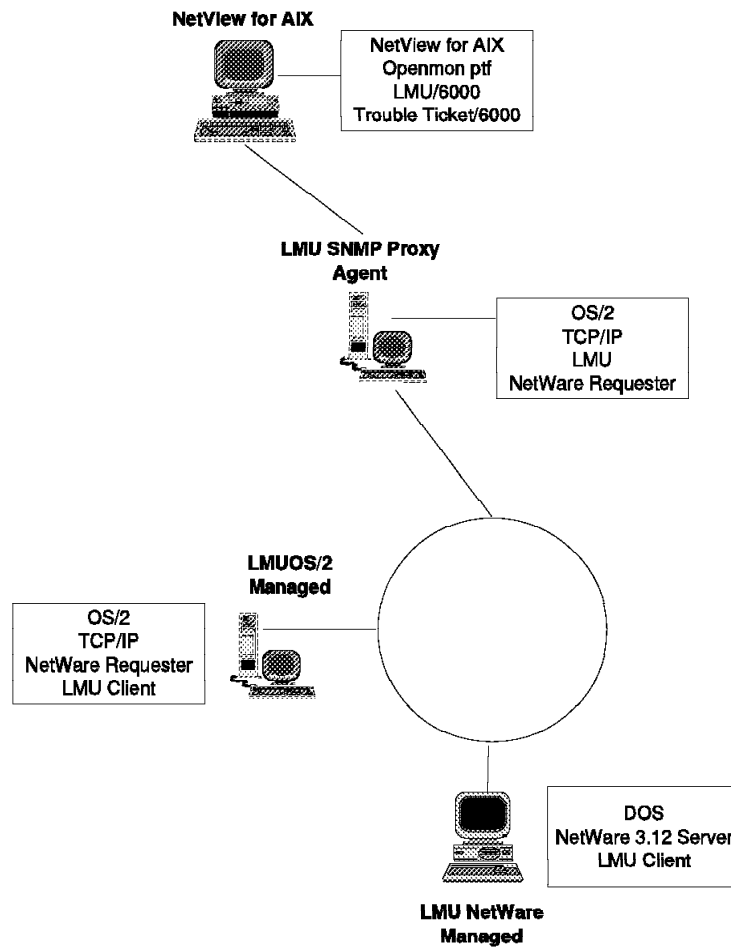
Figure 143. Environment for Scenario 1

In Figure 144 on page 177 we illustrate the steps necessary to complete our scenario.
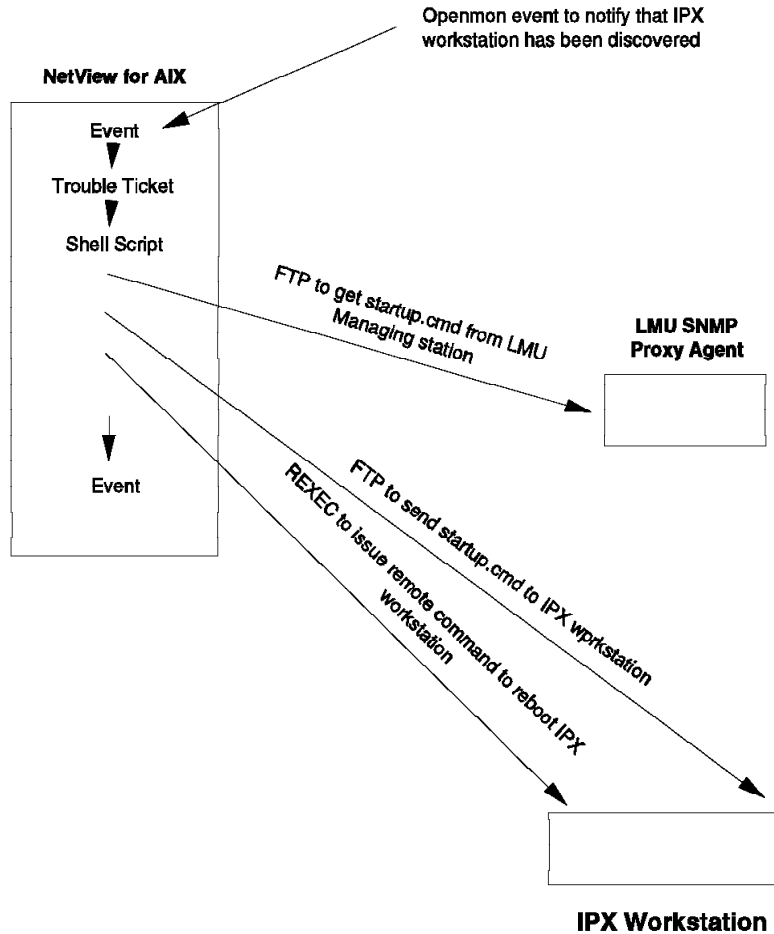
Figure 144. Flow of Events for Scenario 1

6.1 Openmon Event

We need an event that will start off our scenario. While Openmon does not generate an event when a node is added, a function like that would be good to have, especially when a resource is added to the GTM database. In NetView for AIX V3.1 we had to simulate this.

To simulate this event, we used the snmptrap command to send a trap to NetView for AIX. We created our own dummy enterprise and trap. Our enterprise name was Openmon and our enterprise ID was 1.3.6.1.2.3. We also created trap number 123456, specific to this new enterprise.
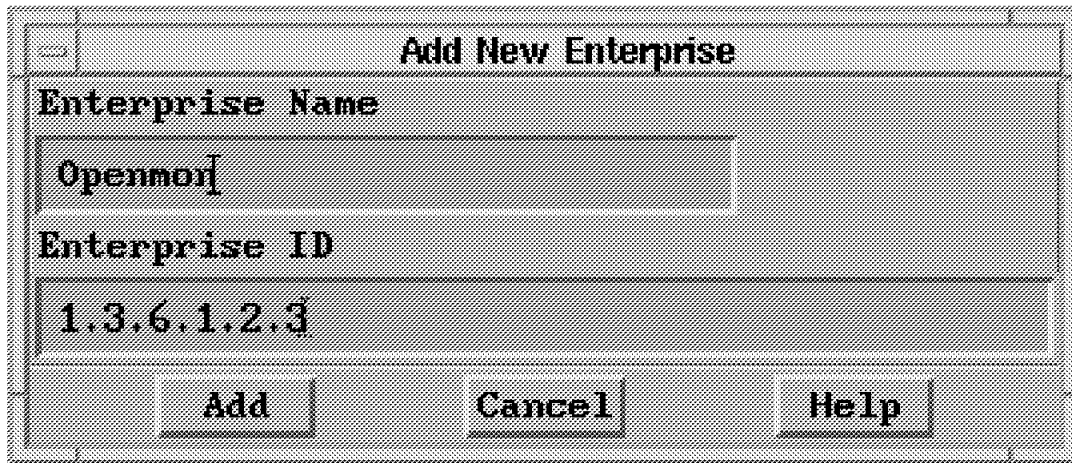
Figure 145. Adding a New Enterprise

To add an enterprise, you have to use the Options pull-down menu, and select
Event Configuration, then **Trap Customization** to get a window similar to
Figure 146. If you click on **Add**, you will get a window similar to Figure 145.
Enter your new enterprise name and enterprise ID, and select **Add**.

Figure 146. Event Configuration

Figure 147. Event Configuration

In order to configure the enterprise specific trap 123456, you can add a trap by clicking on **Add** in the event configuration window as shown in Figure 146 on page 178. This will cause Figure 147 to be displayed, and you can fill in the following information:

- Event Name
- Specific Trap Number
- Event Description
- Event Log Message
- Any optional commands

We wrote a shell script, *sendtrap*, to generate the Openmon event.

```
snmptrap rs60005 .1.3.6.1.2.3 nv2mgr2 6 123456 "" \
.1.3.6.1.2.3.1 octetstring "Openmon" \
.1.3.6.1.2.3.2 octetstring "9:400052005164" \
.1.3.6.1.2.3.3 octetstring "gtmd"
```

We also made up the variables we sent as octet strings with the trap. They are respectively:

- **Openmon** - The enterprise which sends the trap
- **9:400052005164** - The ipx address of the resource
- **gtmd** - The database to which the resource was added

Figure 148 shows the event generated by our script, snmptrap.
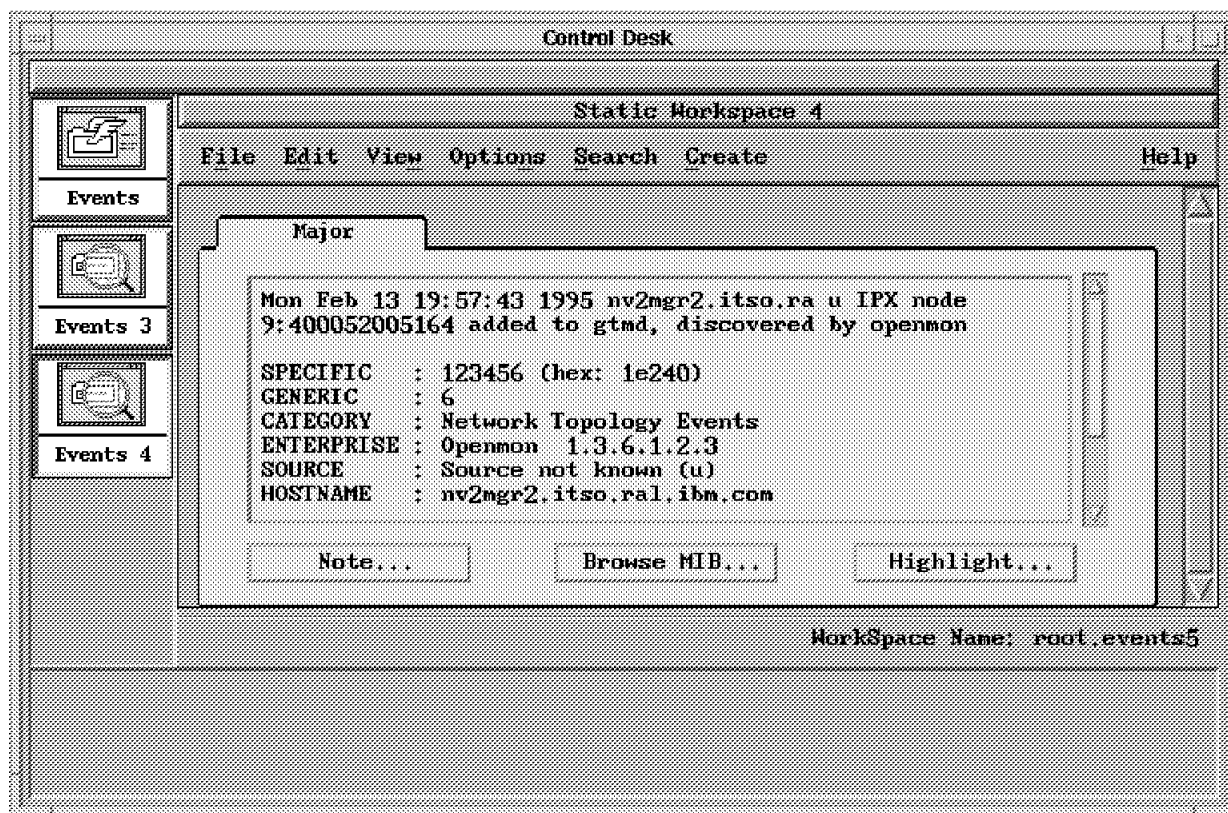
Figure 148. Event Card

6.2 Generating an Incident and a Trouble Ticket

Now that we have an event in NetView for AIX, we want to automatically create an incident and then a trouble ticket. For those not familiar with Trouble Ticket for AIX, two simple concepts that are helpful to know are:

- **Incidents**
  These are equivalent to the events you see in NetView for AIX. They are the symptoms of the problem.

- **Trouble Tickets**

These are the problem records which describe the problem. Many incidents
may be attached to a single problem.

To automatically generate an incident upon receipt of our event, we need to
configure an incident filter in Trouble Ticket for AIX.

From the Problem Management menu, choose **Administration**. Then choose
Incident Filter Rules and **Object New**. Figure 149 shows the detail of the filter
rule we defined. Since the default actions of Trouble Ticket for AIX are to not
generate an incident on events from NetView for AIX, we need to use the filter
rules to specify which events we would like to have an incident created for.

INCIDENT FILTER DETAIL

Object Help...

Incident Filter Detail

Enterprise Name ++	Object ID ++	Generic ++	Specific ++
Openmon	1.3.6.1.2.3	6	123456

Event Description

IPX node $2 added to $3, discovered by $1

Filter Name ++	Device IP Address
Report all events	

Filter Description

All occurrences will be reported. You can specify whether occurrences
should always be reported as separate problems or whether the system
should try to determine whether the occurrences are part of the same
problem

Filter Description

Report occurrences separately? YES

Close

Figure 149. Incident Filter Configuration

If you double-click on the **Enterprise Name** field in Figure 149, you can search for and select the **Openmon Enterprise ID**. In addition, you can select the correct enterprise specific trap that you wish to use in the filter. Most of the fields on this screen can be filled in by double-clicking on the field to get a list of choices. Be sure to change the field for *Report occurrences separately* in the Filter Description to Yes.

> ┌─ **Attention** ──
>
> When you load Incident Filter Rules after adding the new Enterprise and trap in NetView for AIX, you will find that Trouble Ticket for AIX does pick this up. That is, you will find the new enterprise and trap in the list of enterprises and traps. However, an error will be generated in the log, stdlog.0, in directory /usr/lpp/tt6000/log. The error is:
>
> ```
> ovev_nxd  31403  ERROR  ovfilter.c 1112 Unknown enterprise or trap
> ```
>
> The filter will not be activated, so no incident is generated. To get around this problem, stop and restart the NetView for AIX and Trouble Ticket for AIX.

Figure 150 and Figure 151 on page 183 show the incident generated by our filter rule. We can see that Trouble Ticket for AIX has reported the discovery of our IPX resource in the GTM database.
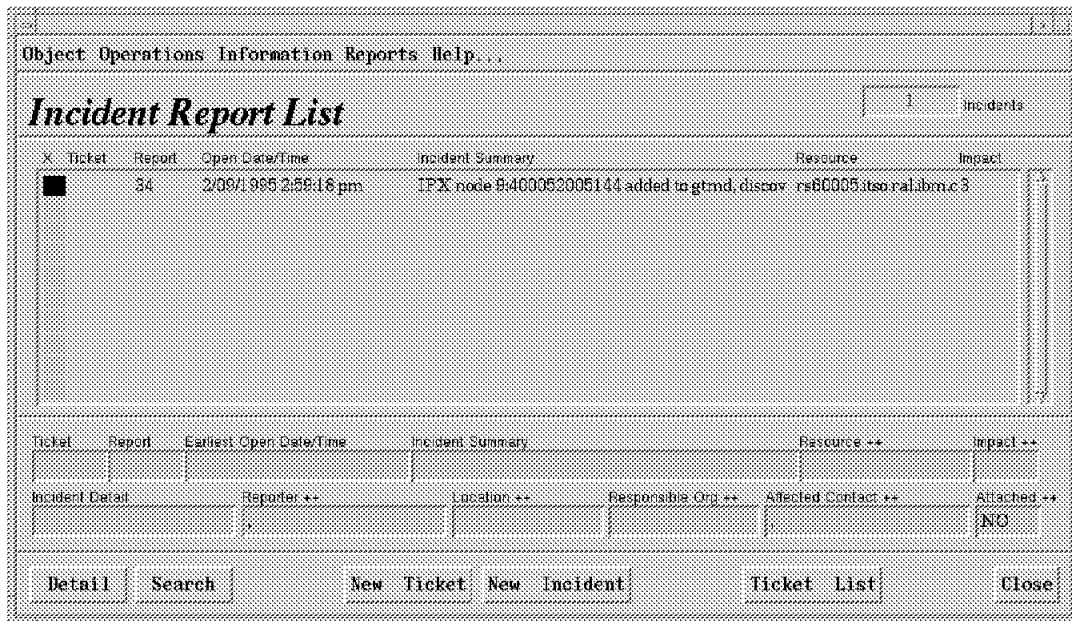
Figure 150. Incident List

Figure 151. Incident Detail

Now that we have the incident, we need to automatically generate a trouble ticket. A sample script, tt_script, is provided to do this. You can find this script in the /usr/lpp/tt6000/samples/ntf_meth directory. Using this sample involves setting up a new notification method to execute the script.

Here are the steps involved:

1. Copy the tt_script file to another directory.

   ```
   cp /usr/lpp/tt6000/samples/ntf_meth/tt_script /temp/scripts/tt_script
   ```

2. Make the copy an executable file.

```
cd /temp/scripts
chmod 777 tt_script
```

3. Create a new notification method called *CreateTicket*. In the Notification Script Name field, type the full path to the copied executable file. To create a new notification method:
   - From the Problem Management menu choose **Administration**.
   - Choose **Notification Setup**.
   - Choose **Notification Methods**.
   - Choose **Object** and **New**.

   Figure 152 shows the detail of the notification method we added.
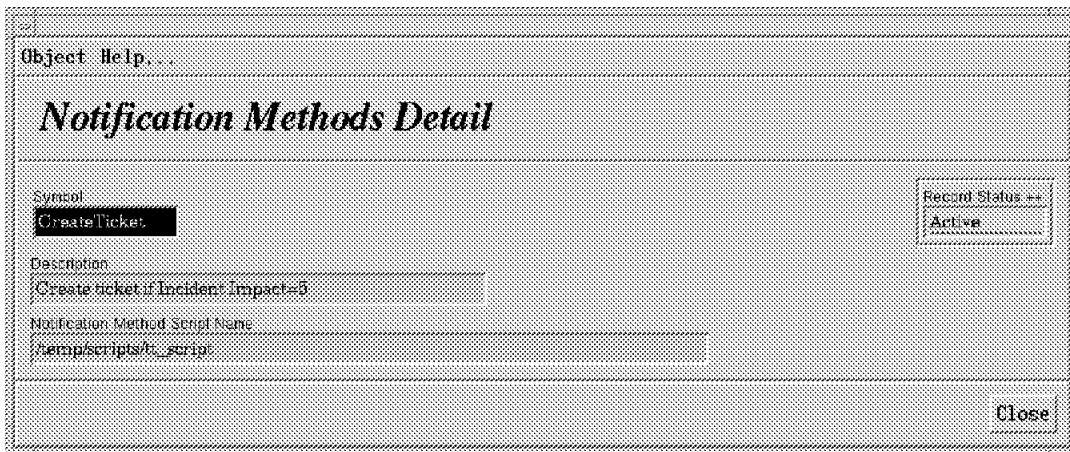
Figure 152. Adding a New Notification Method

4. Create a message template called *NewTicket*. Put the REF_ID variable in both the header and body of the message. To create this message template:
   - From the Problem Management menu choose **Administration**.
   - Choose **Notification Setup**.
   - Choose **Message Templates**.
5. Create a notification rule as follows:
   - From the Problem Management menu choose **Administration**.
   - Choose **Notification Setup**.
   - Choose **Notification Rules**.
   - Populate the fields as shown in Figure 153 on page 185.

Figure 153. Notification Rule Detail

After completing the notification rules detail, if an incident is created which has a *high* impact (that is IMPACT = 1), then the script tt_script will be executed and will create a trouble ticket. You can test this at any time by manually creating an incident which has IMPACT = 1.

Note

It will take a couple of minutes to create the trouble ticket.

To ensure that the incident, which was generated when our Openmon trap was received, had an impact of 1, we configured the event in NetView for AIX to have a severity of *Major*. This can be seen in the event detail in Figure 147 on page 179.

6.3 Shell Script Imuclient

We wrote a shell script, called Imuclient, which has the following three steps:

1. Executes a shell script called from_ftp
2. Executes a shell script called to_ftp
3. Sends a remote command to the IPX workstation to reboot the machine

lmuclient

```
set -x -v
# This script begins execution when a trouble ticket is opened which says
# that an IPX resource has been added to the GTM database by Openmon

# Get startup.cmd from the LMU SNMP Proxy agent
/temp/scripts/from_ftp
sleep 10

# Send startup.cmd to the new IPX station
/temp/scripts/to_ftp
sleep 10

# Send remote boot command to the new IPX station
rexec nv2mgr2 shutdown /b
```

Figure 154. lmuclient Shell Script

from_ftp

```
#!/bin/ksh

command="$root \n"
command="${command} verbose \n"
command="${command} cd d:/junk/lmu2 \n"
command="${command} lcd /temp/scripts \n"
command="${command} ascii \n"
command="${command} get startup.cmd \n"
command="${command} quit \n"

echo ${command} | ftp nvclient
```

Figure 155. from_ftp Shell Script

to_ftp

```
#!/bin/ksh

command="$root \n"
command="${command} verbose \n"
command="${command} cd c: \n"
command="${command} lcd /temp/scripts \n"
command="${command} ascii \n"
command="${command} put startup.cmd \n"
command="${command} quit \n"

echo ${command} | ftp nv2mgr2
```

Figure 156. to_ftp Shell Script

tt_script

```
#!/bin/sh

#
#  Script to collect information from an Incident Report and
#  Generate a New trouble ticket from that info.

set -x

PATH=$NX_ROOT/bin:$PATH; export PATH
IRNUM=$NX_NTF_SUMMARY

# NOTE the () around arch in case it does not exist
if [] "`(arch) 2>/dev/null`" = sun4 "
then
    AWK=nawk
else
    AWK=awk
fi
# Look up the incident report by number.  Extract the resource, impact start
# time description and notes fields.
# Convert the date from 24 hour format to 12 hour format...  Ugly.

 eval "`rgen -c -v -u -f  \"SELECT ir_alarm_nr_did, ir_impact, ir_start_dt,ir_desc,
 ir_notes, ir_tt_id  FROM Initial_Report WHERE
  #ir_num = $IRNUM\" 2> /dev/null | $AWK '{
    if (NF < 5) next
```

Figure 157. tt_script Shell Script Part 1 of 3

```
    # Escape newlines so that cmd_in will accept them.
    detail = $5
    gsub (\"\n\", \"\\\\\\\\\\n\", detail)

    print \"netres=\" $1
    print \"impact=\" $2
    print \"ir_sum=\" $4
    print \"ir_detl=\" detail
    print \"ir_ttid=\" $6
    match ($3, \" [0-9]*:\")
    if (RSTART)
       {
       hour = substr ($3, RSTART + 1, RLENGTH - 2) + 0
       if (hour >= 12)
           {
           ampm = \"p\"
           hour -= 12
           }
       else
           {
           ampm = \"a\"
           }
       if (hour == 0) hour = 12

       last_start = RSTART + RLENGTH - 1
       last_length = length ($3) - last_start
       newdate = substr ($3, 1, RSTART) hour substr ($3, last_start, last_length)
;\" \" ampm \"\\\"\"
       print \"ir_date=\" newdate \";\"
       }
    else
       {
       print \"ir_date=\" $3 \";\"
       }
    exit
}' FS=\"[,]\" RS= '"
```

Figure 158. tt_script Shell Script Part 2 of 3

```
# In order to enter this as a multi-line field later each new line
# has to be escaped, but there should not be a trailing new line at the end.
# so, Used to add backwhacks at the end of each line and then use expr to
# remove the last one.

# Forget it if the incident report is already attached to a ticket
[ "$ir_ttid" -gt 0 ] && exit


# At this point you can add any filtering you want to decide whether or not to
# proceed with the ticket generation.  The criteria available in this example
# are:

# netres - Name of the network resource
# impact - Impact level of of the incident
# ir_sum - text of summary field
# ir_detl - text of detail field

# For example - only create tickets for incident reports with resources
# [ "$netres" ] || exit 0

# or for example only create tickets if the word "AUTO" is in the summary:
# echo "$ir_sum" | grep "AUTO" >/dev/null || exit 0


# See if there is a network resource.  If there is, look it up and call it a
# hardware problem.  Otherwise guess that it is a network problem.

case "$netres" in
    "") tc=Networks ;;
    *)
      tc=Hardware
      nr_name=`rgen -c -u -f \
      "SELECT nr_prim_search_key FROM Network_Resource WHERE #id = $netres" 2> /dev/null`
      nr_name=`expr "$nr_name" : '"\(.*\)"'`
    ;;
esac
case "$impact" in
    "") im=None ;;
    *)
      im=`rgen -c -u -f \
          "SELECT sym  FROM Impact WHERE #enum = $impact" 2> /dev/null`
      im_name=`expr "$im" : '"\(.*\)"'`
    ;;
esac
```

Figure 159. tt_script Shell Script Part 3 of 3

```
# Now Generate a trouble ticket from the above IR fields (w/out NetRes Yet)

#
# If you want to assign these generated tickets to a
# particular person, and/or if assignee is required by your
# system defaults setting, add the following line to this echo statement
#     Assignee= \"Lname, Fname, MI\"
# where the stuff between the escaped quotes is the valid contact name of the
# assignee.
# You may want to do the same for organization
#     Organization=\"OrgName\"
# The TroubleCode that you use must be a valid trouble code
#
output=`echo "Ticket_Submission
{
  TroubleCode= \"$tc\"
  StartDate=\"$ir_date\"
  Priority=\"$im_name\"
  Description=\"$ir_sum\"
  Detail=\"$ir_detl\"
}" | cmd_in 2>/dev/null`

ticket=`expr "$output" : '.*Trouble Ticket \(.*\)'`
ticket_id=`echo $ticket | $AWK ' { print $1}'`

[ "$ticket_id" ] || exit 0

echo "Incident_Report_Submission
{
IrNum = $IRNUM
Ticket = $ticket_id
}" | cmd_in

# If there is a network resource from the incident report create an action
# for the ticket showing the resource on the action.

[ "$nr_name" ] || exit 0

echo "Action_Submission
{
ActionNum = \"1\"
Ticket = $ticket_id
Resource = "$nr_name"
Action=\"$ir_sum\"
}" | cmd_in >/dev/null 2>&1
```

Figure 160. tt_script Shell Script

Figure 161 on page 190 shows the trouble ticket which was created by script
tt_script.

Figure 161. Trouble Ticket Detail

Notice the Ticket Summary field.

6.4 Generating an Incident for LMU Client Activation

The final step was to generate an event which would notify the operator that the LMU client code had been activated on the newly discovered IPX workstation. We wrote another shell script, sendtrap1, to generate this event.

sendtrap1

```
snmptrap rs60005 .1.3.6.1.2.3 nv2mgr2 6 123457 "" \
.1.3.6.1.2.3.1 octetstring "openmon" \
.1.3.6.1.2.3.2 octetstring "9:400052005164" \
.1.3.6.1.2.3.3 octetstring "gtmd"
```

Figure 162. sendtrap1 Shell Script

Figure 163 shows the event that is generated in the event window when this script is executed.
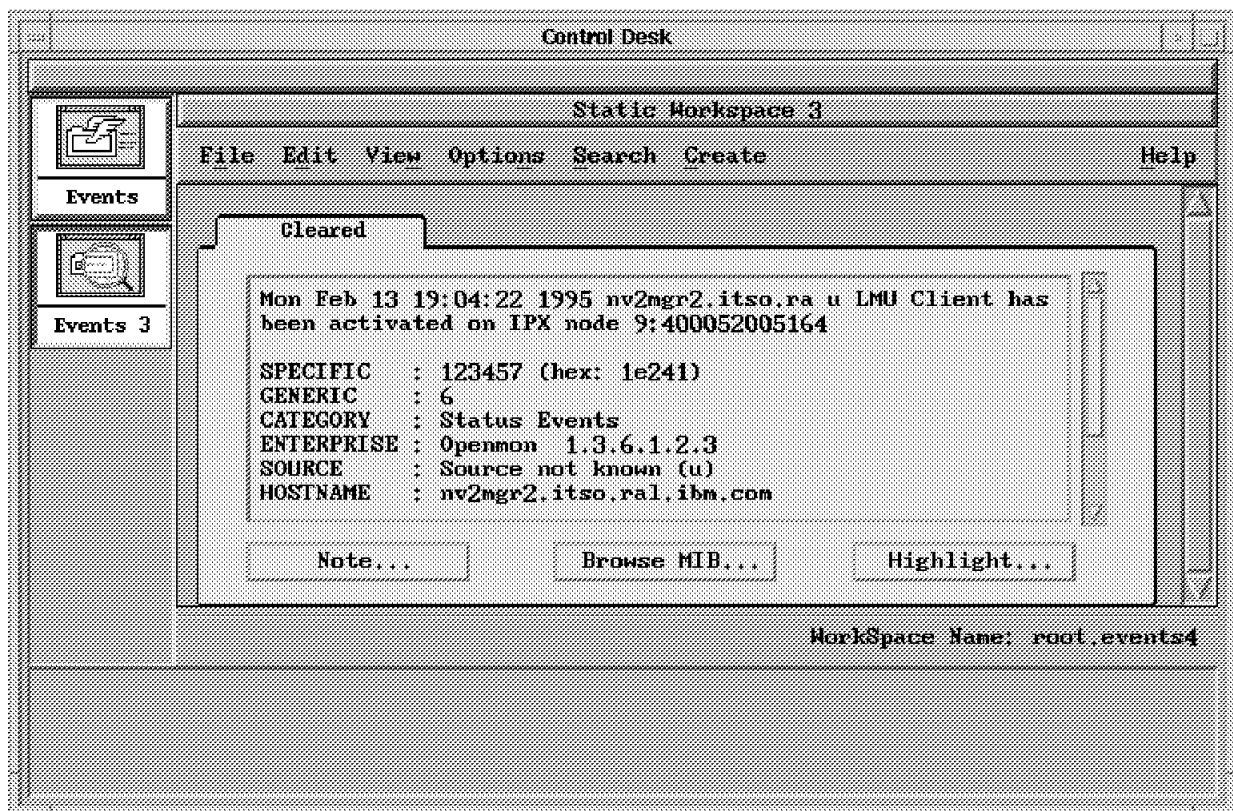
Figure 163. Event Card

We then edited our lmuclient script to include the execution of snmptrap1.

lmuclient

```
set -x -v
# This script begins execution when a trouble ticket is opened which says
# that an IPX resource has been added to the GTM database by Openmon

# Get startup.cmd from the LMU SNMP Proxy agent
/temp/scripts/from_ftp
sleep 10

# Send startup.cmd to the new IPX station
/temp/scripts/to_ftp
sleep 10

# Send remote boot command to the new IPX station
rexec nv2mgr2 shutdown /b

# Wait 7 minutes, a conservative guesstimate at how long it took to
# reboot our OS/2 workstation
sleep 420

# Execute shell script, snmptrap1, which sends an event to say that LMU
# client has been activated on the IPX workstation
/temp/scripts/sendtrap1
```

Figure 164. Modified lmuclient

6.4.1 Openmon Events in NetView for AIX V4.1

In NetView for AIX V4.1 there is a new daemon, called *nvotd*, that receives non-IP topology events and forwards them to the events display application, nvevents.

```
nvotd

Purpose
Receives non-IP topology events and forwards them to the Events
Display application (nvevents)

Description
If API calls are used to send information to the gtmd daemon, the
API establishes a socket connection between the non-IP discovery
application and the gtmd daemon, no traps are used, and the
Events Display application does not receive events sent to the
gtmd daemon.  The nvotd daemon can be used to receive
notification of the following non-IP topology events from the
gtmd daemon and forward them to the the Events Display
application:
Event Type                     Trap Number
Vertex creation                70000030
Vertex deletion                70000031
Vertex status change           70000032
Graph or box creation          70000033
Graph or box deletion          70000034
Arc creation                   70000035
Arc deletion                   70000036
Arc status change              70000037

See the NetView for AIX Administrator's Guide for more
information about NetView for AIX internal traps.

By default, the nvotd daemon is not started when the NetView for
AIX program is started.  You can configure the nvotd daemon
through SMIT indicating that it should be started by the nv6000
command.  In addition, users or an application can add the nvotd
daemon to the startup file without using SMIT, for example, by
using the ovaddobj command.
```
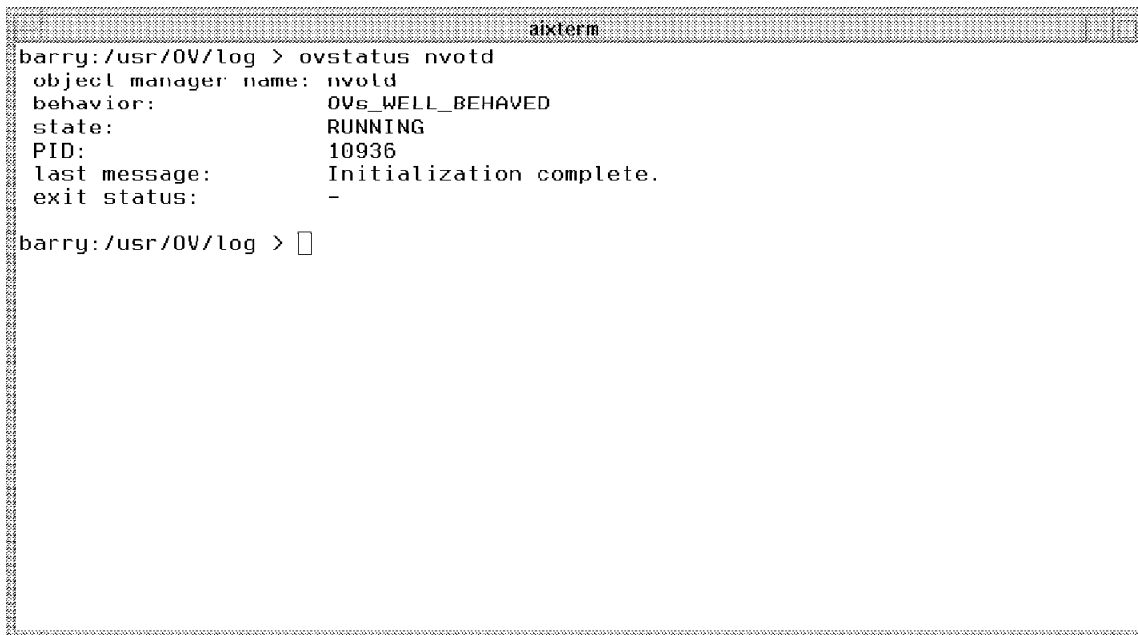
Figure 165. Help for nvotd Daemon


```
                                   aixterm
barry:/usr/OV/log > ovstatus nvotd
 object manager name: nvotd
 behavior:           OVs_WELL_BEHAVED
 state:              RUNNING
 PID:                10936
 last message:       Initialization complete.
 exit status:        -

barry:/usr/OV/log > ☐
```

Figure 166. New Daemon in NetView for AIX V4.1

When we start the Openmon discovery, gtm and nvevents get updated with the
new topology as shown in Figure 167 on page 194.
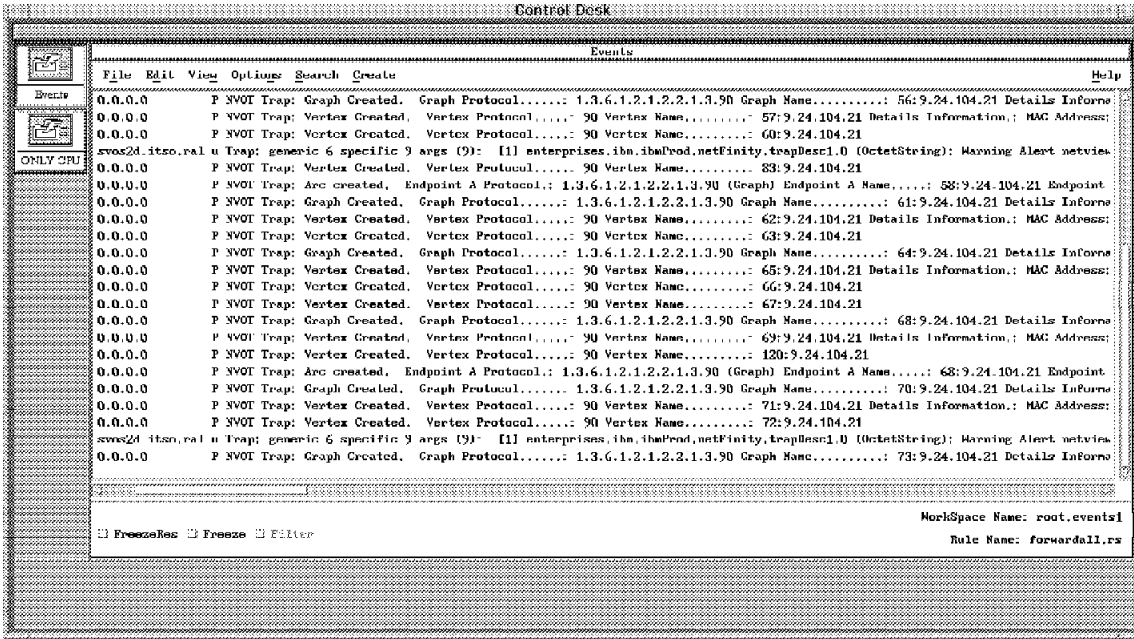
Figure 167. List Format for New Traps
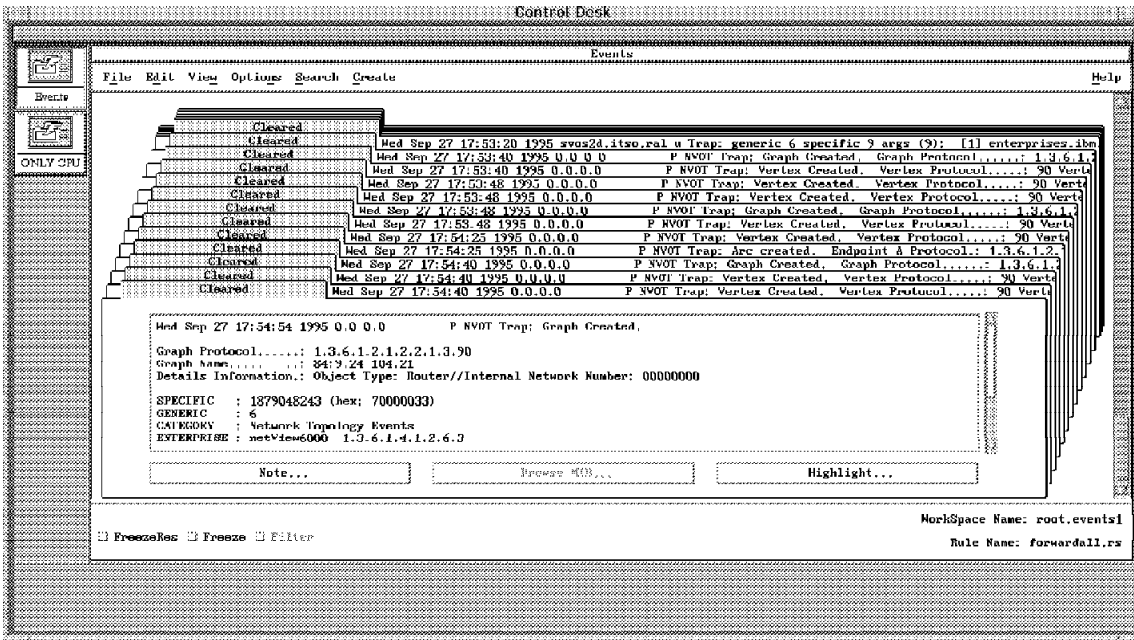
Figure 168. Card Format for New Traps for gtm

Chapter 7. Automated Response to an NMA Alarm/Trap

This chapter will describe a scenario that responds automatically to an alarm/trap received from NMA.

Products used:

- NetView for AIX V3.1 with Openmon PTF U438561
- Trouble Ticket for AIX V3R2
- LMU/6000 V1.1.2
- NMA V1.5 and V1.6
- NMS V2.0c
- LMU for OS/2 V1.1
- NetWare Requester for OS/2
- NetWare Server V3.12 and V4.01

In this scenario, topics that will be covered include the following:

- Event Configuration in NetView for AIX
- Automatic execution of shell scripts
- Incident filtering in Trouble Ticket for AIX
- Notification methods in Trouble Ticket for AIX

The following steps are shown in this scenario:

1. NMA forwards an alarm/trap to NetView for AIX.
2. An event is configured for this specific trap.
3. Upon receipt of the event a trouble ticket is generated.
4. A shell script is driven sending a remote command to the NetWare server where the trap originated from. LMU for AIX and LMU for OS/2 are used to send this command.

Figure 169 on page 196 illustrates the environment for our scenario.

NMS Console
DOS/Windows Workstation
Requester NetWare
TCP/IP

NMS_AIX
NetWare v4.01 server
NMA
LMU Managed
TCP/IP

nvclient
OS/2 Workstation
NetWare Requester
LMU Manager
TCP/IP

RS600011
AIX 3.2.5
NetView for AIX v3
LMU 6000
TT 6000
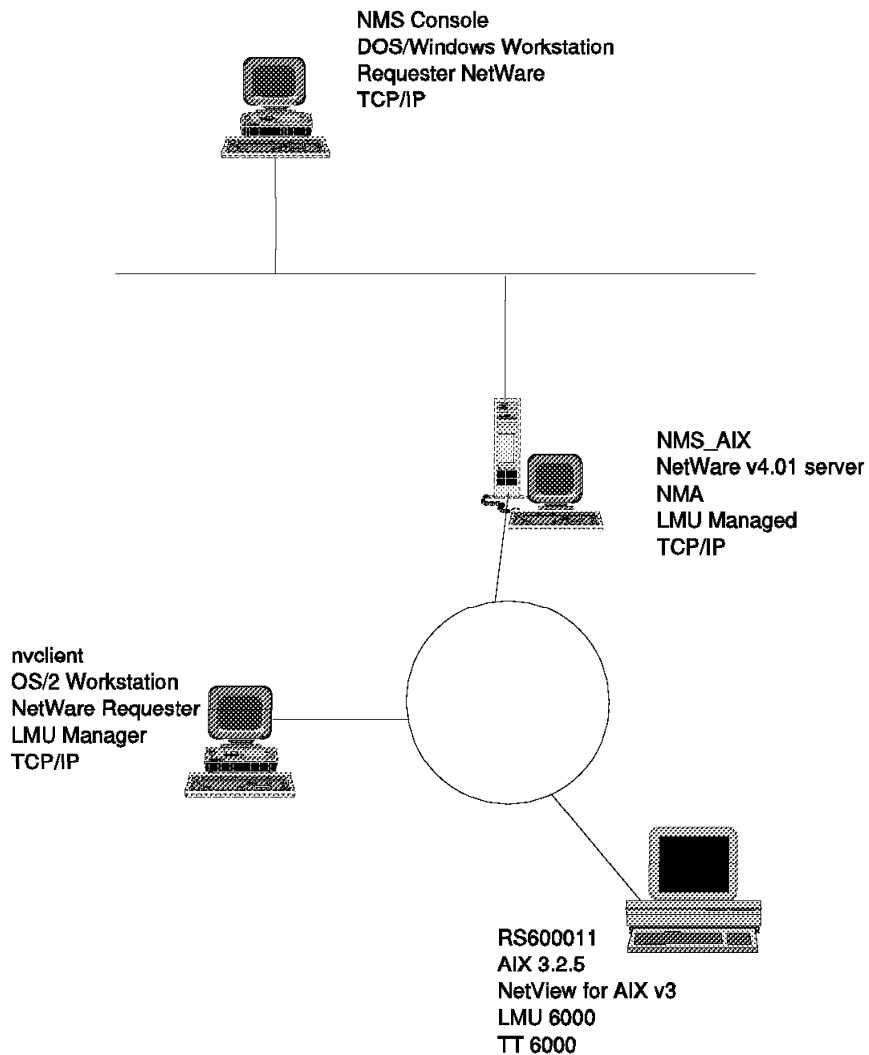
Figure 169. Environment for Scenario 2

7.1 Retrieve the NMA Traps

We needed to know exactly what traps can be sent by NMA servers and how those traps are interpreted. All the NMA traps are documented in the NWALARM MIB file. While this is good for the interpretation and display of the traps and alarms on the NMS console, there is still more work to be done to effectively use them on NetView for AIX. To find out more information about the traps, you will need to look into the NWALARM.MIB. To find out how to set this up, consult the following:

1. On the NMS Console, select the **Fault > Alarm Disposition** option in the menu bar.
2. Select the **SNMP Alarm Family**.

3. List all the traps and select the trap you want; in our scenario we selected the **System: NLM unloaded**.
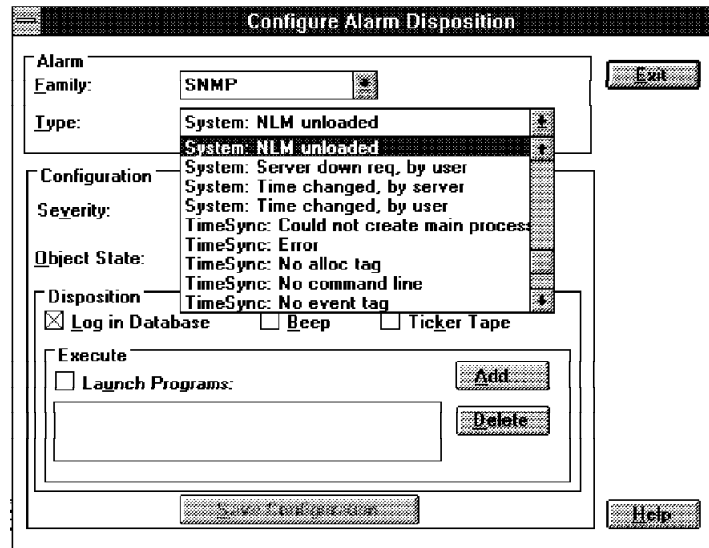
Figure 170. NMS Alarm Disposition Trap Selection

4. Edit the NWALARM MIB and find the trap number corresponding to the alarm that you want.

```
moduleLoad          TRAP-TYPE
                        ENTERPRISE      nwalarm-mib
                        VARIABLES       {
                                        serverName,trapTime,nlmName
                                        }
                        DESCRIPTION
                                "An NLM has been loaded."
                        --#TYPE "System: NLM loaded"
                        --#SUMMARY "%s NLM loaded on server %s."
                    --#ARGUMENTS {2,0}
                        --#SEVERITY MINOR
                        --#TIMEINDEX 1
                        --#HELP "nwalarm.hlp"
                        --#HELPTAG 225
                --#STATE OPERATIONAL

                    ::= 225
```

Figure 171. NWALARM MIB

```
moduleUnLoad        TRAP-TYPE
                    ENTERPRISE      nwalarm-mib
                    VARIABLES       {
                            serverName,trapTime,nlmName
                            }
                    DESCRIPTION
                        "An NLM has been unloaded."
                    --#TYPE "System: NLM unloaded"
                    --#SUMMARY "%s NLM unloaded on server %s."
                    --#ARGUMENTS {2,0}
                    --#SEVERITY MINOR
                    --#TIMEINDEX 1
                    --#HELP "nwalarm.hlp"
                    --#HELPTAG 226
                    --#STATE OPERATIONAL

                ::= 226
```

Figure 172. NLM Unloaded Trap

7.2 Configuring the NMA Traps to Flow to NetView for AIX

Figure 173 shows the logical flow for this piece of the scenario.
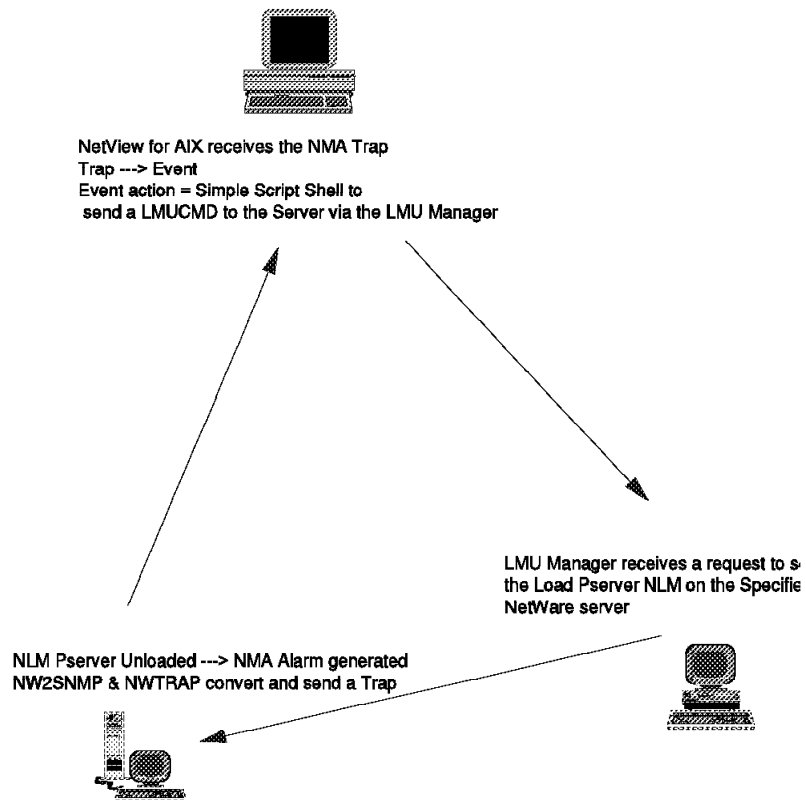
Figure 173. Scenario Action Description

To forward the NMA traps to NetView for AIX, we had to copy the
\NMS\SNMPMIBS\ALLMIBS\nwalarm.mib file into the /usr/OV/snmp_mibs directory
on the RS600011 AIX machine. In the NetView for AIX application, we selected
the **Options > Load/Unload MIBs: SNMP...** and then **Load** to load and compile
the new NWALARM MIB we had copied into the directory. Figure 174 shows how
to load the MIB.
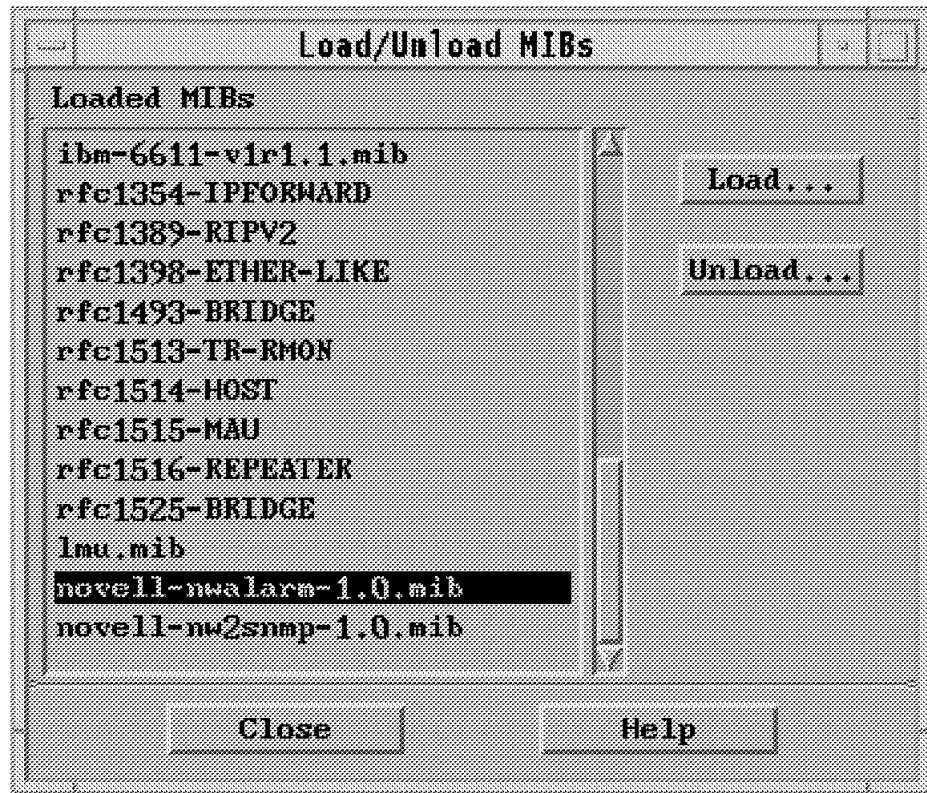
Figure 174. NetView for AIX NWALARM MIB Loaded

If that was all you were to do, you would receive all the NMA traps from all of the
NetWare NMA servers you have. The only problem is they are *not* automatically
formatted.

To format the event (and the event card) to display the information that we think is
important, as well as to execute a command when the event occurs, we did the
following:

- From any NetView for AIX menu bar, select the **Options > Event
  Configuration > Trap Customization: SNMP...** options.
- Find the *Excelan* Enterprise Name or the 1.3.6.1.4.1.23 Enterprise Identification
  which is the default Novell Enterprise Id. It is possible that you have already
  renamed the enterprise ID name, but the value (1.3.6.1.4.1.23) will remain
  constant.
- Click on the **Add** button in the second part of the screen to add a new event,
  and configure it as shown in Figure 175 on page 200.

Figure 175. NetView for AIX Add Event Identification

1. We entered an event name, `System:NLM_Unloaded`, corresponding to a brief description of the event.

2. We entered the Specific Trap Number 226, which was the trap we wanted to configure.

3. We entered a brief description of the event.

4. We specified the new Event Category as NetWare Events.

5. We set the Severity of the event as Minor.

6. We entered the format of the message we wanted to display in the event card, in the Event Log Message field: `NLM $3 Unloaded from $1 NetWare server`.

7. We entered the command, which was a simple shell script we wrote, to be executed upon receipt of the trap, /tmp/sendcmd $1 $3.

- Click on the **OK** button and quit the Event Configuration menu.
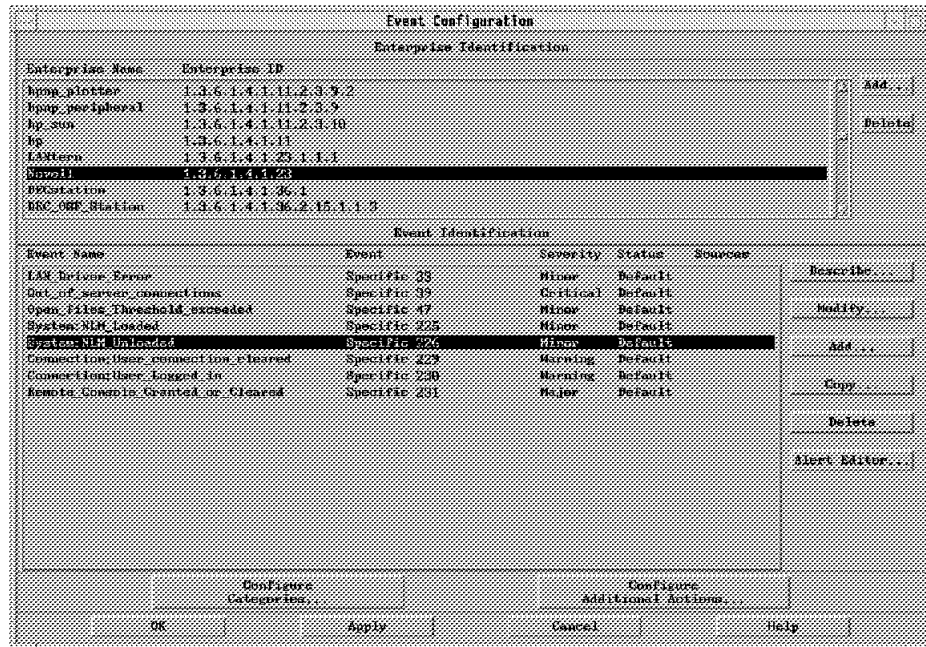
Figure 176. NetView for AIX Event Configuration

7.3 The LMU Send Command Function

The automatic action we decided to execute was to reload the NLM which had been unloaded, but only if it was the PSERVER.NLM. This is the Print Server NLM which is critical for most users.

We wrote a simple shell script which involved the lmucmd command.

From LMU for AIX, we sent a request to the LMU OS/2 manager to re-load the PSERVER NLM on the specified NetWare server.

Our LMU Environment was as follows:
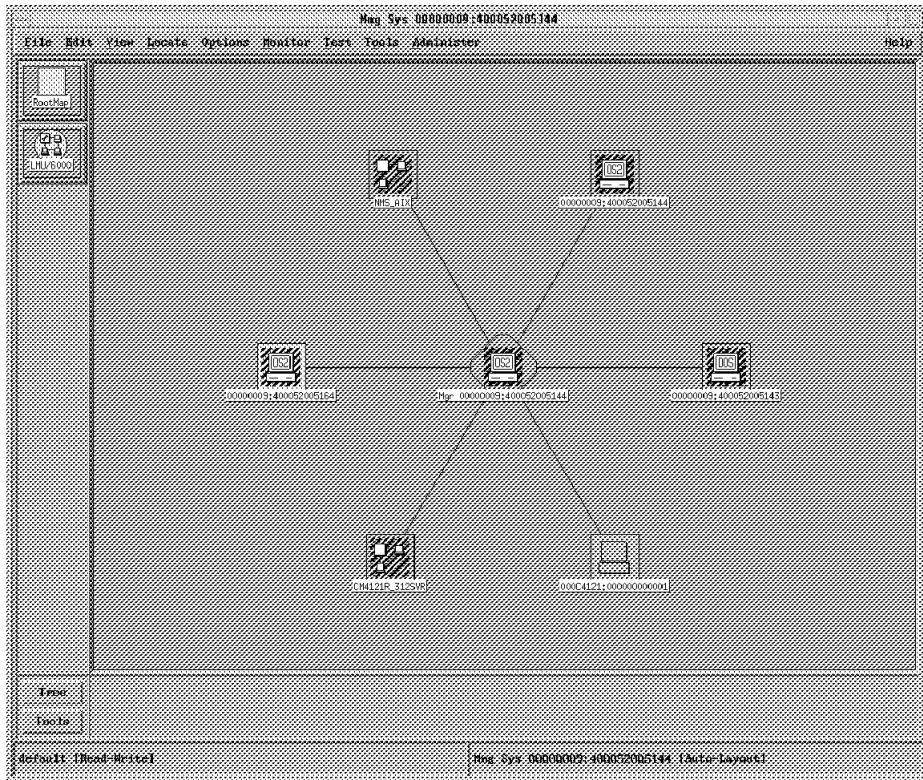
Figure 177. LMU for AIX Environment

The following is the shell script that we created:

```ksh
#!/bin/ksh

server=$1
nlm=$2" "$3" "$4" "$5

pserver="NetWare 386 Print Server"

if [[ $nlm = $pserver ]]
 then
   /usr/OV/bin/lmucmd -S nvclient -U nvclient
   -W cm4121r 00000009:400052005144 -Q lmucmd $server. load pserver
fi
```

Figure 178. Load NLM Pserver

The Event Configuration Field where we specified the shell script execution is seen in Figure 179 on page 203.

Add Event

Event Name

System:NLM Unloaded

Generic Trap   Specific Trap Number

    Enterprise Specific   226

Event Description

System Information:
NLM $3 unloaded on $1 NetWare server

Event Sources (all sources if list is empty)

                                                    Add From Map

                                                       Delete

                                                      Delete All

Source

Event Category   Status   Severity

    NetWare Events   Default Status   Minor

Event Log Message

NLM $3 Unloaded on $1 NetWare server

Popup Notification (Optional)

Command for Automatic Action (Optional)

/tmp/sendcmd $1 $3

        OK   Reset   Cancel   Help

Figure 179. NetView for AIX Event Configuration

When we unloaded the NLM from the NetWare server, the NMA trap 226 flowed to NetView for AIX.

The formatted event card we received in the Control Desk is as follows:
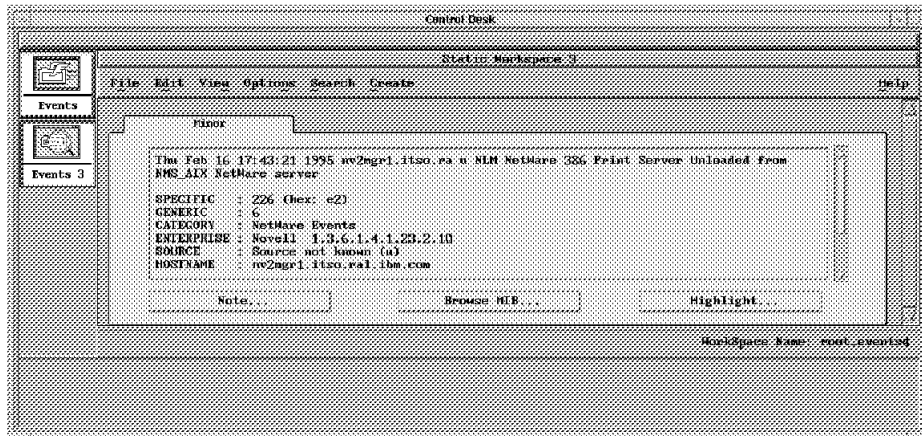
Figure 180. NetView for AIX Control Desk Event Received from NMA

The result which was in the /usr/OV/log/ovactiond.log file is as follows:
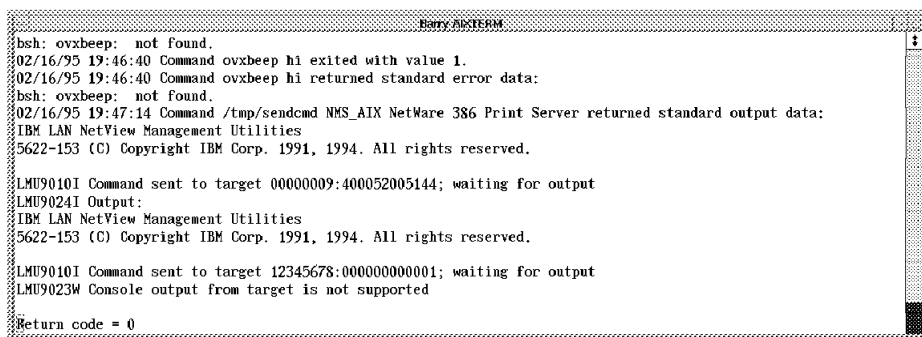
Figure 181. AIX /usr/OV/log/ovactiond.log

The result on the NetWare server was that the PSERVER.NLM is always loaded.

7.4 Generating an Incident and a Trouble Ticket

Now that we have an event in NetView for AIX, we want to automatically create an incident and then a trouble ticket. For those not familiar with Trouble Ticket for AIX, two important concepts are:

- **Incidents**
  These are equivalent to the events you see in NetView for AIX. They are the symptoms of the problem.

- **Trouble Tickets**
  These are the problem records which describe the problem. Many incidents may be attached to a single problem.

To automatically generate an incident upon receipt of our event, we need to configure an incident filter in Trouble Ticket for AIX.
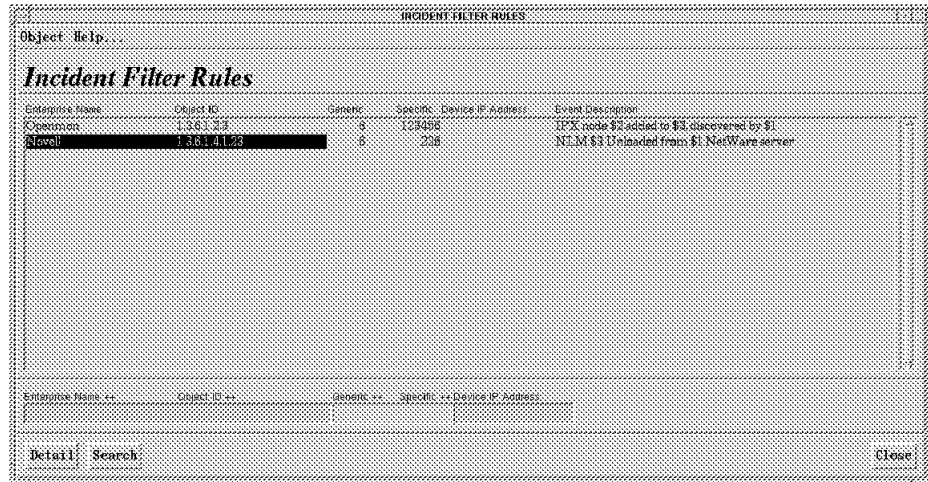
Figure 182. Trouble Ticket for AIX

From the Problem Management menu choose **Administration**. Then choose **Incident Filter Rules**. Then choose **Object** and **New**. Figure 149 on page 181 shows the details of the filter rule we defined.
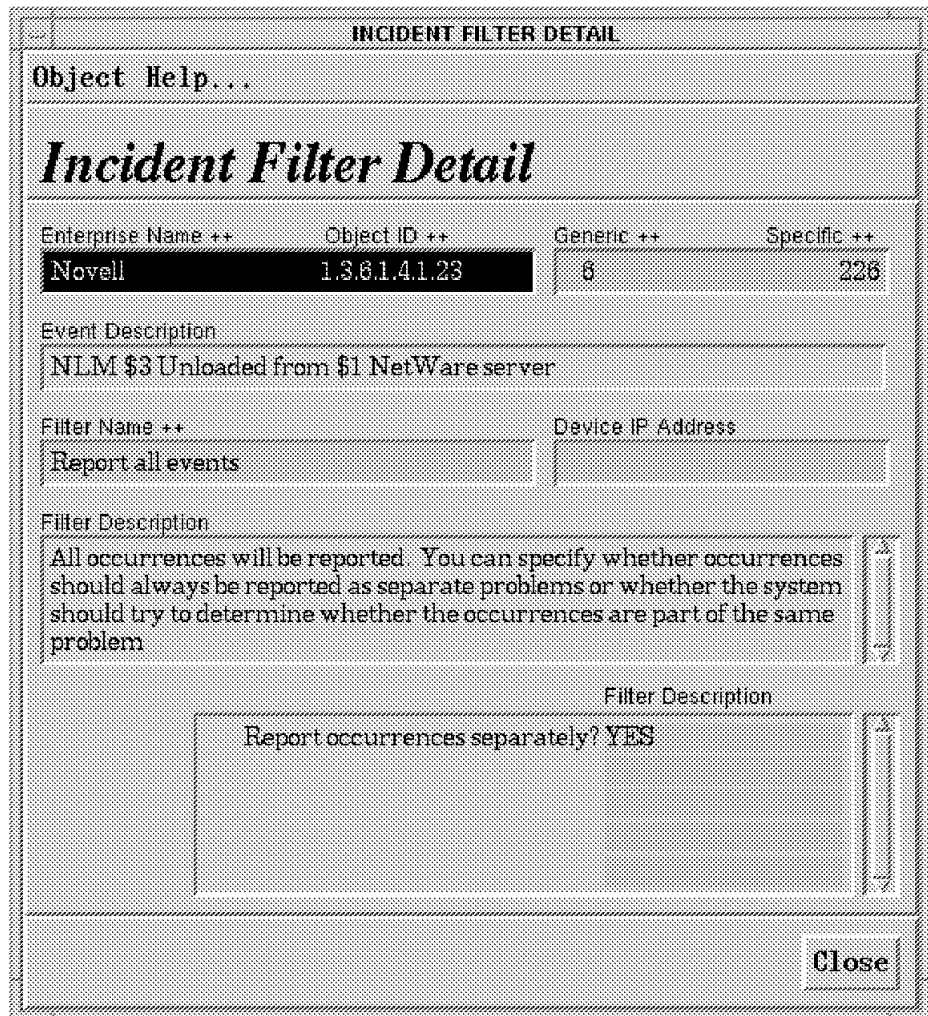
Figure 183. Incident Filter Configuration

Figure 150 on page 182 and Figure 151 on page 183 show the incident generated by our filter rule.

Figure 184. Incident List

Figure 185. Incident Detail

Now that we have the incident, we need to automatically generate a trouble ticket. A sample script, tt_script, is provided to do this. You can find this script in the /usr/lpp/tt6000/samples/ntf_meth directory. Using this sample involves setting up a new notification method for executing the script.

The steps we followed were as follows:

1. Copy the tt_script file to another directory.

   `cp /usr/lpp/tt6000/samples/ntf_meth/tt_script /temp/scripts/tt_script`

2. Make the copy an executable file.

   ```
   cd /temp/scripts
   chmod 777 tt_script
   ```

3. Create a new notification method called `CreateTicket`. In the Notification Script Name field, type the full path to the copied executable file. To create a new notification method complete the following:
   - From the Problem Management menu choose **Administration**.
   - Choose **Notification Setup**.
   - Choose **Notification Methods**.
   - Choose **Object** and **New**.

   Figure 186 shows the notification method we added.
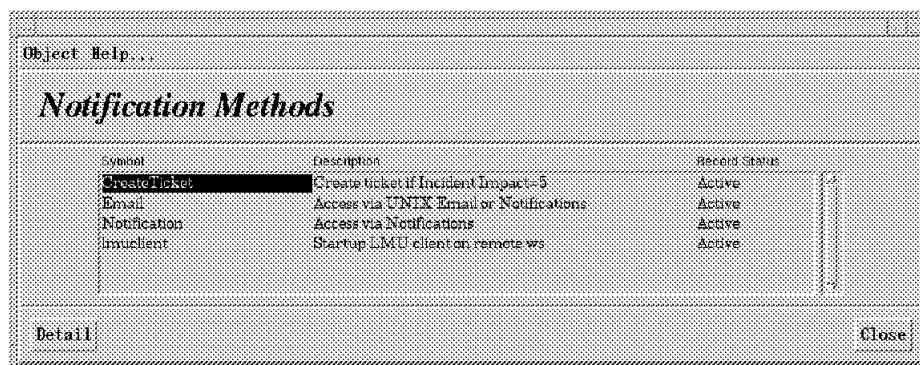
Figure 186. Notification Method

4. Create a message template called NewTicket. Put the REF_ID variable in both the header and body of the message. Create this message template as follows:
   - From the Problem Management menu choose **Administration**.
   - Choose **Notification Setup**.
   - Choose **Message Templates**.
5. Create a notification rule as follows:
   - From the Problem Management menu choose **Administration**.
   - Choose **Notification Setup**.
   - Choose **Notification Rules**.
   - Populate the fields as shown in Figure 187 on page 208:

Figure 187. Notification Rule List

After completing the above, if an incident is created which has a high impact (that is IMPACT = 1), then the script tt_script will be executed and will create a trouble ticket. You can test this now by manually creating an incident which has an IMPACT value of 1.

Note

It will take a couple of minutes to create the trouble ticket.

To ensure that the incident is generated, when our NMA trap is received, with an IMPACT = 1, we configured the event in NetView for AIX to have a severity of Major. This can be seen in the event detail in Figure 175 on page 200.

Note

The action we wanted to set was to close the ticket when the PSERVER.NLM is reloaded. This couldn't be tested, but when the NLM is loaded, a new trap is generated with the 225 number for NLM Loaded. Then it automatically could be created to close the ticket previously opened.

Chapter 8. Using LMU for AIX to Help Manage NetWare Servers and Clients

This chapter will describe how to manage NetWare resources from NetView for AIX. We look specifically at the following:

- Sending a trap from NetWare V4.1 Server to NetView for AIX
- Configuring an event on NetView for AIX to act upon that trap
- Using lmucmd to send a command to a NetWare Server
- Using lmucmd to send a command to a NetWare DOS/Windows client
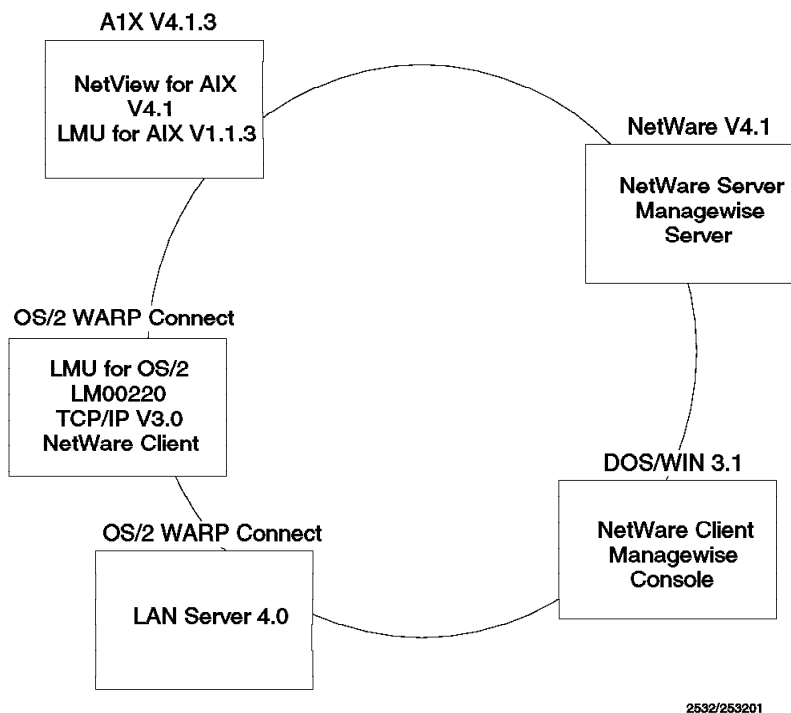
Figure 188. Environment for Scenario 2

8.1 Traps from NetWare to NetView for AIX

There are many conditions that will cause traps to flow from the NetWare Management Agent (NMA) to our SNMP manager (NetView for AIX).

For the first scenario, we have chosen a simple function to trap on to show how this flow works. One of the traps that comes with Managewise's (NMS and Intel LANDesk) NMA function is for when NLM are loaded or unloaded. This section will show the flow between the NetWare Server and NetView for AIX.

The default action in Managewises fault table is for all traps to be sent to the SNMP manager. Therefore, we will begin doing some customization at NetView for

AIX. We ran a script that did an addtrap for all the Managewise traps. An example of that would be as shown in Figure 189 on page 210.

```
addtrap -n nwalarm -l NWALARM_226 -i 1.3.6.1.4.1.23.2.10 -g 6 -s 226 -o A
-S 3 -t 0 -c "Error Events" -F '$3 NLM has been unloaded on server $1.'
```

Figure 189. Unload NLM Trap

When we look at the Event Configuration feature of NetView for AIX, we should find an enterprise specific trap that matches this, as shown in Figure 190.

Enterprise Identification   Read-Write

Enterprise Name	Enterprise ID
nw2snmp	1.3.6.1.4.1.23.2.8
nwalarm	1.3.6.1.4.1.23.2.10
DECstation	1.3.6.1.4.1.36.1
DEC_OSF_Station	1.3.6.1.4.1.36.2.15.1.1.3
DEC_VMS_Station	1.3.6.1.4.1.36.2.15.1.5.5
DEC_ULTRIX	1.3.6.1.4.1.36.2.15.1
DEC-OSF_Version_1	1.3.6.1.4.1.36.2.15.2.1
DEC-OSF_Version_2	1.3.6.1.4.1.36.2.15.2.2

Event Identification

Event Name	Event	Severity	Status	Sources
NWALARM_224	Specific 224	Minor	Default	
NWALARM_225	Specific 225	Minor	Default	
NWALARM_226	Specific 226	Minor	Default	
NWALARM_227	Specific 227	Minor	Default	
NWALARM_228	Specific 228	Minor	Default	
NWALARM_229	Specific 229	Minor	Default	
NWALARM_230	Specific 230	Minor	Default	
NWALARM_231	Specific 231	Minor	Default	
NWALARM_232	Specific 232	Minor	Default	
NWALARM_233	Specific 233	Minor	Default	
NWALARM_234	Specific 234	Minor	Default	
NWALARM_235	Specific 235	Minor	Default	
NWALARM_236	Specific 236	Minor	Default	
NWALARM_237	Specific 237	Minor	Default	
NWALARM_238	Specific 238	Minor	Default	
NWALARM_239	Specific 239	Minor	Default	
NWALARM_240	Specific 240	Minor	Default	
NWALARM_241	Specific 241	Minor	Default	

Describe...   Modify...   Add...   Copy...   Delete   Alert Editor...

Configure Categories...   Configure Additional Actions...

OK   Apply   Cancel   Help

Figure 190. Unload NLM Enterprise Specific Trap

If we click on the **Describe** button in Figure 190, we get a description of the event that NetView for AIX has configured, as shown in Figure 191 on page 211. All of the fields came from the addtrap command. In some cases, numeric values might translate into something more descriptive. For example, the Severity of the trap shows up as Minor instead of the number 3.

Event Name	NWALARM_226
Severity	Minor
Status	Default Status
Event Category	Error Events
Source Character	A
Trap Fowarding	No
Sources	
Generic Trap Name (Number)	erprise Specific (6)
Specific Trap Number	226
Specific Trap (Hex)	0x000000e2
Enterprise ID	l.mibDoc.nwalarm-mib
Enterprise ID (Numeric)	.1.3.6.1.4.1.23.2.10

Event Description

Close   Help

Figure 191. Description of Trap 226, Unload NLM

8.1.1 Configuring Events

If we want to customize a trap to take an automated action, we just click on the **Modify** button. That will bring up a window like Figure 193 on page 212. Many of these fields are already filled in as a result of the addtrap command. We added the information in the Popup Notification field, and often you would add something to

the Command for Automation Action field for automatic execution. The shell that
we used, executed the following simple command:

```
/usr/lpp/X11/bin/aixterm -T ManageWise_Console -e telnet 9.24.104.54
```

Figure 192. Telnet Session to NetWare Server

The AIX shell that executes from this field runs under control of the ovactiond
daemon. You can change any of the fields or push buttons for this event.

Figure 193. Event Fields

As a result of unloading an NLM on our NetWare V4.1 server, a trap flowed over the IP network to our SNMP manager. Since we had configured the trap (226) to create a pop-up window, Figure 194 on page 213 showed up on our AIX console. After running this scenario as a simple example, we added a command to the Automatic action field to open a new aixterm (window) and establish a session with our NetWare server. Using a function called tunnelvision (tvision) from the MSM product, we are able to port a copy of the NetWare console over to our AIX system. This will work on AIX V3.2.5 and AIX V4.1.3. A description of MSM and tunnelvision can be found in *Managing NetWare Environments from MVS Using NPM, MSM-NetWare and MSM-LMU Managing NetWare from MVS*, SG24-4527-00.
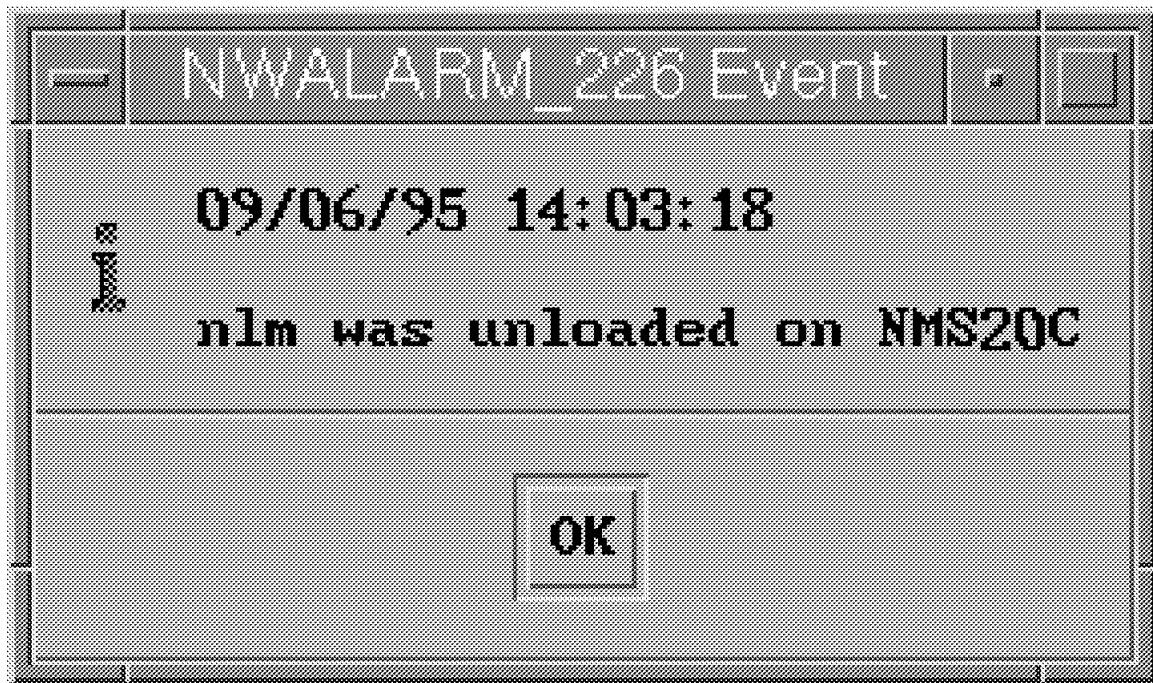
Figure 194. Pop-Up Window from Event Customization

Since we had specified that a new aixterm was to be started when the trap flowed and that it would create a session to 9.24.104.54, we were prompted for a logon to the NetWare V4.1 server.

```
╔══════════════════════════ ManageWise_Console ════════════════════════════╗
║Trying...                                                                  ║
║Connected to 9.24.104.54.                                                  ║
║Escape character is '^]'.                                                  ║
║LOGIN: ▯                                                                    ║
║                                                                           ║
║                                                                           ║
║                                                                           ║
║                                                                           ║
║                                                                           ║
║                                                                           ║
║                                                                           ║
║                                                                           ║
║                                                                           ║
║                                                                           ║
║                                                                           ║
║                                                                           ║
║                                                                           ║
║                                                                           ║
║                                                                           ║
║                                                                           ║
║                                                                           ║
║                                                                           ║
╚═══════════════════════════════════════════════════════════════════════════╝
```
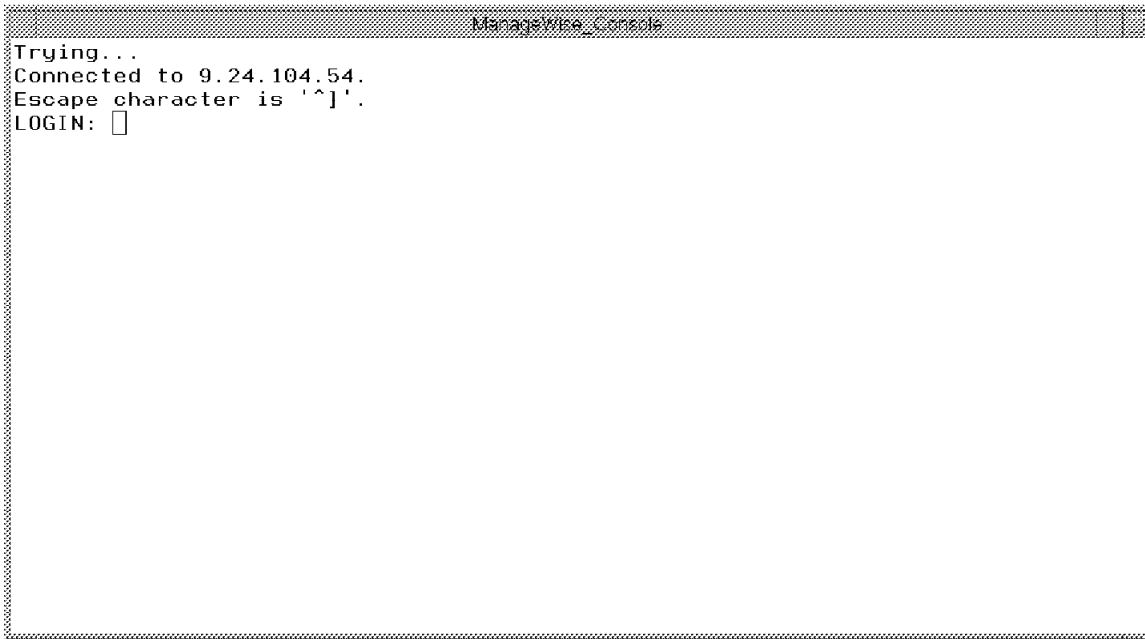
Figure 195. NetWare Console Using TVISION.NLM

After specifying a user ID and a password, we were logged into the NetWare server on our aixterm. This will work for AIX V3.2.5 or V4.1.

```
╔══════════════════════════ ManageWise_Console ════════════════════════════╗
║Trying...                                                                  ║
║Connected to 9.24.104.54.                                                  ║
║Escape character is '^]'.                                                  ║
║LOGIN: supervisor                                                          ║
║PASSWORD:                                                                  ║
║*********************************************                              ║
║*                                           *                              ║
║*        Welcome   to   TunnelVision        *                              ║
║*                   the                     *                              ║
║*    IBM NetView MultiSystem Manager        *                              ║
║*              TELNET Host                   *                              ║
║*    Version 1.00 -- R. Newpol, IBM Inc.    *                              ║
║*                                           *                              ║
║*********************************************                              ║
║*    For TV help, issue the AYT signal      *                              ║
║*    or press Ctrl-i for information        *                              ║
║*********************************************                              ║
║                                                                           ║
║Press Enter to continue...                                                 ║
║▯                                                                          ║
║                                                                           ║
║                                                                           ║
║                                                                           ║
╚═══════════════════════════════════════════════════════════════════════════╝
```
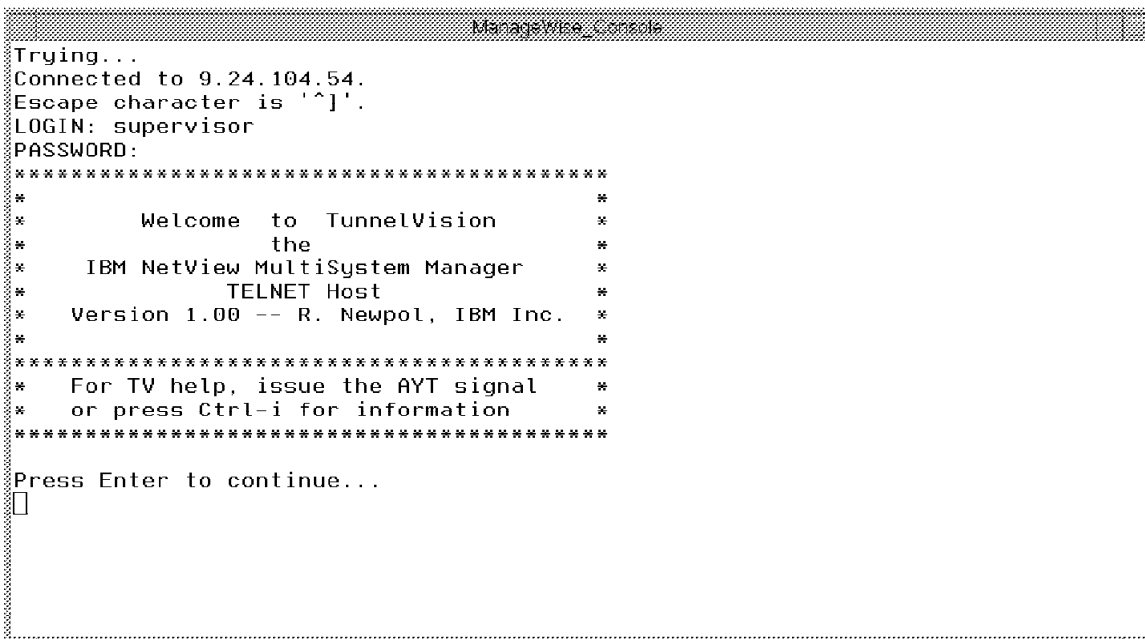
Figure 196. Telnet to NetWare Console over IP

An example of a simple command to execute from the NetWare server is help. Normal non-graphic commands can be done over this telnet session. If you need extended attributes or graphics, you will not be able to do so over this session.

```
┌──────────────────────────────────────────────────────────────────────────────┐
│                              ManageWise_Console                                │
│ ABORT REMIRROR              ADD NAME SPACE              BIND                    │
│ BROADCAST                   CLEAR STATION               CLS                     │
│ CONFIG                      DISABLE LOGIN               DISABLE TTS             │
│ DISMOUNT                    DISPLAY NETWORKS            DISPLAY SERVERS         │
│ DOWN                        ECHO OFF                    ECHO ON                 │
│ ENABLE LOGIN                ENABLE TTS                  EXIT                    │
│ FILE SERVER NAME            IPX INTERNAL NET            LANGUAGE                │
│ LIST DEVICES                LOAD                        MAGAZINE INSERTED       │
│ MAGAZINE NOT INSERTED       MAGAZINE NOT REMOVED        MAGAZINE REMOVED        │
│ MEDIA INSERTED              MEDIA NOT INSERTED          MEDIA NOT REMOVED       │
│ MEDIA REMOVED               MEMORY MAP                  MEMORY                  │
│ MIRROR STATUS               MODULES                     MOUNT                   │
│ NAME                        OFF                         PAUSE                   │
│ #                           PROTOCOL                    REGISTER MEMORY         │
│ REMOVE DOS                  REMIRROR PARTITION          REM                     │
│ RESET ROUTER                RESTART SERVER              SCAN FOR NEW DEVICES    │
│ SEARCH                      SECURE CONSOLE              ;                       │
│ SEND                        SET TIME ZONE               SET TIME               │
│ SET                         SPEED                       SPOOL                   │
│ TIME                        TRACK OFF                   TRACK ON                │
│ UNBIND                      UNLOAD                      VERSION                 │
│ VOLUME                      HELP                                                │
│                                                                                │
│ Type HELP [command] to display specific command help                           │
│ NMS2OC:▯                                                                        │
└──────────────────────────────────────────────────────────────────────────────┘
```

Figure 197. NetWare Help Command

> In Figure 198 we can see all the control character sequences that you would need to change screens on your NetWare server. If you load an NLM that opens a new screen, you can use Ctrl-N to page forward to get to that session.

```
┌──────────────────────────────────────────────────────────────────────────────┐
│                              ManageWise_Console                                │
│                                                                                │
│ Ctrl-A    -- list All current server screens                                   │
│ Ctrl-N    -- switches to next screen                                           │
│ Ctrl-P    -- switches to previous screen                                       │
│ Ctrl-F    -- switches to First screen (System Console)                         │
│ Ctrl-V    -- reView the current screen contents (refresh)                      │
│ Ctrl-C    -- show current screen name                                          │
│ Ctrl-U    -- send UP arrow keystroke                                           │
│ Ctrl-D    -- send DOWN arrow keystroke                                          │
│ Ctrl-L    -- send LEFT arrow keystroke                                          │
│ Ctrl-R    -- send RIGHT arrow keystroke                                         │
│ Ctrl-T    -- Turn off TV Ctrl-chars (pass Ctrl-chars as is)                     │
│              Send the AYT signal to restart TV Ctrl-char processing             │
│ Ctrl-i    -- shows this information                                             │
│ Ctrl-E    -- End session                                                        │
│                                                                                │
│ System Console            (linemode)                                            │
│ Debugger Screen           (linemode)                                            │
│ NETXPLOR                  (linemode)                                            │
│ nxpip                     (linemode)                                            │
│ NXPIPX : Info/Status      (linemode)                                            │
│ LANDesk Virus Protect 2.13 s/n:35514968 (linemode)                              │
│ LMU Managed System        (linemode)                                            │
│ NetWare 4.10 Console Monitor (linemode)   <--- CURRENT SCREEN                    │
│ ▯                                                                               │
└──────────────────────────────────────────────────────────────────────────────┘
```

Figure 198. Controlling the NetWare Console

> Using Ctrl-N we will step through some examples of our NetWare Console, which use ManageWise as well as other NLMs.

```
NetExplorer SNMP/IP DISCOVERY COMPLETED [51]
Restarting NetExplorer SNMP/IP Discovery
NetExplorer IP DISCOVERY INITIATION [8]
NetExplorer IPX DISCOVERY COMPLETED [20]
Restarting NetExplorer IPX Discovery
NetExplorer IPX DISCOVERY COMPLETED [20]
Restarting NetExplorer IPX Discovery
NetExplorer IPX DISCOVERY COMPLETED [20]
Restarting NetExplorer IPX Discovery
NetExplorer IPX DISCOVERY COMPLETED [20]
Restarting NetExplorer IPX Discovery
NetExplorer IPX DISCOVERY COMPLETED [20]
Restarting NetExplorer IPX Discovery
NetExplorer SNMP/IP DISCOVERY COMPLETED [51]
Restarting NetExplorer SNMP/IP Discovery
NetExplorer IP DISCOVERY INITIATION [8]
NetExplorer IPX DISCOVERY COMPLETED [20]
Restarting NetExplorer IPX Discovery
NetExplorer IPX DISCOVERY COMPLETED [20]
Restarting NetExplorer IPX Discovery
NetExplorer IPX DISCOVERY COMPLETED [20]
Restarting NetExplorer IPX Discovery
NetExplorer IPX DISCOVERY COMPLETED [20]
Restarting NetExplorer IPX Discovery
```

Figure 199. NetWare Console - NetExplorer

```
Investigating SNMP object: #[16]   [9.67.46.20] Routers Discovered [6]
Investigating SNMP object: #[17]   [9.24.104.60] Routers Discovered [6]
Investigating SNMP object: #[18]   [9.67.32.15] Routers Discovered [6]
Investigating SNMP object: #[19]   [9.67.32.21] Routers Discovered [6]
Investigating SNMP object: #[20]   [9.67.46.203] Routers Discovered [6]
SNMP/IP DISCOVERY PASS [140] COMPLETE ([6] routers)

NetExplorer IP DISCOVERY INITIATED
Investigating SNMP object: #[0]   [9.24.104.54] Routers Discovered [6]
Investigating SNMP object: #[1]   [9.24.104.1] Routers Discovered [6]
Investigating SNMP object: #[2]   [9.24.104.108] Routers Discovered [6]
Investigating SNMP object: #[3]   [9.24.104.202] Routers Discovered [6]
Investigating SNMP object: #[4]   [9.24.104.127] Routers Discovered [6]
Investigating SNMP object: #[5]   [9.24.104.205] Routers Discovered [6]
Investigating SNMP object: #[6]   [9.24.104.144] Routers Discovered [6]
Investigating SNMP object: #[7]   [9.24.104.240] Routers Discovered [6]
Investigating SNMP object: #[8]   [9.24.104.74] Routers Discovered [6]
Investigating SNMP object: #[9]   [9.24.104.81] Routers Discovered [6]
Investigating SNMP object: #[13]   [9.67.32.10] Routers Discovered [6]
Investigating SNMP object: #[14]   [9.67.38.10] Routers Discovered [6]
Investigating SNMP object: #[15]   [9.67.46.1] Routers Discovered [6]
Investigating SNMP object: #[16]   [9.67.46.20] Routers Discovered [6]
Investigating SNMP object: #[17]   [9.24.104.60] Routers Discovered [6]
Investigating SNMP object: #[18]   [9.67.32.15] Routers Discovered [6]
```

Figure 200. NetWare Console - IP Discovery

```
                       ManageWise_Console
NXPIPX discovered 14: servers (8), routers (0), workstations (6)
NXPIPX reported 15: servers (8+1), routers (0+0), workstations (6+0)

Sep  8 12:32:55 (GLOBAL DISCOVERY): Cycle 734:   IPX discovery is initiated
Sep  8 12:35:04 (GLOBAL DISCOVERY): Cycle 735:   IPX discovery is initiated

Sep  8 12:36:55  (NXPIPX has been running since Sep  7 10:05:10)
NXPIPX connection to NETXPLOR (NMS20C) is (1-0), and self is (1-0)
NXPIPX is in cycle 735 with 3 threads: server (99), router (5), workstation (99

NXPIPX discovered 14: servers (8), routers (0), workstations (6)
NXPIPX reported 15: servers (8+1), routers (0+0), workstations (6+0)

Sep  8 12:37:13 (GLOBAL DISCOVERY): Cycle 736:   IPX discovery is initiated
Sep  8 12:39:22 (GLOBAL DISCOVERY): Cycle 737:   IPX discovery is initiated
Sep  8 12:41:30 (GLOBAL DISCOVERY): Cycle 738:   IPX discovery is initiated

Sep  8 12:41:51  (NXPIPX has been running since Sep  7 10:05:10)
NXPIPX connection to NETXPLOR (NMS20C) is (1-0), and self is (1-0)
NXPIPX is in cycle 738 with 5 threads: server (3), router (1), workstation (1)
NXPIPX discovered 14: servers (8), routers (0), workstations (6)
NXPIPX reported 15: servers (8+1), routers (0+0), workstations (6+0)

Sep  8 12:43:39 (GLOBAL DISCOVERY): Cycle 739:   IPX discovery is initiated
```

Figure 201. NetWare Console - IPX Discovery

```
                       ManageWise_Console
ÚÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
³ Intel LANDesk Virus Protect  2.13                NetWare Loadable Module
ÃÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
°ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
°º                        Monitor: Server NMS20C                            º
°ÌÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¹
°º CPU Utilization:  39%                       Fri Sep  8 12:44:47pm 1995  º
°º Duration of current LANDesk Virus Protect session:  1:02:39:23          º
°º Log File Reporting Date: Sun Sep 17 12:00:00am 1995                     º
°º           Count Down Timer:  8:11:15:13                                 º
°º Next Prescheduled Scan Date: No Scan                                    º
°º                                                                         º
°º Status of Real Time Scan:                                               º
°º Direction of I/O Scan: Both incoming and outgoing files                 º
°º Duration of I/O Scan:  1:02:39:23                                       º
°º Total Files Scanned: 6             Total infected files found: 0        º
°º Action on Virus Detection:  Move infected file to virus directory       º
°º Last File Scanned by Real Time File Scan:                               º
°º User:ADMIN       File was being read from/written to the server:Read    º
°º File:SYS:\PUBLIC\NLS\ENGLISH\RCONSOLE.HEP                               º
°º Last Infected File:             Date/Time:                              º
°º Virus:                          Action taken:                           º
°º File:                                                                   º
°ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
Esc:Quit
```

Figure 202. NetWare Console - Monitor.NLM

```
                              ManageWise_Console
  NetWare 4.10 Console Monitor  4.12              NetWare Loadable Module
   Server name: 'NMS20C' in Directory tree 'NMS_NDS'
   Server version: NetWare 4.10 - November 8, 1994
ooooooooooooooÚÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ¿ooooooooooooo
ooooooooooooooo³            General Information                  ³ooooooooooooo
ooooooooooooooo³ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ´ooooooooooooo
ooooooooooooooo³   Server up time:                  0:00:36:58   ooooooooooooo
ooooooooooooooo³   Utilization:                            19%   Ûooooooooooooo
ooooooooooooooo³   Original cache buffers:              7,077    ooooooooooooo
ooooooooooooooo³   Total cache buffers:                 4,470    ooooooooooooo
ooooooooooooooo³   Dirty cache buffers:                     1    ooooooooooooo
ooooooooooooooo³   Current disk requests:                  7     ooooooooooooo
ooooooooooooooÀÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÙooooooooooooo
ooooooooooooooooooooooooooÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»oooooooooooooooooooooo
ooooooooooooooooooooooooooº       Available Options    ºoooooooooooooooooooooo
oooooooooooooooooooooooooooÌÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¹oooooooooooooooooooooo
ooooooooooooooooooooooooooo³Connection information     ºoooooooooooooooooooooo
ooooooooooooooooooooooooooo³Disk information           ºoooooooooooooooooooooo
ooooooooooooooooooooooooooo³LAN/WAN information        ºoooooooooooooooooooooo
ooooooooooooooooooooooooooo³System module informationºooooooooooooooooooooo
ooooooooooooooooooooooooooo³Lock file server console  ºoooooooooooooooooooooo
ooooooooooooooooooooooooooo³File open/lock activity    ºoooooooooooooooooooooo
oooooooooooooooooooooooooo³Cache utilization           ºoooooooooooooooooooooo
ooooooooooooooooooooooooooÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼oooooooooooooooooooooo
 Tab=Expand data window   Enter=Select option    Alt+F10=Exit        F1=Help
```

Figure 203. NetWare Console - General Information

> Since we don't have graphics capabilities over the telnet session, everything we
> see is in text mode. This is not as easy to use as a native console or a console
> from the NetWare workstation, but it does provide some remote management
> capability. You would probably use RCONSOLE if you were at a DOS/Windows
> workstation.

8.1.2 Sending Commands to a NetWare Server

> In addition to taking actions based upon traps, we can either schedule or execute
> upon demand commands that can run on the NetWare client or the NetWare
> server. Using the GUI interface on NetView for AIX, we can see the topology of
> the NetWare servers; if we want to send commands to them, we can use LMU for
> AIX and LMU for OS/2 to do that. In Figure 204 on page 219 we see the initial
> rootmap which has our Internet view as well as the NetWare and LMU topology
> views.
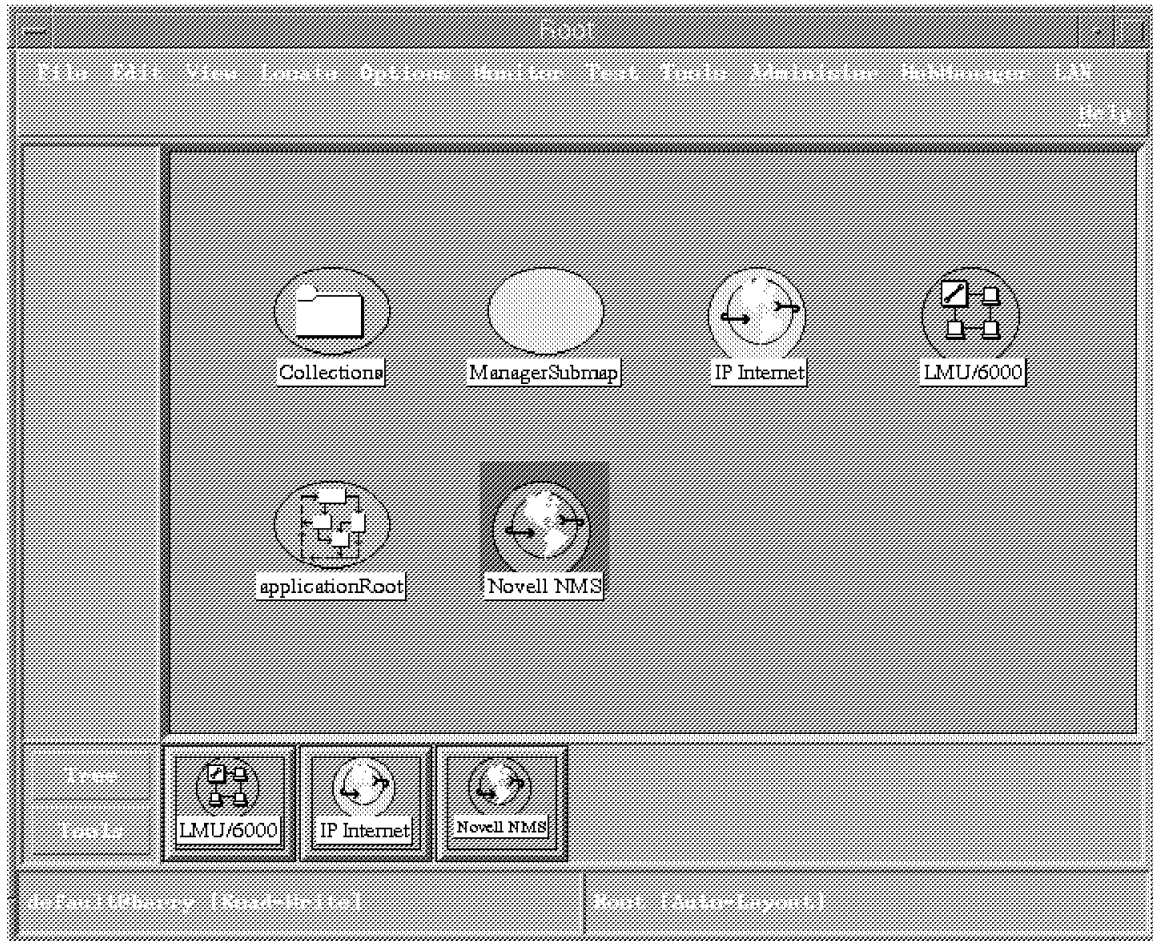
Figure 204. Rootmap for NetView for AIX

If we double-click on the **Novell NMS** symbol on the map, we go to the next layer in the topology. The label on the submap in Figure 205 on page 220 matches a definition set up on the NMS or ManageWise client. If we double-click again, we see that in Figure 207 on page 222 we have some NetWare servers. The other symbol on the submap represents all of the IP-topology that the ManageWise agents have discovered. An example of this is shown in Figure 206 on page 221. In that submap, you see regular host names, as well as IP and IPX addresses. In addition, you see a symbol in the lower left-hand part of the screen that shows discovery in progress. The topology is constantly being checked and updated. If you go to the NetWare console and scroll through the screens, you will see the IP and IPX discovery NLMs running all the time.
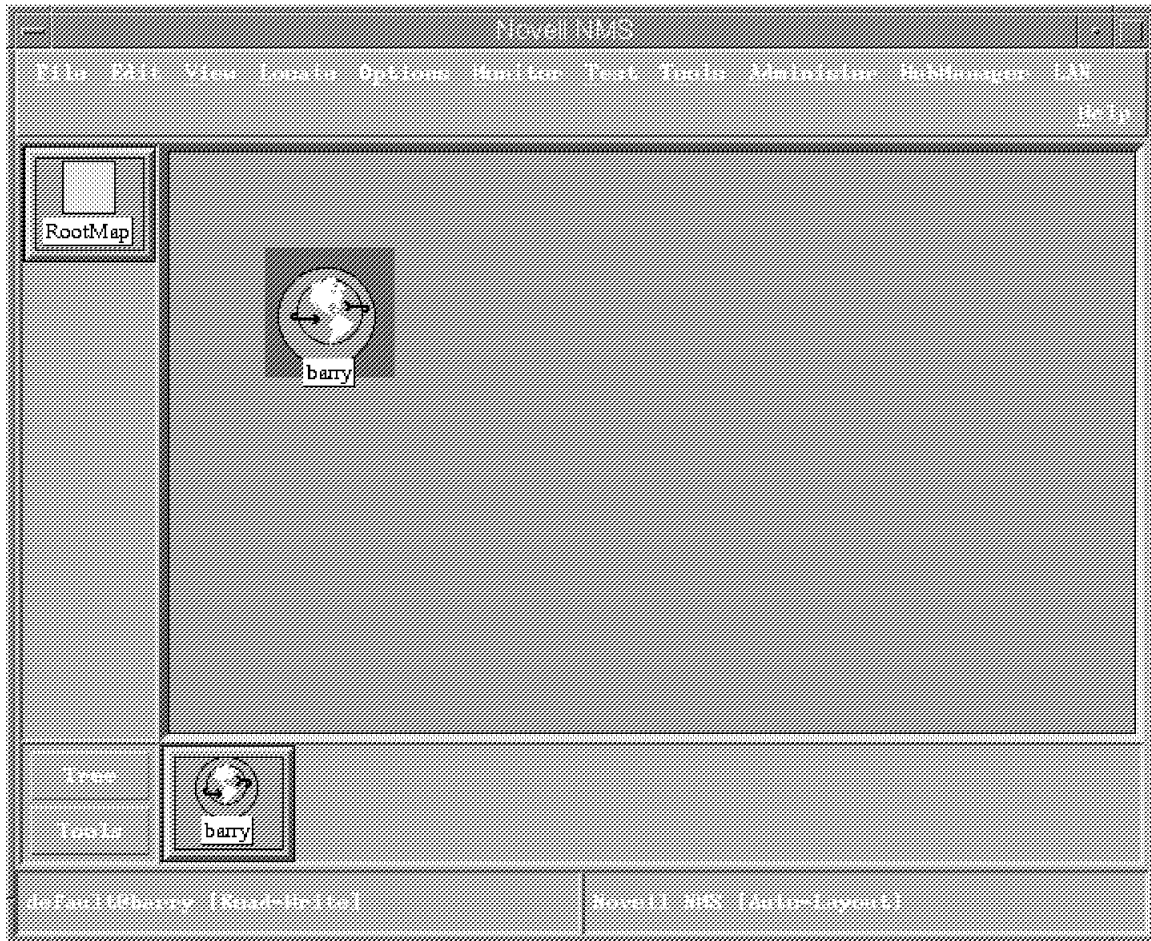
Figure 205. NMS Topology - IPX Topology
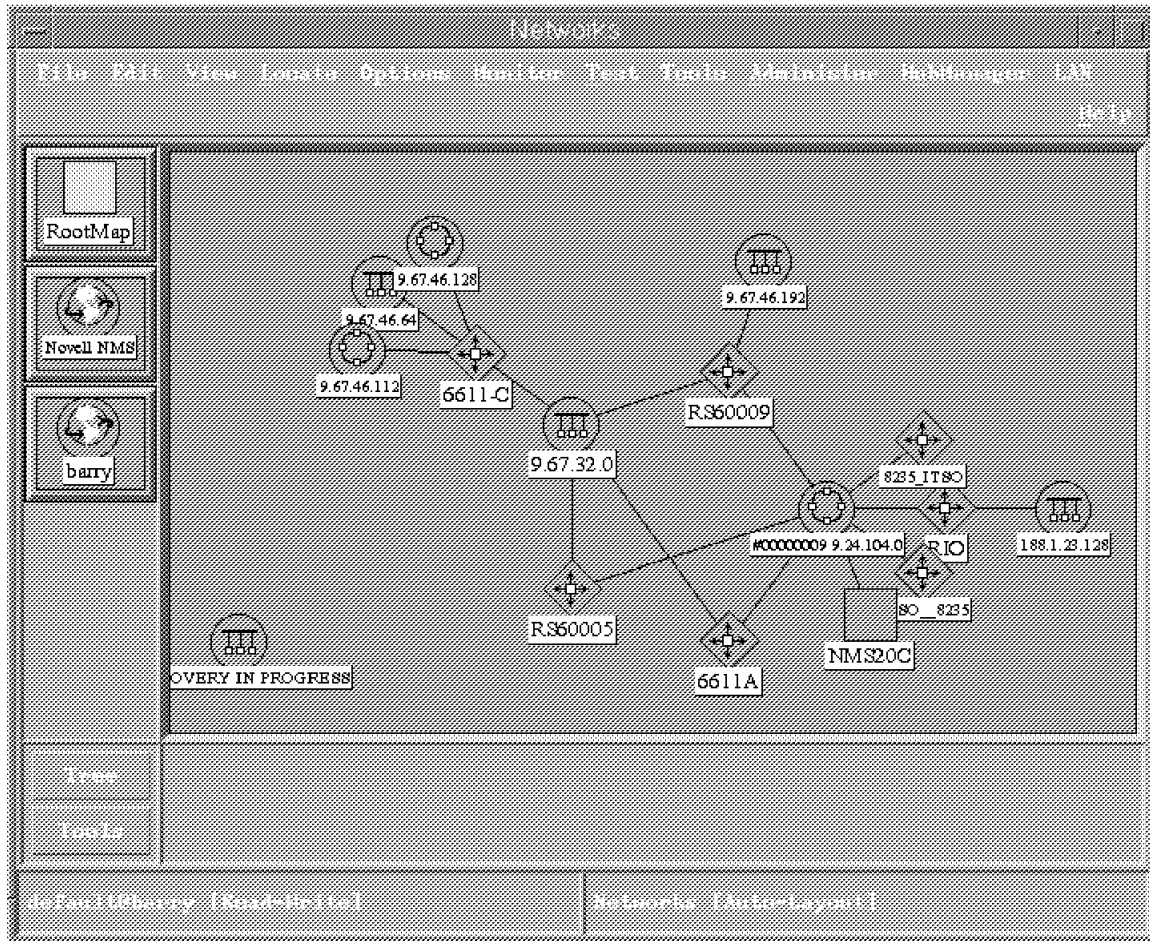
Figure 206. NMS Topology - IP Topology

If you double-click on the **NetWare Servers** symbol, you will get a list of all the servers that were discovered, as shown in Figure 208 on page 223 There are several servers in this environment. We have discovered NetWare V3.11, V3.12, and V4.1 servers. For this part of the scenario, we will be using the server called NMS20C, which is highlighted in Figure 207 on page 222. If we double-click on **NMS20C** and then use the right mouse button for the pull-down menus, we can see that we can issue a remote command using LMU for AIX. This is shown in Figure 209 on page 224.
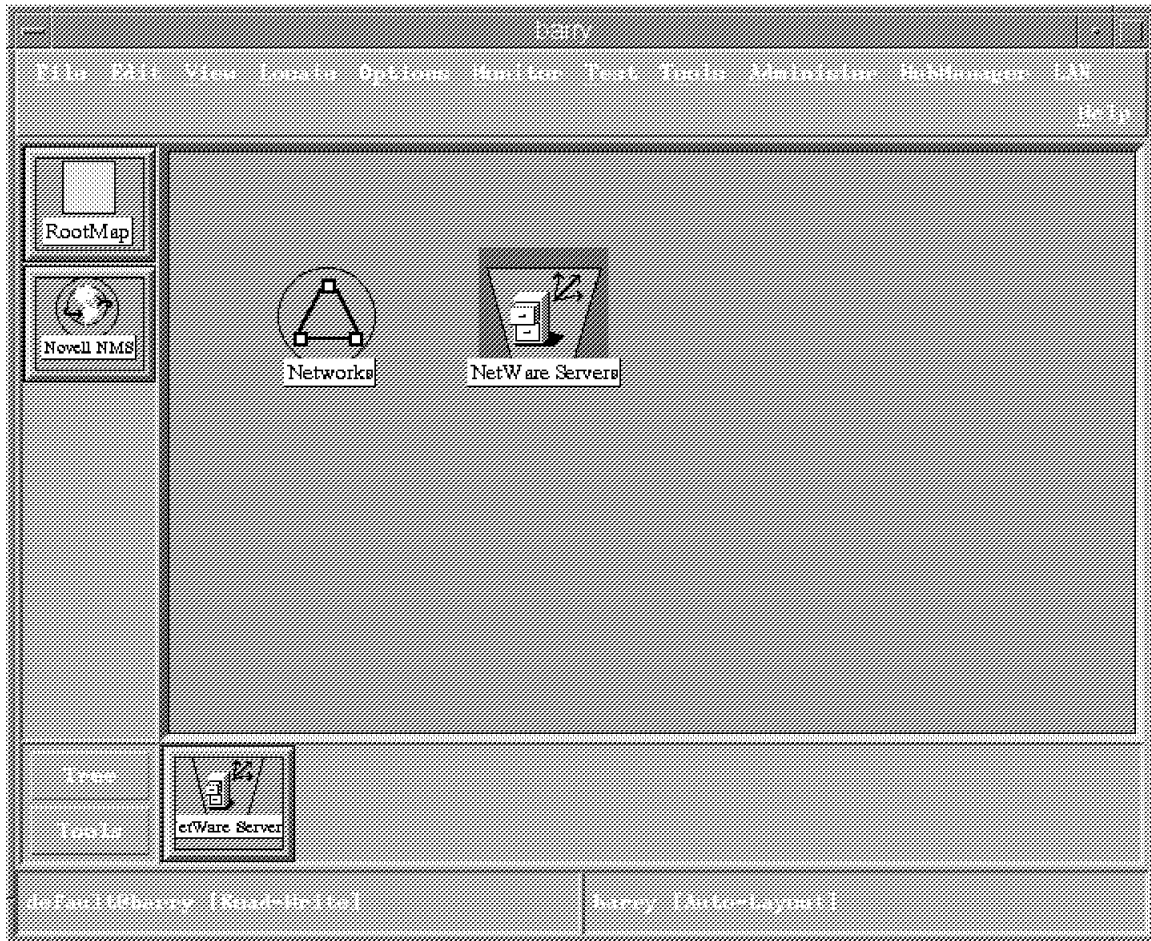
Figure 207. All the NetWare Servers
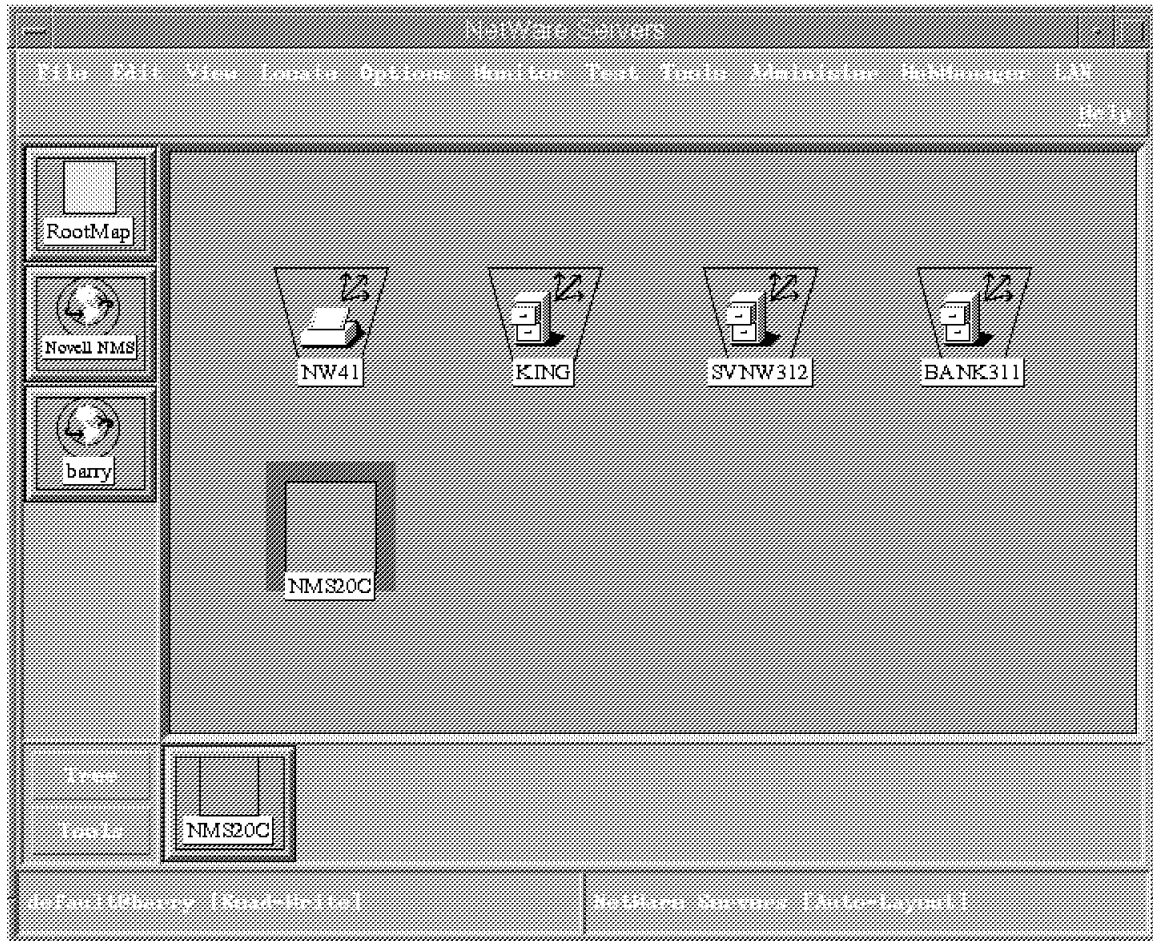
Figure 208. List of All the Discovered NetWare Servers

If we click on **Execute Remote Commands**, the window Figure 210 on page 225 appears. Unfortunately, since we are sending commands to the NetWare Console, not to the client, we can not see the results of the command. In order to see the results we would need access to the console. This can be done remotely using RCONSOLE from a DOS or OS/2 client, or we can telnet to the server and use the TVISION.NLM as shown earlier. Another way that we could look at the result would be to look at the console log that is maintained when you load the CONLOG.NLM.

A simple command that we can execute on the NetWare console is Modules. This command gives you a list of all NLMs that are loaded on this sever as shown in Figure 213 on page 228. From the panel shown in Figure 210 on page 225, we can just type in the command modules.

Figure 209. Display Data or Execute Commands

In this case you can see that we are sending the command to NMS20C. After you click on the **Execute** button, you may get the pop-up window shown in Figure 211 on page 226. Within AIX, you can specify the user ID and password in a file in your root directory, but we chose not to do that for security purposes.
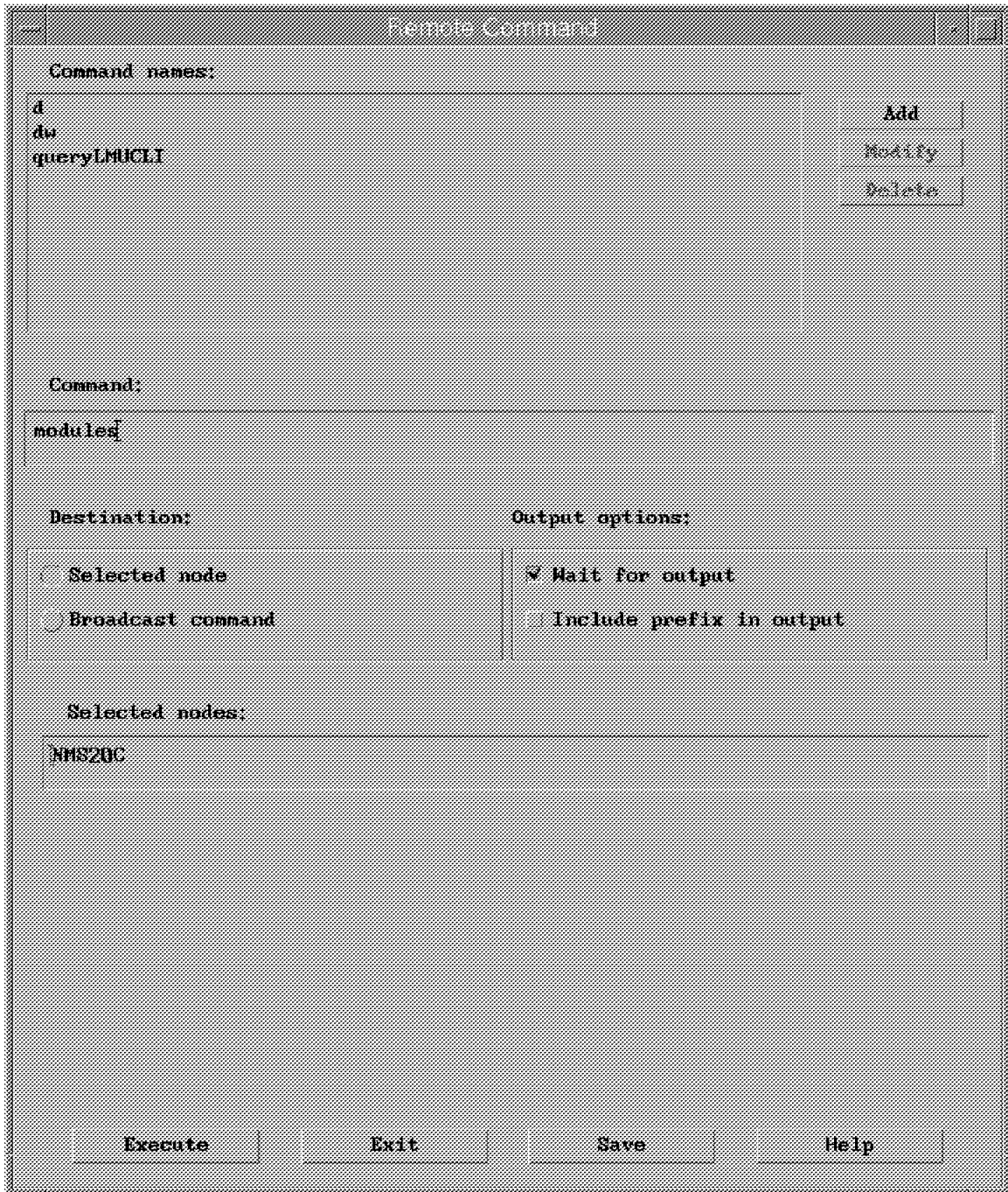
Figure 210. LMU for AIX Remote Execution

Figure 211. REXEC Userid and Password Prompt

When the command is sent over the IP network to the NetWare server, it gets executed on the console. As you can see in Figure 212 on page 227, LMU for AIX acknowledges that the command has been sent to the LMU resource 87654321:000000000001. It also indicates that we will not get any console output back to LMU for AIX from the NetWare console.

The REXEC is actually being sent from LMU for AIX to our LMU for OS/2 machine. From there, it is using the services of LAN Server 4.0 and then sending the command over to our NetWare server.
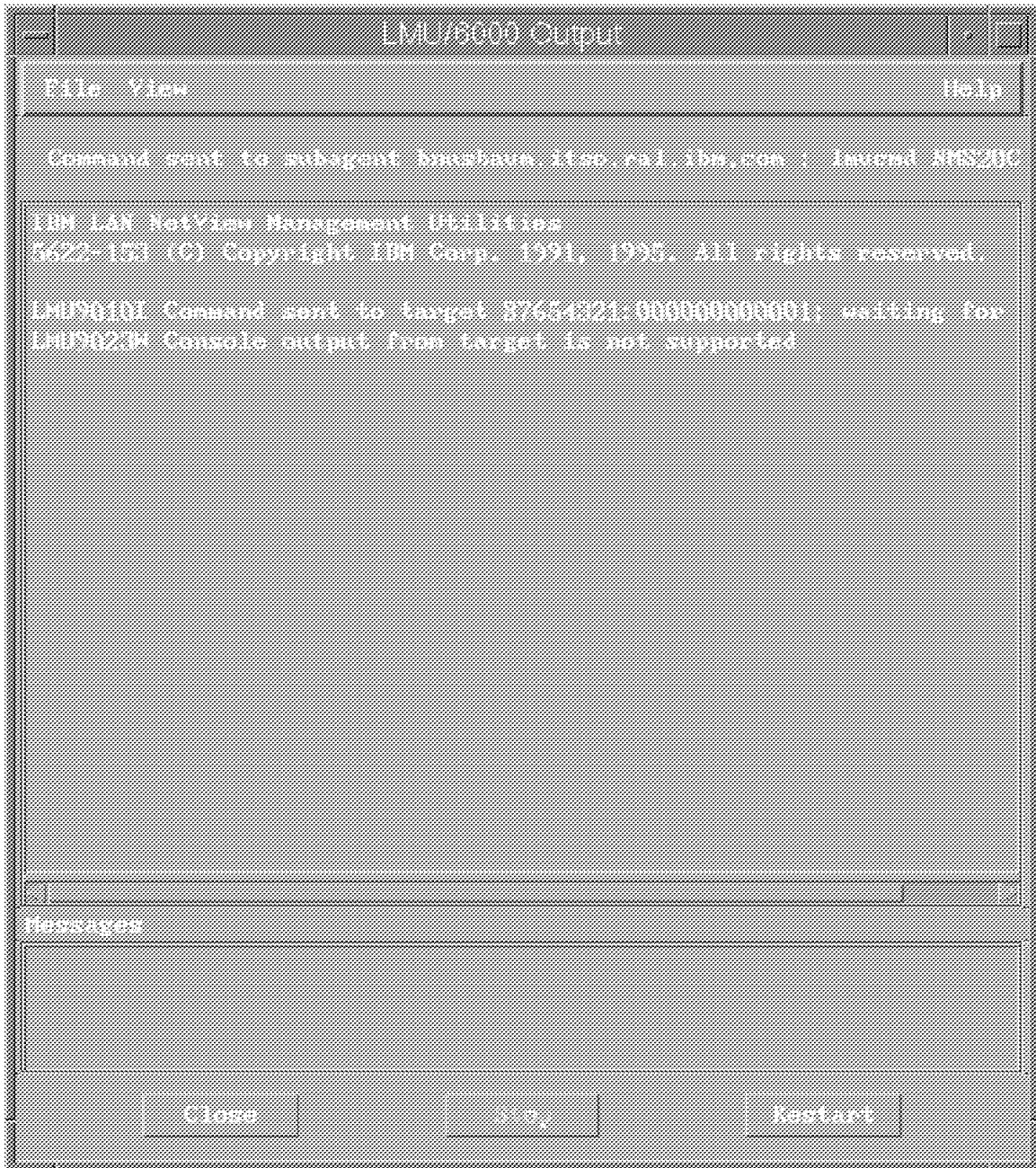
Figure 212. LMU for AIX Output

The following figure is an example of the RCONSOLE screen from our DOS/Windows client.
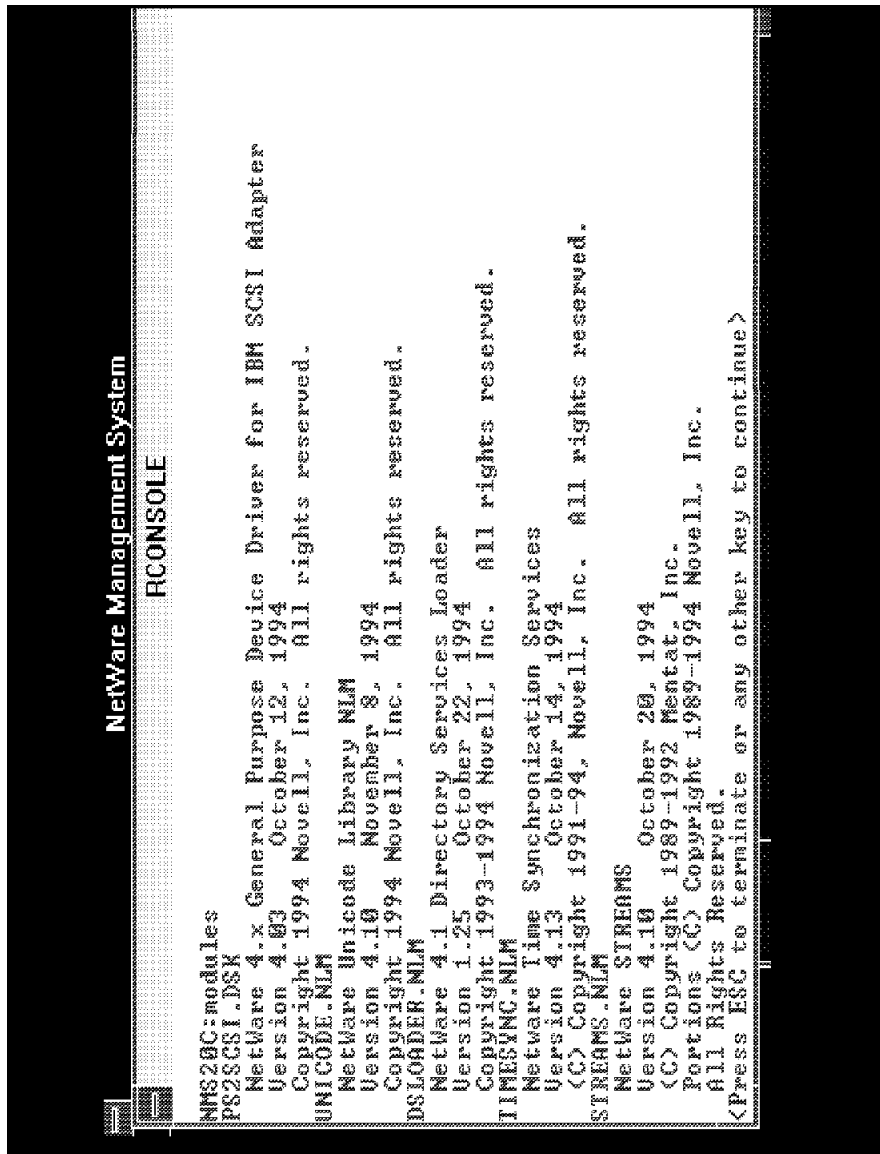
Figure 213. RCONSOLE

In addition to being able to send commands directly to the NetWare console, we
can also use NetView for AIX and LMU for AIX to communicate with the NetWare
clients. In Figure 214 on page 229, we are going to send the nlist command to the
client. The client is connected by IP to NetView for AIX and it uses IPX to
communicate with the NetWare server. Its IPX address is
00000009:400052005204.
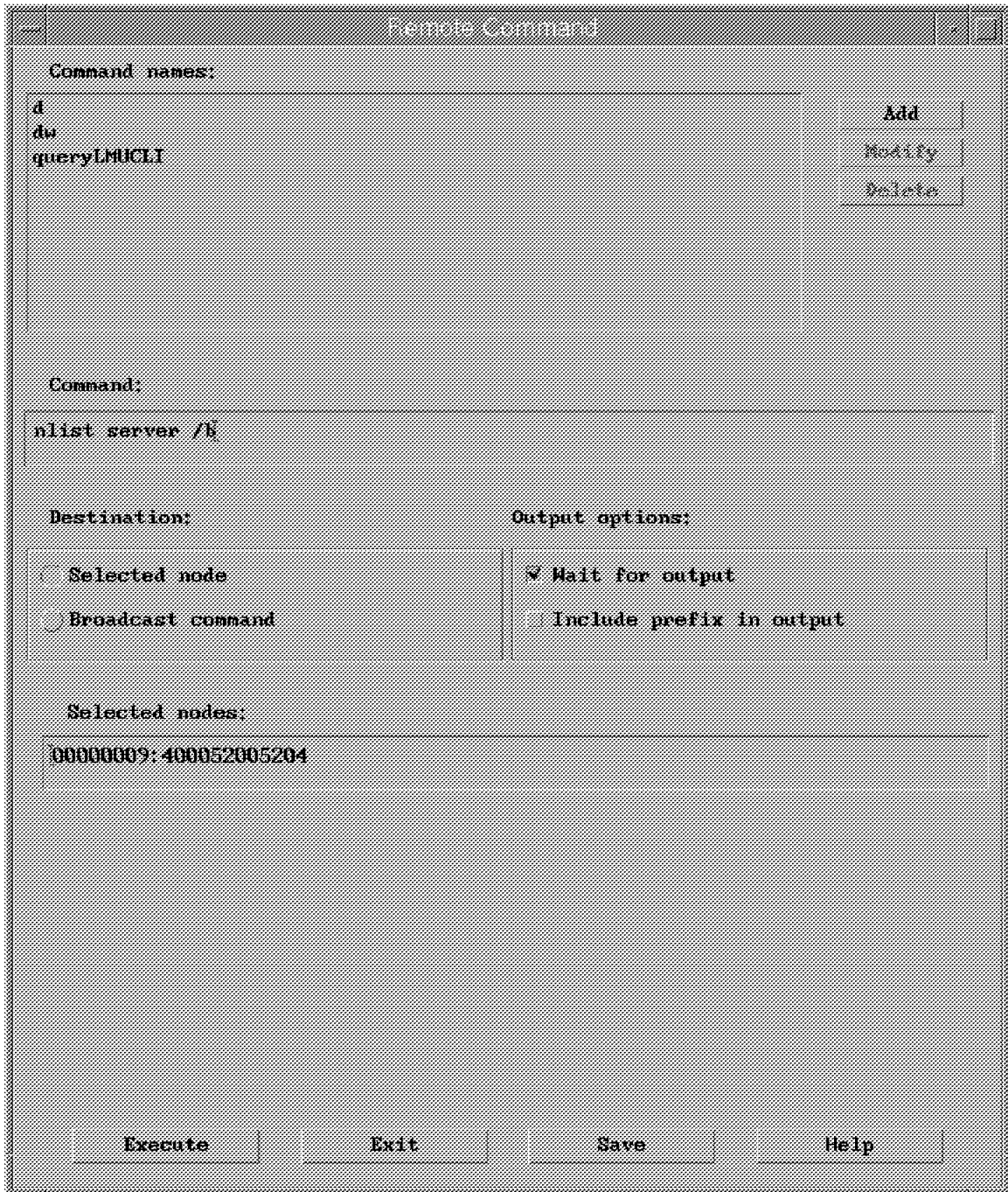
Figure 214. Sending Commands to the NetWare DOS/Windows Client

In Figure 215 on page 230 we can see the results of the command that we issued from the NetView for AIX interface into LMU for AIX. This means that we have many different ways to get information from the NetWare server.
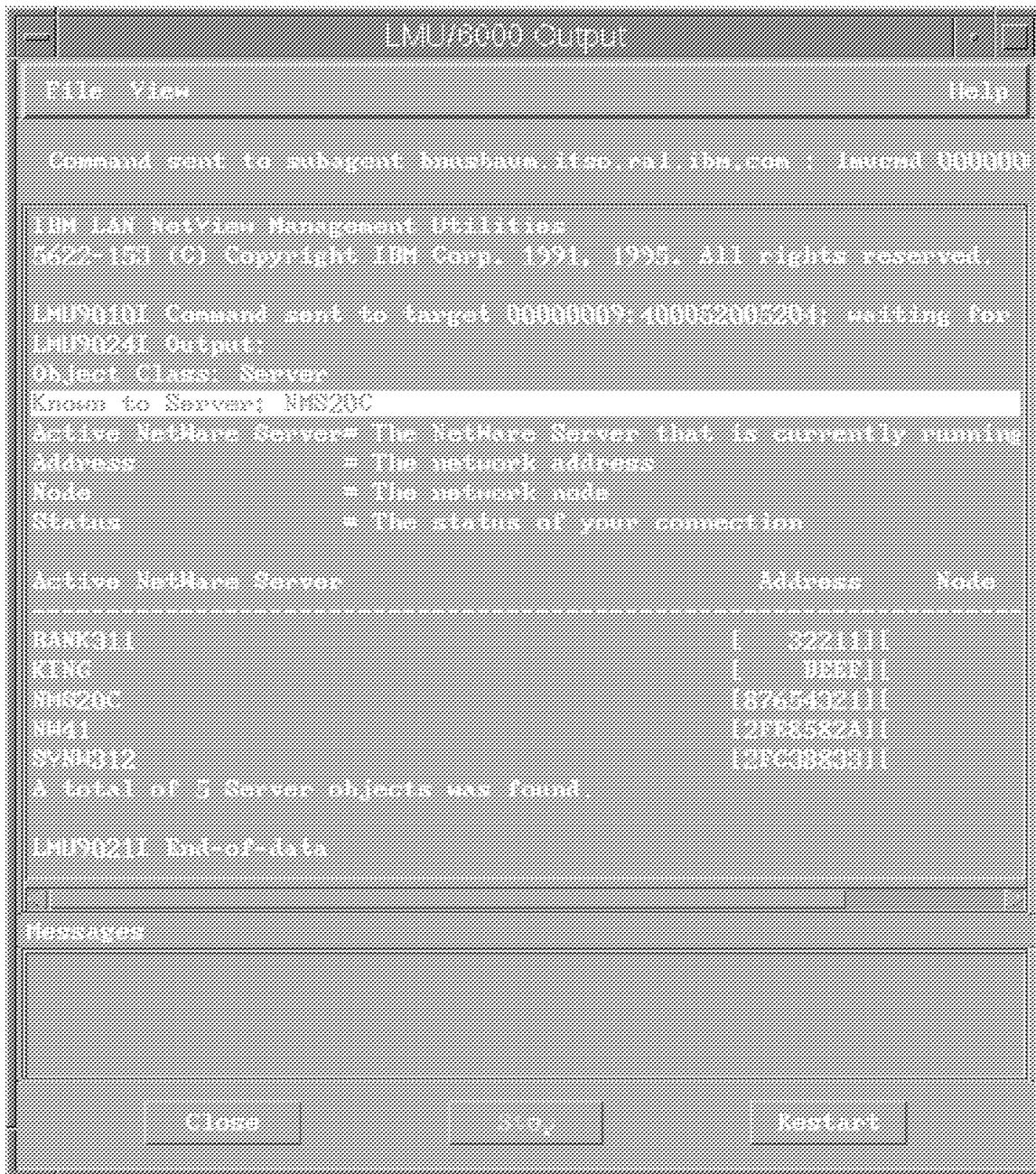
Figure 215. Output from the DOS/Windows Client

Openmon provides us with the topology information, and a combination of ManageWise (or just NMS), IP, LMU for AIX and LMU for OS/2 gives us the capability to have a command interface.

All of the commands that we issued using the DOS/Windows client can also be done from the OS/2 client.

Appendix A. DOS and NetWare Files

A.1 CONFIG.SYS

```
DEVICE=C:\WINDOWS\SMARTDRV.EXE /DOUBLE_BUFFER
FILES= 100
BUFFERS= 40
dos=high
device=C:\DOS\HIMEM.SYS
device=c:\dos\emm386.exe noems ram x=a000-b0ff i=b100-b7ff x=b800-bfff i=c000-cfff x=d000-d7ff i=d800-dbff x=dc00-f7ff h=64 a=7 d=64
device=c:\dos\ramboost.exe load
DEVICE=C:\DOS\SETVER.EXE
DEVICE=C:\DOS\ANSI.SYS
STACKS=9,256

LASTDRIVE=Z
```

A.2 AUTOEXEC.BAT

```
ECHO OFF
CD \VPROTECT.PC
VPRULE
CD ..
@CALL C:\NWCLIENT\STARTNET
C:\WINDOWS\SMARTDRV.EXE /L
@ECHO OFF
SET TZ=EST5EDT
path=C:\WINDOWS;c:\dos;%PATH%
path=D:\NMS\bin;D:\NET\BIN;C:\NWCLIENT\;%PATH%
SET TEMP=C:\DOS
C:\DOS\MOUSE.COM
C:\DOS\DOSKEY.COM
REM C:\DOS\DOSSHELL

SET HELPFILES=D:\NMS\help\*.HLP
CALL C:\lanwp.bat
ROUTE
F:
LOGIN NMS20C/ADMIN /B
REM *** BEGIN Intel LANDesk Manager Section ***
REM The following line loads the Btrieve TSR (39kbytes)
REM required by Inventory Manager.
brequest /r:26
REM ***  END Intel LANDesk Manager Section ***
```

A.3 STARTNET.BAT

```
SHARE
SET NWLANGUAGE=ENGLISH
C:\NWCLIENT\LSL.COM
C:\NWCLIENT\NTR2000.COM
C:\NWCLIENT\IPXODI.COM
C:\NWCLIENT\VLM.EXE
```

A.4 AUTOEXEC.NCF

```
set Time Zone = EST5EDT
set Daylight Savings Time Offset = 1:00:00
set Start Of Daylight Savings Time = (APRIL SUNDAY FIRST  2:00:00 AM)
set End Of Daylight Savings Time = (OCTOBER SUNDAY LAST  2:00:00 AM)
set Default Time Server Type = SINGLE
set Bindery Context = O=IBM_ITSO
file server name NMS20C
ipx internal net 87654321
# $NMSBASE$ DO NOT DELETE THIS LINE
# Netware Management System installation has
# created the following NMSBASE.NCF file.
# Review the load sequence of NLMs in NMSBASE.NCF.
# Make sure that the NLM loaded by NMSBASE.NCF
# do not conflict with your existing setup.
# Uncomment the following line after review....
NMSBASE.NCF
load conlog  maximum=100
; Network driver LOADs and BINDs are initiated via
; INITSYS.NCF. The actual LOAD and BIND commands
; are contained in INITSYS.NCF and NETINFO.CFG.
; These files are in SYS:ETC.
sys:etc\initsys.ncf
LOAD SYS:\SYSTEM\NXPPLUS
#LOAD TCPIP FORWARD=YES TRAP=9.24.104.15
#LOAD TOKEN SLOT=3 NODE=400052005190M FRAME=Token-Ring MSB  NAME=TOKEN_1_TOK
LOAD ROUTE board=2
#BIND IPX TOKEN_1_TOK NET=9
#LOAD TOKEN SLOT=3 NODE=400052005190M FRAME=Token-Ring_SNAP MSB  NAME=TOKEN_1_TSP
#BIND IP TOKEN_1_TSP ADDR=9.24.104.54 MASK=ff.ff.ff.0
mount all
load route
#load nw2snmp ga=on
# $NETXPLOR$ DO NOT DELETE THIS LINE
# Netware Management System installation has
# created the following NETXPLOR.NCF file.
# Review the load sequence of NLMs in NETXPLOR.NCF.
# Make sure that the NLM loaded by NETXPLOR.NCF
# do not conflict with your existing setup.
# Uncomment the following line after review....
NETXPLOR.NCF
# $NMA$ DO NOT DELETE THIS LINE
# Netware Management System installation has
# created the following NMA.NCF file.
# Review the load sequence of NLMs in NMA.NCF.
# Make sure that the NLM loaded by NMA.NCF
# do not conflict with your existing setup.
# Uncomment the following line after review....
NMA.NCF
REM *** BEGIN Intel LANDesk Manager Section ***
REM The following line loads the Inventory Manager NLM with
REM its data file.
load ldinv file=SYS:MW\LDT
REM The following line loads the Inventory Scanner NLM for
REM this server.
load ldiscan inv_serv=NMS20C file=SYS:MW\LDT
REM The following line loads the USER NLM required by
REM Desktop Access.
load user
REM ***   END Intel LANDesk Manager Section ***
REM *** BEGIN Intel LANDesk Virus Protect Section ***
REM The following line starts the LANDesk Virus Protect NLM.
load SYS:MW\LDVP\LPROTECT.NLM
REM ***   END Intel LANDesk Virus Protect Section ***
```

A.5 NET.CFG

```
Link Driver NTR2000
        Frame Token-Ring_SNAP
        Protocol IPX E0 TOKEN-RING
        Frame TOKEN-RING
        PORT A20
        MAX FRAME SIZE 4208
        NODE ADDRESS 400052005204

NetWare DOS Requester
        FIRST NETWORK DRIVE = F
        NETWARE PROTOCOL = NDS BIND


        IPX SOCKETS 60

Link Support
        Buffers 8 4156
        MemPool 4096

Protocol TCPIP
        PATH SCRIPT     D:\NET\SCRIPT
        PATH PROFILE    D:\NET\PROFILE
        PATH LWP_CFG    D:\NET\HSTACC
        PATH TCP_CFG    D:\NET\TCP
        ip_router       9.24.104.1
        ip_netmask      255.255.255.0
        ip_address      9.24.104.21
        tcp_sockets     8
        udp_sockets     8
        raw_sockets     1
        nb_sessions     0
        nb_commands     0
        nb_adapter      0
        nb_domain

PROTOCOL IPX
        BIND #2
```

A.6 NMSINST.LOG

```
NMS 2.0 10/25/93 02:09:01
***************************************************************
                     INSTALL LOG FILE
   If you are unable to successfully install NMS due to an
   installation error, consult the NMS documentation and your
   network administrator.  If the problem cannot be resolved,
   contact Novell technical support and present this file.

***************************************************************
0 Initialize: S=J:\NMS\SETUP T=C:\WINDOWS
0 setDialogStringOptions: S=J:\NMS\SETUP T=C:\WINDOWS
0 DrawBitmap: S=J:\NMS\SETUP T=C:\WINDOWS
0 QueryTutorial: S=J:\NMS\SETUP T=C:\WINDOWS
**************** INSTALL OPTIONS *******************

  [ ] RUN TUTORIAL
  [X] INSTALL NMS

***************************************************
0 SetDLLName: S=J:\NMS\SETUP T=C:\WINDOWS
0 checkSystem: S=J:\NMS\SETUP T=C:\WINDOWS
0 ExecDLL: S=J:\NMS\SETUP T=C:\WINDOWS
  EXECUTING >>> J:\NMS\SETUP\instdll4.dll  ROUTINE=checkWindowsVersion
0 getInstallOptions: S=J:\NMS\SETUP T=C:\WINDOWS
0 doAgain: S=J:\NMS\SETUP T=C:\WINDOWS
0 ExecDLL: S=J:\NMS\SETUP T=C:\WINDOWS
  EXECUTING >>> J:\NMS\SETUP\instdll4.dll  ROUTINE=insNETXLoaded
**************** INSTALL OPTIONS ***************************

  [ ] TUTORIAL
  [ ] CONSOLE
  [ ] TCPIP
  [X] NETEXPLORER
  [X] NETEXPLORER PLUS
***************************************************************
0 MoveLogFile: S=J:\NMS\SETUP T=C:\WINDOWS
0 MoveLogFileReturn: S=J:\NMS\SETUP T=C:\WINDOWS
  TCP path =
  doTcpip=0
0 confirmNMM: S=J:\NMS\SETUP T=C:\WINDOWS
0 NoConsoleNMMFileTransfer: S=J:\NMS\SETUP T=C:\WINDOWS
0 SetDLLName: S=J:\NMS\SETUP T=C:\WINDOWS
5 explodeFiles: S=J:\NMS\SETUP T=C:\TEMP\NMSBIN
  DECOMPRESSING >>> instdlls._dl to C:\TEMP\NMSBIN
5 CopyFiles: S=J:\NMS\SETUP T=C:\TEMP\NMSBIN
  COPYING >>> *.dll to C:\TEMP\NMSBIN
5 CopyFiles: S=J:\NMS\SETUP T=C:\TEMP\NMSBIN
  COPYING >>> launch40.exe to C:\TEMP\NMSBIN
5 ExecDLL: S=J:\NMS\SETUP T=C:\TEMP\NMSBIN
  EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=stripNmsPath
5 SetDLLName: S=J:\NMS\SETUP T=C:\TEMP\NMSBIN
5 CreateCacheDirs: S=J:\NMS\SETUP T=C:\TEMP\NMSBIN
5 chkSnmpPath: S=J:\NMS\SETUP T=C:\TEMP\NMSBIN
5 chkSubDirs: S=J:\NMS\SETUP T=C:\TEMP\NMSBIN
5 chk312dir: S=J:\NMS\SETUP T=C:\TEMP\NMSBIN
5 chk40dir: S=J:\NMS\SETUP T=C:\TEMP\NMSBIN
5 chkSnpplusPath: S=J:\NMS\SETUP T=C:\TEMP\NMSBIN
5 chkDirFailed: S=J:\NMS\SETUP T=C:\TEMP\NMSBIN
5 cacheFilesToDisk: S=J:\NMS\SETUP T=C:\TEMP\NMSBIN
5 QueryProgramDisk: S=J:\NMS\SETUP T=C:\TEMP\NMSBIN
5 GuessNextDiskPath: S=J:\NMS\SETUP T=C:\TEMP\NMSBIN
  nDiskNum=11  Guessed DiskPath=J:\NMS\DISK11
10 CopyFiles: S=J:\NMS\DISK11 T=C:\TEMP\DSKCACHE\NETXPLOR
  COPYING >>> *.* to C:\TEMP\DSKCACHE\NETXPLOR
10 noSnpCache: S=J:\NMS\DISK11 T=C:\TEMP\DSKCACHE\NETXPLOR
10 QueryProgramDisk: S=J:\NMS\DISK11 T=C:\TEMP\DSKCACHE\NETXPLOR
10 GuessNextDiskPath: S=J:\NMS\DISK11 T=C:\TEMP\DSKCACHE\NETXPLOR
  nDiskNum=12  Guessed DiskPath=J:\NMS\NWSYSUPD
```

```
15 CopyFiles: S=J:\NMS\NWSYSUPD T=C:\TEMP\DSKCACHE\NWSYSUPD
  COPYING >>> *.* to C:\TEMP\DSKCACHE\NWSYSUPD
20 CopyFiles: S=J:\NMS\NWSYSUPD\311 T=C:\TEMP\DSKCACHE\NWSYSUPD\311
  COPYING >>> *.* to C:\TEMP\DSKCACHE\NWSYSUPD\311
25 CopyFiles: S=J:\NMS\NWSYSUPD\40 T=C:\TEMP\DSKCACHE\NWSYSUPD\40
  COPYING >>> *.* to C:\TEMP\DSKCACHE\NWSYSUPD\40
25 QueryProgramDisk: S=J:\NMS\NWSYSUPD T=C:\TEMP\DSKCACHE\NWSYSUPD\40
25 GuessNextDiskPath: S=J:\NMS\NWSYSUPD T=C:\TEMP\DSKCACHE\NWSYSUPD\40
  nDiskNum=13  Guessed DiskPath=J:\NMS\SNMP
30 CopyFiles: S=J:\NMS\SNMP T=C:\TEMP\DSKCACHE\NWSYSUPD\311
  COPYING >>> *.nlm to C:\TEMP\DSKCACHE\NWSYSUPD\311
35 CopyFiles: S=J:\NMS\SNMP\tcpip T=C:\TEMP\DSKCACHE\NWSYSUPD\311
  COPYING >>> *.nlm to C:\TEMP\DSKCACHE\NWSYSUPD\311
35 noSnmpCache: S=J:\NMS\SNMP\tcpip T=C:\TEMP\DSKCACHE\NWSYSUPD\311
35 savePrimConn: S=J:\NMS\DISK11 T=C:\TEMP
35 ExecServerDLL: S=J:\NMS\DISK11 T=C:\TEMP
  EXECUTING >>> C:\TEMP\NMSBIN\filesr40.dll  ROUTINE=savePrimaryConn
35 LaunchDLLOwner: S=J:\NMS\DISK11 T=C:\TEMP
35 Launch: S=J:\NMS\DISK11 T=C:\TEMP
  LAUNCHING >>> C:\TEMP\NMSBIN\launch40.exe
35 ExecServerDLL: S=J:\NMS\DISK11 T=C:\TEMP
  EXECUTING >>> C:\TEMP\NMSBIN\filesr40.dll  ROUTINE=loadAssistDll
35 savePrimConn: S=J:\NMS\DISK11 T=C:\TEMP
35 ExecServerDLL: S=J:\NMS\DISK11 T=C:\TEMP
  EXECUTING >>> C:\TEMP\NMSBIN\filesr40.dll  ROUTINE=savePrimaryConn
35 installSnooper: S=J:\NMS\DISK11 T=C:\TEMP
35 installSnpNLM: S=J:\NMS\DISK11 T=C:\TEMP
35 snploop1: S=C:\TEMP\DSKCACHE\NETXPLOR T=C:\TEMP
   Server Name = NMS20C◄   Server Version (x100) = 410◄   Retcode = 0
40 backupSnpNlms: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\NMDISK
45 BackupServerFiles: S=y:\SYSTEM T=y:\NETXPLOR.SAV
50 ExecDLL: S=y:\SYSTEM T=y:\NETXPLOR.SAV
  EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=fileExists
50 BackupFiles: S=y:\SYSTEM T=y:\NETXPLOR.SAV
  COPYING >>> autoexec.ncf to y:\NETXPLOR.SAV
50 BackupServerFiles: S=y:\SYSTEM T=y:\NETXPLOR.SAV
55 ExecDLL: S=y:\SYSTEM T=y:\NETXPLOR.SAV
  EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=fileExists
55 BackupFiles: S=y:\SYSTEM T=y:\NETXPLOR.SAV
  COPYING >>> nxpplus.nlm to y:\NETXPLOR.SAV
55 BackupServerFiles: S=y:\NMDISK T=y:\NETXPLOR.SAV
60 ExecDLL: S=y:\NMDISK T=y:\NETXPLOR.SAV
  EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=fileExists
60 BackupFiles: S=y:\NMDISK T=y:\NETXPLOR.SAV
  COPYING >>> netxplor.nlm to y:\NETXPLOR.SAV
60 BackupServerFiles: S=y:\NMDISK T=y:\NETXPLOR.SAV
65 ExecDLL: S=y:\NMDISK T=y:\NETXPLOR.SAV
  EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=fileExists
65 BackupFiles: S=y:\NMDISK T=y:\NETXPLOR.SAV
  COPYING >>> nxpip.nlm to y:\NETXPLOR.SAV
65 BackupServerFiles: S=y:\NMDISK T=y:\NETXPLOR.SAV
70 ExecDLL: S=y:\NMDISK T=y:\NETXPLOR.SAV
  EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=fileExists
70 BackupFiles: S=y:\NMDISK T=y:\NETXPLOR.SAV
  COPYING >>> nxpipx.nlm to y:\NETXPLOR.SAV
70 BackupServerFiles: S=y:\NMDISK T=y:\NETXPLOR.SAV
75 ExecDLL: S=y:\NMDISK T=y:\NETXPLOR.SAV
  EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=fileExists
75 BackupFiles: S=y:\NMDISK T=y:\NETXPLOR.SAV
  COPYING >>> nxplanz.nlm to y:\NETXPLOR.SAV
75 BackupServerFiles: S=y:\NMDISK T=y:\NETXPLOR.SAV
80 ExecDLL: S=y:\NMDISK T=y:\NETXPLOR.SAV
  EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=fileExists
80 BackupFiles: S=y:\NMDISK T=y:\NETXPLOR.SAV
  COPYING >>> nxpipx.ini to y:\NETXPLOR.SAV
85 installPlusFiles: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\NMDISK
85 CopyFiles: S=C:\TEMP\DSKCACHE\NWSYSUPD\40 T=y:\SYSTEM
  COPYING >>> nxpplus.nlm to y:\SYSTEM
90 copyNlmUpdates: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
95 CopyFiles: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
  COPYING >>> netxplor.ncf to y:\SYSTEM
95 CopyFiles: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
  COPYING >>> unxp.ncf to y:\SYSTEM
```

```
100 ExecDLL: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
  EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=UpdateNcf
100 ExecDLL: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
  EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=updateAuto
100 doNmsBase: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
100 doneReading: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
100 CopyFileFrom: S=y:\SYSTEM T=y:\SYSTEM
  COPYING >>> nmsbase.ncf to nmsbase.tmp
100 updateNcf: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
100 DeleteFiles: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
  DELETING >>> nmsbase.ncf
100 writeVersionLog: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
100 writeVersionLog: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
100 writeVersionLog: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
100 writeVersionLog: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
100 writeVersionLog: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
100 writeSpxs: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
100 writeIpxs: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
100 writeTli: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
100 writeMathlibc: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
100 DeleteFiles: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
  DELETING >>> nmsbase.tmp
100 resetConnection: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
100 ExecServerDLL: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
  EXECUTING >>> C:\TEMP\NMSBIN\filesr40.dll  ROUTINE=resetConnectionTable
100 ResetPrimaryConnection: S=C:\TEMP\DSKCACHE\NETXPLOR T=C:\TEMP
100 ExecServerDLL: S=C:\TEMP\DSKCACHE\NETXPLOR T=C:\TEMP
  EXECUTING >>> C:\TEMP\NMSBIN\filesr40.dll  ROUTINE=resetPrimaryConn
100 savePrimConn: S=C:\TEMP\DSKCACHE\NETXPLOR T=C:\TEMP
100 ExecServerDLL: S=C:\TEMP\DSKCACHE\NETXPLOR T=C:\TEMP
  EXECUTING >>> C:\TEMP\NMSBIN\filesr40.dll  ROUTINE=savePrimaryConn
100 installSnooperPlus: S=C:\TEMP\DSKCACHE\NETXPLOR T=C:\TEMP
100 installSnpplusNlm: S=C:\TEMP\DSKCACHE\NETXPLOR T=C:\TEMP
   Server Name = NMS20C◄   Server Version (x100) = 410◄   Retcode = 0
100 backupSnpPlusNlms: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\
100 BackupServerFiles: S=y:\SYSTEM T=y:\NXPPLUS.SAV
105 ExecDLL: S=y:\SYSTEM T=y:\NXPPLUS.SAV
  EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=fileExists
105 BackupFiles: S=y:\SYSTEM T=y:\NXPPLUS.SAV
  COPYING >>> autoexec.ncf to y:\NXPPLUS.SAV
105 BackupServerFiles: S=y:\SYSTEM T=y:\NXPPLUS.SAV
110 ExecDLL: S=y:\SYSTEM T=y:\NXPPLUS.SAV
  EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=fileExists
110 BackupFiles: S=y:\SYSTEM T=y:\NXPPLUS.SAV
  COPYING >>> nxpplus.nlm to y:\NXPPLUS.SAV
110 installPlusFiles: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
110 CopyFiles: S=C:\TEMP\DSKCACHE\NWSYSUPD\40 T=y:\SYSTEM
  COPYING >>> nxpplus.nlm to y:\SYSTEM
110 copyNlmUpdates: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
```

```
115 ExecDLL: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
  EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=UpdateNcf
115 doNmsBase: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
115 doneReading: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
115 CopyFileFrom: S=y:\SYSTEM T=y:\SYSTEM
  COPYING >>> nmsbase.ncf to nmsbase.tmp
115 updateNcf: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
115 DeleteFiles: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
  DELETING >>> nmsbase.ncf
115 writeVersionLog: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
115 writeVersionLog: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
115 writeVersionLog: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
115 writeVersionLog: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
115 writeVersionLog: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
115 writeSpxs: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
115 writeIpxs: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
115 writeTli: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
115 writeMathlibc: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
115 DeleteFiles: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
  DELETING >>> nmsbase.tmp
115 resetConnection: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
115 ExecServerDLL: S=C:\TEMP\DSKCACHE\NETXPLOR T=y:\SYSTEM
  EXECUTING >>> C:\TEMP\NMSBIN\filesr40.dll  ROUTINE=resetConnectionTable
115 ResetPrimaryConnection: S=C:\TEMP\DSKCACHE\NETXPLOR T=C:\TEMP
115 ExecServerDLL: S=C:\TEMP\DSKCACHE\NETXPLOR T=C:\TEMP
  EXECUTING >>> C:\TEMP\NMSBIN\filesr40.dll  ROUTINE=resetPrimaryConn
115 savePrimConn: S=C:\TEMP\DSKCACHE\NETXPLOR T=C:\TEMP
115 ExecServerDLL: S=C:\TEMP\DSKCACHE\NETXPLOR T=C:\TEMP
  EXECUTING >>> C:\TEMP\NMSBIN\filesr40.dll  ROUTINE=savePrimaryConn
12 ExecDLL: S=J:\NMS\SETUP T=y:\
  EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=UpdateNcf
12 ExecDLL: S=J:\NMS\SETUP T=y:\
  EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=updateAuto
12 ExecDLL: S=J:\NMS\SETUP T=y:\
  EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=checkForOldNmsbase
12 ExecDLL: S=y:\system T=y:\NMA.SAV
  EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=fileExists
15 ExecDLL: S=J:\NMS\SETUP T=y:\
  EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=UpdateNMSBASE_Ncf
17 ExecDLL: S=J:\NMS\SETUP\40 T=y:\system
  EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=CompareFilesDate
17 ExecDLL: S=y:\system T=y:\NMA.SAV
  EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=fileExists
20 ExecDLL: S=J:\NMS\nwsysupd\40 T=y:\system
  EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=CompareFilesDate
35 ExecDLL: S=J:\NMS\SNMP T=y:\system
  EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=CompareFilesDate
35 ExecDLL: S=J:\NMS\SNMP T=y:\system
  EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=CheckNetwareFiles
35 ExecDLL: S=J:\NMS\SNMP T=y:\ETC
  EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=fileExists
35 ExecDLL: S=J:\NMS\SNMP T=y:\ETC
  EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=fileExists
35 ExecDLL: S=J:\NMS\nma\40 T=y:\system
  EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=CompareFilesDate
42 ExecDLL: S=y:\system T=y:\NMA.SAV
  EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=fileExists
45 ExecDLL: S=J:\NMS\nma\40 T=y:\system
  EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=CompareFilesDate
```

```
52 ExecDLL: S=y:\system T=y:\NMA.SAV
   EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=fileExists
55 ExecDLL: S=J:\NMS\nma\40 T=y:\system
   EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=CompareFilesDate
55 ExecDLL: S=J:\NMS\nma\40 T=y:\system
   EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=CompareFilesDate
55 ExecDLL: S=J:\NMS\nma\40 T=y:\system
   EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=CompareFilesDate
62 ExecDLL: S=y:\system T=y:\NMA.SAV
   EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=fileExists
65 ExecDLL: S=J:\NMS\nma T=y:\system
   EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=CompareFilesDate
72 ExecDLL: S=y:\system T=y:\NMA.SAV
   EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=fileExists
75 upgradeFile: S=J:\NMS\nma T=y:\ETC
   Compare file=NWTRAP.CFG
75 ExecDLL: S=J:\NMS\nma T=y:\ETC
   EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=CompareFilesDate
75 ReplaceFile: S=J:\NMS\nma T=y:\ETC
85 backupReplacement: S=J:\NMS\nma T=y:\ETC
85 BackupServerFiles: S=y:\ETC T=y:\NXPPLUS.SAV
90 ExecDLL: S=y:\ETC T=y:\NXPPLUS.SAV
   EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=fileExists
90 CopyFiles: S=J:\NMS\nma T=y:\ETC
   COPYING >>> NWTRAP.CFG to y:\ETC
85 ExecDLL: S=J:\NMS\nma T=y:\ETC
   EXECUTING >>> C:\TEMP\NMSBIN\instdll4.dll  ROUTINE=checkForBinderyEmulation
85 ResetPrimaryConnection: S=y:\ETC T=Creating backup for existing NWTRAP.CFG ...
85 ExecServerDLL: S=y:\ETC T=Creating backup for existing NWTRAP.CFG ...
   EXECUTING >>> C:\TEMP\NMSBIN\filesr40.dll  ROUTINE=resetPrimaryConn
85 savePrimConn: S=y:\ETC T=Creating backup for existing NWTRAP.CFG ...
85 ExecServerDLL: S=y:\ETC T=Creating backup for existing NWTRAP.CFG ...
   EXECUTING >>> C:\TEMP\NMSBIN\filesr40.dll  ROUTINE=savePrimaryConn
85 InstallFinished: S=y:\ETC T=Creating backup for existing NWTRAP.CFG ...
85 WrapUp: S=y:\ETC T=Creating backup for existing NWTRAP.CFG ...
85 ExitOption: S=y:\ETC T=Creating backup for existing NWTRAP.CFG ...
85 noMsgBox: S=y:\ETC T=Creating backup for existing NWTRAP.CFG ...
85 cleanupAndExit: S=y:\ETC T=Creating backup for existing NWTRAP.CFG ...
```

A.7 NMSBASE.NCF

```
#-------------------------------------------------------------
#               Novell NetWare Management System
#                       Version 2.0
#
#-------------------------------------------------------------
# NMSBASE.NCF: NetWare Management System Base NCF file
#-------------------------------------------------------------
# Description: This NCF file loads all the NetWare 4.0
#              system components that are required by:
#
#              $VERSION LOG
#              $VERSION 1.0 NetWare LANalyzer Agent
#              $VERSION 1.5 Netware Management Agent NLM
#              $VERSION NMS 2.0 NetExplorer Plus NLM
#              $VERSION NMS 2.0 NetExplorer NLMs
#
#              You must load the NLMs in the top part of
#              your AUTOEXEC.NCF before you load any protocol
#              stacks (for example, load tcpip) or any network
#              adapter drivers (for example, load ne2000).
#-------------------------------------------------------------

# Step-1: Review the following NetWare system parameters
#         for the IPX network discovery NLM files.
#         Note that these are MINIMUM VALUES. If your NetWare
#         system requires larger values edit the following
#         lines to set the parameters to required values.
#
#$ENVIRONMENTAL VARIABLES
SET MAXIMUM PACKET RECEIVE BUFFERS=500
SET UPGRADE LOW PRIORITY THREADS = ON

# Step-2: Load the following NetWare system software
#         Do not change the order in which the NLM files
#         are loaded.

LOAD SYS:\SYSTEM\STREAMS
LOAD SYS:\SYSTEM\CLIB
LOAD SPXS LDFILE=SYS:\SYSTEM\IPXSPX.CFG
LOAD SYS:\SYSTEM\IPXS
LOAD SYS:\SYSTEM\TLI
LOAD SYS:\SYSTEM\MATHLIBC
```

A.8 NMA.NCF

```
#----------------------------------------------------------------
#                 Novell NetWare Services Manager
#                         Version 1.6
#----------------------------------------------------------------
# NMA.NCF: NetWare Management Agent NCF file
#----------------------------------------------------------------
# Description: This NCF file loads all the NetWare Management Agent
#              software for the NetWare 4.X. The following shows
#              the relationship between the the components loaded by this NCF
#              file. It also shows the dependencies of
#              these components on other system software.
#
#     RELATIVE
#     LOAD-ORDER  +----------------------------------+
#       1.        |    SOFTWARE  FROM  NMSBASE.NCF   |
#                 +----------------------------------+
#                           |        +--------------+
#       2.                  |        |   SNMP.NLM   |----+
#                           |        +--------------+    |
#                 +----------------------------------+   |
#       3.        |          NMAGENT2.NLM            |   |
#                 +----------------+--------+------+  |   |
#                 +--------------+ |        |      |  |   |
#       4.        | SIDEWIND.NLM | |        |      |  |   |
#                 +--------------+ |        |      |  |   |
#                 +--------------+ |        |      |  |   |
#       5.        | RATTLER.NLM  | |        |      |  |   |
#                 +--------------+ |        |      |  |   |
#                 +--------------+ |        |      |  |   |
#       6.        | SPAGENT.NLM  |--+       |      |  |   |
#                 +--------------+          |      |  |   |
#                                    +------+------+  |   |
#       7.                           |  NW2SNMP.NLM |----+
#                                    +--------------+  |   |
#                                    +--------------+  |   |
#       8.                           |  NWTRAP.NLM  |----+
#                                    +--------------+
#
#----------------------------------------------------------------

# Step-1: Load the NetWare Management Agent software.
LOAD SYS:\SYSTEM\NMAGENT2
LOAD SYS:\SYSTEM\SIDEWIND /N /xA0C8
LOAD SYS:\SYSTEM\SPAGENT

# Step-2: Load the NetWare to SNMP trap translator software.
#         OPTION: If you want to change the default community name
#                 of traps from PUBLIC, use COMMUNITY=<CommunityName>
#                 option with NW2SNMP.NLM and /C=<CommunityName>
#                 option with NWTRAP.NLM.  For example:
#                 load SYS:\SYSTEM\NW2SNMP COMMUNITY=administrator
#                 load SYS:\SYSTEM\NWTRAP /C=administrator
#

LOAD SYS:\SYSTEM\NW2SNMP GA=ON
LOAD SYS:\SYSTEM\NWTRAP
```
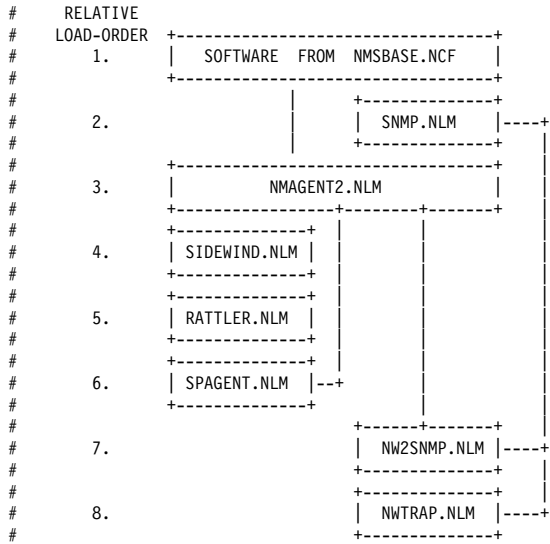
A.9 NETXPLOR.NCF

```
#-----------------------------------------------------------------------------
#                Novell NetWare Management System
#                          Version 2.0
#-----------------------------------------------------------------------------
# NETXPLOR.NCF: NetExplorer NCF File
#
# WARNING:   You should not modify this file unless you need to change
#            one of the configuration parameters documented below.
#            Other changes to this file are not recommended.
#-----------------------------------------------------------------------------
# MODULE DEPENDENCIES
#
# NETXPLOR.NLM  -    STREAMS.NLM SPXS.NLM IPXS.NLM CLIB.NLM TLI.NLM
#                    MATHLIBC.NLM.
# NXPIP.NLM     -    STREAMS.NLM SPXS.NLM IPXS.NLM CLIB.NLM TLI.NLM
#                    MATHLIBC.NLM TCPIP.NLM and SNMP.NLM.
# NXPIPX.NLM    -    STREAMS.NLM SPXS.NLM IPXS.NLM CLIB.NLM TLI.NLM
#                    MATHLIBC.NLM NXPMEM.NLM and SNMP.NLM.
# NXPLANZ.NLM   -    STREAMS.NLM SPXS.NLM IPXS.NLM CLIB.NLM TLI.NLM
#                    MATHLIBC.NLM NXPMEM.NLM TCPIP.NLM and SNMP.NLM.
#
# LOAD ORDER
#
# The order in which the NetExplorer modules are loaded is critical. You
# must follow the same order as listed in this file. Loading NXPIP.NLM
# and NXPLANZ.NLM are optional. For best results, load NXPIP.NLM if your
# internet uses IP, and load NXPLANZ.NLM if you are running NetWare LANalyzer
# Agents or LANtern network monitors.
#
# Load Parameter Description
#
# LOAD SYS:\NMDISK\NETXPLOR /B count
#
# NETXPLOR.NLM module is a repository for topology data. It receives data
# from the discovery modules (NXPIP, NXPIPX, and NXPLANZ) and
# transmits this data to the NetExplorer Manager on request. This module
# must be loaded before any of the other discovery  modules are loaded.
#
# /B count     This optional parameter specifies the maximum number of
#              backups of NETXPLOR.DAT (the NetExplorer data file) that
#              NETXPLOR.NLM can store at any time. The backup copies
#              are stored in SYS:\NMDISK\DATSAV directory. The range
#              is between 0 and 999 inclusive. A 0 indicates no backup
#              copies of NETXPLOR.DAT are made; consequently, repeated
#              execution of the discovery modules overwrites the
#              previous NETXPLOR.DAT file.
#
#              Default: 0 copies if /B option is not used.
#
```

```
# LOAD SYS:\NMDISK\NXPIP /C filename /B /S xxx.x.x.x
#
# NXPIP.NLM module discovers the topology of IP networks. This module
# requires TCPIP.NLM and SNMP.NLM to be loaded.
#
# /C filename   This parameter allows you to specify a file containing
#               a list of SNMP community strings to be used for
#               communicating with IP devices. This file should be
#               placed in the SYS:\NMDISK directory. Each community string
#               must be specified as a separate line in the file.
#               The following is a sample of the community file:
#               _____
#               | public
#               | administrator
#
#               The default is no community file - NXPIP uses the
#               community name "public".
#
# /B            This parameter uses a RIP broadcast to discover the local router
#
# /S xxx.x.x.x  This parameter specifies the IP address of the router that will
#               be used to discover other IP routers.
#
# NOTE:         NXPIP.NLM can be forced to discover only specific networks.
#               This is done by specifying the network addresses of the
#               networks that need to be discovered in the SYS:\NMDISK\NXPIP.INI
#               file. If the file does not exist, the entire IP network, as
#               defined by the class of the IP network number will be discovered
#               For example, if the server's IP address is 133.33.65.100,
#               NXPIP discovers networks with network address 133.33.xx.xx.
#               The following is a sample of the NXPIP.INI file:
#               _____
#               | 11.0.0.0
#               | 130.57.0.0
#               | 200.5.7.0
#
# LOAD SYS:\NMDISK\NXPIPX
#
# NXPIPX.NLM module discovers the topology of IPX networks. The file
# SYS:\NMDISK\NXPIPX.INI specifies the initialization parameters
# associated with this module.
#
# LOAD SYS:\NMDISK\NXPLANZ /N /O /C filename
#
```

```
# NXPLANZ.NLM module discovers NetWare LANalyzer agents and LANtern
# network monitors. This module requires TCPIP.NLM and SNMP.NLM to be loaded.
#
# /N           This parameter disables station discovery. This option, when
#              used discovers only NetWare LANalyzer Agent servers or
#              LANtern network monitors.
#
#              Default: Station discovery is enabled.
#
# /O           This parameter runs NXPLANZ discovery once and
#              then terminates.
#
#              Default: NXPLANZ discovery is continuous.
#
# /C filename  This parameter allows you to specify a file containing a list
#              of SNMP community strings to be used for communicating with
#              NetWare LANalyzer Agents. This file should be placed in the
#              SYS:\NMDISK directory. Each community string must be specified
#              as a separate line in the file. The following is a sample of
#              the community file:
#              _____
#              | public
#              | administrator
#
#              The default is no community file - NXPLANZ uses the
#              community name "public".
#
# NOTE:        To discover NetWare LANalyzer Agents via IP (on networks that
#              do not route IPX), you must enter the IP address of the agent
#              in the file SYS:\NMDISK\NLA.ADR. Also, you must enter the IP
#              address of all LANtern network monitors in this file. You may
#              also enter the internal IPX network number of NetWare LANalyzer
#              Agents in this file only if your internetwork contains SAP
#              filtering and you are not running NXPIPX. The prototype file
#              is as follows:
#              _____
#              | #                                               |
#              | # SYS:\NMDISK\NLA.ADR                           |
#              | #                                               |
#              | # '#' identifies a comment                      |
#              | # Each line describes a single NetWare LANalyzer |
#              | # Agent or LANtern network monitor and is as    |
#              | # follows:                                      |
#              | # <IP Address | IPX Network Number>,[<Name>],<S|L>|
#              | # where:                                        |
#              | # IP Address - the IP node address of the agent |
#              | # IPX Number - the internal network number of a |
#              | #              a NetWare LANalyzer Agent server  |
#              | # Name - an optional name of the agent          |
#              | # S - Server, a NetWare LANalyzer Agent         |
#              | # L - LANtern, a LANtern network monitor        |
#              | #                                               |
#              | 127.1.2.3,LANtern-XYZ,L                         |
#              | 127.4.5.6,SERVER-JUPITER,S                      |
#              | 12345678,SERVER-VENUS,S                         |
#              | 11111111,,S                                     |
#              |_____|
#--------------------------------------------------------------------------
SEARCH ADD SYS:\NMDISK

LOAD SYS:\NMDISK\NETXPLOR /B 2

LOAD SYS:\NMDISK\NXPIP /c comm.dat /b /s 9.24.104.1

LOAD SYS:\NMDISK\NXPIPX

#LOAD SYS:\NMDISK\NXPLANZ
```

A.10 NXPIPX.INI

```
REM  -----------------Do not change the following lines----------------------


REM  ********************************************************
REM     NOVELL's NETWARE MANAGEMENT SYSTEM (NMS) INI FILE
REM  ********************************************************


REM  ********************************************************
REM                    NMS DEBUG SECTION
REM  ********************************************************
REM   The following is to be used only for technical support
REM   reasons.  NSM will enable you create debugging files
REM   which can then be sent to Novell with some of your
REM   problem report.


REM  To run NXPIPX.NLM enter:
REM
REM           LOAD  NXPIPX [input file]
REM
REM           eg.  LOAD  NXPIPX  sys:snoop/nxpipx.ini
REM
REM
REM  All switches are specified in the input file.  If no input file is
REM  specified, default values are used.


REM  To generate normal logging, it is recommended to set the options as
REM  follow:
REM           gMode = 3
REM           gLevel = 2
REM           gConsole = 1
REM           gDisplay = 1
REM           gLogFileName =


REM  The NXPIPX command line switches are optional.
REM  Valid NXPIPX command line switches (must be in order) are:
REM
REM           debug output switch (gMode)
REM           debug level switch (gLevel)
REM           console switch (gConsole)
REM           data switch (gDisplay)
REM           log file name switch (gLogFileName)
REM           log file count switch (gLogFileCount)
REM           log file size switch (gLogFileSize)
REM
REM           auto discovery switch (gAutoDiscovery)
REM           report swtich (gReport)
REM           report log swtich (gReportLog)
REM           standalone switch (gStandAlone)
REM           ipc server switch (gIpcServerName)
REM           Minimum retry switch (gMinRetry)
REM           Maximum retry switch (gMaxRetry)
REM           timeout pad switch (gTimeOutPad)
REM           timeout switch (gMinTimeOut)
REM           display instrumentation switch (gInstrument)
REM           performance switch (gPerform)
REM
REM           display networks switch (gDE_NETWORKS)
REM           display stations per network switch (gDE_NETWORK_STATIONS)
REM           display stations with objects switch (gDE_STATION_OBJECTS)
REM           display routers switch (gDE_ROUTERS)
REM           display workstations switch (gDE_WORKSTATIIONS)
REM           display overall summary switch (gDE_REPORTS)
REM
REM           standalone test switch (gStandAloneTest)
REM           playback switch (gPlayback) (not operational yet)
REM           fixed timeout switch (gFixTimeOut)
REM
REM           test node address switch (gTestData)
REM
```

```
REM
REM  Debug Output Switch (gMode)
REM
REM          1  --  output to log file and screen
REM          2  --  output to screen (default)
REM          3  --  output to log file
REM
REM
REM  Debug Level Switch (gLevel)
REM
REM          Type of outputs are:
REM
REM                  object
REM                  debug
REM                  hex
REM                  entry/exit
REM
REM          Combination of levels are:
REM
REM                  object  debug   hex     entry/exit
REM
REM          0       no      no      no      no              (default)
REM          1       yes     yes     yes     yes
REM          2       yes
REM          3       yes     yes
REM          4       yes             yes
REM          5       yes                     yes
REM          6       yes     yes     yes
REM          7       yes     yes             yes
REM          8       yes             yes     yes
REM          9               yes
REM          10              yes     yes
REM          11              yes             yes
REM          12              yes     yes     yes
REM          13                      yes
REM          14                      yes     yes
REM          15                              yes
REM
REM
REM  Console Switch (gConsole)
REM
REM          0  --  no output to console
REM          1  --  output to console (default)
REM
REM
REM  Data Switch (gDisplay)
REM
REM          Type of data are:
REM
REM                  progress data
REM                  informational data
REM                  object data
REM
REM          Combination of data are:
REM
REM                  progress  information  object
REM          0       no        no          no        (default)
REM          1       yes       yes         yes
REM          2       yes
REM          3       yes       yes
REM          4       yes                   yes
REM          5                 yes
REM          6                 yes         yes
REM          7                             yes
REM
REM          To display/log object data after each cycle, make sure gLevel is
REM          enabled to display/log object.
REM          To display ESC message when unload, gDisplay has to be set > 0.
```

```
REM
REM
REM  Log File Name Switch (gLogFileName)
REM
REM          The default file name is "sys:nmdisk/ipx".
REM          If debug output switch is set to either 1 or 3, specification of
REM          log file name is required.  The log file name should contain
REM          volume, directory, and file name.  The file name portion should
REM          be no longer than 5 characters because the last 3 characters are
REM          used for file counter.  If only file name is specified, log files
REM          will be created on the working directory.  Use backslash (/) to
REM          separate directory and file name.  If log file is specified on
REM          directory that does not exist, no log file will be created.
REM
REM          eg.  sys:snoop/ipx
REM
REM
REM  Log File Count Switch (gLogFileCount)
REM
REM          1    --  min. file count before recycling
REM          999  --  max. file count before recycling (default)
REM
REM
REM  Log File Size Switch (gLogFileSize)
REM
REM          100000  --  min. file size (default)
REM          600000  --  max. file size
REM
REM          Each discovery cycle will start with a new set of log files.
REM
REM
REM  Auto Discovery Switch (gAutoDiscovery)
REM
REM          Type of discoverys are:
REM
REM                  server
REM                  router
REM                  workstation
REM
REM          Combination of discoverys are:
REM
REM                  server  router  workstation
REM          0       no      no      no
REM          1       yes     yes     yes                     (default)
REM          2       yes
REM          3       yes     yes
REM          4       yes             yes
REM          5               yes
REM          6               yes     yes
REM          7                       yes
```

```
REM
REM
REM  Report Switch (gReport)
REM
REM          0  --  do not generate packet to SLAVE
REM          1  --  generate packet to SLAVE (default)
REM
REM
REM  Report Log Switch (gReportLog)
REM
REM          0  --  do not log packet that is sent to SLAVE (default)
REM          1  --  log packet that is sent to SLAVE
REM
REM
REM  StandAlone Switch (gStandAlone)
REM
REM          0  --  run with Slave (default)
REM          1  --  run once by itself, faking communication with Slave
REM          2  --  run continuously by itself, faking communication with Slave
REM
REM
REM  IPC Server Switch (gIpcServerName)
REM
REM          " "  --  use the first SAP as IPC server (default)
REM          "x"  --  use this name as IPC server name
REM
REM
REM  Minimum Retry Switch (gMinRetry)
REM
REM          2  --  minimum poll twice for response (default)
REM          n  --  poll n times for response, and timeout for each
REM                 subsequent retry is set to original timeout;
REM                 n is set >= 1
REM
REM
REM  Maximum Retry Switch (gMaxRetry)
REM
REM          10 --  maximum poll ten times for response (default)
REM          n  --  poll n times for response, and timeout for each
REM                 subsequent retry is set to original timeout;
REM                 n is set >= gMinRetry
REM
REM
REM  TimeOut Pad switch (gTimeOutPad)
REM
REM
REM          10000  --  10000 milliseconds padding for the time out that can
REM                     be determined (default)
REM          n      --  n milliseconds padding for the time out that can be
REM                     determined; n is set >= 5000
REM
REM
REM  TimeOut Switch (gMinTimeOut)
REM
REM          60000  --  60000 milliseconds before time out on waiting for
REM                     response if time out cannot be determined (default)
REM          n      --  n milliseconds before time out on waiting for
REM                     response if time out cannot be determined
REM
REM
REM  Display Instrumentation Switch (gInstrument)
REM
REM          300000 --  300000 millisecond before display/log
REM                     instrumentation periodically (default)
REM          n      --  n milliseconds before display/log instrumentation
REM                     periodically
```

```
REM
REM
REM  Performance Switch (gPerform)
REM
REM          0  --  using more CPU in percentage (default)
REM          1  --  using less CPU in percentage
REM
REM
REM  Display Networks Switch (gDE_NETWORKS)
REM
REM          0  --  do not display summary of networks (default)
REM          1  --  display summary of networks
REM
REM
REM  Display Stations Per Network Switch (gDE_NETWORK_STATIONS)
REM
REM          0  --  do not display stations by network (default)
REM          1  --  display stations by network
REM
REM
REM  Display Stations With Objects Switch (gDE_STATION_OBJECTS)
REM
REM          0  --  do not display station with objects
REM          1  --  display station with objects (default)
REM
REM
REM  Display Routers Switch (gDE_ROUTERS)
REM
REM          0  --  do not display routers info
REM          1  --  display routers info (default)
REM
REM
REM  Display WorkStations Switch (gDE_WORKSTATIONS)
REM
REM          0  --  do not display workstation list
REM          1  --  display workstation list (default)
REM
REM
REM  Display Overall Summary Switch (gDE_REPORTS)
REM
REM          0  --  do not display overall summary
REM          1  --  display overall summary (default)
REM
REM
REM  StandAlone Test Switch (gStandAloneTest)
REM
REM          0  --  global config discovery (default)
REM          1  --  local server config discovery
REM          2  --  specific remote server config discovery
REM          3  --  local workstation config discovery
REM          4  --  specific remote workstation config discovery
REM          5  --  local server detail config discovery
REM          6  --  specific remote server detail config discovery
REM          7  --  specific workstation detail config discovery
REM          8  --  specific server status monitoring
REM
REM  Playback Switch (gPlayback) (not operational yet)
REM          0  --  uses normal discovery process (default)
REM          1  --  generates discovery by reading from a log file
REM
REM
REM  Fixed TimeOut Switch (gFixTimeOut)
REM          0  --  uses dynamic timeout (default)
REM          1  --  uses fixed timeout from the value of TimeOut Switch
REM
REM  Test Node Address Switch (gTestData)
REM
REM          gTestData is an array of char separated by a dash;
REM          the first 4 bytes is usually for network address of the node;
REM          the next 6 bytes is usually for node address of the node;
REM          the last 4 bytes depends on the specific test case;
REM
REM          0-0-0-0-0-0-0-0-0-0-0-0-0-0  --  specify the address of the
REM                                          node in the test case  (default)
REM
REM  Test Node Name Switch (gTestServerName)
REM          " "  --  no server name (default)
REM          "x"  --  specific server name
REM  ----------------Do not change the above lines--------------------------
```

```
IPXQNET=00000009
IPXQNET=0000BEEF
IPXQNET=00032211
IPXQNET=2FC38833
IPXQNET=2FE8582A
IPQXNET=87654321


REM  To specify the option, remove 'REM' and change the value after
REM  the '='.
REM  Spacing before and after '=' is required for processing.
REM  Refer to the above section for the support value of each option.
REM
REM  Default settings are:
REM
REM gMode = 2
REM gLevel = 0
REM gConsole = 1
REM gDisplay = 0
REM gLogFileName = sys:nmdisk/ipx
REM gLogFileCount = 999
REM gLogFileSize = 100000
REM
REM gAutoDiscovery = 1
REM gReport = 1
REM gReportLog = 0
REM gStandAlone = 0
REM gIpcServerName =
REM gMinRetry = 2
REM gMaxRetry = 10
REM gTimeOutPad = 10000
REM gMinTimeOut = 60000
REM gInstrument = 300000
REM gPerform = 0
REM
REM gDE_NETWORKS = 0
REM gDE_NETWORK_STATIONS = 0
REM gDE_STATION_OBJECTS = 1
REM gDE_ROUTERS = 1
REM gDE_WORKSTATIONS = 1
REM gDE_REPORTS = 1
REM
REM gStandAloneTest = 0
REM gPlayback = 0
REM gFixTimeOut = 0
REM
REM gTestData = 0-0-0-0-0-0-0-0-0-0-0-0-0-0
REM gTestServerName =
REM
```

A.11 NXPIP.INI

```
9.24.104.0
9.24.96.0
9.24.97.0
```

A.12 NWADMIN.INI

```
[Snapin View DLLs]
NWBRWS=NWBRWS.DLL

[Snapin Object DLLs]

[Browser Preferences]
Filters=none
Confirmations=Move, Delete
Scope=Any
```

A.13 NMS.INI

```
;********************************************************
;   NOVELL's NETWARE MANAGEMENT SYSTEM (NMS) INI FILE
;         NetWare Management System Version 2.1
;********************************************************

[global]
;********************************************************
;              SYSTEM WIDE GLOBALS
;********************************************************

; G.0: Absolute Path Name of the root of the NMS product
Root=e:\NMS\

; G.1: Absolute Path Name of the NMS Database Directory
DataPath=e:\NMS\nmsdb
EmptyDBPath=e:\NMS\EmptyDB

; G.2: Absolute Path Name of the NMS Windows HLP files
HelpPath=e:\NMS\help

; G.3: CUSTOMIZATION BOX in the Sign-On Screen and About box
;       If you change the following message-lines make sure
;       each line is not more that 40 characters wide.
CustomMsg1=For information about what to do after installation,
CustomMsg2=select Help > Procedures and choose the topic
CustomMsg3="Getting Started After Installation."

; G.4: Automatic registration for Alarms from NetWare Servers
;       NMS uses Service-Advertising Protocol (SAP) to register
;       with all the NetWare SNMP Agents to put this NMS Console
;       on the Alarm Notification List. Subsequently, all the
;       NetWare Server alarms (which are SNMP/IPX Traps) will be
;       forwarded to your console. Enter 1 to enable or 0 to disable.
SapBroadcast=1

; G.5: Connectivity test
PingOnceTimeout=2
PingOnceRetries=2

; G.6: Program Group Name
NMS Program Group Name=Novell-NMS
ProductVersion=NetWare Management System v2.10 ( 5/23/95 03:06:00 )
CloseAllNMSComponents=1

[map]
```

```
;********************************************************
;        NETWARE MANAGEMENT SYSTEM CONSOLE TASK
;********************************************************

; A. NMS CONSOLE GLOBAL OPTIONS:
;==============================
;-----------------Do not change the following lines---------------------
AutoExecute=snmpsrv,n-shell alarmmanager
Modules=nmm,nsm,dds,rmon,rsm,hsm,SFT3,nma,oldnma,IPXWS,IPWS,UnixWare,Printer,nmsaamgr,nwconn,netxplor
RunModules=nmm,nsm,hsm,rsm,rmon,dds,SFT3,nma,oldnma,IPXWS,IPWS,UnixWare,Printer,nmsaamgr,nwconn,netxplor
DllPath=e:\NMS\bin
OlfPath=e:\NMS\olf
AppIcon=e:\NMS\bin\map.ico
RemoveUnusedMenu=1
AppType=map
AppTitle=NetWare Management System
SBTextPointSize=13
SBTickTapeTimerInterval=3
SBAnimationTimerInterval=3
SBField1=n-resdll,BS_ANIMATEDICON,1,1
SBField2=n-eventlog,BS_TICKERTAPE,1,1,40
SBField3=n-resdll,BS_ICON,1,1,431
SBField4=map,BS_CURRENTDATE,1,1
SBField5=map,BS_CURRENTTIME,1,1
;-----------------Do not change the above lines---------------------

[alarmmanager]
;********************************************************
;                    ALARM-MANAGER TASK
;********************************************************
; A. ALARM-MANAGER GLOBAL OPTIONS:
;================================
;-----------------Do not change the following lines---------------------
AutoExecute=n_strsap
DllPath=e:\NMS\bin
DllFiles=n-evmgr
AppType=background
AppTitle=Alarm Manager
AppIcon=e:\NMS\bin\alarmmgr.ico
EIModuleNames=n_aisnmp,n-smgrei,n_rsmei
; Number of milliseconds Alarm Manager waits between logging alarms
IntervalBetweenLogging=10000
AppInfoDll=n-evmgr.dll
AppInfoProc=ALMAboutBoxInfo
;-----------------Do not change the above lines---------------------
```

```
[snmp]
;*****************************************************
;                    SNMP MIB BROWSER OPTIONS
;*****************************************************
; A.1: Location of the compiled SNMP MIBs. To compile
;       SNMP MIBs they have to be in "concise mib format".
;       Use the mibc.exe compiler which is part of NMS.
MIBFILE=e:\NMS\bin\snmpmibs.bin
MIBPATH=e:\NMS\snmpmibs\current
MIBPROFILES=e:\NMS\SNMPMIBS\PROFILES
;
; A.2: Global Preference for SNMP Options.
;       Time-out (in seconds) - default=10
;       Retries - default=1
;       Community string for Get request (max length=64 chars) - default = public
;       Community string for Set request (max length=64 chars) - default = public
;
SNMPTIMEOUT=10
SNMPRETRIES=1
GetCommunityString=public
SetCommunityString=public
DllPath=e:\NMS\bin
ALLMIBS=e:\NMS\snmpmibs\allmibs
TRAPMIBPATH=e:\NMS\snmpmibs\current


[netexplorer]
;*****************************************************
;                    NETEXPLORER-MANAGER TASK
;*****************************************************
; A. NETEXPLORER MANAGER GLOBAL OPTIONS:
;-----------------Do not change the following lines---------------------
DllPath=e:\NMS\bin
DllFiles=n-snoopr,n-ipclnt,n_lsmmgr
AppType=background
AppTitle=NetExplorer Manager
AppIcon=e:\NMS\bin\netxplor.ico
DupMac1=AA0004
DupMac2=0000A2
DupMac3=000000
AppInfoDll=n-snoopr.dll
AppInfoProc=NXPAboutInfo


;-----------------Do not change the above lines---------------------

; B.1: Enter the name of the NetWare server running the
;       Autodiscovery NLMs. Note that you can connect to the
;       same NetWare Server running Autodiscovery NLMs from
;       several NMS Consoles.
SPX Slave Server=NMS21

RunContinually=1
RuleFiles=rmonserv,lantern,n-sft3io,n-sft3ms,nma,oldnma,n-ipxws,n_ipws,n-unixwa,n_print,n_iprint,n-nwsaa,n-nwconn,n_nxp
transid.lanz=0
IP TransID=23
Current TransID=32
IP Router Sequence Number=1
Current Unnum IPX=1
Segment Consolidation Level=1
```

```
[debug]
;*******************************************************
;                   NMS DEBUG SECTION
;*******************************************************
; The following section is to be used only for technical support
; reasons. NMS will enable you to create debugging files which can
; then be sent to Novell with some of your problem report.

; A.1: LOGGING TO FILE:
; ---------------------
; To create a database log file, set DBFileLog=1.  NMS will generate
; the database log files and place them under the directory with the
; Pathname field.  You can control the size of each database log file
; using the DBFilesize field and entering the value in bytes.  The DBNumfiles
; parameter will enable you to ensure that database log files will
; never exceed the specified number.  NMS will wrap around to the first debug
; file after it reaches the maximum file count.
; To create error and trace debugging files, set the ErrorFileLog=1 and
; TraceFileLog=1. The NMS will generate debug files and place
; them under the directory with the Pathname field. You can control
; the size of each debug file by the Filesize field by entering the value
; in bytes. The Numfiles parameter will enable you to ensure that
; debug files never exceed these numbers. NMS will wrap around to
; the first debug file after it reaches the maximum file count.
DBFileLog=1
ErrorFileLog=0
TraceFileLog=0
Pathname=e:\NMS\logfiles
DBFilesize=10000
DBNumfiles=5
Filesize=1000000
Numfiles=99

; A.2: LOGGING TO DEBUG WINDOW:
; ----------------------------
; NMS will create a table window which will display the debugging
; information. The table window is independent of all the NMS tasks and
; can be closed at any time without affecting the running NMS tasks.
; Set the following lines to 1 to enable this debug window.
DBWinLog=0
ErrorWinLog=0
TraceWinLog=0

; A.3: LOGGING TO AUXILIARY CONSOLE:
; ---------------------------------
; If you have an auxiliary monitor attached to your system, then you can
; display all the debugging information.
DBAuxLog=0
ErrorAuxLog=0
TraceAuxLog=0

; A.4: TIME & DATE FLAG:
; ---------------------
; Set this to 1 to see Time and Date with each line of debug information.
Timeformat=1


[nmm]
; *******************************************************
;                 NETWARE MANAGEMENT MAP
; *******************************************************
DllFiles=n-mex,n_locmap,n_ilm,n_elm,n_fas,n-evlog,n-nmping,n-config,n-snmpui,n_secure,n_cob,n_aldisp,n_alrep,n_snpdaq
OlfFiles=n_locmap,n_ilm,n_elm,n_fas,n-evlog,n-ipxpng,n-ipping,n-config,n-cfg2,n-snmpui,n_secure,n-snmpxx,n_aldisp,n_alrep,n_fas2
ProductVersion=NetWare Management Map v2.10 ( 5/23/95 03:06:00 )
HelpFile=nms.hlp
WallPaperPath=e:\NMS\wallpapr
IconPath=e:\NMS\icons
GrayIconPath=e:\NMS\icons\gray
PicturePath=e:\NMS\pictures
```

```
; A. CUSTOM MAP OPTIONS:
;==========================
; A.1: ASIS/Minimize/Close the Custom Map window whenever link/goto
;       another map.
;       Enter 0 to keep window as is
;       Enter 1 to minimize the window
;       Enter 2 to close the window
Custom Map Action On Link or Goto=0
; A.2: background color of the Custom map window (changeable only
;       by the Configure>>Set Color... menu item of NMS Console).
Custom Map background color=16777215
; A.3: Each object (icon) bounding width in term of pixels.
;       More text is shown as the width grows larger.
;       Minimum value is 64 and maximum value is 300.
;       Default value is large enough to fit a MAC address.
Custom Map Horizontal Object Spacing=

; A.4: This option forces the icon object name to be truncated
;       to fit the horizontal object spacing specified in A.3 above.
;       1 to force the truncation.
;       0 to move the remaining text to the next line; default selection.
Custom Map Truncate Object Name=0

; B. ALARM-MONITOR OPTIONS:
;==========================
; B.1: option to show buttons with PIE charts (1=yes, 0=no)
EVShowPieButtons=1

; B.2: index to the global status bar field
EventLogAnimatedField=0
EventLogTickerField=1
```

```
; C. INTERNETWORK MAP OPTIONS:
;========================
; C.1: Reduces the Internetwork Map window to an icon whenever opening
;       a segment icon.
;       Enter 0 to not minimize
;       Enter 1 to minimize
;       Enter 2 to close
Internetwork Map Action On Opening ELM=0
; C.2: Background color of the Internetwork Map window (changeable only
;       by the Configure>>Set Color... menu item of NMS Console).
Internetwork Map background color=15269887
; C.3: Option to snap all the ICONs on the Internetwork Map to grid.
;       Enter 0 to snap to grid (default) or 1 to not-snap to grid.
Internetwork Map Do Not SnapToGrid=0
; C.4: Option to show the elbow style links between objects in the Internetwork
;       Map as opposed to the diagonal style links
;       Enter 1 to use Elbow Tree Style or
;            0 to use Connected Graph Diagonal Style
Internetwork Map Presentation Style=1
; C.5: Option to show the internetwork map when NMS starts up
;       Enter 1 to start up internetwork map
;            0 to not start up internetwork map
Start Internetwork Map=0
; C.6: This key saves the anchor id when 'View > Set Anchor'
;       menu command is requested.
;       0 means use the default algorithm which is the island
;       that has the most objects connected; otherwise it uses
;       the database id of the last saved anchor object id.
Internetwork Map Anchor=0
; C.7: This option forces the icon object name to be truncated
;       to fit the horizontal object spacing specified in C.8 below.
;       1 to force the truncation.
;       0 to move the remaining text to the next line; default selection.
Internetwork Map Truncate Object Name=0
; C.8: Each object (icon) spacing is in term of pixels.
;       More text is shown as the width grows larger.
;       Minimum value is 64 and maximum value is 300.
;       Default value is 4 times system icon size, which is 128.
Internetwork Map Horizontal Object Spacing=
; C.9: Each object (icon) spacing is in term of pixels.
;       More space is given in between objects per row
;       as the height grows larger.
;       Minimum value is 85 and maximum value is 300.
;       Default value is 3 times system icon size, which is 96.
Internetwork Map Vertical Object Spacing=
; C.10&cololon.Option to update the internetwork map automatically when user
;       changes a DB object.
;       Enter 1 - update internetwork map
;            0 - don't update internetwork map
Internetwork Map Update Object=1
```

```
; D. SEGMENT MAP OPTIONS:
;=======================
; D.1: Width of the Segment by number of icons horizontally.
Segment Map width=
; D.2: Height of the Segment by number of icons Vertically. Note that
;       by limiting the height, the segment will be broken into pieces
;       with each segment end-point ending with a number.
Segment Map height=
; D.3: Background color of the Segment Map window (changeable only
;       by the Configure>>Set Color... menu item of NMS Console).
Segment Map background color=8454143
; D.4: Each object (icon) spacing is in term of pixels.
;       More text is shown as the width grows larger.
;       Minimum value is 64 and maximum value is 300.
;       Default value is large enough to fit a MAC address.
Segment Map Horizontal Object Spacing=
; D.5: Each object (icon) bounding height in term of pixels.
;       More space is given in between objects per row
;       as the height grows larger.
;       Minimum value is 85 and maximum value is 300.
;       Default value is 3 times system icon size, which is 96.
Segment Map Vertical Object Spacing=
; D.6: This option forces the icon object name to be truncated
;       to fit the horizontal object spacing specified in D.4 above.
;       1 to force the truncation.
;       0 to move the remaining text to the next line; default selection.
Segment Map Truncate Object Name=0
; D.7: Option to update the segment map automatically when user
;       changes a DB object.
;       Enter 1 - update segment map
;             0 - don't update segment map
Segment Map Update Object=1

; E. FIND-ARRANGE-SEARCH SERVICE OPTIONS:
;======================================
; E.1: Maximum objects that FAS will attempt to locate
Find Max=800

; F. ALARM MONITOR OPTION:
;=======================
; F.1: Automatically start alarm monitor when NMS management station starts
;       set 1 means auto start
;       set 0 means do not auto start
StartAlarmMonitor=1

; G. Edit> Database Object OPTIONS:
;    Edit> Add OPTIONS:
;=================================
```

```
INNReq1=NetWare Server
INNReq2=NetWare Management Agent
INNReq3=NetWare LANalyzer Agent
INNReq4=Hub: HMI
INNReq5=SFTIII: MS Engine
INNReq6=SFTIII: IO Engine

INNOption1=Router: IPX

ESList1_1=SFTIII: MS Engine
ESList1_2=SFTIII: IO Engine

ESList2_1=NetWare LANalyzer Agent
ESList2_2=LANtern

;----------------Do not change the above lines---------------------
[SubSNMPAIModules]
DllPath=e:\NMS\bin
SubSNMPAIModuleCount=3
;;; RMON alarms
SubSNMPAIModule1=n_lsmais
SubSNMPAIID1=1.3.6.1.2.1.16
;;; Dead station alarms from LANtern
SubSNMPAIModule2=n_lsmais
SubSNMPAIID2=1.3.6.1.4.1.23.1.1.3
;;; Dead station alarms from Netware LANalyzer Agent
SubSNMPAIModule3=n_lsmais
SubSNMPAIID3=1.3.6.1.4.1.23.2.13

[Preferences/Map/DefaultFont]
lfHeight=-11
lfWidth=0
lfEscapement=0
lfOrientation=0
lfWeight=400
lfItalic=0
lfUnderline=0
lfStrikeOut=0
lfCharSet=0
lfOutPrecision=3
lfClipPrecision=2
lfQuality=1
lfPitchAndFamily=34
lfFaceName=Arial

[Preferences/Table/DefaultFont]
lfHeight=-11
lfWidth=0
lfEscapement=0
lfOrientation=0
lfWeight=400
lfItalic=0
lfUnderline=0
lfStrikeOut=0
lfCharSet=0
lfOutPrecision=3
lfClipPrecision=2
lfQuality=1
lfPitchAndFamily=34
lfFaceName=Arial
```

```
[nsm]
; *****************************************************************
;                    NETWARE SERVICES MANAGER
; *****************************************************************
DllFiles=n_daq,n_snpdai,n-nwdai,n_nwlist,n_nwcf,n_nwap,n_nwprf,n_snmpcf,n_snmpap,n_thr,n_trend,n_rconso,n_nwps
OlfFiles=n_nwfs,n_nwps,n_snmpcf,n_ps,n_nwcf,n_nwap,n_nwprf,n_snmpap,n_thr,n_trend,n_rconso,n_nwadmn
ProductVersion=NetWare Services Manager v2.10 ( 5/23/95 03:06:00 )
HelpFile=nms.hlp

; A. OLD NMA SUPPORT MAP OPTIONS:
;======================================
; A.1: Number of columns of icons in the Configuration Map window.
NWCF schematic width=6
; A.2: Number of rows of icons in the Configuration Map window.
NWCF schematic height=9
; A.3: Background color of the Configuration Map window (changeable only
;      by the Configure>>Set Color... menu item of NMS Console).
;      The default is white. Default=16777215 (White).
NWCF BackgroundColor=16777215
; A.4: NetWare Server Reconnect Delay option: This is the number of
;      seconds to wait before trying to reestablish connection with
;      the manageable NetWare Server whose configuration is being
;      viewed. The minimum reconnect delay is 300 seconds or five
;      minutes (which is also the default). To never reconnect with
;      the server after a disconnect, use a value of -1.
NWDAI server reconnect delay=300

; B. VIEW ALL NETWARE SERVER MAP OPTIONS:
;======================================
; B.1: Show NetWare File Servers and Print Servers on (a) Database
;      only or (b) database plus visible local-segment
;      Enter:  1 for (a) - (db only)
:              0 for (b) - (db + visible)
NWLIST DatabaseOnly=0
;======================================
; B.2: Select Timezone to display the trends
;      Enter:  0 for Server timezone (this is default)
;              1 for Local timezone - NMS console timezone
;              2 for Greenwich Mean timezone - UTC
NTREND Timezone=0

; C. NEW NETWARE CONFIGURATION MAP OPTIONS:
;======================================
; C.1: Background color of the All Netware Servers window
;      (changeable only by the Configure>>Set Color...
;      menu item of NMS Console). Default=16777215 (White).
SNMPCF BackgroundColor=16777215
; C.2: Horizontal distance between icons.  Default=7.
SNMPCF icon width=7
; C.3:  Vertical distance between icons.  Default=2.
SNMPCF icon height=2
```

```
; D. NETWARE SERVICES POLL OPTIONS
;==================================
; D.1: NetWare Server Number of Retries option: This is the number of
;      retries which will occur in a No Response situation.  The
;      minimum number of retries is 1 and the maximum is 3.
SNMPDAI number of retries=1
; D.2: NetWare Server Retry Timeout option: This is the number of
;      seconds to wait before trying to get the desired information
;      in a No Response situation.  The minimum number of seconds is 10
;      and the maximum is 300 seconds ( 5 min )
SNMPDAI retry timeout=10
; D.3: Polling options for NetWare Services windows.
;      There is a No Polling option, a minimum of 10 seconds,
;      a maximum of 1 hr (3600 seconds).
SNMPAP Bound protocol poll interval=60
SNMPAP Connections poll interval=60
SNMPAP CPU poll interval=60
SNMPAP Disks poll interval=300
SNMPAP Installed software poll interval=300
SNMPAP Memory poll interval=60
SNMPAP MSL poll interval=60
SNMPAP network poll interval=300
SNMPAP nlm poll interval=300
SNMPAP open file poll interval=60
SNMPAP Queue job poll interval=60
SNMPAP Queue print server poll interval=300
SNMPAP Queues poll interval=300
SNMPAP server uptime poll interval=60
SNMPAP server config poll interval=300
SNMPAP User poll interval=600
SNMPAP Logged-in user interval=60
SNMPAP volume usage poll interval=300
SNMPAP volume poll interval=300
Print Server Poll Interval=300

; Trend Defaults - Start
; Value of 1 indicates selection of trend parameter for display
; Value of 0 indicates trend parameter will not be displayed
[cpu]
pctCpuUtilization=1

[volume]
volumePctFreeSpace=1

[disk]
diskPctFreeRedirectionArea=1
[users]
numberLoggedInUsers=1
[connections]
numberConnections=1
[filesystem]
change=0
fileReads=1
fileWrites=1
fileReadKBytes=1
fileWriteKBytes=1
pctCacheHitRate=0
[interfaces]
change=0
lslInPackets=1
lslOutPackets=1
physIfInPackets=0
physIfOutPackets=0
physIfInBytes=0
physIfOutBytes=0
[memory]
change=0
pctCacheBuffersAvailable=1
allocMemoryKB=1
pctPacketReceiveBuffers=1
codeAndDataMemoryKB=1
[queue]
change=0
queueNumReadyJobs=1
queueNumReadyKBytes=1
queueNextJobWaitTime=1
; Trend Defaults - Finish
```

```
[NW_TRANSIENT_FUNCTIONS]
; Description:
;   Rules to add "transient" function icons in the NetWare
;   Server Configuration Window based on the NLM loaded on that server.
;   The NetWare server management software coorelates the NLMs loaded on
;   a server to the corresponding function icons. Note that this information
;   is derived by determining in real-time the NLMs loaded on a server and
;   no part of it is stored in the NMS database - thus it is transient
;   functions. When adding a rule, select the next sequential number
;   in your rule specification. For example, if Rule1 through Rule10
;   exist, the next rule should start with Rule11.
;
; Syntax:
;   Rule?=<NLM name>,<icon text>,BOX,<func class>,[<icon file>,<resdll id>]
;
; Note: The last two parameters <icon file> and <resdll id> are
;       optional and can be ignored. The default icon specified
;       with the function class is selected in this case.
;
;---------------- DEFAULT RULES: DO NOT CHANGE ----------------------
Rule1=NFSSERV.NLM,NFS,,,,2184
Rule2=FTAMSVR.NLM,FTAM,,,,2184
Rule3=AFP.NLM,AFS,,,,2184
Rule4=COMMEXEC.NLM,COMSERV,BOX,CommServer,,2088
Rule5=HUBSNMP.NLM,HUB,BOX,HUB: HMI
;-----------------------------------------------------------------------------


;*******************************************************
;                    TRACE DISPLAY
;*******************************************************

[protocols]
NMS DllPath=e:\NMS\bin
DllFiles1=n_tdlnk,n_tdatk,n_tdnw,n_tdsnmp,n_tdtcp,n_tdnfs,n_tdsna,n_tdnwip
;
; DataLink
;
802.2(802.3)=DataLink,802.3,DataLink,0x0000
802.2(802.5)=DataLink,802.5,DataLink,0x40
;
; AppleTalk
;
aarp(ether)=AppleTalk,ether,DataLink,0x80F3
aarp(snap)=AppleTalk,802.2,DataLink,0,0x80F3
adsp(sddp)=AppleTalk,s-ddp,AppleTalk,0x07
adsp(eddp)=AppleTalk,e-ddp,AppleTalk,0x07
aep(sddp)=AppleTalk,s-ddp,AppleTalk,0x04
aep(eddp)=AppleTalk,e-ddp,AppleTalk,0x04
afp=AppleTalk,asp,AppleTalk,0x0010
asp=AppleTalk,atp,AppleTalk,0x0002
atp(sddp)=AppleTalk,s-ddp,AppleTalk,0x03
atp(eddp)=AppleTalk,e-ddp,AppleTalk,0x03
e-ddp(ether)=AppleTalk,elap,AppleTalk,0x02
e-ddp(snap)=AppleTalk,802.2,DataLink,0,0x809B
elap(ether)=AppleTalk,ether,DataLink,0x809b
nbp(sddp)=AppleTalk,s-ddp,AppleTalk,0x02
nbp(eddp)=AppleTalk,e-ddp,AppleTalk,0x02
pap=AppleTalk,atp,AppleTalk,0x0001
rtmp(eddp)=AppleTalk,e-ddp,AppleTalk,0x01
rtmp(qsddp)=AppleTalk,s-ddp,AppleTalk,0x05
rtmp(qeddp)=AppleTalk,e-ddp,AppleTalk,0x05
rtmp(sddp)=AppleTalk,s-ddp,AppleTalk,0x01
s-ddp=AppleTalk,elap,AppleTalk,0x01
zip(atp)=AppleTalk,atp,AppleTalk,0x06
zip(eddp)=AppleTalk,e-ddp,AppleTalk,0x06
zip(sddp)=AppleTalk,s-ddp,AppleTalk,0x06
;
```

```
; NetWare
;
bcast=NetWare,ipx,NetWare,0,0,0,32,!,0,0
diag=NetWare,ipx,NetWare,0,0x456,0,0,0,0,0
ipx(ether)=NetWare,ether,DataLink,0x8137
ipx(802.3)=NetWare,802.3,DataLink,0xFFFF
ipx(802.2SAP)=NetWare,802.2,DataLink,0xE0,0
ipx(802.2SNAP)=NetWare,802.2,DataLink,0,0x8137
ipx(udp)=NetWare,udp,TCP/IP,213,0,213,0,0
lsp(req9023)=NetWare,ipx,NetWare,0,0x9023,0,0,0,0,0
lsp(req9024)=NetWare,ipx,NetWare,0,0x9024,0,0,0,0,0
lsp(req901F)=NetWare,ipx,NetWare,0,0x901F,0,0,0,0,0
nbios=NetWare,ipx,NetWare,0,0x455,0x455,0,0,0
ncp=NetWare,ipx,NetWare,17,0x451,0,0,0,0,0
nds(ncp)=NetWare,ncp,NetWare,104,2
nlp(req)=NetWare,ipx,NetWare,25,0,0,0,0,0,0
nlp(rep)=NetWare,ipx,NetWare,26,0,0,0,0,0,0
nlsp=NetWare,ipx,NetWare,0,0x9001,0x9001,0,0,0,0
rip(nw)=NetWare,ipx,NetWare,0,0x453,0,0,0,0,0
sap=NetWare,ipx,NetWare,0,0x452,0,0,0,0,0
ser=NetWare,ipx,NetWare,0,0x457,0,0,0,0,0
spx=NetWare,ipx,NetWare,5,0,0,0,0,0,0
wdog=NetWare,ipx,NetWare,0,0,0,32,?,Y,N
;
; TCP/IP
;
arp(ether)=TCP/IP,ether,DataLink,0x0806
arp(snap)=TCP/IP,802.2,DataLink,0,0x0806
ftp=TCP/IP,tcp,TCP/IP,21
ip(ether)=TCP/IP,ether,DataLink,0x0800
ip(icmp)=TCP/IP,icmp,TCP/IP,0
ip(802.2SAP)=TCP/IP,802.2,DataLink,6,0
ip(802.2SNAP)=TCP/IP,802.2,DataLink,0,0x0800
icmp=TCP/IP,ip,TCP/IP,1
ospf=TCP/IP,ip,TCP/IP,0x59
rarp(ether)=TCP/IP,ether,DataLink,0x8035
rarp(snap)=TCP/IP,802.2,DataLink,0x8035
rip(ip)=TCP/IP,udp,TCP/IP,0x0208,0,0,0,0
snmp(udp161)=TCP/IP,udp,TCP/IP,0x00A1,0,0,0,0
snmp(udp162)=TCP/IP,udp,TCP/IP,0x00A2,0,0,0,0
snmp(IPX1)=TCP/IP,ipx,NetWare,4,0x900F,0x900F,0,0,0,0
snmp(IPX2)=TCP/IP,ipx,NetWare,4,0x9010,0x9010,0,0,0,0
tcp=TCP/IP,ip,TCP/IP,6
telnet=TCP/IP,tcp,TCP/IP,23
tftp=TCP/IP,tcp,TCP/IP,69
tftp(udp)=TCP/IP,udp,TCP/IP,0,0,69,0,0
udp=TCP/IP,ip,TCP/IP,0x11
dns=TCP/IP,udp,TCP/IP,53,0,0,0,0
mount=NFS,rpc,NFS,100005,1
nfs=NFS,rpc,NFS,100003,2
prtmp=NFS,rpc,NFS,100000,2
rpc(udp)=NFS,udp,TCP/IP,0,0,0,0,1
rpc(tcp)=NFS,tcp,TCP/IP,111
;
; NetWare IP
;
ipx(UDP/EMU)=NetWare,udp,TCP/IP,0xABCD,0,0,0,0
ipx(TCP/EMU)=NetWare,tcp,TCP/IP,0xABCD,0,0,0,0
nwipu(UDP/DSS)=NWIP,udp,TCP/IP,0x18C,0,0,0,0
nwipt(TCP/DSS)=NWIP,tcp,TCP/IP,0x18C,0,0,0,0
nwipn(UDP/NWIP)=NWIP,udp,TCP/IP,0xABCE,0,0,0,0
nwipn(TCP/NWIP)=NWIP,tcp,TCP/IP,0xABCE,0,0,0,0
;
```

```
; SNA
;
th(sna4)=SNA,802.2,DataLink,0x04,0,0,0
th(sna8)=SNA,802.2,DataLink,0x08,0,0,0
th(snaC)=SNA,802.2,DataLink,0x0C,0,0,0
rh=SNA,th,SNA,0
ru(xid)=SNA,xid,SNA,0
ru(rh)=SNA,rh,SNA,0
; The 'xid(sna)' lines must be specified after the 'th' lines
xid(sna4)=SNA,802.2,DataLink,0x04,0,0x03,0xAC
xid(sna8)=SNA,802.2,DataLink,0x08,0,0x03,0xAC
xid(snaC)=SNA,802.2,DataLink,0x0C,0,0x03,0xAC

[Trace Display Save State]
NMS Default Decode Options=3,16,14,1,

[rmon]
DllFiles=n_mon,n_matrix,n_netsum,n_rmonst,n_dshbrd,n_statns,n_rngtab,n_tc_adp,n_tdgui,n_alarms
OlfFiles=n_menu,LANTERN,RMONSERV
HelpFile=nms.hlp
ProductVersion=LANalyzer Services Manager v2.10 ( 5/23/95 03:06:00 )
Dlg=lantern

[rsm]
DllFiles=n_sts,n_routst,n_netadd,n_rtsum,n_nlsp,n_ipx,n_ipxrtr,n_rtcach,n_ipxbm
OlfFiles=n_sts,n_routst,n_ipadd,n_ipxadd,n_rtsum,n_ipbox,n_ipxbox,n_innbox,n_ipxrtr,n_ipx,n_nlsp,n_ipxbm
HelpFile=nms.hlp
ProductVersion=Router Services Manager v2.10 ( 5/23/95 03:06:00 )

[dds]
DllFiles=n-diag, n-diasrv
OlfFiles=n-diag

[Table Tool Column Settings]
Alarm Report=1 11 4,20,0 3,4,0 2,4,0 6,23,0 7,80,0 5,18,0 8,15,0 1,4,0 9,14,0 10,22,0 11,20,0
```

A.14 NMA.INI

```
[nma]
OLFFiles=nma
ProductVersion=nma class
```

A.15 NETXPLOR.INI

```
[netxplor]
OLFFiles=n_nxp
ProductVersion=NetExplorer
```

A.16 NSM.INI

```
[nsm]
; ****************************************************************
;                     NETWARE SERVICES MANAGER
; ****************************************************************
DllFiles=n_daq,n_snpdai,n-nwdai,n_nwlist,n_nwcf,n_nwap,n_nwprf,n_snmpcf,n_snmpap,n_thr,n_trend,n_rconso,n_nwps
OlfFiles=n_nwfs,n_nwps,n_snmpcf,n_ps,n_nwcf,n_nwap,n_nwprf,n_snmpap,n_thr,n_trend,n_rconso,n_nwadmn
ProductVersion=1.1
HelpFile=nmm.hlp


; A. OLD NMA SUPPORT MAP OPTIONS:
;==================================
; A.1: Number of columns of icons in the Configuration Map window.
NWCF schematic width=6
; A.2: Number of rows of icons in the Configuration Map window.
NWCF schematic height=9
; A.3: Background color of the Configuration Map window (changeable only
;      by the Configure>>Set Color... menu item of NMS Console).
;      The default is white. Default = 16777215 (White).
NWCF BackgroundColor=16777215
; A.4: NetWare Server Reconnect Delay option: This is the number of
;      seconds to wait before trying to reestablish connection with
;      the manageable NetWare Server whose configuration is being
;      viewed. The minimum reconnect delay is 300 seconds or five
;      minutes (which is also the default). To never reconnect with
;      the server after a disconnect, use a value of -1.
NWDAI server reconnect delay=300


; B. VIEW ALL NETWARE SERVER MAP OPTIONS:
;====================================
; B.1: Show NetWare File Servers and Print Servers on (a) Database
;      only or (b) database plus visible local-segment
;      Enter:  1 for (a) - (db only)
:              0 for (b) - (db + visible)
NWLIST DatabaseOnly=0
;====================================
; B.2: Select Timezone to display the trends
;      Enter:  0 for Server timezone (this is default)
;              1 for Local timezone - NMS console timezone
;              2 for Greenwich Mean timezone - UTC
NTREND Timezone=0


; C. NEW NETWARE CONFIGURATION MAP OPTIONS:
;====================================
; C.1: Background color of the All Netware Servers window
;      (changeable only by the Configure>>Set Color...
;      menu item of NMS Console). Default = 16777215 (White).
SNMPCF BackgroundColor=16777215
; C.2: Horizontal distance between icons.  Default = 7.
SNMPCF icon width=7
; C.3:  Vertical distance between icons.  Default = 2.
SNMPCF icon height=2
```

```
; D. NETWARE SERVICES POLL OPTIONS
;====================================
; D.1: NetWare Server Number of Retries option: This is the number of
;      retries which will occur in a No Response situation.  The
;      minimum number of retries is 1 and the maximum is 3.
SNMPDAI number of retries=1
; D.2: NetWare Server Retry Timeout option: This is the number of
;      seconds to wait before trying to get the desired information
;      in a No Response situation.  The minimum number of seconds is 10
;      and the maximum is 300 seconds ( 5 min )
SNMPDAI retry timeout=10
; D.3: Polling options for NetWare Services windows.
;      There is a No Polling option, a minimum of 10 seconds,
;      a maximum of 1 hr (3600 seconds).
SNMPAP Bound protocol poll interval=60
SNMPAP Connections poll interval=60
SNMPAP CPU poll interval=60
SNMPAP Disks poll interval=300
SNMPAP Installed software poll interval=300
SNMPAP Memory poll interval=60
SNMPAP MSL poll interval=60
SNMPAP network poll interval=300
SNMPAP nlm poll interval=300
SNMPAP open file poll interval=60
SNMPAP Queue job poll interval=60
SNMPAP Queue print server poll interval=300
SNMPAP Queues poll interval=300
SNMPAP server uptime poll interval=60
SNMPAP server config poll interval=300
SNMPAP User poll interval=600
SNMPAP Logged-in user interval=60
SNMPAP volume usage poll interval=300
SNMPAP volume poll interval=300
Print Server Poll Interval=300

; Trend Defaults - Start
; Value of 1 indicates selection of trend parameter for display
; Value of 0 indicates trend parameter will not be displayed
```

```
[cpu]
pctCpuUtilization=1

[volume]
volumePctFreeSpace=1

[disk]
diskPctFreeRedirectionArea=1

[users]
numberLoggedInUsers=1

[connections]
numberConnections=1

[filesystem]
change=0
fileReads=1
fileWrites=1
fileReadKBytes=1
fileWriteKBytes=1
pctCacheHitRate=0

[interfaces]
change=0
lslInPackets=1
lslOutPackets=1
physIfInPackets=0
physIfOutPackets=0
physIfInBytes=0
physIfOutBytes=0

[memory]
change=0
pctCacheBuffersAvailable=1
allocMemoryKB=1
pctPacketReceiveBuffers=1
codeAndDataMemoryKB=1

[queue]
change=0
queueNumReadyJobs=1
queueNumReadyKBytes=1
queueNextJobWaitTime=1

; Trend Defaults - Finish

[NW_TRANSIENT_FUNCTIONS]
; Description:
;   Rules to add "transient" function icons in the NetWare
;   Server Configuration Window based on the NLM loaded on that server.
;   The NetWare server management software coorelates the NLMs loaded on
;   a server to the corresponding function icons. Note that this information
;   is derived by determining in real-time the NLMs loaded on a server and
;   no part of it is stored in the NMS database - thus it is transient
;   functions. When adding a rule, select the next sequential number
;   in your rule specification. For example, if Rule1 through Rule10
;   exist, the next rule should start with Rule11.
;
; Syntax:
;   Rule?=<NLM name>,<icon text>,BOX,<func class>,[<icon file>,<resdll id>]
;
; Note: The last two parameters <icon file> and <resdll id> are
;       optional and can be ignored. The default icon specified
;       with the function class is selected in this case.
;
;---------------- DEFAULT RULES: DO NOT CHANGE ----------------------
Rule1=NFSSERV.NLM,NFS,,,,2184
Rule2=FTAMSVR.NLM,FTAM,,,,2184
Rule3=AFP.NLM,AFS,,,,2184
Rule4=COMMEXEC.NLM,COMSERV,BOX,CommServer,,2088
Rule5=HUBSNMP.NLM,HUB,BOX,HUB: HMI
;-----------------------------------------------------------------------------
```

A.17 TRAPTARG.CFG

```
#######################################################
# traptarg.cfg
#
# Snmp Agent Trap Target (Destination) Configuration
#
# This file specifies all managers that are to receive
# snmp trap messages generated by the Snmp Agent (snmp.nlm)
#
# File Format:
#
# Protocol <name>
#       Specifies the beginning of a list of names or
#       address of managers to which to send traps using the
#       protocol specified by <name> if that protocol is
#       registered as a service provider to the snmp agent.
#
#       All destinations must be preceeded by white space
#       Each destination must be listed on a separate Line
#
#       The Protocol keyword, left justified, signifies the
#       start of a new protocol section.
#
#       Comments are preceeded by the hash mark and proceed
#       to the end of the line.
#
#######################################################
Protocol IPX
    # In this section you can put SNMP managers that want to receive
    # traps from the local node over IPX.  Managers can be identified
    # by NetWare service name (a NetWare file server name, for example)
    # or by IPX address.  To specify by IPX address, use the following
    # format:
    #          IPX Network Number: MAC Address
    #
    # for example, c9990111:00001B555555

Protocol UDP
    127.0.0.1
    9.24.104.14
    9.24.104.15
```

A.18 TCPIP.CFG

```
AutonomousSystem 0
Protocol rip on {
    Interface {
        Address 9.24.104.54
        Port TOKEN_1_TSP
        Status on
        Cost 1
        Poison off
        OriginateDefault off
        Mode ripI
        Neighbor {
        }
    }
}
Protocol egp off {
}
Protocol ospf off {
    Interface {
        Address 9.24.104.54
        Port TOKEN_1_TSP
        Status on
        Cost 1
        AreaId 0.0.0.0
        Priority 1
        RetransmissionInterval 5
        TransitDelay 1
        HelloInterval 10
        RouterDeadInterval 40
        Nbma {
            PollInterval 120
            Neighbor {
            }
        }
    }
}
Interface {
    Address 9.24.104.54
    Port TOKEN_1_TSP
    Type lan
    RouterDiscovery yes
    SolicitationAddress multicast
}
```

A.19 SNMP.CFG

```
Name
    NMS20C
Hardware
    9595
Location
    BB106
Contact
    Barry D. Nusbaum
```

A.20 NWTRAP.CFG

```
#####################################################################
#
# nwtrap.cfg
#
# NWTRAP Configuration File
#
# This file specifies operational parameters to be used by NWTRAP.
# The file is read and the parameters set when NWTRAP is loaded.  It must
# reside on volume SYS in the directory SYS:\ETC and must be named nwtrap.cfg
# to be found by NWTRAP.  To change the parameters, first edit this file,
# then unload NWTRAP and load it again.  Any changes to this file will not
# take effect until the time NWTRAP is next loaded.  The parameters are
# specified by using a parameter keyword followed by the desired parameter
# value, as outlined below.
#
#
# File Format:
#
# The parameters are specified as follows:
#
# keyword
#    value
#
# There may be one keyword/value pair for each of the four parameters
# settable in NWTRAP.CFG.  The keyword signifies the parameter to be set,
# value is the value of the parameter as outlined below.
#
# All Information must start on a new line, one line per keyword and one line
# per value (except for mask value where the value set may span several lines
# as shown below).
#
# Maximum line length, including the newline character, is 128.  There may be
# no data past column 127 and the line must end immediately thereafter with
# no intervening white space.
#
# Comment lines begin with the hash mark (#).  A comment must use an entire
# line; it may not appear at the end of a keyword or value line.
#
# Upper or lower case allowed; not case sensitive.
#
# Parameter Specification:
#
# Keyword           Community | Time Interval | Mask | Severity
#
# Value Specification:
#
# Community
#                 SNMP community name e.g. Public.  If not specified, the
#                 default Community value is PUBLIC.
#
#
# Time Interval
#                 The minimum time interval in seconds between the
#                 transmission of any two instances of the same trap.  Alert
#                 conditions resulting in duplicate traps which occur before
#                 the time interval has elapsed will be ignored.  If not
#                 specified, the default Time Interval value is 10.
#
#
```

```
# Mask
#               The traps to be masked out.  The trap numbers specified
#               are from NWALARM.MIB.  Each trap number in the list will
#               suppress the transmission of that trap number.  If not
#               specified, the default Mask value is no traps masked.
#               Delimiters between trap numbers are commas, space, <CR>.
#               e.g.
#               Mask
#                       123, 278, 370
#                       242 76 362
#                       59
#                       299
#                       321
#
#               In the mask section below, all trap numbers from
#               NWALARM.MIB along with the corresponding #TYPE descriptions
#               are listed but commented out.  Initially, since all the
#               listed traps are commented out, the "mask" keyword itself
#               is also commented out.  To mask a trap, be sure the "mask"
#               keyword is uncommented by deleting the hash mark (#) in
#               front of the word "mask".  Then find the desired trap in
#               the list and uncomment just the line containing the number,
#               again by deleting the hash mark (#) at the beginning of
#               that line.  If no traps are to be masked (all trap numbers
#               commented out) be sure the "mask" keyword is also commented
#               out to avoid a NWTRAP.CFG parse error.
#
#
# Severity
#               Any traps of severity less than the value of this parameter
#               will be suppressed.  Individual trap severities are
#               specified in NWALARM.MIB.
#               Parameter value can be:
#                 INFORMATIONAL | WARNING | RECOVERABLE | CRITICAL | FATAL
#               where
#                 INFORMATIONAL < WARNING < RECOVERABLE < CRITICAL < FATAL
#               If not specified, the default Severity value is WARNING.
#
########################################################################

Community
        public

Time Interval
        10

Severity
        Warning
```

```
#mask
#         "Memory: Short term alloc failed"
#          1

#         "FileSys: Directory write err (no vol)"
#          2

#         "FileSys: File write err, by server (no path)"
#          3

#         "FileSys: File write err, by user (no path)"
#          4

#         "FileSys: File write err, by server (path)"
#          5

#         "FileSys: File write err, by user (path)"
#          6

#         "FileSys: File read err, by server (no path)"
#          7

#         "FileSys: File read err, by user (no path)"
#          8

#         "FileSys: File read err, by server (path)"
#          9

#         "FileSys: File read err, by user (path)"
#          10

#         "FileSys: File pre-read err, by server (no path)"
#          11

#         "FileSys: File pre-read err, by user (no path)"
#          12

#         "FileSys: File pre-read err, by server (path)"
#          13

#         "FileSys: File pre-read err, by user (path)"
#          14

#         "Memory: Cache buffer low limit exceeded"
#          15

#         "Memory: Cache buffers exhausted"
#          16

#         "Memory: Cache buffers too low"
#          17

#         "FileSys: Vol out of space, no deleted files"
#          18

#         "FileSys: Vol out of space, files not purgeable"
#          19

#         "FileSys: Vol low on space"
#          20
```

```
#         "FileSys: FAT write err"
#           21

#         "FileSys: Directory write err (vol)"
#           22

#         "FileSys: Directory read err, one copy "
#           23

#         "FileSys: Directory read err, both copies"
#           24

#         "Disk: Err writing new block"
#           25

#         "Disk: Err expanding dir, write err"
#           26

#         "Disk: Err expanding dir, size limit"
#           27

#         "Disk: Err expanding dir, no space"
#           28

#         "Memory: Err expanding directory, no memory"
#           29

#         "Memory: Directory table too big for memory"
#           30

#         "Network: LAN receive buffer limit reached"
#           31

#         "Connection: Cleared, by watchdog"
#           32

#         "System: Copyright violation"
#           33

#         "OS: Write fault"
#           34

#         "OS: Read fault"
#           35

#         "Network: Bad IPX packet"
#           36

#         "FileSys: VOL$LOG.ERR create err, "
#           37

#         "FileSys: VOL$LOG.ERR write err, "
#           38

#         "Disk: Deactivated, mirrored drive"
#           39

#         "System: Login disabled, by user #1"
#           40
```

```
#        "System: Login enabled, by user #2"
#         41

#        "Connection: Cleared"
#         42

#        "Connection: Cleared at user console"
#         43

#        "System: Server downed, by user"
#         44

#        "Router: Err opening RIP socket"
#         45

#        "Router: Config err #1"
#         46
#        "Network: LAN driver loopback err"
#         47

#        "Router: Duplicate internet address"
#         48

#        "Network: LAN board unreachable"
#         49

#        "Network: IPX unbound"
#         50

#        "Router: Err opening SAP socket"
#         51

#        "Router: Two routers claim same address"
#         52

#        "OS: Spurious interrupt"
#         53

#        "Network: Invalid checksum"
#         54

#        "OS: Lost interrupt, primary controller"
#         55

#        "OS: Lost interrupt, secondary controller"
#         56

#        "OS: Exception"
#         57

#        "OS: Invalid screen ID"
#         58

#        "OS: Control not relinquished"
#         59

#        "User: Account deleted, by server"
#         60

#        "User: Account deleted, by user"
#         61

#        "OS: Bad resrc tag passed to ParseDriverParms"
#         62
```

```
#        "Disk: Deactivated, cause unknown"
#         63

#        "Disk: Deactivated, driver unloaded"
#         64

#        "Disk: Deactivated, device failure"
#         65

#        "Disk: Deactivated, by user"
#         66

#        "Disk: Deactivated, media dismount"
#         67

#        "Disk: Deactivated, media eject"
#         68

#        "Disk: Deactivated, server downed"
#         69

#        "Disk: Deactivated, file system failure"
#         70

#        "OS: NLM did not release resource."
#         71

#        "Disk: Partition not remirrored"
#         72

#        "Disk: Partitions all synchronized"
#         73

#        "Disk: Partition synchronized"
#         74

#        "Disk: Partition not synchronized"
#         75

#        "Disk: Partition being remirrored"
#         76

#        "Disk: Partition remirror failed"
#         77

#        "Disk: Partition inconsistent"
#         78

#        "FileSys: Threshold, system file lock"
#         79

#        "FileSys: Threshold, station file lock"
#         80
```

```
#        "FileSys: Threshold, system record lock"
#          81

#        "FileSys: Threshold, station record lock"
#          82

#        "FileSys: NET$ACCT.DAT open err"
#          83

#        "NCP: Directory search limit exceeded, by server"
#          84

#        "NCP: Directory search limit exceeded, by user"
#          85

#        "MediaMgr: Media Insert ack'd"
#          86

#        "MediaMgr: Media insert aborted"
#          87

#        "MediaMgr: Media remove ack'd"
#          88

#        "MediaMgr: Media remove aborted"
#          89

#        "MediaMgr: DS-media Insert req"
#          90

#        "MediaMgr: Media remove req"
#          91

#        "Disk: Hotfix, block redirected"
#          92

#        "Disk: Hotfix, redirect failed"
#          93

#        "Disk: Hotfix, out of redirection blocks"
#          94

#        "Disk: Hotfix, low on redirection blocks"
#          95

#        "Disk: Hotfix, inconsistencies not fixed"
#          96

#        "Disk: Hotfix, inconsistencies fixed"
#          97

#        "OS: Bad resrc tag passed to RegisterHWOptions"
#          98

#        "OS: Resource tag allocation failure"
#          99

#        "OS: RemoveHardwareOptions failed "
#          100

#        "OS: NLM unloaded with exported vars."
#          101

#        "OS: Bad resrc tag passed to CreateProcess"
#          102

#        "OS: CreateProcess err, stack size too small"
#          103

#        "OS: CreateProcess err, no memory"
#          104

#        "FileSys: File preservation err"
#          105

#        "FileSys: File not salvageable, no dir space"
#          106

#        "Network: MLID reset LAN board"
#          107
```

```
#          "Router: Reset"
#           108

#          "FileSys: Vol DOS type mismatch"
#           109

#          "FileSys: Name space not found"
#           110

#          "FileSys: Migration support module changed"
#           111

#          "FileSys: TTS$LOG.ERR create err"
#           112

#          "FileSys: TTS$LOG.ERR write err"
#           113

#          "TTS: Not available"
#           114

#          "TTS: Disabled, by user"
#           115

#          "TTS: Disabled, by server"
#           116

#          "TTS: Disabled, reading backout file"
#           117

#          "TTS: Disabled, writing backout file"
#           118

#          "TTS: Disabled, too many volumes"
#           119

#          "TTS: Disabled, volume information"
#           120

#          "TTS: Disabled, record generation"
#           121

#          "TTS: Disabled, growing TTS tables"
#           122

#          "TTS: Disabled, no disk space"
#           123

#          "TTS: Disabled, directory error"
#           124

#          "TTS: Enabled"
#           125

#          "TTS: Transaction aborted"
#           126

#          "TTS: Hit active transaction limit"
#           127

#          "TTS: Ran out of memory"
#           128

#          "Audit: Invalid req, volume #"
#           129

#          "Audit: Threshold overflow"
#           130

#          "Audit: Disabled, invalid config file"
#           131

#          "Audit: Out of memory"
#           132
```

```
#        "Audit: File write error"
#          133

#        "Audit: File full"
#          134

#        "OS: Invalid connection type"
#          135

#        "OS: Bad resrc tag passed to AllocConnNumber"
#          136

#        "System: Server out of connections"
#          137

#        "Connection: Cleared, 5-min notice"
#          138

#        "User: Account disabled"
#          139

#        "Security: Unencrypted password"
#          140

#        "Security: Supervisor lockout cleared"
#          141

#        "System: Time changed, by server"
#          142

#        "System: Time changed, by user"
#          143

#        "FileSys: Vol dismounted, drive deactivation"
#          144

#        "Router: Reporting wrong addresses"
#          145

#        "Router: Server address changed"
#          146

#        "FileSys: File extend err, no owner"
#          147

#        "Router: Config err #3"
#          148

#        "Router: Config err #2"
#          149

#        "FileSys: Migration NLM not loaded"
#          150

#        "FileSys: Migration support NLM not loaded"
#          151

#        "FileSys: Compression err, no memory"
#          152

#        "FileSys: Compression err, disk I/O"
#          153

#        "FileSys: Compression err, sparse count"
#          154

#        "FileSys: Compression err, disk write"
#          155

#        "FileSys: Decompression err, no disk space"
#          156

#        "FileSys: Decompression err, unknown format "
#          157

#        "FileSys: Decompression err, unknown (no path)"
#          158

#        "FileSys: Decompression err, no RAM (no path)"
#          159
```

```
#       "FileSys: Compressed file corrupt (no path)"
#          160

#       "NCP: Rejected incomplete NCP packet"
#          161

#       "NCP: Processed incomplete NCP packet"
#          162

#       "NCP: Rejected bad NCP packet"
#          163

#       "NCP: Processed bad NCP packet"
#          164

#       "FileSys: Compressed file corrupt (path)"
#          165

#       "FileSys: Compressed file corrupt, in use"
#          166

#       "OS: NLM not letting other threads run"
#          167

#       "OS: Work-to-do took too much CPU"
#          168

#       "FileSys: Compression err, inconsistent temp file "
#          169

#       "FileSys: Compression err, length totals"
#          170

#       "FileSys: Compression err, offset totals"
#          171

#       "FileSys: Compression err, data encode counts"
#          172

#       "FileSys: Compression err, length/offset counts"
#          173

#       "FileSys: Compression err, large length/offset"
#          174

#       "FileSys: Compression err, EOF on intermediate"
#          175

#       "FileSys: Compression err, Shannon tree depth"
#          176

#       "FileSys: Compression err, projected size"
#          177

#       "Security: Invalid signature #1"
#          178

#       "System: License invalid"
#          179

#       "Disk: Deactivated, hotfix failure"
#          180

#       "FileSys: Decompression err, unknown (path)"
#          181

#       "FileSys: Decompression err, no RAM (path)"
#          182

#       "FileSys: Decompression err, not committed"
#          183

#       "NCP: Rejected large packet req."
#          184

#       "System: Login disabled, by server"
#          185

#       "System: Login enabled, by server"
#          186
```

```
#         "OS: Stack creation failed."
#          187

#         "MediaMgr: DS-media insert ack'd"
#          188

#         "MediaMgr: Magazine insert ack'd"
#          189

#         "MediaMgr: DS-media insert aborted"
#          190

#         "MediaMgr: Magazine insert aborted"
#          191

#         "MediaMgr: DS-media remove ack'd"
#          192

#         "MediaMgr: Magazine remove ack'd"
#          193

#         "MediaMgr: DS-media remove aborted"
#          194

#         "MediaMgr: Magazine remove aborted"
#          195

#         "MediaMgr: Magazine insert req"
#          196

#         "MediaMgr: DS-media remove req"
#          197

#         "MediaMgr: Remove magazine from server"
#          198

#         "OS: NLM did not release resources"
#          199

#         "System: Bindery did not open, server"
#          200

#         "System: Bindery did not open, user"
#          201

#         "System: Bindery opened, by server"
#          202

#         "System: Bindery opened, by user"
#          203

#         "System: Bindery closed, by server"
#          204

#         "System: Bindery closed, by user"
#          205

#         "User: Account disabled, temporarily"
#          206

#         "DS: Database open failed"
#          207

#         "DS: Database inconsistent"
#          208

#         "DS: Database open"
#          209

#         "DS: Database closed"
#          210

#         "DS: Skulking err"
#          211

#         "Security: Intruder lockout"
#          212

#         "OS: Domain quarantined"
#          213
```

```
#       "System: Command processor faulted."
#        214

#       "System: RCONSOLE connection granted"
#        215

#       "System: RCONSOLE connection cleared"
#        216

#       "System: RCONSOLE connection refused"
#        217

#       "System: Trap NLM loaded"
#        218

#       "System: Trap NLM unloaded"
#        219

#       "FileSys: Vol mounted"
#        220

#       "FileSys: Vol dismounted"
#        221

#       "System: Server downed, at server console"
#        222

#       "Network: Protocol bound to driver"
#        223

#       "Network: Protocol unbound from driver"
#        224

#       "System: NLM loaded"
#        225

#       "System: NLM unloaded"
#        226

#       "Network: MLID registered board"
#        227

#       "Network: MLID de-registered"
#        228

#       "Connection: User connection cleared"
#        229

#       "Connection: User logged in"
#        230

#       "NLM: Critical alert"
#        231

#       "Connection: User logged out"
#        232

#       "User: Account deleted, single connection"
#        233

#       "FileSys: Compression err, EOF on original"
#        234

#       "Disk: Deactivated, cause specified"
#        235

#       "Disk: Mounted"
#        236

#       "Disk: Hotfix, redirection block mismatch"
#        237

#       "Memory: Short term limit exceeded"
#        238

#       "Memory: Semi-permanent memory exhausted"
#        239
```

```
#        "Disk: Dismounted"
#           240

#        "Disk: Added"
#           241

#        "Disk: Activated"
#           242

#        "TTS: Disabled, for reason"
#           243

#        "Disk: Partitions not synchronized"
#           244

#        "Router: Reset, dynamic"
#           245

#        "Security: Invalid signature #2"
#           246

#        "Security: Duplicate but different NCP received"
#           247

#        "Security: Invalid packet burst signature"
#           248

#        "FileSys: Failed to delete migrated file"
#           249

#        "Security: Unsigned remote connection refused"
#           250

#        "Security: Unsigned remote connection granted"
#           251

#        "Network: Response packet dropped"
#           252

#        "Network: Workstation not located"
#           253

#        "Async: Connection timed-out"
#           254

#        "Async: Modem connection cleared"
#           255

#        "Async: Connection cleared"
#           256

#        "Async: Call-back # not received"
#           257

#        "Async: Call-back file open err"
#           258

#        "Async: Call-back file read err"
#           259

#        "Async: Call-back # unauthorized"
#           260

#        "Async: Modem cleared, call-back attempted"
#           261

#        "Async: Call-back attempted"
#           262

#        "Async: Connection refused"
#           263

#        "Async: Connection granted"
#           264

#        "Async: Modem connection established"
#           265

#        "AuditDS: File write error"
#           266
```

```
#       "AuditDS: File full"
#        267

#       "AuditDS: Threshold overflow"
#        268

#       "AuditDS: Out of memory"
#        269

#       "System: Server up"
#        270

#       "FileSys: EA restricted space limit"
#        271

#       "TimeSync: Not initialized"
#        272

#       "TimeSync: Not started"
#        273

#       "TimeSync: No SAP socket tag"
#        274

#       "TimeSync: No SAP socket"
#        275

#       "TimeSync: No settable parameter tag"
#        276

#       "TimeSync: No timer tag"
#        277

#       "TimeSync: No alloc tag"
#        278

#       "TimeSync: No resource tag"
#        279

#       "TimeSync: No process tag"
#        280

#       "TimeSync: No event tag"
#        281

#       "TimeSync: No global information"
#        282

#       "TimeSync: No command line"
#        283

#       "TimeSync: No timesync NCP verb"
#        284

#       "TimeSync: No main stack"
#        285

#       "TimeSync: Could not create main process"
#        286

#       "TimeSync: Synchronization radius"
#        287

#       "TimeSync: Unrecognized parameter"
#        288

#       "TimeSync: Unrecognized config option"
#        289

#       "TimeSync: Server polled"
#        290

#       "TimeSync: Servers incompatible"
#        291

#       "TimeSync: Time synchronization lost"
#        292
```

```
#          "TimeSync: Time synchronization established"
#           293

#          "Connection: Terminated"
#           294

#          "Connection: Cleared by user"
#           295

#          "System: Login disabled, by user #2"
#           296

#          "System: Server down req, by user"
#           297

#          "System: Login enabled, by user #1"
#           298

#          "SFT-III: Err transferring IOEngine err log"
#           299

#          "System: Command handler fault"
#           300

#          "SFT-III: MSL activated"
#           301

#          "SFT-III: MSL failure"
#           302

#          "SFT-III: MSL de-activated"
#           303

#          "SFT-III: Synchronization attempt"
#           304

#          "SFT-III: MSL comm. re-established"
#           305

#          "SFT-III: Synchronization starting"
#           306

#          "SFT-III: Invalid initialization message"
#           307

#          "SFT-III: MSL failure, initialization"
#           308

#          "SFT-III: Synchronization failure"
#           309

#          "SFT-III: MSL driver loaded during activate"
#           310

#          "SFT-III: Err writing status dump"
#           311

#          "SFT-III: MSL driver on primary server"
#           312

#          "SFT-III: MSL failure, hold off"
#           313

#          "SFT-III: Err finishing status dump"
#           314

#          "SFT-III: Reason string"
#           315

#          "SFT-III: Unexpected error"
#           316

#          "SFT-III: Sync error generated by custom MSL"
#           317

#          "SFT-III: Server link has plugged packet"
#           318
```

```
#        "SFT-III: Mirrored Server will be revived"
#           319

#        "SFT-III: Mirrored servers are synchronized"
#           320

#        "SFT-III: Unable to route to secondary via IPX"
#           321

#        "SFT-III: IPX route to secondary"
#           322

#        "SFT-III: MSEngine, err adding RAM"
#           323

#        "SFT-III: MSEngine, more RAM added"
#           324

#        "SFT-III: Mirrored servers now synchronized"
#           325

#        "SFT-III: Unable to route to primary via IPX"
#           326

#        "SFT-III: IPX route to primary"
#           327

#        "SFT-III: Primary failed, secondary down"
#           328

#        "SFT-III: Primary failed, secondary up"
#           329

#        "SFT-III: Memory segments exceeds limits"
#           330

#        "SFT-III: Screen modes exceeds limits"
#           331

#        "SFT-III: Mismatch, IOEngine software version"
#           332

#        "SFT-III: Mismatch, Protection level"
#           333

#        "SFT-III: Mismatch, Screen address"
#           334

#        "SFT-III: Mismatch, IOEngine address"
#           335

#        "SFT-III: MSEngine, active on both servers"
#           336

#        "SFT-III: MSEngine, not active on either server"
#           337

#        "SFT-III: Secondary is missing RAM"
#           338

#        "SFT-III: Duplicate internal net#, IO & IO"
#           339

#        "SFT-III: Duplicate internal net#, MS & IO"
#           340

#        "SFT-III: Mismatch, IOEngine LAN recv buffers"
#           341

#        "SFT-III: Duplicate IOEngine names"
#           342

#        "SFT-III: No memory to store IOEngine name"
#           343

#        "SFT-III: MSL beginning synchronization"
#           344

#        "SFT-III: MSEngine, activated"
#           345
```

```
#        "SFT-III: MSEngine, activated...will synchronize"
#         346

#        "SFT-III: IOEngine to MSEngine comm. unloaded"
#         347

#        "SFT-III: Out of comm. message codes"
#         348

#        "SFT-III: Secondary IOEngine no support modules"
#         349

#        "SFT-III: Unable to transfer status dumps"
#         350

#        "SFT-III: Failure checking primary via IPX"
#         351

#        "SFT-III: Err starting 2nd processor"
#         352

#        "SFT-III: Server Failed"
#         353

#        "SFT-III: Mirrored server synchronizing"
#         354

#        "SFT-III: MSL connection established"
#         355

#        "SFT-III: Secondary's LAN more functional"
#         356

#        "SFT-III: IPX net now returning status checks"
#         357

#        "SFT-III: IPX net not returning status checks"
#         358

#        "SFT-III: IPX net LAN adapter jammed"
#         359

#        "SFT-III: Failure detected by other server"
#         360

#        "SFT-III: IPX Internet is back up"
#         361

#        "SFT-III: IPX internet too slow"
#         362

#        "SFT-III: IPX internet path Hop Count large"
#         363

#        "SFT-III: IPX Internet appears down"
#         364

#        "SFT-III: IPX route discovered"
#         365

#        "SFT-III: IPX route to other server new"
#         366

#        "SFT-III: IPX route to the other server lost"
#         367

#        "SFT-III: Secondary will initiate error"
#         368

#        "SFT-III: Primary will initiate err, after sync"
#         369

#        "SFT-III: Primary will initiate err"
#         370

#        "SFT-III: IOEngine screen mem alloc fail"
#         371
```

```
#       "TimeSync: Error"
#        372

#       "DS: Unable to communicate with server"
#        373

#       "DS: Re-established communication with server"
#        374

#       "Disk: Hotfix, redirection err table mismatch"
#        375

#       "NLM: Major alert"
#        376

#       "NLM: Minor alert"
#        377

#       "NLM: Informational alert"
#        378
```

A.21 NETINFO.CFG

```
#!VERSION=2.2
#!
#! --- WARNING -- WARNING -- WARNING -- WARNING -- WARNING -- WARNING ----
#! This file was created by the Internetworking Configuration Console.
#! It is intended to be modified ONLY by the configurator (INETCFG.NLM).
#! Tampering with this file may cause severe malfunctioning of the system.
#! The configurator will check for tampering and abort if it is detected.
#! ----------------------------------------------------------------------
#!
#!SERVERTYPE=NORMAL
#!SERVERNAME=NMS20C
#!
#!BEGINGENLOAD
LOAD SNMP ControlCommunity= TrapCommunity=public verbose
#!END
#!
#!BEGINTSMLOAD
#!END
#!
#!BEGINBOARD DRVR=TOKEN NAME=TOKEN_1 STATUS=ENABLED NUMPORTS=1 DRVRTYPE=LAN VARIABLEPORTS=NO PORTPARAM=CHANNEL SLOT=3
NODE=400052005190M MSB
#Transferred from AUTOEXEC.NCF
#!BEGINPORT NAME=TOKEN_1 NUMBER=1 STATUS=ENABLED FRAMES=YES NUMLINKS=1 MEDIA=TokenTsm WANFRAME=UNCONFIGURED
#Transferred from AUTOEXEC.NCF
#!REFCOUNT=2
LOAD TOKEN NAME=TOKEN_1_TOK FRAME=TOKEN-RING SLOT=3 NODE=400052005190M MSB
#!REFCOUNT=2
LOAD TOKEN NAME=TOKEN_1_TSP FRAME=TOKEN-RING_SNAP SLOT=3 NODE=400052005190M MSB
#!END
#!END
#!
#!BEGINPROTO PROTO=TCPIP STATUS=ENABLED
LOAD Tcpip RIP=Yes Forward=Yes
#
LOAD IPConfig Screen=no
#
#!BEGINBIND STATUS=ENABLED
BIND IP TOKEN_1_TSP ARP=Yes Mask=FF.FF.FF.0 Address=9.24.104.54
#9.24.104.54
#!END
#!END
#!
#!BEGINPROTO PROTO=IPX STATUS=ENABLED
#!BEGINBIND STATUS=ENABLED
BIND IPX TOKEN_1_TOK NET=9
#9
#!END
#!END
#!
#!BEGINPROTO PROTO=SRCROUTE STATUS=ENABLED
#!END
#!
#!BEGINREMOTE
LOAD REMOTE
LOAD RSPX
#!END
```

A.22 LANZ.NCF

```
#----------------------------------------------------------------------------
#
#                           NetWare LANalyzer Agent
#                                 Version 1.0
#
#----------------------------------------------------------------------------
# LANZ.NCF: NetWare LANalyzer Agent Load File
#
# This NCF file is created by the NetWare LANalyzer Agent install program.
# It is used to load the NetWare Loadable Module files that make up NetWare
# LANalyzer Agent.
#
# WARNING:   You should not modify this file unless you need to change
#            one of the configuration parameters documented below.
#            Other changes to this file are not recommended.
#
# NOTE:      If you are using Token-Ring drivers, you must uncomment the
#            LANZTR.NLM line below in order to monitor token-ring nets.
#
#----------------------------------------------------------------------------
# Load Parameter Descriptions
#
# load LANZMEM bound=KB age=HHH
#
# bound=KB   This is the upper limit on memory that can be allocated
#            dynamically by the NetWare LANalyzer Agent.
#
#            Increasing this number allows you to create larger packet
#            capture buffers and maintain data for inactive stations
#            for a longer period of time.
#
#            Decreasing this value reduces the amount of memory that
#            can be used by NetWare LANalyzer Agent.  This leaves more
#            memory for the other server tasks.
#
#            NetWare LANalyzer Agent automatically purges data for
#            inactive stations as the memory bound is approached.
#            This allows NetWare LANalyzer Agent to adjust to
#            the memory that is available to it dynamically.
#
#            If the bound is low, purging occurs frequently, saving
#            only data for stations that have been recently active on
#            the network.  If this happens, a message appears on the
#            system console indicating that not enough memory has been
#            allocated to NetWare LANalyzer Agent.
#
#            KB is the memory bound in kilobytes.
#
#            Initial value:                 set by the install program
#                                           based on memory usage
#
#            Minimum recommended value:     512
#
#            Maximum recommended value:     75% of free server memory
#                                           when NLM files are loaded
#
#            Default value:                 If bound=KB is not specified,
#                                           it defaults to 2048.
```

```
# age=HHH    NetWare LANalyzer Agent purges data for stations that have
#            not been active on the network recently. This parameter
#            controls how long data for inactive stations is maintained.
#
#            Memory that is used by the station table is not available
#            for other uses, such as capturing packets.  Reducing the
#            age value tends to increase the amount of memory
#            available for capturing packets.
#
#            If you cannot allocate capture buffers that are large,
#            you may need to reduce the age value.
#
#            HHH is the inactivity period, in hours, before station data
#            is purged.
#
#            Minimum recommended value:      1
#
#            Default value:                  If age=HHH is not specified,
#                                            it defaults to 168  (1 week)
#
# load LANZDI level=1
#
# level=1    It indicates that the LANZDI will stop receiving packets
#            when CPU utilization gets high.
#
#            Default is OFF. LANZDI will continue to receive packets even
#            when CPU utilization gets high.
#
# load LANZSM topn=N
#
# topn=N     The number of concurrent top N station sorts that are
#            allowed by NetWare LANalyzer Agent.
#
#            Recommended value:              4
#            Minimum value:                  2
#            Maximum value:                  10
#
# load LANZCTL trapreg=1
#
# trapreg=1  Causes SNMP traps to be sent to management consoles
#            advertising themselves on the network as well as stations
#            listed in sys:\etc\traptarg.cfg.  Omitting this parameter
#            or setting it to 0 causes traps to be sent only to those
#            stations listed in sys:\etc\traptarg.cfg.
#
#-----------------------------------------------------------------------------

LOAD LANZSU.NLM
LOAD LANZMEM.NLM bound=2048
LOAD LANZLIB.NLM
LOAD LANZDI.NLM
LOAD LANZAEL.NLM
LOAD LANZHIS.NLM
LOAD LANZFCB.NLM
LOAD LANZSM.NLM topn=4
#LOAD LANZTR.NLM
LOAD LANZCTL.NLM trapreg=1
```

Appendix B. OS/2 System Files

B.1 CONFIG.SYS for OS/2, TCP/IP, NetWare Requester, LAN Requester, LMU and DB2/2

```
IFS=C:\OS2\HPFS.IFS  /CACHE:2048 /CRECL:32 /AUTOCHECK:CD
PROTSHELL=C:\OS2\PMSHELL.EXE
SET USER_INI=C:\OS2\OS2.INI
SET SYSTEM_INI=C:\OS2\OS2SYS.INI
SET OS2_SHELL=C:\OS2\CMD.EXE
SET AUTOSTART=PROGRAMS,TASKLIST,FOLDERS,CONNECTIONS
SET RUNWORKPLACE=C:\OS2\PMSHELL.EXE
SET COMSPEC=C:\OS2\CMD.EXE
LIBPATH=D:\SQLLIB\DLL;C:\IBMCOM\DLL;.;C:\USERDLLS;C:\OS2\DLL;C:\IBMLAN\NETLIB;
C:\MUGLIB\DLL;C:\OS2\APPS\DLL;C:\CMLIB\DLL;C:\OS2\MDOS;C:\;\\WTRDC\LANDLLS;
D:\TCPIP\DLL;D:\LMU2;D:\NETWARE;
SET PATH=D:\SQLLIB;C:\CMDS;C:\OS2UTILS;C:\OS2;C:\IBMLAN\NETPROG;C:\MUGLIB;
C:\CMLIB;C:\OS2\SYSTEM;C:\OS2\APPS;C:\OS2\MDOS\WINOS2;C:\OS2\INSTALL;
C:\OS2\MDOS;C:\;D:\TCPIP\BIN;D:\LMU2;D:\NETWARE;L:\OS2;P:\OS2;L:\NLS;P:\NLS;
SET DPATH=D:\SQLLIB;C:\IBMCOM;C:\OS2UTILS;C:\OS2;C:\IBMLAN\NETPROG;C:\IBMLAN;
C:\MUGLIB;C:\CMLIB;C:\OS2\SYSTEM;C:\OS2\APPS;C:\OS2\MDOS\WINOS2;
C:\OS2\INSTALL;C:\OS2\BITMAP;C:\OS2\MDOS;D:\LMU2;C:\;D:\NETWARE;L:\OS2;
P:\OS2;L:\NLS;P:\NLS;
SET PROMPT=$effl7mOS2$effl0m $P$G
SET HELP=D:\SQLLIB;C:\OS2\HELP;C:\HELPLIB;C:\OS2\HELP\TUTORIAL;C:\CMLIB;
D:\TCPIP\HELP;D\LMU2;D:\LMU2;
SET BOOKSHELF=D:\SQLLIB\BOOK;C:\IBMLAN\BOOK;C:\OS2\BOOK;C:\INFLIB;
C:\CMLIB\BOOK;D:\TCPIP\DOC;D\LMU2;D:\LMU2;
SET EPMPATH=C:\EBOOKIE2;C:\OS2\APPS;
SET GLOSSARY=C:\OS2\HELP\GLOSS;
SET CMPATH=C:\CMLIB
SET IPF_KEYS=SBCS
SET KEYS=ON
rem ** ** ** ** ** ** ** ** ** **
PRIORITY_DISK_IO=YES
FILES=40
BUFFERS=60
IOPL=YES
MAXWAIT=3
MEMMAN=SWAP,PROTECT
SWAPPATH=D:\ 2048 12288
BREAK=OFF
THREADS=1024
PRINTMONBUFSIZE=134,134,134
COUNTRY=001,C:\OS2\SYSTEM\COUNTRY.SYS
rem ** ** ** ** ** ** ** ** ** **
PROTECTONLY=NO
SHELL=C:\OS2\MDOS\COMMAND.COM C:\OS2\MDOS
FCBS=16,8
RMSIZE=640
DOS=LOW,NOUMB
rem ** ** ** ** ** ** ** ** ** **
BASEDEV=PRINT02.SYS
BASEDEV=IBM2FLPY.ADD
```

```
BASEDEV=IBM2SCSI.ADD /LED
BASEDEV=OS2DASD.DMD
BASEDEV=XGA.SYS
rem ** ** ** ** ** ** ** ** ** **
DEVICE=C:\IBMCOM\PROTOCOL\LANPDD.OS2
DEVICE=C:\IBMCOM\PROTOCOL\LANVDD.OS2
DEVICE=C:\OS2\TESTCFG.SYS
DEVICE=C:\OS2\DOS.SYS
DEVICE=C:\OS2\PMDD.SYS
DEVICE=C:\OS2\POINTDD.SYS
DEVICE=C:\OS2\MOUSE.SYS
DEVICE=C:\OS2\COM.SYS
DEVICE=C:\OS2\XGARING0.SYS
DEVICE=C:\OS2\EPWDD.SYS
DEVICE=C:\OS2\LOG.SYS
rem ** ** ** ** ** ** ** ** ** **
DEVICE=C:\OS2\MDOS\VEMM.SYS
DEVICE=C:\OS2\MDOS\VXMS.SYS /UMB
DEVICE=C:\OS2\MDOS\VDPMI.SYS
DEVICE=C:\OS2\MDOS\VDPX.SYS
DEVICE=C:\OS2\MDOS\VCDROM.SYS
DEVICE=C:\OS2\MDOS\VWIN.SYS
DEVICE=C:\OS2\MDOS\VMOUSE.SYS
DEVICE=C:\OS2\MDOS\VCOM.SYS
DEVICE=C:\OS2\MDOS\VVGA.SYS
DEVICE=C:\OS2\MDOS\VXGA.SYS
rem ** ** ** ** ** ** ** ** ** **
CODEPAGE=850,437
DEVINFO=KBD,US,C:\OS2\KEYBOARD.DCP
DEVINFO=SCR,VGA,C:\OS2\VIOTBL.DCP
SET VIDEO_DEVICES=VIO_XGA
SET VIO_XGA=DEVICE(BVHVGA,BVHXGA)
rem ** ** ** ** ** ** ** ** ** **
DEVICE=C:\IBMCOM\LANMSGDD.OS2 /I:C:\IBMCOM
DEVICE=C:\IBMCOM\PROTMAN.OS2 /I:C:\IBMCOM
DEVICE=C:\IBMCOM\PROTOCOL\NETBEUI.OS2
DEVICE=C:\IBMCOM\PROTOCOL\NETBIOS.OS2
DEVICE=C:\IBMCOM\PROTOCOL\LANDD.OS2
DEVICE=C:\IBMCOM\PROTOCOL\LANDLLDD.OS2
DEVICE=C:\IBMCOM\MACS\IBMTOK.OS2
rem ** ** ** ** ** ** ** ** ** **
DEVICE=C:\IBMLAN\NETPROG\RDRHELP.200
REM --- NetWare Requester statements BEGIN ---
SET NWLANGUAGE=ENGLISH
DEVICE=D:\NETWARE\LSL.SYS
RUN=D:\NETWARE\DDAEMON.EXE
DEVICE=C:\IBMCOM\PROTOCOL\ODI2NDI.OS2
REM -- ODI-Driver Files BEGIN --
DEVICE=D:\NETWARE\ROUTE.SYS
REM -- ODI-Driver Files END --
DEVICE=D:\NETWARE\IPX.SYS
DEVICE=D:\NETWARE\SPX.SYS
RUN=D:\NETWARE\SPDAEMON.EXE
DEVICE=D:\NETWARE\NMPIPE.SYS
DEVICE=D:\NETWARE\NPSERVER.SYS
RUN=D:\NETWARE\NPDAEMON.EXE
DEVICE=D:\NETWARE\NWREQ.SYS
IFS=D:\NETWARE\NWIFS.IFS
```

```
RUN=D:\NETWARE\NWDAEMON.EXE
DEVICE=D:\NETWARE\NETBIOS.SYS
RUN=D:\NETWARE\NBDAEMON.EXE
DEVICE=D:\NETWARE\VIPX.SYS
DEVICE=D:\NETWARE\VSHELL.SYS PRIVATE
REM --- NetWare Requester statements END ---
IFS=C:\IBMLAN\NETPROG\NETWKSTA.200 /I:C:\IBMLAN /N
DEVICE=C:\IBMLAN\NETPROG\VNETAPI.OS2
rem ** ** ** ** ** ** ** ** ** **
DEVICE=C:\CMLIB\ACSLANDD.SYS
DEVICE=C:\CMLIB\CMKFMDE.SYS
rem ** ** ** ** ** ** ** ** ** **
RUN=C:\IBMCOM\PROTOCOL\NETBIND.EXE
RUN=C:\IBMCOM\LANMSGEX.EXE
RUN=C:\IBMCOM\PROTOCOL\LANDLL.EXE
RUN=C:\IBMLAN\NETPROG\LSDAEMON.EXE
RUN=C:\IBMLAN\NETPROG\VNRMINIT.EXE
RUN=C:\OS2\EPWDDR3.EXE
RUN=C:\OS2\EPW.EXE
RUN=C:\OS2\SYSTEM\LOGDAEM.EXE
RUN=C:\OS2\EPWROUT.EXE 1
DEVICE=C:\IBMCOM\PROTOCOL\INET.SYS
DEVICE=C:\IBMCOM\PROTOCOL\IFNDIS.SYS
SET ETC=D:\TCPIP\ETC
SET TMP=D:\TCPIP\TMP
SET READIBM=D:\TCPIP\DOC;D:\LMU2;
SET HOSTNAME=nvclient
RUN=D:\TCPIP\BIN\CNTRL.EXE
IFS=D:\TCPIP\BIN\NFS200.IFS
SET DISPLAY=nvclient:0
SET XFILES=D:\TCPIP\X11
SET TZ=est5edt
SET NFS.PERMISSION.BITS=700
SET NFS.PERMISSION.DBITS=700
SET USER=nvclient
SET PASSWD=cm4121r
SET TELNET.PASSWORD.ID=cm4121r
SET SYSCONTACT=Debbie Sparg
SET SYSLOCATION=ITSO, Raleigh
SET INCLUDE=D:\SQLLIB;
SET LIB=D:\SQLLIB;
DEVICE=D:\LMU2\LMUIPL.SYS
SET BOOKMGR=D:\LMU2;
SET QRWDR=D:
SET QRWINST=D:\SQLLIB
```

B.2 PROTOCOL.INI for OS/2, TCP/IP, NetWare Requester, LAN Requester, LMU and DB2/2

```
[PROT_MAN]

    DRIVERNAME = PROTMAN$

[IBMLXCFG]

    landd_nif = landd.nif
```

```
                    netbeui_nif = netbeui.nif
                    odi2ndi_nif = odi2ndi.nif
                    tcpip_nif = tcpip.nif
                    IBMTOK_nif = ibmtok.nif

                [landd_nif]

                    DriverName = LANDD$
                    Bindings = IBMTOK_nif
                    NETADDRESS = "T400052005144"
                    ETHERAND_TYPE = "I"
                    SYSTEM_KEY = 0x0
                    OPEN_OPTIONS = 0x2000
                    TRACE = 0x0
                    LINKS = 32
                    MAX_SAPS = 30
                    MAX_G_SAPS = 0
                    USERS = 5
                    TI_TICK_G1 = 255
                    T1_TICK_G1 = 15
                    T2_TICK_G1 = 3
                    TI_TICK_G2 = 255
                    T1_TICK_G2 = 25
                    T2_TICK_G2 = 10
                    IPACKETS = 250
                    UIPACKETS = 100
                    MAXTRANSMITS = 6
                    MINTRANSMITS = 2
                    TCBS = 64
                    GDTS = 30
                    ELEMENTS = 800

                [netbeui_nif]

                    DriverName = netbeui$
                    Bindings = IBMTOK_nif
                    NETADDRESS = "T400052005144"
                    ETHERAND_TYPE = "I"
                    USEADDRREV = "YES"
                    OS2TRACEMASK = 0x0
                    SESSIONS = 100
                    NCBS = 100
                    NAMES = 65
                    SELECTORS = 5
                    USEMAXDATAGRAM = "NO"
                    ADAPTRATE = 1000
                    WINDOWERRORS = 0
                    MAXDATARCV = 4168
                    TI = 30000
                    T1 = 500
                    T2 = 200
                    MAXIN = 1
                    MAXOUT = 1
                    NETBIOSTIMEOUT = 500
                    NETBIOSRETRIES = 8
                    NAMECACHE = 0
                    PIGGYBACKACKS = 1
                    DATAGRAMPACKETS = 2
```

```
      PACKETS = 350
      LOOPPACKETS = 1
      PIPELINE = 5
      MAXTRANSMITS = 6
      MINTRANSMITS = 2
      DLCRETRIES = 5
      FCPRIORITY = 5
      NETFLAGS = 0x0

[odi2ndi_nif]

      DriverName = odi2ndi$
      Bindings = IBMTOK_nif
      NETADDRESS = "T400052005144"
      TOKEN-RING = "yes"
      TOKEN-RING_SNAP = "no"
      ETHERNET_802.3 = "no"
      ETHERNET_802.2 = "no"
      ETHERNET_II = "no"
      ETHERNET_SNAP = "no"
      TRACE = 0x0

[tcpip_nif]

      DriverName = TCPIP$
      Bindings = IBMTOK_nif

[IBMTOK_nif]

      DriverName = IBMTOK$
      ADAPTER = "PRIMARY"
      MAXTRANSMITS = 6
      RECVBUFS = 2
      RECVBUFSIZE = 256
      XMITBUFS = 1
```

Index

Numerics

A

B

C

D

E

O

ITSO Technical Bulletin Evaluation
RED000

International Technical Support Organization
Integrating NetWare Management into NetView for AIX
October 1995

Publication No. SG24-2532-00

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. _____

ITSO Technical Bulletin Evaluation RED000
SG24-2532-00

IBM®

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 HZ8, Building 678
P.O. BOX 12195
RESEARCH TRIANGLE PARK NC
USA 27709-2195

Fold and Tape   **Please do not staple**   Fold and Tape

IBM ®

Printed in U.S.A.