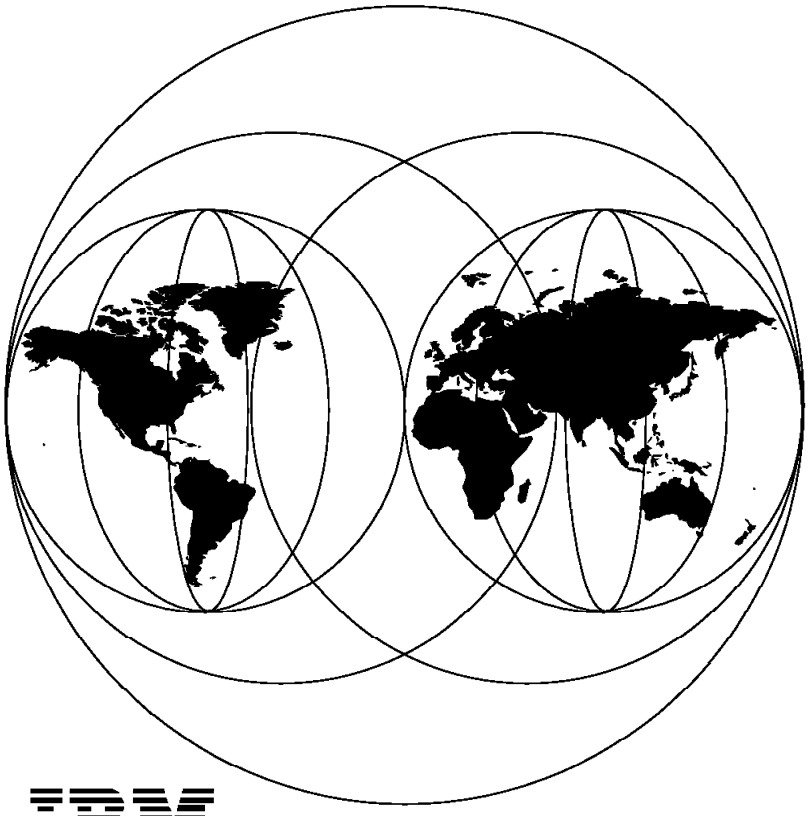
SG24-4756-00

Local Area Network Concepts and Products: LAN Operation Systems and Management

May 1996



IBM

International Technical Support Organization
Raleigh Center

International Technical Support Organization

SG24-4756-00

Local Area Network Concepts and Products: LAN Operation Systems and Management

May 1996

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix A, “Special Notices” on page 187.

First Edition (May 1996)

This edition applies to the most recent IBM LAN products and LAN architectures.

Comments may be addressed to:
IBM Corporation, International Technical Support Organization
Dept. HZ8 Building 678
P.O. Box 12195
Research Triangle Park, NC 27709-2195

Contents

Preface

Local Area Network Concepts and Products is a set of four reference books for those looking for conceptual and product-specific information in the LAN environment. They provide a technical introduction to the various types of IBM local area network architectures and product capabilities. The four volumes are as follows:

- SG24-4753-00 - *LAN Architecture*
- SG24-4754-00 - *LAN Adapters, Hubs and ATM*
- SG24-4755-00 - *Routers and Gateways*
- SG24-4756-00 - *LAN Operating Systems and Management*

To obtain all four books, order the set SK2T-1306.

These redbooks complement the reference material available for the products discussed. Much of the information detailed in these books is available through current redbooks and IBM sales and reference manuals. It is therefore assumed that the reader will refer to these sources for more in-depth information if required.

These documents are intended for customers, IBM technical professionals, services specialists, marketing specialists, and marketing representatives working in networking and in particular the local area network environments. Details on installation and performance of particular products will not be included in these books, as this information is available from other sources.

Some knowledge of local area networks, as well as an awareness of the rapidly changing intelligent workstation environment, is assumed.

How This Redbook Is Organized

The redbook is organized as follows:

- Chapter 1, “LAN Operating Systems and Resource Services”

  This chapter provides information relating to LAN operating systems that are currently available. Included are LAN Server, NetWare and Lotus Notes.

- Chapter 2, “LAN Management”

  This chapter describes IBM′s LAN management products and functions. It also includes information on how to position IBM′s products.

The Team That Wrote This Redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization Raleigh Center.

The advisors for this project were:

Ricardo Haragutchi
International Technical Support Organization, Raleigh

John Parker
International Technical Support Organization, Raleigh

The authors of this document were:

Edmilson Barbosa
IBM Brazil

Ingvar Hyleborg
IBM Sweden

Jefferson da Silva
IBM/GSI Brazil

Klaus Wichmann
ITSO Raleigh

Marcello Belloni Gomes
IBM Brazil

Thanks to the following people for their invaluable contributions to this project:

Toshi Shimizu
International Technical Support Organization, Austin

Aroldo Yai
Barry Nusbaum
Donna Fox
Fergus Stewart
Jose Boo
Juan Rodriguez
Mark DeCain
Mohammad Shabani
Robert Macgregor
Stephen Breese
Volkert Kreuk
International Technical Support Organization, Raleigh

Alan Millard
Arthur Bond
Bert Wendle
Carol Carson
Dean Stockwell
Erik Dixon
H. Parrish

Paul Carter
IBM Research Triangle Park, Raleigh NC.

Comments Welcome

We want our redbooks to be as helpful as possible. Should you have any comments about this or other redbooks, please send us a note at the following address:

redbook@vnet.ibm.com

Your comments are important to us!

Chapter 1. LAN Operating Systems and Resource Services

When LAN workstations are installed with LAN adapters (for example, the IBM Token-Ring adapter or IBM Ethernet adapter) and connected, a physical LAN is set up but it is not functional yet. In the layered network architecture, this is the lowest layer called the physical layer. Within the LAN adapter itself exists built-in logic for part of the medium access control (MAC) sublayer of the data link control (DLC) layer. The other part of the MAC sublayer is handled by the LAN adapter device driver.

When LAN workstations are loaded with communications software, for example, the IBM LAN Support Program (LSP) or IBM Multiple Protocol Transport Services (MPTS), to provide protocols for transferring messages across the physical link between two workstations, a communicating LAN is established. A commonly used protocol, logical link control (LLC) sublayer is IEEE 802.2. This is supported in the LSP which is a DOS-based product and in MPTS which is an OS/2-based product. Please refer to Chapter 1 in *Local Area Network Concepts and Products: LAN Adapters, Hubs and ATM*, SG24-4754 for more details on LAN adapters and supporting software.

Note

An SNA backbone ring with 3745 communications controllers and 3174 establishment controllers connected for the purpose of communications only is, strictly speaking, not a LAN. The controllers are using the token-ring merely as a means of passing SNA frames.

For the LAN to be fully functional, with the capability of sharing network resources like files and printers, a LAN operating system is required. A device that enables other workstations to share its files is called a *file server* and one that enables other workstations to share its printers is called a *print server*. The beginning of this chapter introduces you to the IBM ServerGuide, which is a package of different LAN server products. The ServerGuide is shipped with IBM PC Server Systems, and helps you to set up your LAN server software.

This chapter takes a closer look at two commonly used LAN operating systems in the PC environment, also shipped with the IBM ServerGuide:

- IBM OS/2 LAN Server 4.0
- Novell NetWare

With the ever-changing complexity of computer networking, the boundary of LANs has grown beyond that of just PCs; mid-range computers and even mainframes are playing a more significant role in the LAN environment. Some of the common LAN environments with mid-range computers or mainframes are also discussed:

- AS/400 PC Support
- IBM LANRES
- IBM LAN File System

With the increasing number of users connected to a LAN, the desire for people to work together over the LAN came up. Groupware is a client/server solution to

provide people with E-mail and the possibility of interacting over a network. Many people share the same databases stored on one or more servers on the LAN. This chapter discusses the basics of:

- Lotus Notes

1.1 IBM ServerGuide

The IBM ServerGuide V2.4 is a package of different LAN servers and operating systems as well as LAN Management tools. ServerGuide is only shipped with IBM PC Server systems or as an upgrade to the previously available ServerGuide versions. Of course all products included in the ServerGuide are available as separate products.

The ServerGuide is shipped with the following products:

- IBM PC Server 720
- IBM PC Server 500 series
- IBM PC Server 310
- IBM PC Server 320
- IBM PS/2 Server 95A
- IBM PS/2 Server 95
- IBM PS/2 Server 85
- IBM PS/2 Server 77i and Enhanced 77i

The ServerGuide comes on eight CDs, which contain both encrypted and non-encrypted software products. When you receive your IBM PC Server system you can order activation keys, at a charge, to decrypt (those software products encrypted) and install the software products you require. The following software is shipped with ServerGuide:

- OS/2 Warp V3.0 with WIN-OS/2
- NetFinity V3.05
- OS/2 2.11 SMP (1 to 2 processors)
- OS/2 2.11 SMP (1 to 7 processors)
- LAN Server 4.0 Entry
- LAN Server 4.0 Advanced
- Upgrade LAN Requester V3.0 to LAN Requester V4.0
- Upgrade LAN Server 3.0 Entry to 4.0 Entry
- Upgrade LAN Server 3.0 Advanced to 4.0 Advanced
- Upgrade LAN Server 4.0 Entry to 4.0 Advanced
- NetWare 3.12 (1)
- NetWare 4.1 (1)
- NetWare 4.1 SMP for 1 to 4 processors
- SCO Open Server Enterprise 3.0 (2)
- SCO Multi Processing Extensions (2)

- TCP/IP 2.0 Base Kit
- System Performance Monitor/2

You can install and configure the operating system and networking operating system of your choice by simply inserting the first compact disc from the ServerGuide package into your CD-ROM drive, inserting the diskette into the diskette drive, and starting the IBM PC Server. An easy-to-use graphical interface guides you through the simple installation steps. The ServerGuide menus take you through a series of configuration choices after which you type in a unique activation key (which can be purchased from your IBM remarketer or IBM representative) to unlock the software and install it. During installation, ServerGuide automatically detects and identifies specific hardware configurations and fills in all configuration choices with sensible defaults, so you can simply accept ServerGuide's suggestions, or if you want, change them to reflect different requirements. ServerGuide then automatically installs the necessary device drivers.

After using ServerGuide to install the operating system and network operating system you can still use ServerGuide's additional utilities and extensive online reference documentation and diskette images to support and enhance your day-to-day running of your LAN.

1.1.1.1 IBM OS/2 LAN Server and NetWare Integration Guides

The IBM Server Integration Guides, one for OS/2 LAN Server and one for NetWare, provide detailed information about IBM Servers. They are available on the ServerGuide CDs for viewing.

The IBM Server Integration Guides cover:

- Server planning and implementation
- Factors affecting server performance
- Optimizing server performance
- Server security, fault tolerance, and backup
- Network management

1.2 OS/2 LAN Server

The IBM OS/2 LAN Server is a LAN product, that allows you to share different resources like drives or printers over your LAN.

The IBM OS/2 LAN Server program provides you with:

- OS/2 LAN Server (Entry or Advanced)
- OS/2 LAN Requester
- DOS LAN Services (DLS)
- Multiple Protocol Transport Services (MPTS)
- LAN Support Program (LSP)
- LAN utilities

The OS/2 LAN Server is a network operating system that provides LAN capabilities to interconnect workstations on the IBM PC Network, token-ring LAN and Ethernet LAN, and manages the sharing of LAN resources. The LAN Server

Entry is running in a non-dedicated mode on an OS/2 machine, which means, that the server machine can also be used as a workstation.

Each requester workstation needs to install either the OS/2 LAN Requester or the DOS LAN Services in order to access the shared devices of the LAN server. DOS LAN Services is the component of LAN Server that provides LAN connectivity for users of workstations running DOS. You can use DOS LAN Services in a DOS environment with or without Windows.

LAPS (LAN adapter and protocol support) configures the LAN adapter by installing the NDIS (network driver interface specification) interface and sets up the protocol support. LAPS is used for OS/2 workstations and OS/2 servers and is part of MPTS (multiprotocol transport services). The LAN Support Program is the equivalent for DOS. With MPTS it is possible to use TCP/IP over NetBIOS or NetBIOS over TCP/IP. The AnyNet/2 product from IBM enhances the possibilities to use multiple protocols over one or more transport protocol.

The OS/2 LAN Server 4.0 is available in two different versions: LAN Server Entry and LAN Server Advanced. The LAN Server Advanced provides a high-performance, high-availability file and print server. It has a more advanced recovering system and can handle up to 1000 users. The requester functions are the same as those of the LAN Server Entry package.

In this section, the fundamentals of the IBM OS/2 LAN Server are first discussed, followed by the key features of the current level of IBM OS/2 LAN Server 4.0.

1.2.1 IBM OS/2 LAN Server Fundamentals

A LAN server is a workstation with the OS/2 LAN Server software loaded. A LAN server shares different resources or devices with other workstations. OS/2 LAN Server provides a single system image to its users, using the concept of *domain*. A domain is a group of servers that provide resources as if they were one server. Each domain has its domain controller, that is designated to manage the domain and to coordinate communication between servers and requesters.

A LAN requester is a workstation with the OS/2 LAN Requester software loaded. Each workstation in a domain has to log on to the domain controller, that must be running, before a user can use its resources. If a password is needed to access the domain, the user is prompted for his password, before he can use resources of the domain. A requester uses the services of the server in accessing the LAN resources. An application running on a workstation can send requests over the LAN Requester or the DOS LAN Services to the LAN server, that processes the request. The LAN server receives the request, supplies the shared resource, and passes the response back.

A peer workstation is a special type of requester. Like a server, a peer workstation shares resources with other users on a LAN. However, a peer workstation can share resources with only one user at a time. A peer workstation can also function as a requester. Both OS/2 and DOS LAN requesters can be peer workstations.

Shared resource in a LAN can be the following:

- Disks, directories, files
- Printers
- Serial devices

- Applications

Both, the server and the requester are using a graphical user interface (GUI). In addition, commands can be used for the same purpose. The requester uses the GUI to change user-specific assignments or to change user definitions such as the password. The LAN administrator uses the GUI for managing users, groups, servers, domains and for controlling, defining and managing access to the LAN resources.

1.2.2 Server

A server is a workstation that provides resources (such as disks, printers, plotters, serial devices, and remote computing) to users on the LAN. The following server functions are provided with the OS/2 LAN Server 4.0:

- Server and requester functions
- First Failure Support Technology/2 (FFST/2)
- Generic alerter
- LAN Server Applications Development Toolkit
- Migration Import Utility (for PCLP migration)
- Network DDE and Clipboard
- Network messaging
- Remote IPL (OS/2 and DOS)
- Uninterruptible power supply
- User profile management
- Virtual DOS LAN API support

A LAN server is always part of a domain. Each domain has one domain controller. If the server is the only server in the LAN, it must also be the domain controller. As a domain is a group of servers, there can be additional servers in the domain. One of the additional servers can be used as the backup domain controller. IBM LAN Server 4.0 defines three different workstation types for server, that are discussed in the following:

- Domain controller
- Backup domain controller
- Additional server

Note

A server with OS/2 LAN Server 4.0 Entry installed can also function as a requester. LAN Server 4.0 Advanced is designed as a dedicated server.

1.2.2.1 Domain Controller

A domain consists of one or more servers that allocate resources as a single logical system. A physical LAN can be divided into several logical domains, with each domain independently managed by a domain controller. The network administrator will designate one server within the domain to be the domain controller and thus, each domain has only one domain controller. The network

administrator is a person who organizes LAN servers into domains and defines resources and users within the domain.

Note

A domain must have at least one server, and that one server will also be the domain controller. A domain can have several servers but a server can belong to only one domain.

The domain controller coordinates communications between servers and requesters. The domain controller must be installed and running before users can log on to the domain and use its resources. Servers will not start unless the domain controller is running. The other servers in the domain receive information about users and groups of users from the domain controller.

Each user in a domain is assigned a user ID, which identifies the user to the domain. A special user is the administrator of a domain, who can log on at any OS/2 workstation within the domain and access any resource in the domain from that workstation. A user ID can be valid on more than one domain in the network. You can log on to any domain from any requester in the network. However, you can log on to only one domain at a time. You cannot log on to a domain from a server in a different domain.

Definitions for network resources reside at the domain controller in the domain control database (DCDB). The DCDB contains files, applications and machine definitions. In addition, the domain controller maintains the master user and group definitions file (NET.ACC). Updates to the file are made at the domain controller and then copied to all servers on the domain.

1.2.2.2 Backup Domain Controller

A backup domain controller maintains a copy of the DCDB. When a backup domain controller is defined and started, users can log on to and use the domain, even if the domain controller has failed or is busy retrieving information stored in the DCDB. The administrator can define one or more backup domain controllers to receive DCDB information, during LAN Services installation and configuration. Any existing server in the domain, including the domain controller, can be redefined as a backup domain controller.

In order for replication of the DCDB information to occur, a DCDB replicator service is started on the domain controller and backup domain controller, using the autostart feature or the `NET START DCDBREPL` command. The DCDB replicator service is not related to the replicator service, and both may reside on the domain controller or backup domain controllers. After the DCDB replicator service is started, information in the DCDB on the domain controller is automatically copied to the backup domain controllers whenever updates occur. The replicated DCDB information includes all files in the \IBMLAN\DCDB subdirectory, except remote IPL files.

1.2.2.3 Additional Server

Besides the server, which is designated as the domain controller, all other servers in the domain are called *additional servers*. Additional servers receive user and group information from the domain controller. Any additional server in the network can be redefined as a backup domain controller.

1.2.3 Requester

A requester is a workstation from which a user can log on to a domain and access shared resources or use the processing capability of the server. There are two main types of requesters in the IBM OS/2 LAN Server 4.0 environment, namely the OS/2 LAN Requester and the DOS LAN Services. Each of the requesters can be stated via remote IPL. A requester can use peer services to share resources with other users. The following types of LAN requesters are discussed in more detail on the next pages:

- OS/2 LAN Requester
- DOS LAN Services (LAN Requester)
- OS/2 and DOS Remote IPL
- OS/2 and DOS Peer Server

1.2.3.1 OS/2 LAN Requester

The OS/2 LAN Requester offers a graphical user interface to access and manage resources of the domain that the user is allowed to access. You can use the OS/2 LAN Requester GUI, to change your password, to define logon assignments and applications you use. As in OS/2 LAN Server 3.0, you can issue commands in an OS/2 window to use these functions. The OS/2 LAN Server 4.0 provides the following functions to your requester workstation:

- Requester functions
- Fault Tolerance administration
- First Failure Support Technology/2 (FFST/2)
- Network DDE and Clipboard
- Network messaging
- Peer
- Requester installation/configuration program
- User profile management
- Virtual DOS LAN API support

An OS/2 LAN Requester consists of an OS/2 LAN Requester program running on an IBM OS/2 base operating system, with the LAN Adapter Protocol Support (LAPS) installed and configured appropriately. A DOS application running in a virtual DOS machine (VDM) at an OS/2 LAN Requester workstation can access disk and printer resources of the OS/2 LAN Server. Likewise, a Windows application running in WIN-OS2 at an OS/2 LAN Requester workstation can gain access to the OS/2 LAN Server.

1.2.3.2 DOS LAN Services (LAN Requester)

The DOS LAN Services will provide you with the following functions at your DOS requester workstation:

- Log on and log off an OS/2 LAN Server domain
- Change logon assignments, passwords, user comments
- List logged on users
- Broadcast, send and receive messages
- View, connect, and disconnect shared directory aliases

- View, install, and use LAN Server shared applications
- Manage print jobs in shared print queues
- View, connect, and disconnect shared printers
- View directory-limit information for a shared directory (Windows only)
- Share local directories and printers with other network users
- View, connect, and disconnect any LAN Server shared serial printer that is configured as a shared printer rather than as a serial device

A DOS LAN Requester is a workstation that runs DOS as its base operating system, with the LAN Support Program (LSP) installed and loaded appropriately. The DOS LAN Services program also provides an interface to Microsoft Windows. It allows users of Microsoft Windows V3.x to access the network files, printers, applications, and other services available on the OS/2 LAN Server domain through the graphical user interface (GUI) of Windows. The DOS LAN Services Windows support is available only on DOS V5.0 or higher. When you use DOS LAN Services without Windows, you can access the network resources through the DOS LAN Services graphical user interface.

1.2.3.3 OS/2 and DOS Remote IPL

A requester with the appropriately configured hardware (an adapter that supports remote IPL) is needed and the use of a remote initial program load (remote IPL), which allows both DOS and OS/2 workstations to receive the initial program image from a LAN Server instead of from a local fixed disk or diskette. This function supports requesters with or without local media (hard-disk or diskette drives). OS/2 LAN Server 4.0 supports remote IPL for OS/2 LAN Requester and DOS LAN Services. To make use of remote IPL, a requester must have the supported adapters. The DOS remote IPL is supported only on DOS V5.0 or higher. A DOS LAN Requester workstation without a fixed disk but with a diskette drive can also be started from diskette.

1.2.3.4 OS/2 and DOS Peer Server

A requester with the peer service installed can act as a peer server. Like a server, a peer server provides resources to users on a LAN. A peer server is, however, limited to providing resources to only one user at a time. A peer server running on a requester needs not to be defined to the domain controller. OS/2 LAN Server 4.0 supports peer services for DOS and OS/2 workstations. DOS requester can access shared resources on an OS/2 peer server and vice versa.

You can administer the peer service both locally and remotely though a command line interface. A graphical user interface (GUI) is not provided to administer a peer workstation. In order for you to administer a peer workstation, you must be defined as an administrator in the peer workstation local user accounts database.

It is common for the owner of a peer workstation to be defined as an administrator on the peer workstation but defined as a user on the domain. The peer administrator can manage resources for only the peer workstation, but not the rest of the domain. Since the peer workstation is not part of a LAN Server domain, it cannot be administered through the LAN Server Version 4.0 GUI.

1.2.4 The Graphical User Interface (GUI)

OS/2 LAN Server 4.0 provides a graphical user interface to manage requesters and servers. The user interface is object-oriented and allows the user or administrator to configure and use the network via the manipulation of visual objects. The paradigm used has a consistent look and feel with the Workplace Shell (WPS) that is currently in the OS/2 2.X and OS/2 Warp product set. The requester offers only a subset of the functions from the LAN server.

The object-oriented graphical user interface enables you to take advantage of drag-and-drop capabilities used in other OS/2 applications and OS/2 itself. Instead of drag-and-drop, you can use the pull-down menus. LAN Server 4.0 does not replace the commands used in LAN Server 3.0 to manage and access the network and its resources; they can still be used. LAN Server commands have the following format:

```
NET command options
```

Each user, group, server, domain or resource is represented by an object. The symbol of an object is an icon residing in a folder. Like any other OS/2 object, you can change its settings by double-clicking the icon or by opening its settings. For example you can change your password by simply double-clicking our user account icon in the user account folder. The settings notebook for your user account object will be opened and you can make your changes.

The drag-and-drop capabilities make it very easy to manage resources, groups, users and servers in your domain. If, for example, you want to give a user access to a resource, you simply drop the icon representing the user on the icon representing the resource. A notebook will be open to define the access rights of the user to that resource. Another example is to make users members of a group. You simply select all icons of the users and drop them on to the group icon.

To create new user accounts, groups, resources, additional servers applications or resources, you only have to drop a template of the specific type into the corresponding folder. A notebook will be opened to let you make the definitions of the object.

1.2.5 Connectivity

All these different LAN servers and LAN requester configurations can coexist in the same domain, sharing resources of the OS/2 LAN Servers and resources from requesters with peer services installed. Figure 1 on page 10 shows a typical LAN domain, with two servers, one configured as the domain controller and one configured as the backup domain controller. Different requesters are running under different operating systems, sharing the resources of the servers. In addition, both servers function as printer server to share their printers. Two clients are configured as peer server. One only shares its printer with one other workstation, the other shares its files.

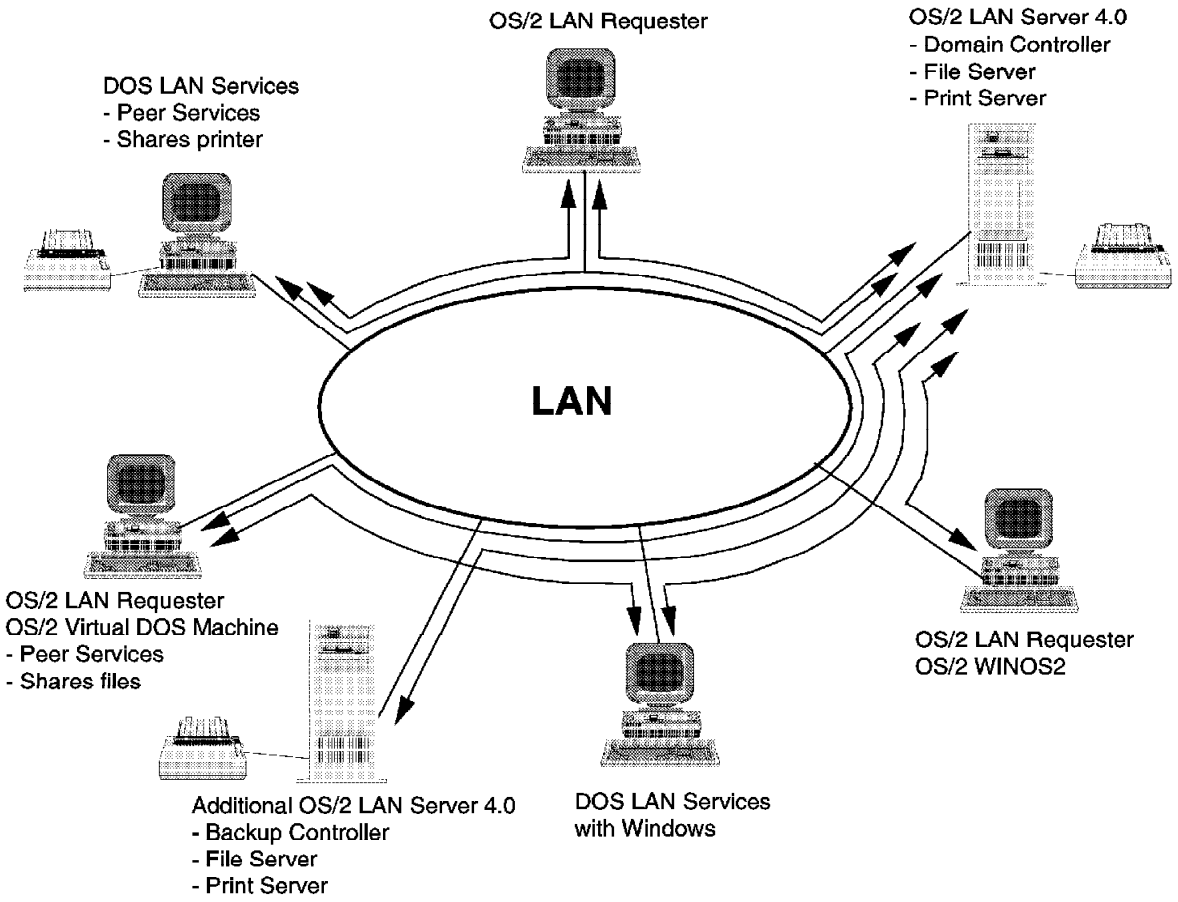


Figure 1. An OS/2 LAN Server V4.0 Environment

A user (or network administrator) at an OS/2 or DOS requester on a LAN may access any domain in which the appropriate access control profiles have been defined. The access control profiles are defined by the administrator who manages the resources. An administrator can perform administrator tasks only at an OS/2 workstation as the IBM OS/2 LAN Server is an OS/2-based program. A user can log on to only one domain at a time. For each domain the user wants to access, access control must be defined for his user ID. A single user ID that is configured for multiple logons can be used to log on from multiple requesters as long as they are in the same domain.

1.2.5.1 Multiprotocol Transport Services (MPTS)

Multiprotocol Transport Services provides a comprehensive solution to interconnecting LANs. It supports LAN adapters, protocols, and programming interfaces. It also provides a transport framework for accessing various protocols using the socket API. Don't mix up the socket API with the TCP/IP sockets. Socket is an abstract object that is used to send and receive messages.

Adapters and protocols are defined by using the LAPS component of MPTS. LAPS contains network adapter drivers that provide communication between a protocol and network adapters using the network driver interface specification

(NDIS) as the interface. LAPS provides definitions for many different token-ring and Ethernet adapters.

On top of the NDIS interface, different protocols can be set up. LAPS supports in its base version the following protocols: IBM NetBIOS, IBM NetWare Requester Support, IBM NetBIOS over TCP/IP, IBM IEEE 802.2 and a NetWare NetBIOS emulation. More than one protocol can be bound to one adapter.

The configured protocols can be used by applications supporting these protocols for native communication or as transport protocols for the sockets/MPTS. The socket/MPTS component provides a transport framework that lets socket applications communicate using TCP/IP, NetBIOS, or local IPC. Socket/MPTS also allows TCP/IP applications to run on top of NetBIOS, using the non-native networking feature of socket/MPTS.

1.2.6 Resource Sharing

The files, printers, and serial devices attached to or residing on a server are called resources. When a user logs on to a domain, it generally gives the user access to resources on this particular domain. The user can also have access to resources on other domains if the network administrator defines those resources as external resources and grants the user access to them. Before users can use the resource by assigning the resource to a local device name, the network administrator must make the resource available by sharing it. Once a user has redirected a device to the shared resource, requests to access the resource are granted as specified in an access control profile.

1.2.6.1 Names of Shared Resources

You can share a resource by creating either a *netname* or an *alias* referring to the resource. A netname is a name that, in conjunction with the server name, identifies a resource on the network when the resource is shared. An alias is a resource definition that an administrator sets up for a directory, printer, or serial device on a particular server. All shared resources are assigned a netname, even if they are shared by the alias definition.

Alias: An alias is a nickname for a resource. Aliases are LAN Server′s intradomain directory service that makes connections to resources on multiple servers as easy as if there were one large server. For example, the network administrator could create an alias called PHYDATA to refer to a directory on SERVER1, C:\PHY\DATASET. Users can then refer to that directory simply as PHYDATA. When an alias has been assigned to a resource, there is no longer any need to specify the server where the resource is located and no need to specify the path to the resource. The network administrator can delete an alias name and recreate it to define another resource. Users can continue using the same alias name to refer to the new resource. A useful situation will be when a resource has to be changed or relocated; the user can continue to use the alias without any need to know about these changes.

Netname: Instead of an alias, the network administrator can use a netname to define a shared resource temporarily. A netname is a name that identifies a shared resource on a specific server. The netname of a resource on a server must differ from netnames of other resources on that server. However, the same netname can be used at other servers in the domain (possibly identifying a different resource at each server). To use such a resource, the user must refer to it by its netname and must also specify the server where the resource is located. It is easier to refer to a resource by an alias than by a netname as the

user does not need to specify the server when referring to a resource by an alias. Netnames are used in conjunction with server names, to specify the location of shared resources. Most commonly, a server name and a netname are combined to form a *Universal Naming Convention* (UNC) name that identifies a resource in the domain.

Universal Naming Convention: A UNC name consists of a server name and a netname, which together identify a resource in the domain. A UNC name has the following format:

```
\\servername\netname\path
```

where the path is optional. For example, suppose that a netname of MONEY has been assigned to the directory C:\RECEIPTS on SERVER1. The UNC name for that directory would be:

```
\\SERVER1\MONEY
```

If this directory had a subdirectory called APRIL, the UNC name of that subdirectory would be:

```
\\SERVER1\MONEY\APRIL
```

If that subdirectory APRIL contained a file called BALANCE.TXT, the UNC name of that file would be:

```
\\SERVER1\MONEY\APRIL\BALANCE.TXT
```

UNC names can be used by application programming interfaces (APIs) as well as OS/2 and DOS applications that are designed to be recognized by the network. UNC names are also used at the OS/2 and DOS prompts. For example, to copy the file BALANCE.TXT from the LAN to the local diskette drive A:, the following command (OS/2 or DOS) can be issued:

```
COPY \\SERVER1\MONEY\APRIL\BALANCE.TXT A:\BALANCE.TXT
```

However, not all OS/2 or DOS commands are LAN-aware and support UNC names. For a list of OS/2 and DOS commands that do not work with UNC names, please refer to *IBM OS/2 LAN Server Version 4.0 Commands and Utilities*, S10H-9686.

1.2.7 Types of Network Resources

There are three types of network resources: files resources, printer resources, and serial device resources.

1.2.7.1 Disks, Directories, Files

A files resource is a directory or a drive that contains data files or programs. The network administrator or the user can assign a files resource to a local drive letter (D through Z) to make that directory or drive and its files available for use. When making this assignment, the user must specify a drive letter that is not already assigned to a disk drive or partition of the local workstation. After a local drive letter (for example, K) has been assigned to a files resource, the user can use the files resource as if it resided on drive K at the workstation. This is possible even though there is no physical drive K on the workstation.

For example, drive K could be assigned to a remote files resource identified by the alias DATASET. The files in DATASET could then be used as if DATASET were the root directory of a disk in drive K. When the user accesses drive K and requests a directory listing, a list of the files in the alias DATASET is displayed (if the network administrator has given the user permission to view that directory):

```
[C:\]k:

[K:\]dir
```

Notice that the files resource is now referred to as drive K rather than as the alias DATASET.

- Home Directory

  The network administrator can also define a files resource on the server for a user such that the files resource is assigned when the user logs on and serves as the user's personal storage space. An access control profile granting all permissions to that user is automatically created. Such a file directory is called a *home directory*. This home directory can also be shared with other users by either modifying the access control profile, or creating home directories for other users, specifying the same drive and path.

- Limiting Space

  With OS/2 LAN Server 4.0 you have the ability to limit the size of 386 HPFS-directories. Directory limits provide management of disk space at the directory level on servers. The allocation scheme works in the same way as the partition of a logical drive. When a directory tree is full, no user can append data to its files or create subdirectories within the tree. For example, a limit of 100 MB applied to the C:\IBMLAN directory allows only those requests for disk space that do not cause the usage count to exceed 100 MB.

  Limits are independent of each other. For example, you can set a limit of 100 MB at the root and another limit of 120 MB at the C:\IBMLAN directory. LAN Server uses these limits when a request for disk space is received. For a request to be granted, it must satisfy all the limits placed within its path. In this example, a request for space in the C:\IBMLAN directory must satisfy both the 120 MB limit and the 100 MB limit.

  When limits are set on the size of a directory or tree, the users of that directory cannot exceed the limit. Therefore, you should notify the appropriate people, not only when the directory is full, but as it increases to the point (threshold) that it might not hold the necessary files. After the threshold is reached, the directory can decrease or increase in size over an unpredictable time span. Administrators and other users appreciate being alerted on a timely basis as the directory approaches and crosses the threshold.

- Limiting Users / License Control

  You can limit the number of users, who can access a resource at the same time. This function offers you the possibility to control licenses for your software. For example, if you purchase ten licenses to an application program, you can install that program on a server, create a directory alias pointing to the subdirectory where the program resides, and specify a maximum of ten users. Although many users can access the application program, only ten can use it concurrently. The eleventh user trying to use the application program cannot access it until one of the first ten users releases the application.

1.2.7.2 Printers

Printers are another type of network resource that can be shared. To handle print jobs more efficiently, the network administrator can create print *spooler queues* and printer pools. Network printers are accessed through shared spooler queues. A spooler queue is an ordered list of print jobs waiting to be printed. A spooler queue can be serviced by one printer or by a group of several printers called a printer pool. A print job, waiting in a spooler queue serviced by a *printer pool*, is processed by the first available printer in the pool (unless another queue for that printer pool has a higher priority).

For example, suppose a user has permission to use a shared network spooler queue identified by the alias PRINTQ1 and the user has assigned PRINTQ1 to a local device name, such as LPT2. Assume that PRINTQ1 is serviced by a printer pool consisting of two printers. If the user sends a print job to LPT2, the output appears at one of the two printers in the printer pool. However, the output may not be printed immediately because there may be other print jobs ahead of it. While the print job waits in the queue, the user can continue with other tasks. When the print job is completed, the network sends a message to the user′s workstation indicating that the print job is done. This message is automatically displayed on the user′s workstation if the Messenger service and the Message Pop-up service (or Netpopup service) are active. The Alerter service must be started on the print server.

Sometimes a network administrator arranges for more than one spooler queue to be serviced by a particular printer or a printer pool. For example, the network administrator can create a spooler queue for the majority of users and another queue for users who need to have their printer requests handled quickly.

An administrator, or a user with print operator privilege, can manage any print job, printer queue, or printer object. Users can hold, release, and cancel their own print jobs. You can also allow a user to manage network printing.

1.2.7.3 Serial Devices

A third type of shared resource is the serial device. Examples of this are modems, plotters, and serial printers. Such devices are assigned to LPT or COM ports for direct input/output (I/O) use.

Note

Users at DOS requesters can access serial printers set up as printer resources, but they cannot access other serial devices.

To handle serial device requests more efficiently, the network administrator can create serial device queues and serial device pools, like the printers resource.

A serial device queue is an ordered list of user requests waiting to use a shared serial device. A serial device pool is a group of similar serial devices that services a serial device queue. A user can use a shared queue by assigning a local device name (COM1 through COM9 or LPT1 through LPT9) to the serial device queue. The network administrator can also create an alias for a serial device queue that can be used in place of the full path to that queue.

A serial device can service more than one queue, each possibly having a different priority. The network administrator can create a serial device queue for the majority of users and another queue for users who need to have their serial

device requests handled quickly. A serial device request waits in a serial device queue until one of the serial devices in its pool becomes available. While the serial device request waits in a queue, the user cannot proceed with a task that requires the serial device. However, the user can perform other OS/2 tasks in other OS/2 sessions.

1.2.7.4 External Resources

In previous releases of LAN Server, an external resource was a resource (directory resource, spooler queue, or serial device queue) on a server in another domain. Special configuration requirements and considerations were required. However, in LAN Server Version 4.0, access to resources on servers in other domains is automatic. For this reason, such resources are no longer called external resources. In LAN Server Version 4.0 aliases used to represent resources on other servers are called cross-domain aliases.

1.2.8 Assigning Shared Resources

For users to access a shared network resource, a local device name must be assigned to the resource. For a files resource, the local device name is a drive letter (D to Z). For a printers resource or serial devices resource, the local device name is a port number (COM1 to COM9 or LPT1 to LPT9). A user can use the NET USE command to connect to a resource. NET USE lists the network resources you have in use and connects or disconnects your workstation to or from shared resources on the network. For example, local drive K could be assigned to a files resource (a shared directory on a server called SERVER) with its netname (LIBRARY) or alias name(BOOKS):

```
NET USE K:  \\SERVER\LIBRARY
```

or

```
 NET USE K: BOOKS
```

The local parallel port LPT2 could be assigned to a shared printer spooler queue to access a network printer:

```
NET USE LPT2 \\SERVER\LPRINTQ1
```

or

```
 NET USE LPT2 LASER
```

The local serial port could also be assigned to a serial spooler queue:

```
NET USE COM2 \\SERVER\HSPEEDQ1
```

or

```
 NET USE COM2 MODEM
```

After a local device name is assigned to a shared network resource, the resource can be accessed only if the network administrator has given the user the requested access permission to the resource.

1.2.8.1 Using the GUI for assignments

You can also use the GUI of LAN Server 4.0 to assign resources to a local device name. All you have to do is select **current assignment** from the menu of our local workstation icon. A list box will be shown, that contains all devices with their currently assigned resources.

To assign a new resource to a device, you have to select the **Add** button. That will give you the choice to add a directory, a printer or a serial device resources.

By selecting one of this options, a list of available resources of that specific type will be shown. You simply select the resource, that you want to assign. A second list shows you your available local devices to which the selected resource could be assigned. Select the device and the resource will be assigned to it.

When accessing a resource on a server, the local device name is simply a label on the user′s workstation that points to the shared resource on the server. A local device assignment to a shared network printer or serial device overrides a device assignment made to a printer or serial device physically located on the user′s workstation. For example, if LPT1 is assigned to a local printer, assigning this device LPT1 to a shared printer overrides the local assignment. Now all print jobs sent to printer port LPT1 are redirected to and printed on the shared printer, not on the local printer. The device is called a *redirected device*.

You can re-enable local printing on LPT1 with this command to disconnect from the network resource:

```
NET USE LPT1:  /d
```

Using the LAN Server 4.0 GUI you have to open the panel for current assignments. You will see a list of currently assigned resources. Select the assignment, that you want to remove or change, and click on the corresponding button.

Redirected device names can be used with DOS or OS/2 applications that are designed to work across a network. However, not all DOS or OS/2 commands work across a network and support redirected drives. For a list of DOS and OS/2 commands that do not work with redirected drives, please refer to *IBM OS/2 LAN Server Version 4.0 Commands and Utilities*, S10H-9686.

1.2.8.2 Logon Assignment

Resources can be assigned automatically, when a user logs on to the domain. In previous LAN Sever versions particular logon profiles were used for each user to assign file aliases, printer and serial device aliases. A typical PROFILE.CMD for OS/2 would have looked like the following:

```
/* User Profile for USER1 */
'@ECHO OFF'
trace 0;
'NET USE LPT1: \\SERVER\LPRINTQ1'
'IF EXISTS X:\LANUSER.CMD CALL X:\LANUSER.CMD'
exit 0;
```

The graphical interface used by LAN Server 4.0 allows you to drag-and-drop resources to a user or a group. All you have to do is drag the resource icon and drop it on the user icon. The Grant Access to a Resource settings notebook will open up where you can specify the device, that the resource will be assigned to. The next time, the user logs on, the resources will be available.

1.2.9 Network Applications

An application is a set of program files and data files necessary to do a specific job or function, such as word processing. A network application is an application that is defined to and usually shared on the domain. A network application can be stored in a directory on a requester or in a shared directory on a server but the program runs on the requester. If the application′s files are stored on a server, the files are downloaded from the server to the requester, as required. Network applications can be DOS/Windows and OS/2 applications. All network applications are displayed with their icon in a single application folder on the requester.

There are two types of network applications:

Public A public application is one that is defined and managed by the network administrator for users on the network.

Private A private application is one that users define for their own use so that network resources can be assigned automatically when the private application is run.

Both public and private applications can reside on either a server or a requester.

For example, a word processing program that resides on a requester could be defined as a private network application, allowing output to be sent automatically to a network printer. A user could also arrange for a shared directory to be made current when the private application is started. The directory could contain documents that the user wants to edit.

Each time a user logs on to the domain, OS/2 LAN Server adds all private and public OS/2 and DOS/Windows applications assigned to that user ID to the user′s desktop. All network applications are listed in one singled folder named Network Applications. In LAN Server 4.0, they are displayed with their actual product icons. In a previous version of OS/2 LAN Server, command files were used for DOS and Windows applications to invoke them from OS/2 requesters.

Note

Licenses for network application must be controlled. To make sure, only the number of users you have a license for may use the application at the same time. Some applications come with their own license control for networks. Others can be controlled by limiting directory access on the server.

To create a network application, you first have to create an alias for the subdirectory where the application resides. Simply drop a directory template to the resource folder. In the opening notebook, you can make your definitions and control the number of users having access to the directory at the same time. The next step is to create an access control profile, to give access to different users. After defining the access rights, you can propagate these rights down the directory structure to give the same access to following subdirectories. To define the network application using the defined resource, you drag an OS/2 or DOS/Windows template and drop it to Public Application folder. The Application Definition notebook will open, where you can define the application. When you have created a network application, you may assign it to a user or a group.

1.2.10 Access Control

Access to resources on a LAN is governed in two ways. First, user profile management (UPM) provides validation for a user ID and password at logon. Second, OS/2 LAN Server's own access control system provides a set of permissions that allow the network administrator to grant users various levels of access to shared resources. The LAN Server administration GUI is used to define users and groups. In addition, definitions can be made using the user profile management as in previous versions of the OS/2 LAN Server.

1.2.10.1 UPM and the LAN Server Administration GUI

User profile management (UPM) performs the user ID and password validation function at logon time and provides facilities for the management of IDs and groups within the domain that help control access to information. User IDs and optional passwords are used to regulate data access. These IDs and passwords are assigned by a user with administrative authority. UPM operates within an OS/2 Presentation Manager window environment and its tasks are completed through a menu interface. Online help is available to assist both the user and the administrator. Note that up to 16,000 user IDs can be defined through UPM, but the full list cannot be displayed in the Presentation Manager window environment.

OS/2 LAN Server 4.0 uses the LAN Server administration GUI to manage user and group definitions. You can perform more user and group management functions with the LAN Server administration GUI than with user profile management. Some of the functions only available from the LAN Server administration GUI are:

- The capability to define up to 16,000 users per domain
- User and group ID cloning

  Cloning saves time by allowing you to use your mouse to take existing user and group objects and make clones (copies) that can be renamed and changed as required.
- Drag and drop enablement for logon assignments, user and group definitions

  You can drag and drop aliases onto user and group objects to create logon assignments automatically. In addition, you can drag and drop user accounts into groups, or groups into user accounts, to update a user or group definition automatically.
- The ability to define home directories for users

  You can specify home directories on a server for a user's personal use.
- The ability to set directory limits on users

  You can set size limits on home directories. Alerts are sent to the users when the space used is nearing the limit.

OS/2 LAN Server 3.0 allows the user and group definitions file, created and updated through the LAN Server administration GUI or user profile management, to be centralized. This file is named NET.ACC and is maintained on the domain controller. Whenever a change is made to the user and group definitions, the NET.ACC file is copied from the domain controller to all servers, which must be running the Netlogon service in the domain. The Netlogon service allows a server to receive a copy of the user and group definitions file.

LAN requesters do not get copies of the NET.ACC file changes. Therefore, if user and group definitions are needed locally for an application, such as Database Manager, users must also be defined on the LAN requester workstation through the LAN Server administration GUI or user profile management for the Database Manager requirements.

The LAN Server administration GUI provides the following processes to manage user and group IDs on the network. User profile management is used for user ID validation. Each installation of the user profile management is local to the particular workstation where it is installed, and it validates users who access controlled data or use programs that reside on that particular workstation.

UPM provides three levels of authority: user, local administrator, and administrator.

- User - Users can perform the following tasks:
  - Log on
  - View the user profile
  - Change their own passwords
  - Add comments to the user profile
  - Log off

  In addition operator privileges can be assigned for each user. Operator privileges allow you to delegate specific administrative tasks, such as print management or group management to designated users. The LAN Server product provides four types of operator privileges:

  Accounts A user with accounts operator privilege is allowed to manage users and groups within the domain. The user can add, change, or delete users and groups. The user cannot create or change user accounts with administrative or any operator privilege.

  Print A user with print operator privilege is allowed to manage print queues and print jobs. The user can create, modify, and delete printers and queues on servers within the domain. The user can also share print queues and manage remote jobs on shared queues.

  COMM A user with comm operator privilege is allowed to manage serial devices.

  Server A user with server operator privilege is allowed to manage aliases and other shared resources and to display network status within the domain. The user can create, modify, or delete aliases or other shared resources.

- Local Administrator - A local administrator has Database Manager authority for local databases residing on that user′s machine, but has only user privileges on the OS/2 LAN. A local administrator does not have administrative authority for UPM. The local administrator user-type must be defined at the local workstation on which the user is a local administrator. To access databases on a remote Database Manager server, there must be one and only one local administrator user-type defined at each Database

Manager client. As the local administrator user-type is tied to the machine ID, it cannot be defined remotely.

- Administrator - The person with this administrative authority is a LAN network administrator. In addition to being able to perform all user tasks, the network administrator has overall network administrative authority and Database Manager authority for all databases on the LAN.

  The network administrator can perform the following tasks:

  – Administration of users:
    - Add or delete users and administrators
    - Specify user authority (user or administrator)
    - Specify special operator privileges
    - Specify password options (optional or required)
    - Specify a home directory for users
    - Specify user status (access allowed or denied)
    - Specify allowable logon workstations for users
    - Specify logon assignments for users
    - Add public applications to users′ Network Applications folders
  – Administration for groups of users:
    - Create or delete groups
    - Add users to or remove users from groups
  – Manage access to network resources

  An administrator can establish groups so that access to protected objects can be granted to all members of a department or to all persons performing similar tasks. Access can then be granted to the group as a whole. The members of the group can be changed through UPM. If a user ID is deleted, it is removed from all groups. But deleting a group does not affect the individual user IDs and their associated user profiles.

Note

OS/2 LAN Server 3.0 supports the stand-alone logon feature, which allows a user to log on without being verified by the domain controller. LAN Server 3.0 saves the ID and password specified by the user when logging on, and user validation takes place only when access to a server′s resource is requested. The user ID and password are validated by the specified server before access is granted. The stand-alone logon feature allows a requester to continue to access servers (including peer servers) outside the domain, even if no logon server in the domain is active.

1.2.10.2 LAN Server Access Control System

The network administrator can grant, restrict, or deny users the access to a shared resource by creating an access control profile for the resource. The network administrator can also grant permission to a user to create an access control profile or change an existing profile. An access control profile defines who can use a resource and the level of access.

Note

A shared resource can have only one access control profile, although a profile is not required, and by default all resources are protected.

When the network administrator creates an access control profile for a resource, an audit trail can optionally be set up to record access attempts to that resource.

An access control profile can contain a user access list and a group access list. A user access list is a list of user IDs and the various permissions assigned each of them. A group access list is a list of group IDs and the various permissions assigned to each group ID. A group is a set of user IDs that can be referred to by a single name, or group ID. New users added to an existing group inherit the permissions given to the group. The number of entries in the combined user and group lists for each access control profile is limited to 64. It is therefore recommended that a group list be established if there is a large number of users with common needs.

Once a user is logged on to a domain, the user's access to a given resource is controlled by the access control profile for that given resource. The network administrator can specify the following permissions in the access control profile of the resource:

None = No access to the resource

Execute = Use the resource (an application program), but not able to copy to your diskette or hard file

Read = Read only

Write = Write only

Create = Create a file or directory

Delete = Delete a file or directory

Attribute = Change the attributes of a file

Permission = Gives a user the ability to grant other users access to this resource

Combinations of appropriate permissions may be flexibly constructed to give very specific control of a resource to a user. For more detailed descriptions of the various access permissions, please refer to *OS/2 LAN Server Network Admin Ref Vol 3: Network Administrator Tasks*, S10H-9682.

There are two ways the LAN administrator can create access control profiles for different resources:

- Through the LAN Server Administration GUI, for resources with and without aliases
- At the OS/2 command prompt, using the NET ACCESS command

The user IDs, group IDs, and passwords for all users within a server's domain are stored in a user accounts database (NET.ACC) on the server. On an OS/2 LAN Server Entry workstation, with either the FAT or HPFS file system, the access control profile information is stored in the NET.ACC file. However, on an OS/2 LAN Server Advanced workstation with the 386 HPFS installed, the access control profiles for the 386 HPFS files and directories are stored within the file system.

The access control profiles for all other resources (for example, FAT files, print spooler queues, and serial device queues) and drive-level access control profiles for 386 HPFS drives are stored in the NET.ACC file. Up to 8192 access control profiles can be stored in the NET.ACC file. A 386 HPFS workstation stores an unlimited number of access control profiles for directories and files residing on the 386 HPFS drives.

Administrators are automatically granted all permissions by LAN Server and are not subject to access control processing. For all other users, LAN Server denies access to a resource unless you specifically grant access for a user ID or its corresponding group IDs. When a user attempts to use a resource, LAN Server searches for that user ID in the resource's access control profile, checking first the user access profile and then the group access profile.

Because of the search process described in Access Control Profile Searching, a user might be able to gain access to a resource even if no profile exists for that resource. LAN Server searches for the existence of an access control profile for that resource, then it searches for the parent, and then it searches for the root. If a profile exists and the user is listed in the access control profile, or if the permissions for USERS group value is any value but none, the user has the access permissions specified.

1.2.11 Network DDE and Clipboard

Network DDE and Clipboard allows application programs and users to copy text from one workstation to another through the clipboard. You can also create dynamic data links (copies of data that are automatically updated across the network when changes are made to the original data) between different workstations. In order to use Network DDE and Clipboard, you must use applications that support the clipboard and dynamic data linking functions. You can also use Network DDE and Clipboard with DOS LAN Services if you are using the Windows interface.

1.2.12 First Failure Support Technology/2 (FFST/2)

FFST/2 is a software problem determination tool for OS/2 system software and applications. FFST/2 is designed to capture error data when the error occurs, provide immediate problem notification to predefined locations, and furnish unique error code identification. Because FFST/2 remains inactive until a software error is detected, impact on system performance is minimal. The services FFST/2 provides include:

- Pop-up messages
- A message log formatter
- Access to the OS/2 system error log
- A dump formatter
- A message console
- A command line interface for FFST/2 initialization and configuration

1.2.13 Generic Alerter

The Generic Alerter service is a LAN Server service that gives a server the ability to generate generic alerts when it detects or anticipates certain problems. This allows a network management services control point, which can be a host system running NetView software, or a PS/2 computer running IBM LAN Network Manager, to manage OS/2 servers along with the rest of the network.

1.2.14 Network Messaging

The LAN Server product provides a network messaging function for sending messages to and receiving messages from other users on the network. You must be logged on to be able to send and receive messages using network messaging. The network messaging function uses the Messenger service to accomplish these tasks. When a new message arrives on your workstation, the Messenger service adds it to the list of messages waiting to be read and, if you have configured the pop-up option, informs you of its arrival through a pop-up window. All messages you receive are saved in a message log on your workstation until you delete them.

Messages can be sent to users who are logged on or to workstations that are started and running the Messenger service. If you defined users and groups on the domain, they are listed as possible recipients of your messages in the List Users and List Groups windows when you are sending a new message.

1.2.15 Performance Tuning Assistant

This utility program assists in fine tuning the resources of the LAN Server 4.0 system to match the users′ configuration requirements. This utility is, with minor modifications, a stand-alone version of a configuration spreadsheet tool that has been in use by LAN Server administrators for a long time. It goes beyond the spreadsheet tool by actually updating the servers′ configuration files automatically.

1.2.16 Uninteruptible Power Supply (UPS)

Uninteruptible Power Supply is an OS/2 LAN Server service that provides protection against loss of data during power failures. Upon power interruption, users with active sessions to the affected server are notified of the impending shutdown and an orderly server shutdown is performed.

1.3 Novell NetWare Products

The network operating system (NOS) from Novell is called NetWare. Novell offers different versions of NetWare. NetWare enables users of different operating systems to share files, printer and other services. With the IBM ServerGuide the version 3.12, 4.1 and 4.1 SMP are delivered. This allows IBM to offer the customer the products that best fit their environment. This section will briefly describe the major Novell products shipped with the IBM ServerGuide.

1.3.1 NetWare 3.12

NetWare 3.x is currently the most prevalent version of NetWare found in the industry. The latest version is Version 3.12, which is delivered with the IBM ServerGuide. NetWare 3.12 is an updated release of NetWare 3.11. This latest version incorporates all fixes and patches that have been distributed for NetWare 3.11 since its introduction. Many LAN drivers, disk drivers, NetWare management utilities, and NLM services have been updated to their latest versions.

The central component of NetWare 3.12 is the real-time operating system. It is designed around the 32-bit 386 and 486 environments, providing a foundation of speed and reliability. NetWare 3.12 provides a high-performance network service platform for businesses with multivendor computing environments. NetWare 3.12 is shipped with all the software necessary to install and operate the network server and connect as many as 250 DOS, OS/2 or Windows workstations to the network. NetWare supports workstations (clients) on the following operating systems:

- OS/2
- Windows
- DOS
- UNIX
- Macintosh

NetWare 3.12 can be combined with all other NetWare products from Novell. For example, you can use NetWare 3.12 with NetWare for SAA to interoperate with IBM hosts. With the NetWare Management Agent for NetView, you can use IBM NetView to manage our combined NetWare and IBM host environment.

The major advantage of the version 3.x compared to previous NetWare versions (NetWare 2.x) is the use of NetWare loadable modules (NLM) to make it more modular and easier for third parties to write applications. The structure of the NLM software bus is shown in Figure 2 on page 25.

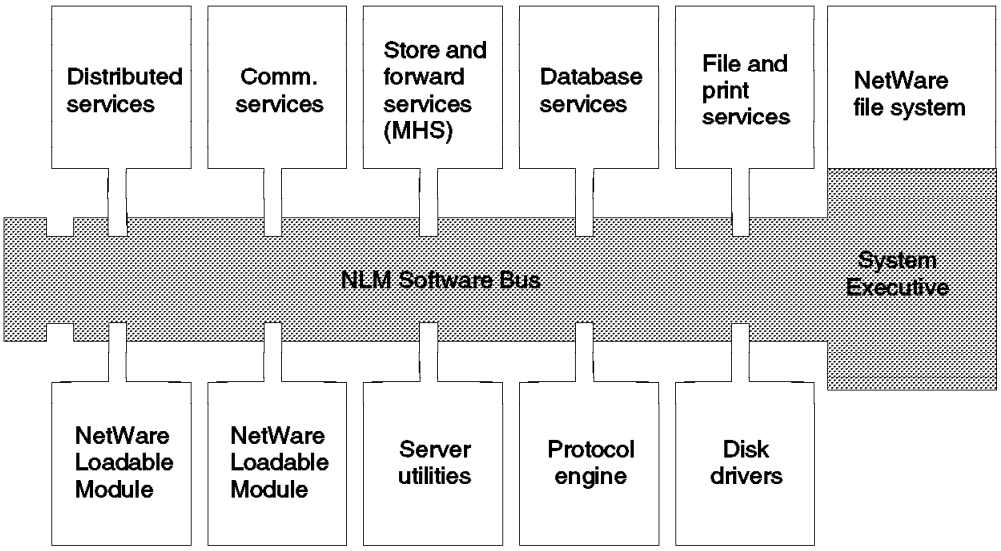


Figure 2. NetWare Loadable Module (NLM) Structure

NetWare 3.12 is based on a system architecture for network computing services, Novell's integrated computing architecture (NICA), which is designed to provide integration of heterogeneous desktops and other computing environments.

By integrating heterogeneous computing environments, NetWare 3.12 allows DOS, Windows, Macintosh, OS/2 and UNIX computer users to transparently share information and resources. NetWare 3.12 allows any of these desktop computers to share file and print services and access information on IBM mainframes. NetWare 3.12 also supports the integration of NetWare networks into networking environments based on Transmission Control Protocol/Internet Protocol (TCP/IP) and Open Systems Interconnection (OSI).

With NetWare 3.12, support for Macintosh and many UNIX workstations is available through optional NetWare Loadable Modules (NLM) products: NetWare for Macintosh 3.12 and NetWare NFS 1.0. The NetWare 3.12 Universal File System provides full support for file systems based on DOS/Windows, OS/2 High-Performance File System (HPFS), Macintosh, NFS, and File Transfer Access and Management (FTAM). Support for multiple protocols is shown in Figure 3 on page 26.

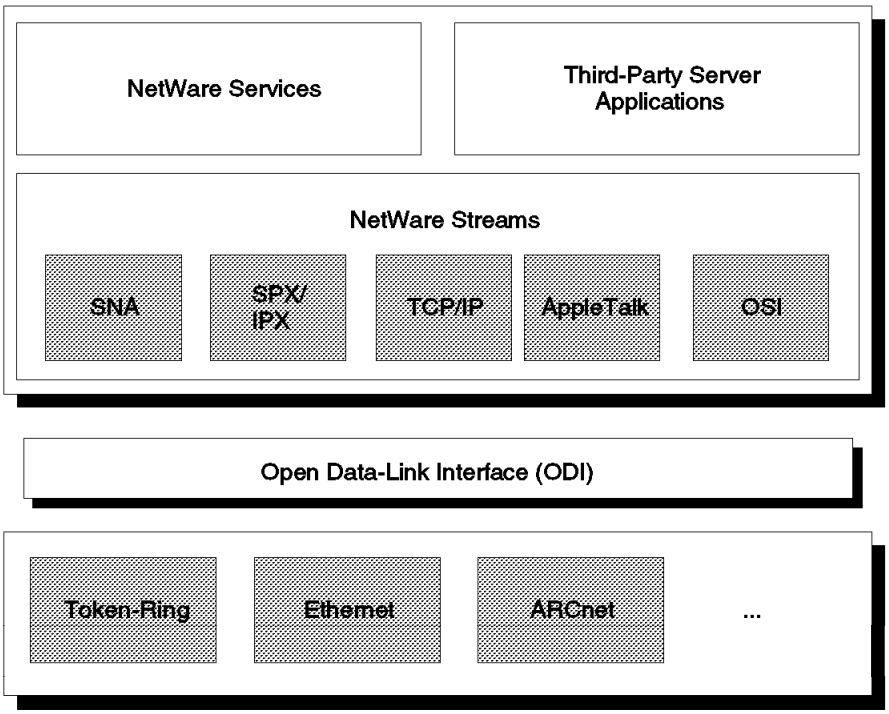


Figure 3. NetWare Protocol Support

1.3.1.1 Media Independence and Internetworking

NetWare 3.12 enables you to integrate different types of hardware within one single network.

The internal router from NetWare 3.12 enables the server to connect up to 16 different networks and let them appear as one big logical network. The different subnetworks connected together must not use the same media or topology. Workstations can be used as external routers for optional routing services and can connect up to 16 subnetworks of different media and topology. NetWare 3.12 can support multiple internal and external routers. This lets users access servers on any connected subnetwork.

The Protocol Engine of NetWare 3.12 enables several protocol stacks to operate concurrently. Protocols that can operate with NetWare 3.12 include IPX/SPX, TCP/IP, SNA, AppleTalk and OSI TP4 protocols.

1.3.1.2 NetWare Messaging

NetWare 3.12 is delivered with two messaging products:

- NetWare Basic MHS
- FirstMail

NetWare Basic MHS is a messaging system, which enables users to exchange messages with other users on the same NetWare server. To send messages to

users on other NetWare servers or to receive messages from these users, you can use Global MHS for messaging.

FirstMail is an electronic mail utility available in DOS and Macintosh versions. Users have the following possibilities with FirstMail:

- Send and receive messages
- Reply and forward messages
- Attach files to messages
- Create and maintain an address directory
- Organize messages in folders

1.3.1.3 Print Server

NetWare 3.12 offers print services through a print server application. The NetWare Print Server enables users to share as many as 16 printers. Multiple print servers can be run on a single network. The NetWare Print Server 3.12 includes user alert and user notification capabilities. It can be configured to inform users when print jobs are finished or notify print operators about paper jams, low paper or that the printer is offline.

1.3.1.4 Capacity/Performance

Using the packet burst sliding window architecture, NetWare servers and clients can send and receive multiple packets at one time, without acknowledging each packet individually. The technology is referred to as a sliding window because the number of packets sent increases or decreases depending upon the amount of traffic on the wire. Unlike other sliding window architectures, lost packet retries require retransmission of only the lost packet, not the entire burst session.

When transmitting across multiple segment hops, NetWare 3.12 will negotiate the largest size packet that may be accommodated by any router along the route. If all routers between point A and point B are able to handle a 4 KB packet, NetWare 3.12′s LIPX feature insures that 4 KB packets are transmitted across routed segments. Earlier versions of NetWare reduced the size of the packet to 512 bytes, the least common denominator, when transmitting across routers to ensure delivery across possible ARCnet segments.

NetWare 3.12 provides a number of performance improvements that allow the network operating system to perform faster in various configurations. Dynamic read-ahead increases server performance by loading to available server memory additional contiguous information to that specifically requested. If the client application then requests this information, which is often the case, the operating system simply retrieves the information from cache, which is much faster than making an additional disk read.

1.3.1.5 Security

NCP Packet Signature provides the options for the network administrators to further restrict trusted client sessions by signing each packet received and sent on the wire. This feature prevents unauthorized users from submitting a packet in behalf of a trusted user who currently has an open session. Clearly, such an intrusion would require a high degree of technical knowledge or special tools.

1.3.1.6 NetWare Management System

The NetWare Management System includes two sets of software:

- NetWare Services Manager (console)
- NetWare Management Agents

Server management is available for different platforms like Windows and OS/2. The management agents reside on NetWare servers on the internetwork, collecting data that is accessed and displayed by the console. Third-party developers and customers can create their own resources and devices that send information to the NetWare Management System and that can operate transparently in the NetWare Management System environment.

NetWare 3.12 includes the NetWare Management Agent for NetView, an NLM that supports an interface from NetWare server to IBM NetView network management system.

1.3.1.7 Upgradeability

The ability to upgrade a server from NetWare 2.x to NetWare 3.x using only a single machine is possible with NetWare 3.12. In addition, an across-the-wire migration utility may be used to migrate data, along with network management and security information from earlier versions of NetWare and certain non-NetWare platforms to NetWare 3.12. This utility also helps to consolidate multiple servers into a single multidepartment server.

1.3.2 NetWare 4.1

NetWare 4.1 is designed as an enterprise LAN operating system. It allows a large corporation to be tied together into a single tree structure using NetWare Directory Services. This way, a user logs into the network, rather than logging into a specific server. The user would then have access to resources anywhere in the network, provided they have authorization to them.

There will be a large number of current NetWare 3.x users who will need the capabilities offered by NetWare 4.1. At the same time, Novell has made a commitment to continue to enhance the NetWare 3.x product as it has demonstrated with the announcement of NetWare 3.12. If a company's needs are static, and their structure is not complex, they can continue to run on NetWare 3.x.

NetWare 4.1 is Novell's advanced network operating system that turns a multiserver NetWare environment into a single integrated system. NetWare 4.1 builds on the familiar NetWare architecture to provide easier network management and better access to network resources.

NetWare 4.1 is delivered with all software to install and operate the network server. Up to 1,000 DOS, UNIXWare, OS/2, Macintosh, Windows or UNIX NFS workstations can be connected.

NetWare 4.1 inherits all the power and capabilities of NetWare V3.12 and adds the following new features:

NetWare Directory Services (NDS) provides a single view of the network and gives customers seamless, global access to all company resources allowing them to reduce administrative costs and increase productivity.

Security enhancements such as new security and auditing capabilities that utilize public key cryptography, provide a more secure environment for protecting vital corporate data and ensure that security policies are maintained.

Wide-area connectivity improvements allow for faster response, lower bandwidth utilization, and greater productivity across the network locations.

Administrator productivity improved by new graphical administration tools.

Improved management capabilities give network managers more information about the server for easier and more effective management.

Multiple language support allows customers to access and manage the network using their native language.

Additional Storage Management Service (SMS) and Target Service Agents (TSAs) allow customers to back up DOS, Windows, and OS/2 clients, as well as NetWare V3.12 and NetWare 4.1 servers.

Upgrade utilities automate the transfer of information from NetWare V2.x or V3.x binderies to the NetWare 4.1 directory, greatly reducing the cost and time needed to upgrade to NetWare 4.1.

NetWare co-residence with OS/2 allows NetWare 4.1 to run in a non-dedicated mode on the OS/2 2.x platform, giving customers the functionality of NetWare in OS/2′s multitasking environment.

1.3.2.1 Highlights

- Includes NetWare Directory Services, which lets a multiserver network be viewed as a single information system.
- Provides a single, integrated interface for all network administration.
- Secures the network against any unauthorized intrusion.
- Restricts user access to network resources.
- Allows the administrator to retain central network control or to delegate administrative responsibilities.
- Lets all network activity be monitored.
- Includes file-by-file compression, which increases the capacity of network drives.
- Includes burst mode technology that increases the speed of data transfer over wide area links.
- Provides large packet capability for increased network throughput.
- Provides controlled service broadcasting for decreased network overhead.
- Supports all popular client operating systems, including DOS, OS/2, Windows, UNIX and Macintosh.
- Integrates messaging with NetWare MHS, that supports server-based event monitoring, operational statistics and message flow control.
- Includes migration tools that make it easy to upgrade from previous versions of NetWare.
- Makes network printing easier to set up, use and manage.

- Includes RCONSOLE for remote network management.

1.3.2.2 NetWare Directory Services

NetWare Directory Services (NDS) is a distributed database that provides seamless, global access to all network resources regardless of physical location. NDS replaces the bindery used in previous versions of NetWare. While the bindery was designed to support a single server, NDS supports an entire network. Rather than logging in to individual servers, you log in once to the entire network. Only one password is needed to access all of the user′s authorized network resources. Connections to these resources are transparent, shielding the user from the underlying complexity of the network.

NDS enables one administrator to oversee all the servers on the network. NDS provides the administrator with a single image of the network. This makes a significant difference on large networks where, until now, each server required its own administrator. With NDS, administration costs can be reduced and user and administrator productivity can increase.

With its object-oriented structure, NDS gives the user-flexible network security. NDS maintains a directory of information about every resource on the network, for example, users, groups, printers and volumes. These resources are known as objects and are organized in a hierarchical tree structure. Hierarchies can be specified according to the way people access and use resources in their company. With this structure, it is easy to specify rights for resources, and everyone on the network can easily locate the resources they are authorized to use.

An NDS object consists of fields of information, called properties. If the object is a network user, for example, its properties may include the user′s telephone number, fax number, E-mail address and so on. Information entered in each property field is called a value. Users on the network can locate an object such as a printer or another user by searching for the object′s values. Because access control rights can be assigned to any object and its associated properties, NDS provides the flexibility to set up the ideal network security scheme. A NetWare development toolkit is also available from Novell to enable developers to add new types of resource objects and properties to the directory.

For added reliability and efficiency, the NDS database can be distributed over various servers on the network by dividing it into partitions. Partitions can be copied or replicated to various servers on the network to share the processing and eliminate any single point of failure.

NDS is based on the X.500 public directory standard that allows NDS to work with other X.500 directories when they become available.

1.3.2.3 Administration

NetWare 4.1 includes the NetWare Administrator, a new utility that consolidates all NetWare administrative functions found in a variety of NetWare utilities into a single, intuitive interface. NetWare Administrator provides all the tools needed to administer the entire network. NetWare 4.1 includes two versions of the NetWare Administrator: a graphical version and a command-line version. The graphical version lets you view and manage the hierarchical directory trees created by NetWare Directory Services. You can tell at a glance what network resources are available and where they are located. By pointing and clicking on an object, you can see all the information associated with that resource. Drag

and drop functions let you quickly assign access control rights to any NDS object or move objects within the directory tree. In addition, for administrators who would rather use the command-line utilities found in NetWare V3.12, NetWare 4.1 includes those utilities as well.

1.3.2.4 Security

NetWare 4.1 security is provided in layers that overlap to protect network resources. When users log in to the network, an encrypted public key is passed over the wire from the server to the workstation. The user types in his or her password, which authenticates the user and changes the public key into a private key. The private key identifies the user much as a signature would. Whenever a user requests a resource on the network, the private key is sent to authenticate the user′s right to use that resource. An access control list is scanned to ensure the user has been granted rights to the resource by an authorized administrator. The authentication is done as a background task, and users are not required to reenter their password. Each time a user logs in to the network a new private key is generated by the security algorithm, and the user′s password never passes over the network wire.

NetWare security can be made as simple or as complex as an installation requires. Access control rights let you limit users to operating within specific files, within designated directories, at a specified workstation or during specific hours of the day. You can base access control rights on the properties of individual user objects, such as phone number or password.

NetWare 4.1 lets you choose whether to retain centralized control of the network or to delegate some administrative responsibilities to other users throughout the network. You retain strict control over who has access to supervisory privileges.

You can charge users for the use of network resources when situations require. Charges can be based on connection time, the number of blocks read or written to disk, disk storage space used, and the number of requests made by the workstation. Rates can vary by time of day and day of the week.

1.3.2.5 Auditing

NetWare auditing features monitor and record network-wide events for any designated network resource. Auditing helps ensure company security policies are maintained.

NetWare 4.1 lets you create an independent auditor. This network user can monitor and record designated events but cannot access any resource other than the audit reports. This enables you to set up an independent auditor for greater control over network accounting. Two levels of passwords are required to access audit information. Even administrators with rights to the rest of the network cannot gain access to audit information without the audit passwords.

1.3.2.6 Capacity

NetWare 4.1 lets you store more information at a lower cost. File-by-file compression increases the storage capacity of server volumes with no additional hardware cost or loss of performance. You can choose which files, directories or volumes to compress as well as when and how often they are compressed. Compression is always a background task, which means it has no effect on server performance. When a user or network service requests a file that has been compressed, it is decompressed automatically in real time.

Data migration lets you automatically transfer infrequently accessed data from expensive online storage devices to less expensive storage devices, such as near-line optical or offline tape devices. Users still see the migrated files as if they were physically located on the online volume. If users request a migrated file, it is automatically retrieved into primary storage.

The High Capacity Storage System (HCSS) extends the storage capacity of a NetWare server by allowing you to integrate rewritable optical disks into the network. HCSS provides the capacity needed to add imaging technology to your network.

NetWare 4.1 can suballocate data within a hard disk's allocation block, enabling you to decrease wasted storage space.

1.3.2.7 Wide Area Performance

NetWare 4.1 improves the performance of wide area networks. It includes three new features that allow for faster response times, lower bandwidth usage and greater productivity across the network.

Burst mode technology, sometimes called "packet burst," improves data delivery speeds over wide area links by allowing a network packet to be sent before the receipt of the previous packet is verified. This can significantly improve performance in wide area networks where line speeds often create a bottleneck.

Large packet capability increases network throughput. Both sides of the transmission negotiate the size of the largest packet that can be sent. Sending more information per packet decreases the number of packets that have to be sent, which increases the speed of transmission.

Controlled service broadcasting, or SAP Restrict, controls and reduces the distribution of service information broadcasts between servers throughout the network. This reduces the overhead traffic that flows over the link, so bandwidth is freed for data and other vital transmissions.

1.3.2.8 Integration of All Popular Desktop Computers

NetWare 4.1 provides seamless integration for Macintosh, OS/2, DOS, Windows and UNIX desktop operating systems. No matter what type of workstation your users choose, they will have simultaneous access to the same data and the same set of network resources. Users retain the workstation that lets them work most productively, and you protect your investment in hardware and software.

The integration of multiple desktop operating systems is made possible through the NetWare file system's named spaces. A named space appears as an extension of a client's native file system and allows the server to keep multiple names for each file, one for each supported desktop operating system.

1.3.2.9 Memory Protection and Management

With NetWare 4.1, you have the option of running NetWare loadable modules (NLMs) in a protected memory domain. This allows you to evaluate the reliability of new NLMs, particularly those being developed, in a protected environment before loading them alongside the operating system. For situations in which reliability is more important than performance, you can choose to run all NLMs within the protected memory area.

A new method of memory allocation allows the server to operate more efficiently. NetWare 4.1 from IBM consolidates all memory allocation into a single pool and uses this pool to reallocate memory that has been released by NLMs. This reduces memory fragmentation and increases system reliability.

1.3.2.10 Reliability

NetWare 4.1 ensures that your corporate data is protected and that network services are always available.

Disk mirroring allows NetWare 4.1 to protect the network drives. NetWare 4.1 duplicates an entire physical volume on a second hard disk. Disk writes to the original volume are mirrored to the image by the server. The server also verifies writes on both disk surfaces. If the original disk fails, the duplicate takes over automatically with no loss of data.

Disk duplexing provides a higher level of protection by duplicating the entire disk channel. This protects the system against data loss due to defective disk drives, disk controllers, interfaces and power supplies. Controller and disk channel faults are automatically detected, corrected and logged. If any component in a disk channel fails, the redundant channel takes over automatically without loss of operation or data.

NetWare 4.1 includes additional reliability features that have become NetWare hallmarks. These features include read-after-write verification, duplicate directory structures, Hot Fix and the Transaction Tracking System (TTS).

1.3.2.11 Modular Server and Client Architecture

NetWare 4.1 offers a modular server architecture that gives you the flexibility to build the network you need. The core of NetWare 4.1 is the real-time operating system, which provides the foundation for all system operation. To this foundation you can add additional services through NetWare loadable modules. Because NetWare 4.1 is an evolution of the NetWare operating system, many of the NLMs developed for NetWare V3.12 are fully compatible with the new operating system. Other NLMs may need to be upgraded to take advantage of the new features of NetWare 4.1. Novell maintains an NLM testing program to ensure the quality and compatibility of third-party NLMs.

The NetWare client software, known as the NetWare shell, is now modular as well. The modular components of the shell are known as virtual loadable modules (VLMs). You can now customize the shell by loading only those VLMs you need, which helps you maximize workstation memory. VLMs also enable you to upgrade the shell without having to replace it entirely. The new shell is compatible with all previous versions of NetWare, and previous versions of the shell are compatible with NetWare 4.1. However, you must use the new shell to take full advantage of the encrypted key technology included in NetWare 4.1.

1.3.2.12 Easy Upgrade

NetWare 4.1 includes a migration utility that transfers bindery information to NetWare Directory Services, making it easy for you to upgrade from NetWare V2.x or V3.x to NetWare 4.1. You can upgrade your network from local media, or you can upgrade across the wire. NetWare 4.1 also includes a utility for moving the domains from an IBM LAN Sever network to NetWare Directory Services.

Another upgrade option is bindery emulation, which enables you to upgrade network servers at your own pace rather than all at once. With bindery

emulation, a NetWare 4.1 server can be viewed and administered as a V3.12 server. Bindery emulation also provides compatibility with NetWare V3.x drivers, utilities, NLMs and applications.

1.3.2.13 Network Management

Novell provides a family of network management products that enable you to monitor, control and troubleshoot network components, both hardware and software. NetWare 4.1 works with these management products by providing them with comprehensive network information, including network alerts. NetWare 4.1 provides management products with more information and alerts than any previous NetWare operating system.

NetWare 4.1 also includes a Simple Network Management Protocol (SNMP) agent that provides network information to all SNMP management consoles. Via NetWare for SAA and Novell′s LAN-to-IBM host gateway, NetWare 4.1 provides network information to IBM′s NetView management application.

1.3.2.14 Print Services

Print services in NetWare 4.1 are provided through a print server application that is bundled with the operating system. The NetWare Print Server allows users to share up to 255 printers on the network per print server, and multiple print servers can be run on the network. NetWare 4.1 includes several features that make it even easier for you to set up, use and administer network print services.

You can now use a single utility to configure DOS, NFS and Apple printers. Users can select system-wide print job configurations, which are set up by the administrator, to simplify print job setup. A Quick Setup option in the PCONSOLE utility makes it easy to define and link printers, print servers and print queues.

With NetWare 4.1, printers and queues are defined in NetWare Directory Services. Users can query the directory to easily locate them. Print objects in the directory allow users to capture to both printers and queues.

All print management utilities have been integrated into the Network Administration utility. This utility gives you a graphical view of the network, making it much easier to administer network print services. Traditional NetWare print utilities are also included and have been enhanced.

1.3.2.15 Remote Management

NetWare 4.1 enables network administrators to use their own workstation to administer remote servers. RCONSOLE greatly increases the flexibility of the network by allowing supervisors to install and upgrade the operating system, configure network services and maintain NetWare operating systems remotely. Using the RCONSOLE utility over a network connection or telephone lines, you can remotely load and unload NLMs, mount or dismount volumes, and execute any console commands as if you were at the network server.

1.3.2.16 Implementation

NetWare 4.1 includes two utilities that provide a simple way for you to upgrade from NetWare V2.x, NetWare V3.x or another network operating system: the NetWare Across-the-Wire Migration utility and NetWare In-Place Upgrade utility. In an across-the-wire migration, data files are transferred across the network to the destination server. Bindery information is transferred to the working directory on a local hard drive, translated into the NetWare 4.1 format, and then

moved to the destination server where it becomes accessible through bindery emulation.

The in-place upgrade method lets you upgrade a NetWare V2.x server without having to move data across the network. The conversion takes place in two steps: first converting the bindery information from the NetWare V2.x format to the NetWare V3.x format, then from NetWare V3.x to NetWare 4.1.

Before installing NetWare 4.1, you will need to plan your NetWare directory tree. Planning your tree before installation is essential to creating a tree that provides the most efficient use of network resources. You can develop the directory based on your company′s organizational chart, physical location or the type of work you do.

1.3.2.17 Options

NetWare 4.1 can be used with every other product Novell provides. For example, it provides the platform for Novell′s NetWare Communication Services products, which include NetWare for SAA, NetWare Communication Services Manager and NetWare 3270 LAN Workstations for DOS, Macintosh and Windows. You can obtain Novell add-on services that enable Apple Macintosh, NFS and OSI FTAM clients to connect directly to the NetWare 4.1 server. You may need to acquire the NetWare Supplemental Driver kit to use some network adapters. Novell supports a variety of network adapters but bundles drivers only for those that are widely used.

1.3.3 NetWare 4.1 for OS/2

NetWare 4.1 for OS/2 is enabling software that allows NetWare 4.1 to run as an application on OS/2 2.x. This provides NetWare services in a non-dedicated environment. It enables one computer to function as a NetWare server, an OS/2 application server and a network client at the same time. You can work in an OS/2, DOS or Windows session on your workstation while concurrently the NetWare server supports you and other users on your network. NetWare data is stored on a disk partition that is formatted and managed by NetWare. Because of security reasons, transparent access between the NetWare partition and the OS/2 partitions is not allowed. OS/2 applications can′t use the space allocated by the NetWare file system and vice versa. All NetWare 4.1 features and NLMs are supported in this environment.

1.3.3.1 Features

- Enables concurrent access to NetWare and OS/2 services
- Enables NetWare and OS/2 to share network adapters and hard disks
- Provides low-cost, high-capacity data storage
- Preserves NetWare′s unsurpassed performance
- Supports dynamic performance tuning
- Provides full security for NetWare and OS/2 files
- Includes an OS/2 graphical monitor
- Runs NLMs, device driver unmodified
- Provides all features as NetWare 4.1

1.3.3.2 Business Solutions

This is a very effective solution when a company may have multiple remote sites needing their own servers but not wanting to purchase dedicated servers for every site. Using NetWare for OS/2, they can use one machine for server and client, running multiple applications on the OS/2 platform.

This also makes an excellent platform for marketing demonstrations. With one machine, and no cables, the demonstrator can show network applications such as client/server.

Note

NetWare 4.1 for OS/2 requires OS/2 2.x and NetWare 4.1 products to be installed on the same machine. NetWare 4.1 for OS/2 does not include a license for OS/2 or for NetWare 4.1.

1.3.4 NetWare 3.2.5 for AIX/6000

NetWare for AIX/6000 from IBM V3.2.5 allows RISC System/6000 workstations to act as servers for NetWare LANs. Based on Novell's NetWare for UNIX V3.12 (formerly known as Portable NetWare), NetWare for AIX/6000 brings the resources and applications of the full-function, multipurpose AIX operating system to PC LAN users. It provides file and print sharing among DOS, Windows 3.x, and OS/2 NetWare clients, and AIX/6000 Version 3.2 users, as well as network connectivity. NetWare for AIX/6000 from IBM V3.2.5 combines the function of NetWare LAN server with the RISC System/6000 hardware and UNIX operating system.

NetWare for AIX/6000 from IBM 3.2.5 is designed to meet the needs of the client/server segment of the network computing market, offering a reliable, full-featured product, which is easy to install, use and administer. NetWare for AIX/6000 from IBM 3.2.5 combines NetWare server functions with the general purpose, AIX/6000 operating system, bringing functions of UNIX to the PC user.

1.3.4.1 Product Positioning

NetWare for AIX/6000 from IBM should be considered in the following environments:

- Existing users of NetWare who want UNIX servers and applications
- NetWare users and AIX/6000 users who need to share common resources
- DOS, and/or OS/2 users who desire to be added to an existing AIX/6000 system and access to the AIX resources
- Users who have large numbers of PCs unconnected to a LAN

1.3.4.2 Highlights

- Integrates RISC System/6000 into existing NetWare personal computer LANs
- Transparent to existing NetWare clients
- Preserves existing PC desktop environment while adding access to AIX/6000
- Common file and print resources shared by personal computer and AIX/6000 environments
- Open AIX/6000 server

- Support for IPX/SPX protocols in AIX/6000
- PC access to AIX/6000 applications via Novell Virtual Terminal
- DOS and OS/2 are supported as personal computer NetWare clients

1.3.4.3 Adaptability

NetWare for AIX/6000 from IBM is compatible with other implementations of NetWare, such as NetWare 3.12. Existing NetWare clients need no additional hardware, software, or training to access these resources of the RISC System/6000. The new services are viewed as transparent extensions to the existing NetWare services. NetWare for AIX/6000 from IBM V3.2.5 is based on a system architecture for network computing services, Novell′s Integrated Computing Architecture (NICA), designed to provide integration of heterogeneous desktops and other computing environments. By integrating heterogeneous computing environments, NetWare for AIX/6000 from IBM allows DOS, Windows, OS/2 and now AIX/6000 computer users to share information and resources transparently. NetWare for AIX/6000 from IBM allows any of these desktop computers to easily share file and print services on the RISC System/6000.

1.3.4.4 File Services

NetWare for AIX/6000 from IBM V3.2.5 provides transparent file access over the network for DOS, Windows and OS/2 clients. For example, a DOS user views the file as an eight-character file name, while an OS/2 user can manipulate long file names with extended attributes, just as they would with local files. NFS files can be shared by AIX/6000, DOS, OS/2 and Windows users through NetWare for AIX/6000. Files can also be moved freely between NetWare for AIX/6000 from IBM V3.2.5, NetWare 3.12 and other supported clients. Files and directories stored by NetWare for AIX/6000 from IBM reside in their hierarchical directory tree managed by AIX/6000. This ensures that NetWare for AIX/6000 from IBM employs many of native NetWare′s advanced networking features, including directory hashing, directory caching, disk caching and elevator seeking. The network can share files, application software, printers and other peripherals. In addition, since AIX/6000 actually manages the data, AIX/6000 applications have access to the same data as is available to the PCs on the network.

1.3.4.5 Print Services

NetWare for AIX/6000 from IBM redirects network print jobs to the AIX/6000 spooler or local printers. The PC users can share the same print queues and system printers as other AIX/6000 users.

1.3.4.6 Security

NetWare for AIX/6000 from IBM offers the same access protection and security features as native NetWare. This includes user names, group names, passwords, directory rights and trustee rights. All of this is offered in addition to the high level of security implemented throughout the AIX/6000 system.

1.3.4.7 Program Interfaces

In addition to file and print sharing capabilities, NetWare for AIX/6000 from IBM provides support for NetWare application program interfaces (APIs) such as Sequenced Packet Exchange (SPX). These APIs are the foundation for many important client/server applications on PC Networks.

1.3.4.8 Terminal-Based Applications

Terminal-based applications are also supported from PC NetWare clients. Novell Virtual Terminal (NVT) capability works with off-the-shelf PC terminal emulation software to provide login and access to the AIX/6000 operating system. With NVT, DOS and DOS Windows users gain access to the many AIX/6000 multiuser applications that are available in this environment. NVT delivers seamless terminal emulation with off the shelf terminal emulations since the IPX protocol is used to communicate with AIX/6000.

1.3.4.9 Usability

NetWare for AIX/6000 from IBM provides access to AIX/6000 resources while preserving the PC user′s environment. File access is transparent; a DOS user views the file as an eight-character file name.

Standards: NetWare for AIX/6000 from IBM delivers the benefits of an open systems architecture to the PC user through AIX/6000 and offers integration between existing NetWare servers, PCs, and the AIX/6000 world.

1.3.4.10 Performance

NetWare for AIX/6000 from IBM will be tuned to the communications transport of AIX Version 3.2 for RISC System/6000. In addition, files and directories will be stored employing many of native NetWare′s advanced performance features, including directory hashing, directory caching, disk caching, and seeking.

1.4 IBM LAN Resource Extension and Services (LANRES)

IBM developed LAN Resource Extension and Services (LANRES) in response to the requirements of today′s new system integration of Novell NetWare LANs and IBM hosts (including IBM AS/400s). This client/server application enhances the overall value of your network by combining the advantages of local area networking with mainframe or mid-range computer resources. LANRES ties the LAN closely to the host while preserving the autonomy and operating independence of the LAN. This means that NetWare workstation users can retain the advantages of LANs for workstation response and interworkstation communications, while benefiting from the powerful computing capabilities of System/390, System/370 and AS/400 resources. These resources include storage devices, wide area networking, enhanced data integrity and security, print sharing and transparent access to information.

There are four LANRES products, each meant for its respective host′s base operating system:

- LANRES/MVS
- LANRES/VM
- LANRES/VSE
- LANRES/400

These four products provide similar functions. They differ only in the base operating systems they run on and the different support inherent in the base operating systems.

1.4.1 IBM LANRES/MVS, LANRES/VM and LANRES/VSE

IBM LANRES/MVS, LANRES/VM and LANRES/VSE establish a server environment on MVS, VM and VSE respectively, to allow NetWare clients transparent access to IBM mainframe resources. With LANRES/MVS, LANRES/VM or LANRES/VSE, the host system, NetWare LAN servers, and heterogeneous clients, can be integrated in a way that helps maximize user productivity and provides unique business solutions as shown in Figure 4.

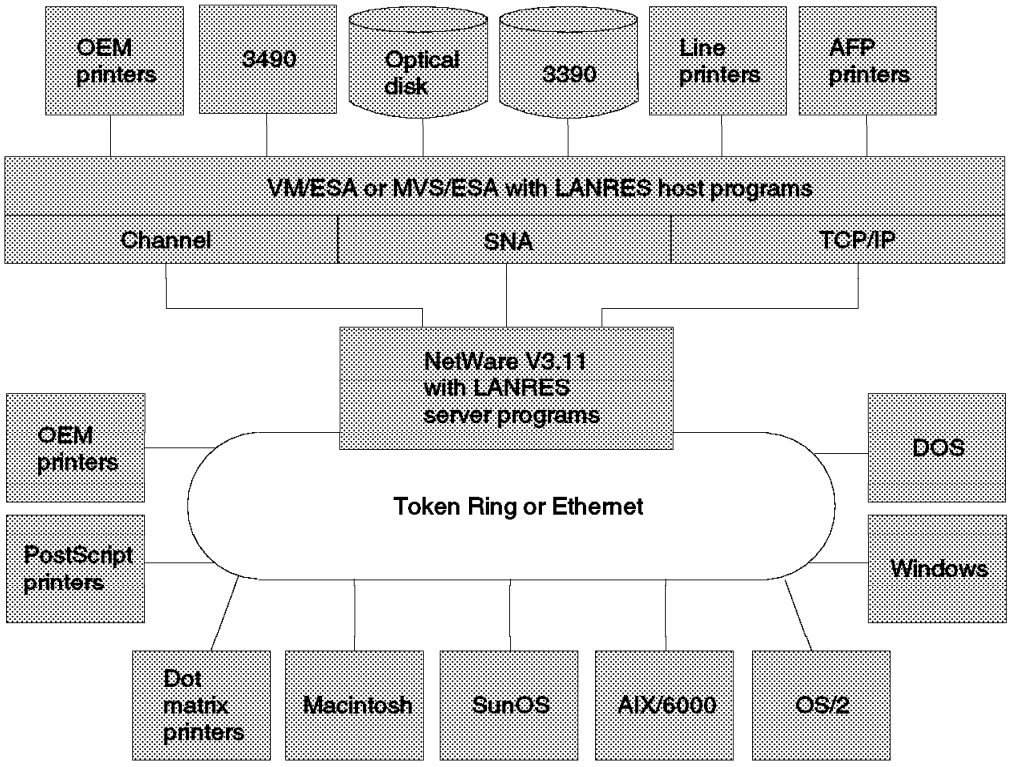


Figure 4. LANRES/MVS or LANRES/VM Environment

Connectivity options include channel-attach, SNA LU 6.2, and TCP/IP. All NetWare clients are supported. The LANRES services include disk serving, print serving, data distribution, and LAN administration. The current version of LANRES/MVS, LANRES/VM and LANRES/VSE is Version 3.0. In this subsection, *LANRES* is used as a collective term for LANRES/MVS, LANRES/VM and LANRES/VSE products. Where there is a distinction between them, the individual product name is used.

Some of the main new functions in LANRES 3.0 are:

- Support for NetWare 3.11, 3.12, 4.01, 4.02 and 4.1
- NetWare for SAA channel driver
- Print transformation; conversion of simple, text only data streams from AFPDS to HPPCL and Postscript, and vice versa
- Support for 3172-3 Pentium processor, Auto LANStreamer and Ether streamer

- Support for ES/9000 Data Compression (LANRES/MVS and LANRES/VSE)

1.4.1.1 Connectivity

All LANRES services are available to a NetWare Version 3.12 LAN server that is channel-attached to an MVS or VM processor. The following channel-attach options are supported:

- A PS/2 with an IBM PS/2 Micro Channel to mainframe connection (MMC)
- An IBM 3172 Interconnect Controller Model 003 with an IBM ESCON Adapter
- An IBM 3172 Interconnect Controller Model 003 with an S/370 Parallel Channel Adapter

In LANRES, enhancements are made to support the IBM 3172 Interconnect Controller Model 003 (3172-3) as a server platform, providing either IBM Enterprise System CONnection (ESCON) or parallel channel-attachment options to host systems. The 3172-3 is an ideal server platform for LANRES users that require high reliability and high availability workgroup servers that are channel-attached to the host. Rack mounting, field installation, service, and options for either ESCON channel or parallel channel attachment, uniquely position the 3172-3 to satisfy LANRES user needs.

With a direct ESCON attachment from the 3172-3 platform LANRES users can now take full advantage of the many benefits of ESCON. Fiber optic links can extend the distance between channels and control units up to 23 kilometers. ″Chained″ ESCON directors can increase this range up to 43 kilometers. Thus, channel-attached LANRES servers are no longer restricted to being physically located on the data center raised floor. Servers can now be placed much closer to the LANs they support. In addition, the standard parallel channel allows for data transfer rates up to a maximum of 4.5 million bytes per second. ESCON supports channel data rates up to 17 million bytes per second. This means that LANRES users using direct ESCON attachments may see improved performance.

All LANRES services are also available to indirectly-attached NetWare LAN servers (NetWare LAN servers attached to a NetWare server that is registered to use LANRES) where the NetWare server registered to use LANRES is channel-attached to the mainframe via one of the supported channel-attach options.

In addition, all LANRES services are available to NetWare servers communicating with MVS, VM or VSE via any of the following remote communications methods:

- SNA

  LANRES support of SNA LU 6.2 communications is provided via NetWare for SAA (NLM) on the NetWare server. SNA LU 6.2 connectivity is perhaps the most flexible method of connecting a Novell NetWare LAN to a System/390 when using LANRES. The IBM Advanced Communications Function Virtual Telecommunications Access Method (ACF/VTAM) and APPC/MVS VTAM or APPC/VM VTAM support must be installed and configured on the MVS or VM host respectively.

- TCP/IP

  To use this method of communications you need to load the TCP/IP NLM on the NetWare server. TCP/IP comes as part of NetWare. You also need to install the TCP/IP Program Product on the VM or MVS or VSE Host system.

The S/390 Host controls the 3172 Interconnect controller and communicates with LANRES using TCP/IP sockets interface.

- VM Programmable Workstation Communication Services (VM PWSCS)

  For LANRES/MVS, VM PWSCS connectivity is supported via the VM PWSCS OS/2 SNA LU 6.2 gateway. To communicate with ACF/VTAM on the MVS host, VM PWSCS requires that the NetWare server running LANRES/MVS be on the same LAN as the VM PWSCS OS/2 domain controller running the SNA gateway feature. For LANRES/VM, this connectivity requires the NetWare server running LANRES/VM to be channel-attached to the host, or an additional OS/2 domain or NetWare domain controller which is attached to the VM host via one of the supported connection methods.

Indirectly-attached NetWare LAN servers are supported for all LANRES services and connectivity options, including direct channel-attach, SNA, TCP/IP, and VM PWSCS.

1.4.1.2 LANRES Services

The following are the four main services in LANRES:

- Disk serving
- Print serving
  - Host-to-LAN printing
  - LAN-to-host printing
- Data distribution
- LAN administration

Disk serving allows workstation hard disks to be stored as single files on MVS, VM or VSE. To the end user, there is no difference between files stored on host DASD and files stored on hard drives on the NetWare server. Print serving provides for both LAN-to-host and host-to-LAN printing. Data distribution allows authorized host users to manipulate files and directories controlled by NetWare. LAN administration allows authorized host users to perform LAN administration tasks.

- **Disk Serving**

  Through LANRES disk services, workstation users can store files on the host system disks. The disks can be configured to be used by the NetWare server and the LAN clients.

  For LANRES/MVS and LANRES/VSE, user files are stored on virtual storage access method (VSAM) linear data sets (LDS), controlled by the LANRES/MVS disk server. Each LDS contains many client files and is treated by NetWare as a separate disk. The LDSs created by the LANRES/MVS disk server function are managed by DFSMS as normal LDSs. Multiple NetWare servers connected to a single MVS or VSE host can share disks stored on MVS or VSE in read-only mode.

  LANRES/VM provides a disk server for NetWare that can store entire PC disks on the VM system as a single conversational monitor system (CMS) file. There can be multiple files on the VM host. Each file is managed as a separate PC disk by NetWare. Multiple NetWare servers connected to a single VM host can share disks stored on VM in read-only mode.

  To the end user, there is no difference between files stored in disks on the host, and files stored on hard drives on the NetWare server. Each NetWare

volume can be mapped to a disk drive letter in the client. The client can access a combination of local disk drives, drives on the NetWare server, and disk drives on the host. DOS, Microsoft Windows, OS/2, Macintosh, and UNIX clients are supported.

Host users and programs cannot directly access individual files on LANRES controlled disks. However, they can indirectly access files using the respective LANRES data distribution.

- **Print Serving**

  LANRES provides a print server for NetWare V3.12 that dequeues files from the NetWare print queues and sends them to the host system for processing. DOS, Microsoft Windows, OS/2, Macintosh, and UNIX clients are supported.

  There are various exits for processing the files:

  – Line exit

    With this exit, client data is converted from ASCII to EBCDIC and directed to a printer. Print Services Facility/MVS (PSF/MVS, PSF/VM, PSF/VSE) enables the data to be printed on any advanced function printer (AFP) With LANRES/MVS, you now can print directly to either VTAM or JES.

  – PostScript exit

    This exit allows client PostScript files to be printed on host printers using the PostScript Interpreter. The data can be printed on any advanced function printers (AFPs).

  – 5152 Model 2 printer emulation

    With this exit, client data is processed for printing on a host printer the same way it would be processed for printing on a 5152 Model 2 IBM PC graphics printer. The data can be printed on any advanced function printers (AFPs).

  – ASCII exit (VM, VSE)

    This exit passes print data to remote spooling communications subsystem (RSCS) for printing on an ASCII printer attached to an ES/9000 or ES/9370 ASCII port. Any data supported by an attached printer may be printed.

  – Sendfile/Transmit Exit

    Using this exit allows NetWare client data to be sent to a host user ID. In this way the data will appear in the same way as it would if it had been sent by another local or remote IBM S/390 user ID.

  – Installation-defined

    This allows the installation to define customized print exits for different types of printing processes.

  LANRES provides the required routing information to the host system. The host system then uses this information to route the output to the correct printer.

  In addition to NetWare client printing on host printers, MVS, VM or VSE users can print line data on NetWare supported printers. A NetWare user ID is not required. The following exits are supported:

  – Line exit

With this exit, line data may or may not be translated from EBCDIC to ASCII. The data stream is adjusted to handle printer control characters such as form feeds.

- PostScript exit

  This exit enables PostScript files generated on the host system to be printed on a LAN-attached PostScript printer.

- Installation-defined exit

  The installation may define one or more customized exits for different types of printing processes.

- **LAN Administration**

  The LAN administration component of LANRES allows an authorized host systems administrator to add, delete and rename users on the LAN. The administrator can also set passwords, set password restrictions, limit space utilization, control file and directory access, and perform other administration functions. Many of the functions provided by the NetWare SYSCON and PCONSOLE utilities are supported.

  LAN administration requires the host administrator to supply a valid NetWare user ID and password. If the NetWare user ID has supervisor authority, then the host administrator′s authority will be unrestricted. If the NetWare user ID has limitations, the host administrator′s authority will be limited accordingly.

  There are two objectives for this administration facility: first, to have host administrator control of the LAN from any host authorized user ID; second, to allow administration commands to be combined together in REXX EXECs to automate LAN administration tasks.

- **Data Distribution**

  The data distribution component of LANRES allows authorized host users to manipulate files and directories controlled by NetWare V3.12. The volumes containing these files may be on the NetWare server or on the host system.

  Data distribution requires the host user to supply a valid NetWare user ID and password. If the NetWare user ID has supervisor authority, then the host user′s authority will be unrestricted. If the NetWare user ID has limitations, the host user′s authority will be limited accordingly. This function implements a central data distribution capability and allows users the ability to create their own applications for moving data between the system and the LAN.

1.4.2 IBM LANRES/400

LAN Resource Extension and Services/400 (LANRES/400) establishes a server environment on AS/400 to provide NetWare clients transparent access to host resources. Its functions are basically similar to LANRES/MVS, LANRES/VM or LANRES/VSE as discussed in the previous subsection. With LANRES/400, AS/400 systems, NetWare LAN servers, and heterogeneous clients, can be integrated in a way that helps increase user productivity and provides unique business solutions. Customers who use LANRES/400 can save time and leverage skilled resources while they provide their NetWare clients with improved services.

LANRES/400 allows users to retain the advantages of LANs for workstation responsiveness, availability, and interworkstation communications, while bringing to the LAN, host-based LAN administration and data distribution. With LANRES/400, AS/400 users can handle administration problems and changes, as

well as manage NetWare server files and directories, from a central location. The AS/400 user also has access to conveniently located LAN or personal printers. In addition, LANRES/400 brings to the LAN such AS/400 resources as large capacity DASD, system printers, and wide area networking (WAN). LANRES/400 services complement existing NetWare functions. All these LANRES/400 services, combined with the reliability of AS/400 storage, and the systems management discipline typically associated with AS/400, make LANRES/400 an attractive extension to the integration of AS/400 and LAN environments.

1.4.2.1 Connectivity

All LANRES/400 services are available to NetWare servers communicating with AS/400 via:

- APPC

  LANRES/400 support of APPC communications is provided via NetWare for SAA on the NetWare server.

- TCP/IP

  This connectivity option requires that IBM TCP/IP Connectivity Utilities/400 be installed on the AS/400 host. No additional server software is required.

LANRES/400 supports NetWare Version 3.12 and NetWare Version 4.1. NetWare V4.1 support is provided via bindery emulation. Bindery emulation allows a NetWare Version 4.1 server to be viewed and administered just like a NetWare Version 3.12 server. It provides compatibility with NetWare V3.12 drivers, utilities, NLMs, and applications. NetWare V4.1 features not supported via bindery emulation are also not supported by LANRES/400.

1.4.2.2 LANRES/400 Services

The following are the four main services that LANRES/400 provides:

- Disk serving
- Print serving
  - Host-to-LAN printing
  - LAN-to-host printing
- LAN administration
- Data distribution

LANRES/400 provides a disk serving facility that allows workstation hard disks to be stored on the AS/400 host as single files. Besides making AS/400 system printers available to NetWare servers and clients, LANRES/400 makes LAN printer resources available to AS/400 users. Data distribution service helps with change management. Authorized AS/400 users can send data to, and retrieve data from, the NetWare server. They can list server files and directories, and create and delete server files. LANRES/400 lets users move the LAN administration to the AS/400, where tasks can be automated and where multiple LANs can be centrally administered. In effect, LANRES/400 extends the NetWare environment to include the AS/400 host. It does this transparently, so NetWare clients are unaware of the LAN-to-AS/400 interaction. They retain all the advantages of working in a LAN environment and receive use of AS/400 large-capacity DASD and system printers.

- **Disk Serving**

  With LANRES/400 disk serving, workstation users can transparently store files on AS/400 disks. Entire workstation fixed disks are stored on the

AS/400 host as single files. User files are stored as a single document in a folder. To the LAN workstation end user, there is no functional difference between files stored on host disks and files stored on fixed disks on the NetWare server. The end user can access a combination of local disk drives, drives on the NetWare server, and LANRES/400 drives on the AS/400 host. However, the AS/400 users and programs cannot directly access individual client files, but they can indirectly access these files using the LANRES/400 data distribution service.

The following are some advantages of using the AS/400 environment for disk serving:

- Increased disk space available to NetWare file servers

  LANRES/400 disk serving enables growth by using AS/400 storage capacity to relieve capacity constraints of workstation-based servers. Adding additional drives to the NetWare server may require the installation of additional physical fixed disks. However, adding server managed disk space on the AS/400 only involves the assignment of additional space, which is a considerably easier task and less disruptive to the NetWare server.

- Enhanced reliability, security and recovery

  Generally, the reliability of AS/400 disks is higher than hard disks of the workstation and this benefit can be used to enhance the protection of the LAN files. The higher security of the AS/400 data processing (DP) center operation and control of disks provides the LAN environment added protection in storing sensitive information. Mission critical data stored on LANRES/400 host disks can be backed up as part of the normal host backup process. In a disaster situation, entire server volumes on AS/400 disks can be restored quickly and efficiently.

- Improved worker productivity

  LANRES/400 disk serving is functionally transparent to end users. Users interact with NetWare in their usual manner and are virtually unaffected by the LANRES/400 software running on the NetWare server and the AS/400 host. Disk resources on the AS/400 are accessed by specifying a drive letter (for example, H:), the same way resources on the workstation are used.

- **Print Serving**

  LANRES/400 provides both LAN-to-host and host-to-LAN printing services. LAN users may direct output to AS/400 system printers and AS/400 users can send output to conveniently located LAN or personal printers. That is, all AS/400 users and NetWare clients may direct their print files to printers located throughout the enterprise. As a result, users have the power and flexibility to choose an individual printer based on physical proximity and convenience, security needs, and functional requirements of the file to be printed. LANRES/400 provides support for converting print files from workstation to host formats and vice versa.

  LAN-to-host printing

  LANRES/400 gives NetWare clients access to AS/400 printers. Clients can use print utilities such as the NetWare CAPTURE or NPRINT commands. CAPTURE routes print data that would otherwise go to a local printer, from the client to the NetWare server. NPRINT is used to print a data set.

NetWare clients can direct their output to different host printers. DOS, Microsoft Windows, OS/2, Macintosh, and UNIX clients are supported.

LANRES/400 supports the following LAN-to-host printer exits:

- Line exit

  With this exit, client data is converted from ASCII to EBCDIC and directed to an AS/400 printer.

- Sendfile exit

  This allows the print file to be sent to an AS/400 user.

- ASCII exit

  This exit passes print data to an ASCII printer attached to an AS/400. Any data supported by an attached printer may be printed.

- Installation-defined

  This allows the installation to define customized print exits for different types of printing processes.

Host-to-LAN Printing

LANRES/400 gives AS/400 users access to LAN printers. Using the LANRES PRINT command, any user on the AS/400 can print data on a LAN printer supported by a NetWare server. This gives users the convenience of working with local printers. The status of print jobs can be queried with the LANRES QUERY PRINT command. Users do not need a NetWare user ID to print their files on the LAN printers. Additionally, using a set of default values, host-to-LAN print serving can print output generated without using the LANRES PRINT command. Host-to-LAN printing tasks can also be automated using REXX procedures and Control Language (CL) programs.

LANRES/400 supports the following host-to-LAN printer exits:

- Line exit

  With this exit, line data may or may not be translated from EBCDIC to ASCII. The data stream is adjusted to handle printer control characters such as form feeds.

- Standard Character String (SCS) exit

  This exit converts data that is in SCS format (that is it contains control characters for a virtual printer) into ASCII format (it translates/transforms the SCS control characters into ASCII carriage return, line feed, space).

- Installation-defined

  This allows the installation to define customized print exits for different types of printing processes.

- **LAN Administration**

  LANRES/400 provides the ability to administer NetWare servers from the AS/400. Systems management is enhanced with support for centrally administering the LAN environment from the AS/400 host. Multiple servers can be administered from a single AS/400 host. This includes NetWare servers with LANRES/400 installed as well as NetWare servers connected to those with LANRES/400 installed. Commands to perform these activities can be combined together in REXX procedures or CL programs to automate server administration tasks.

LANRES/400 has both a command-line interface and a system menu interface for administration commands. Each authorized AS/400 user can:

- Add and delete LAN users and user groups
- Modify their access to directories and files (their trustee rights)
- Limit the disk space available to them
- Change their passwords
- Administer print queues
- Perform other LAN administration tasks

Many of the functions provided by the NetWare Version 3.12 SYSCON and PCONSOLE utilities are supported.

- **Data Distribution**

  The LANRES/400 data distribution service enables authorized AS/400 users to manipulate files and directories controlled by NetWare. The files can be physically on LANRES/400 host disks or on the NetWare server itself. From an authorized AS/400 user ID a user can:

  - Distribute data to the server
  - Retrieve data from the server
  - List files and directories on the server
  - Create files and directories on the server
  - Delete files and directories from the server
  - Perform other tasks associated with data distribution

  Data can be distributed from a central location and end users can create applications for moving data between AS/400 shared objects and the NetWare server. The distribution service consists of both a command-line interface and a system menu interface for issuing data distribution commands. Users can automate tasks using REXX procedures or CL programs. Data distribution enables LAN users to access host data and host users to access data generated on the LAN. Enterprise data can be shared among host and LAN users as necessary, without impacting the host and LAN user work environment.

1.5 IBM LAN File Services/ESA

LAN File Services/ESA provides workstation clients with transparent access to S/390 resources and brings the strengths of S/390 (data management discipline, high-capacity I/O, bandwidth, and cross application data access) to the workstation environment. LAN File Services/ESA enables the reduction of LAN storage costs and improves the security, consistency and integrity of LAN data by providing an enterprise-wide LAN file system on MVS and VM. LAN File Services/ESA is a component of the MVS System Open and Distributed Strategy providing OS/2 LAN Serving.

LAN File Services/ESA enables the implementation of an enterprise-wide file system strategy where data is positioned based on requirements for sharing. A key feature of LAN File Services/ESA is the transparent manner in which it provides services to end users who are accustomed to receiving services from workstation-based servers. In addition to transparency, the performance of LAN File Services/ESA will compare favorably to the performance of a local workstation-based server.

1.5.1 Description

LAN File Services/ESA is comprised of an S/390 component and one client component, the OS/2 LAN Server client which runs on the OS/2 LAN Server Version 4.0 Advanced. The S/390 component provides storage for workstation files. The workstation repository on S/390 supports hierarchical directories, long names, byte-level locking and extended attributes. These facilities can be used by DOS and OS/2 users connected to the OS/2 LAN Server. To the workstation end user the files stored on S/390 look like files stored on the OS/2 LAN Server. They can be accessed and used like any other workstation-based file. In addition, LAN File Services/ESA provides the capability to share workstation data between multiple OS/2 LAN Servers. A channel attachment between the OS/2 LAN Server and the S/390 provides high-speed data transfer for the OS/2 LAN Server user. The channel connection can use the IBM PS/2 Micro Channel to Mainframe Connection, an ESCON connection through an IBM 3172 Interconnect Controller Model 003 or an IBM System/370 Emulator/A card. The use of SNA connectivity for wide area networks is also supported. A set of administrative commands is provided to maintain the workstation data stored on S/390. The IBM Software License Monitor/MVS and VM is used to monitor the use of LAN File Services/ESA.

1.5.2 Functions

The following functions are available in LAN File Services/ESA on the VM platform and on the MVS platform. TCP/IP NFS users can also store data in the S/390 workstation repository. OS/2 LAN Server users and NFS users can transparently share data stored on S/390. The full suite of NFS Version 2 Remote Procedure Calls (RPC) is supported, including hierarchical directories, long names, hard and symbolic links, and UNIX style permissions. LAN File Services/ESA also provides the capability to perform file level backup between the LAN File Services/ESA repository and WDSF/VM or ADSTAR Distributed Storage Manager. This eliminates the overhead of moving files between the workstation and S/390 in order to perform backup.

In addition, workstation clients of LAN File Services/ESA can access data stored on VM CMS minidisks. The CMS minidisk data will look like a workstation directory to LAN users. When workstation clients access CMS minidisk files, LAN File Services/ESA will automatically translate the file data between the VM code page and the workstation code page. The code page support is provided for both DBCS and single-byte character set (SBCS) code pages.

1.5.2.1 Business Solutions

Enabling new applications, LAN File Services/ESA supports storage intensive workstation applications. LAN File Services/ESA allows the capacity of System/390 to be used for the storage and retrieval of large data objects such as multimedia images, graphics and video clips. The large storage capacity of S/390 enables the implementation of these applications that use S/390 as a repository for their data. This reduces the requirement for large amounts of storage at each LAN-based server, since the data can be stored once on S/390 and accessed by numerous LANs.

1.5.2.2 Growth Enablement

- Increased capacity

  Large files or libraries that would have previously been replicated across numerous LAN servers can now be stored once on S/390. This reduces the DASD requirements for the LAN servers and ensures a more consistent view of data throughout the enterprise since the data is not maintained in multiple places. In addition, maintenance tasks on the LAN server that require temporary disk space, such as database maintenance, can now use DASD space on the S/390 instead of maintaining extra DASD on the LAN server.

- Connectivity improvements

  With direct ESCON LAN File Services/ESA customers can now take full advantage of the many benefits of ESCON. Fiber optic links can extend the distance between channels and control units up to 23 kilometers (14.3 miles). ″Chained″ ESCON directors can increase this range to 43 kilometers (26.7 miles) and expand the channel-to-channel range up to 60 kilometers (37.3 miles). Thus, channel-attached LAN File Services/ESA servers are no longer restricted to being physically located on the data center raised floor. Servers can now be placed much closer to the LANs they support. ESCON will provide additional bandwidth and enable campus-wide connectivity.

1.5.2.3 End User Productivity

- Improved worker productivity

  The use of S/390 resources is completely transparent to the end user. Resources on S/390 are accessed by specifying a drive letter (for example, H:), the same way resources on the workstation would be used.

- Interoperability

  Workstations connected via coaxial cable to a 3174 with Peer Communications can access LAN File Services/ESA resources via the OS/2 LAN Server. This enables coax-attached workstations to use LAN File Services/ESA and share data with workstation users that are LAN attached.

  NFS users and OS/2 LAN server users can transparently share data between the two environments using LAN File Services/ESA. In addition, data stored in S/390 format on CMS minidisks can be accessed by VM users, OS/2 LAN server users and NFS users, subject to CMS minidisk sharing restrictions.

1.5.2.4 System Management

- Improved LAN system availability

  The workstation data that is stored on S/390 can be quickly backed up using the high-speed devices available on S/390. Since the backups can be performed on a scheduled basis by data center personnel, the exposure of data not being backed up is greatly reduced. The time required to back up or restore data should be reduced when using the facilities of S/390. A DASD failure on a LAN-based server will not affect the integrity of data stored on the S/390. When additional DASD space is required on a LAN server connected to LAN File Services/ESA, the required space can be easily added without requiring any downtime on the LAN server.

- Managing multiple systems

  The storage of workstation data on S/390 can reduce the burden on LAN-based administrators. Many of the routine LAN administration tasks, such as backup and increasing DASD space on the server, can now be

performed by the central information systems organization. This allows the LAN administrator to focus on other tasks.

- Security

  LAN File Services/ESA allows the use of an external security manager (for example, RACF) for access control when running on MVS/ESA and for the NFS feature on VM/ESA.

- License management

  The IBM Software License Monitor/MVS and VM provides an automated method of monitoring the number of OS/2 LAN Server machines accessing the LAN File Services/ESA host component and/or use of the NFS host server. The IBM Software License Monitor/MVS and VM provides notification of unauthorized access attempts. Each OS/2 LAN Server machine or the NFS host server is registered to the IBM Software License Monitor/MVS and VM as a client of LAN File Services/ESA.

1.5.3 Benefits

The following are the main benefits of LAN File Services/ESA:

- Increased storage capacity

  LAN File Services/ESA reduces the amount of redundant data and number of applications stored across multiple LAN servers and increases the storage capacity of the existing LAN servers by using S/390 resources.

- Transparency to the end user

  The use of the LAN File Services/ESA workstation repository will be transparent to the end user. LAN File Services/ESA will appear, to the end user, as another file sharing resource on the OS/2 LAN Server.

- Interoperability among all clients supported by LAN File Services/ESA

  Any client of LAN File Services/ESA will be able to transparently share data and applications with any other LAN File Services/ESA client. For example, an OS/2 LAN Server client will be able to share data with an NFS client by using LAN File Services/ESA services.

- Performance

  LAN File Services/ESA supports a channel attachment between the OS/2 LAN Server and S/390.

- Per-client pricing

  The pricing structure of LAN File Services/ESA is based on per-client pricing, which provides an attractive entry level for S/390 client/server computing. A LAN File Services/ESA client is defined as an OS/2 LAN Server machine running the LAN File Services/ESA OS/2 LAN Server component.

In addition, LAN File Services/ESA supports the enhanced IBM 3172 Interconnect Controller Model 003, as an alternative LAN server platform. This configuration provides several advantages including direct ESCON attachment, rack mounting and CE service.

1.6 Lotus Notes

Lotus Notes is a client/server groupware product, working on distributed and shared databases. It simplifies the exchange and the organization of data from different people working together in different locations. In addition it offers E-mail and a development environment for new Lotus Notes applications to satisfy individual needs.

The Notes client provides a full graphical user interface (GUI) with Smarticons that enhance the ease of use and the ease of learning. Documents in a database can store all different kinds of data, that can be worked on at the client. A document can hold text, rich text, images, graphics, sound and motion picture images.

Lotus Notes provides multilevel security, which is based on the RSA algorithm. Access is controlled for servers, databases and individual documents. It also includes user authentication, encryption and digital signatures.

Lotus Notes is running on many different platforms all working together over different networks. All clients, regardless of the platform can access all servers, exchange information and send and receive E-mail. Today, the Lotus Notes server and client is available for OS/2, Windows, and UNIX. The Lotus Notes server is also supported by NetWare and Windows NT. For the Apple Macintosh a client version is available. Supported network protocols are: NetBios, TCP/IP, AppleTalk, IPX/SPX, X.PC and remote dial-up.

1.6.1 Fundamentals

Lotus Notes is a real client/server product, where the client accesses data stored on the server. A Lotus Notes server is not the same as a network file server, that shares resources like, files, printers or serial devices. It is an independent server and needs not to be defined in an existing domain of a network. The Notes server stores, shares and distributes databases, which can be accessed by other servers or clients.

The same databases can reside on many different servers and can be used by the clients. Changes to documents in a database, stored on multiple servers are replicated to all the other servers, that hold the same database. After a certain time, each server holds the same updated database with all the new and changed documents. Databases may also exist locally on clients and therefore can only be accessed by the client until they are replicated to a server.

All servers, users, connections and replication schedules are defined in the public *Name & Addressbook* of a domain. All members of a domain (group of servers and their clients) share the same addressbook. A user will use the addressbook to look up E-mail addresses of other users. Notes servers use the Name & Addressbook to find routes for mail-routing and replication of databases to other servers. For the Lotus Notes administrator, it is an administration tool to manage the domain. It stores information about access rights and is used for authentication of users and servers.

For authentication between servers or clients and servers, certificates are used. Two communication partner must be certified by the same certifier (flat domains) or must have a parent certifier in common (hierarchical domains) in order to communicate. Only if they have the same certificates, is access to the other system allowed. A server or a client can hold more then one certificate in order

to communicate with multiple systems. Certificates are stored in a private ID file. An ID file is certified by a certifier and is a kind of passport, that identifies a server or a client.

Additional security is given by the server access list and the database access list. Even if a user or server is certified, to use a server, access is controlled by a server access list and can be denied for individual users, groups and servers. Once a server can be accessed, the database access list controls the access to individual databases. Therefore, Notes uses the principle of private and public keys.

1.6.1.1 The Name & Addressbook

The Name & Addressbook is the management tool of a domain. Each domain has one public Name & Addressbook. The addressbook contains information about connections to other servers in the same or a different domain. Servers from other domains and over which connection they can be reached are defined here. It also holds the cross-certificates necessary to control access of other servers and users. The information, stored in the Name & Addressbook are used by the Lotus Notes server for mail-routing, replication of databases with other servers and access control. Replication schedules can be set up in connection documents. Access rights for users, groups and servers are managed in server documents. The Name & Addressbook gives the administrator the possibility to monitor databases and statistics about the domain. It also provides information about installed Notes licenses.

The main views and documents of the Name & Addressbook are the following:

- Domains
- Servers
- Connections
- Groups
- People
- Certificates
- Cross-certificates
- Database and statistic monitor
- Licenses

1.6.2 The Lotus Notes Server

The Notes server holds several databases, that can be accessed by other servers or clients. The server controls the access to the server and to the individual databases. To update and receive changes from the same databases stored on other servers, the Notes server is responsible for replication. Replication is scheduled in the Name & Addressbook and managed by the administrator.

One particular database is the mail database, that stores mail for users. The server, which holds the mail directory of a client is called the client′s home server. The server manages the mail database and stores new incoming mail in the mail directory of the client. Outgoing mail will be routed to its destination on the foreign server, where it is delivered to the addressed users′ mail directory. Mail routing is a store and forward process. Mail can be routed through different servers until it reaches its destination.

The Notes server can provide several connections to other servers. These servers may be part of the same or a different domain or located in the same or a different network. In addition remote connections via modem can be set up and scheduled. Notes uses different ports for each connection to a network. For example, you can set up one port for TCP/IP, one port for NetBIOS and another port for a serial connection. Each server has an ID file, that stores certificates to access other server.

All definitions made for server, clients, groups, connections, replication, access control and mail routing are stored in the public Name & Addressbook. The server always refers to the addressbook, to find the information to perform different jobs.

The Lotus Notes server consists of two parts, a full screen non-graphical server component and a client component with a graphical user interface. The client component is used by the Lotus Notes administrator to manage the server and the domain. The server component runs several programs and server tasks. On the server console the administrator can issue server commands to start tasks or to view activities running on the server.

The following are the main tasks performed on a server:

Replicator	Replication of databases with other servers or a client.
Router	The router task is used for delivering data to its destination and to route mail to other servers or domains.
Login	Listens to port requests by users of add-in programs.
Indexer	Updates all indexes for a database for full text search.
Designer	Updates all databases to conform to their design templates.
Database fixup	Fixes databases, when they are corrupted.
Statistics	Updates the database statistic in the server′s log file.

Server commands can be directly entered at the server′s console or at a remote server console on each client, if the client has the permission. The following list shows the most important server commands:

LOAD	Starts the specified server program/task on the server
REPLICATE	Forces unscheduled replication
PULL	Forces unscheduled replication in one direction
ROUTE	Forces unscheduled mail routing
SHOW	Shows tasks, user, ports, memory, disk space and the configuration

The Notes server is configured in the NOTES.INI file. Most of the variables are set, when the server is installed. They can be changed or new variables can be set, to customize the server. If for example more than one addressbook should be used by the server, you will specify the addressbooks in the NOTES.INI file.

1.6.3 The Lotus Notes Client

The Lotus Notes client is available in two versions. The Lotus Notes client and the Lotus Notes Express client. The express version of Lotus Notes offers only a subset of functions. Application development for example is not supported. The Lotus Notes Express version can be updated to a full version by simply using an ID file, that is certified for the full version. The certifier is provided by your administrator. Of course you need a license to do so, but no re-installation of the client code is necessary.

The Notes client uses a graphical user interface (GUI) as its desktop. You can customize the desktop for your individual needs. All databases that you want to access can be added to the desktop as an icon. Smarticons, that are available for almost every Notes function, help you to use Notes more efficiently.

You can install the client either as a stand-alone system with no connection to a server, as a remote client with a modem connection or as a client with a network connection to a server. Normally your client has a home server, which is the server that holds our mail directory for incoming and outgoing mail. This is called server-based mail. You can work with the databases stored on your home server and make changes to them, if you are allowed. If your client is certified by other servers, you can, of course, access them if you have a connection.

Each client holds an ID file that stores the certificates giving them access to servers. Only if the client is certified, is it possible to use a server. The initial ID file is supplied by the home server and holds its certificate.

Like other servers, you can store copies of the servers database on your local system. This is especially interesting if you are traveling and don′t have the possibility to access your server. You can then work on your local copy and when you are back in your office and connected to the network, replicate changes to your server. In that case, you will use workstation-based mail to write mail on your local system and replicate them to your home server, when you are connected.

The client uses the public Names & Addressbook to look up other users of its domain. A client has also a private addressbook to store frequently used addresses and information about remote connections to other servers.

If you use a full client license, you can write Lotus Notes applications for your individual use. These applications are databases stored on your local system and can only be accessed by you. If you want to share your applications with other users, you have to replicate them to a server and give access to selected users.

1.6.4 Connectivity

Lotus Notes use the concept of domains and networks, to organize client and server connections. A domain is a group of Notes servers that belong together and are managed in the same Names & Addressbook. An example for a domain is, a group to which belong all servers of one company or of one department. A network is an additional group, that contains servers, which can directly connect to each other. An example for a network is the LAN in one building. Networks are also managed in the Name & Addressbook. Each domain share the same public Name & Addressbook. The idea of Name & Addressbook is explained in more detail on the following pages.

A typical Lotus Notes environment could look like the following:

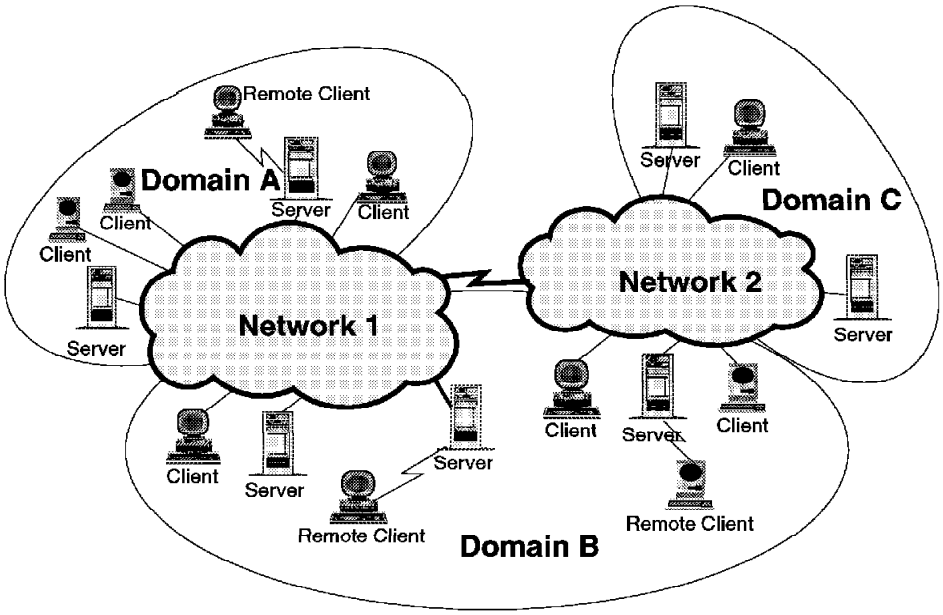


Figure 5. A Lotus Notes Environment

Lotus Notes knows two different kinds of connections. On one side you have connections between servers and clients, on the other side you have server or domain connections. Connections can be remote or network connections.

Client connections have to be set up at your client. Only the remote connection the modem must be configured and operational at the server. Once you have defined a port for your client connection you can access the server, if you are certified. For remote connections, a connection document in the private addressbook needs to be created that holds information about the server and the phone number that is used for dial in.

To set up a connection you have to define the following:

- Ports (COM, LAN0, TCP/IP, etc.)
- Home server
- Home domain
- Phone number (if you use a remote client)

Server connections are set up at the server and in the public Name & Addressbook. For each network protocol that is supported by the server a port has to be defined. You must create a connection document in the public addressbook for each remote or network connection to a server. For network connections only one connection document for replication needs to be created and scheduled at one of the servers. Servers on the same Notes network and domain, route mail to each other automatically. Remote connections use two

connections documents, one on each side. You have to set up replication schedule, and mail routing between the servers in these documents.

1.6.4.1 Connection Documents

The connection to other servers in the same or a different domain are defined in either a remote or a network document in the Name & Addressbook. Network documents are used to set up a connection to a server in the same network. Servers on a different network are set up in the remote document and is mostly used for modem connections. A connection document defines the port that the two servers use for communication, the schedule for replication and mail routing.

1.6.4.2 Server Documents

Each server of an domain is defined in a server document in the public Names & Addressbook of that domain. The server document specifies the name, domain name and the ports that a server uses for communication. In addition, the server access list, which defines who can access the server, is maintained in that document. Foreign servers, from other domains, are not defined in a connection document.

1.6.5 Mail Routing

With Lotus Notes, you can send mail to every other user on your domain. The address of a user can be found in the public addressbook. If your domain is connected to other domains, it is possible to route your mail to destinations on that domain. Even if the domain of the user is not directly connected to your domain, mail can be sent through another domain. Of course your domain and the destination domain must be somehow connected through other domains. This domain is called a *non-adjacent domain* and must be specified in a special document in the addressbook.

Each user of a server has a mail directory and a mail database stored on their home server, if they use server-based mail. They are the only one that has access to this mail database. Workstation-based mail is stored in a local database on the client until it is replicated to the server.

Mail routing is a store and forward process, which means that mail is routed from server to server until it reaches its destination. Each server has a mailbox file called MAIL.BOX. All mail, that a server receives from clients or other servers is stored in that file. The router task, running on every server, is responsible for delivering the mail stored in the MAIL.BOX file. If the destination is on the same server, the mail is simply stored in the mail database of the recipient.

If the destination is on another server in the same domain, the router has to look up a connection to that server in the public Name & Addressbook. The router routes the mail to the destination server, which receives the mail in his MAIL.BOX file. The router at the destination server delivers the mail to the mail database of the receipient.

If the mail is addressed for a destination in a non-adjacent domain, the router routes the mail to the domain, which is defined in the non-adjacent domain document for that domain. The mail can pass through several domains until it reaches its destination.

The MAIL.BOX file of a server also holds dead mail that could not be delivered by the router. It is the job of the administrator to maintain the mailbox file of the server from time to time. Old mail must be deleted or resent with the correct address.

1.6.5.1 Encryption

You have the ability to encrypt your mail. With encryption, you can ensure, that only the intended recipient can read your document. Encryption uses public and private keys of the users stored in the addressbook and the ID file, to encrypt mail.

You can specify three types of mail encryption:

Outgoing Mail When you send your mail, the system will ask you, if you want to encrypt it. Your mail will be encrypted at your client, before it is sent to the destination.

Incoming Mail All incoming mail can be encrypted. The mail will be stored in encrypted form in the users mail database.

Saved Mail You can encrypt copies of your mail, that are store in your mail database.

Server-Specified You can automatically encrypt the mail received by all mail files on a server.

1.6.5.2 Mail Interfaces

Lotus Notes has the ability to exchange mail with other mail systems such as IBM′s PROFS, DEC′s VAX/VMS Mail, SMTP, X.400, cc:Mail or other VIM-compliant mail systems and with mail handling systems such as MHS or SoftSwitch. Also incoming and outgoing faxes can be handled by Lotus Notes.

The vendor independent messaging (VIM) interface is supported by Lotus Notes. This means, that a user can select the mail client independently from the Lotus Notes server. The mail client must, of course, be adopted to the VIM interface. For example cc@colon.Mail clients are able to use the Notes server as a mail back end.

To exchange mail with other mail systems, Notes uses mail gateways. A mail gateway is a Notes server add-in. For example, to exchange mail with IBM′s Profs, you can use Mail Gateway/2. When the Notes user sends mail to a user, who uses another mail system, the router will route the mail to the mail gateway, which is specified in the addressbook as a foreign domain. The mail gateway receives the mail and converts it to the format used by the foreign system and delivers the mail.

1.6.6 Security

Lotus Notes provides different levels of security. The highest level is the authentication of users and servers with certified ID files and passwords. The second level is a server access list, which holds the names of groups, servers and users, that are allowed access to the server. The third level is the ACL (access control list) for each database, where the database manager can give access to individual people. The lowest level is the access rights to individual documents in a database.

1.6.6.1 Certifier and ID Files

A certifier is a kind of stamp which the administrator uses to give Lotus Notes users and servers access to a server or domain. Each Notes client and server has their own ID file that identifies it. The ID file must be certified (stamped) by the certifier of a domain or a server. A domain has one main certifier, that is created at the first installation of a Lotus Notes server in one domain. Each additional server and each client will be certified by that certifier. A server can create its own certifier to give other servers or users access to its databases.

When the client or server wants to accesses a server, that server asks for the ID file. The server will check the ID file of the client for at least one certificate in common with its own certificates. If the client is certified to access that server, the user is prompted for his password, to ensure that he is the owner of the ID file.

Lotus Notes uses the following three different types of ID files:

CERT.ID This is the certifier, which the administrator uses to stamp users, servers and to create other certifiers. An organizational certifier will be created by the system, the first time you install a server for your organization. This certifier is then used to certify users and additional servers.

SERVER.ID This is the ID file of the server. It is stamped by at least one certifier. The server ID holds information about the server and all its certificates to access other servers and domains.

USER.ID This is the ID file of a user. The user ID file must be certified by the same certifier then the server or domain that the user wants to access. It holds all the information about a user and all its certificates. The user ID file will be created, when the administrator creates a new user.

1.6.6.2 Hierarchical Domains

Hierarchical certificates are used as the default certificates in Lotus Notes 3.x and are not available in previous versions. The idea of a hierarchical structure is related to the CCITT X.500 naming standard. The choice of a hierarchical, distinguished naming, has the advantage of avoiding naming conflicts in larger organizations. It also simplifies the access between servers in the same domain. Each server or user, that has an ancestral certifier with another server in common, is allowed to that server. A distinguished name may consist from the following four parts:

User name A user′s name is defined by his first name, middle initials and his last name. An example for a user name is Peter R. Smith.

Organizational Unit An organizational unit is a department in an organization. An example for an organizational unit is ITSO, Consulting.

Organization An organization is the company which is divided into the organizational units. An example for an organization is IBM, Lotus.

Country Two letter county code defined by the CCITT. An example for a country is US for United States, DE for Germany.

Each level of an organization has its own certifier to certify users, servers and to create new certifier for additional organizational units. In hierarchical domains, a user or server name is determined by the certifier, that was used for certification. If, for example, Peter R. Smith is certified by the certifier /ITSO/IBM/US, his full distinguished name will be Peter R. Smith/ITSO/IBM/US. Each server and client of an organizational unit will be certified by a certifier of the corresponding level. The certifier of an organizational unit is created by a certifier of a higher level in that hierarchies. Since all servers and users are certified by a certifier that is a successor of the organizational certifier, it is possible for them to communicate. If, for example, server RALN1ITS is certified by the certifier /RAL/ITSO/IBM/US and a second server POKN1ITS is certified by the certifier /POK/ITSO/IBM/US, both servers can access each other because they share the same ancestral certifier /ITSO/IBM/US.

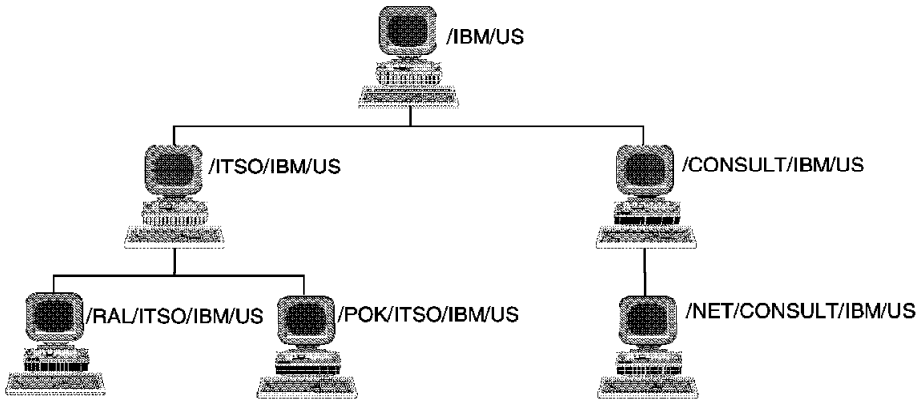


Figure 6. Hierarchical Domain

Cross-Certificates To gain access to servers in other hierarchical domains, the domains have to exchange their certificates. To exchange their certificates, they have to cross-certify. The cross-certificates will be stored in the public Name & Addressbook of a domain.

1.6.6.3 Non-Hierarchical Domains

The non-hierarchical or flat certificates are supported in Lotus Notes since the first release and still exist in the newest version. Non-hierarchical certificates are issued by a single certifier. To communicate, all servers and clients must be certified by the same non-hierarchical certifier, that trusts all clients and servers with the same certificate. To control access certificates can trust or not trust other certificates. If a server trusts other certificates, all clients and servers with the same certificate can access that server. If the server doesn′t trust other certificates, other servers or clients cannot access the server even if they are certified by the same certifier. By default, a certificate trusts other certificates.

For example RALN1ITS and RALN2ITS are certified by the certifier ITSORAL. RALN1ITS trusts and RALN2ITS doesn′t trust other certificates. Then RALN2ITS can access RALN1ITS because they are certified by the same certifier and RALN1ITS trusts other certificates. RALN1ITS can not access RALN2ITS because RALN2ITS doesn′t trust other certificates.

All servers in one organization normally use trusted certificates in order to communicate. To communicate with other organizations, both organizations have to exchange their certificates, which means, they have to stamp the other servers, that they want to allow to access. Therefore they send their server ID to the other domain, which stamps the ID file and sends it back. The other server can then access the server with the new stamp, because they have the same certificates. Normally a server which holds a certificate from another server will not trust other servers with that certificate in order to avoid access from other servers or clients with that certificate.

For example, RALN1ITS from the organization ITSORAL and POKN1ITS from the organization ITSOPOK both hold the certificates ITSORAL and ITSOPOK. RALN1ITS trusts only certificates from ITSORAL and POKN2ITS trusts only certificates from ITSOPOK. RALN1ITS can access POKN1ITS by showing the certificate ITSOPOK. POKN1ITS needs to show the certificate ITSORAL to RALN1ITS in order to communicate. A server that is certified by ITSOPOK and does not hold the certificate ITSORAL cannot access RALN1ITS.

1.6.6.4 Server Access Control

The first step to control access to a server is to check the certificates in the ID file of users or other servers. They must have the same certificates or the same parent certifier as the server that they want to access. Otherwise access is denied.

Additional access control is given by the server access list. The server access list is maintained in the server document in the public Name & Addressbook. It defines the access of users, other servers and groups to a server. Each server of a domain has a server document.

A server document defines the following access rights:

Access server	Who can access the server. If the field is blank, every certified user can access the server.
Not access server	Who is not allowed to access the server.
Create new databases	Who can create databases. If the field is blank, anyone can create databases on the server.
Create replica databases	Who can create replicas. If the field is blank, *no one* can create replicas.

1.6.6.5 Database Access Control

The access to a database by a user or by a server for replication is controlled by the access control list (ACL). Each database has its own ACL. The ACL defines access rights for groups, users or servers. Individual definitions for a server or a user in the ACL always take precedence before group definitions. If a user or server appears in more than one group, the highest access defined for a group is given.

The following access levels are defined in Notes:

No Access	No access to the database.
Depositor	A document can be composed, but can't be read.
Reader	Documents can only be read.

Author	All documents can be read but only be edited by the one who created them.
Editor	All documents can be read and edited regardless of who created them.
Designer	Editor access, plus the ability to change the design of documents and views.
Manager	Designer access, plus management of the database (ALC, replication, etc.).

1.6.6.6 Document and View Access Control

Normally all users who have at least read access to a database can read all documents and select all views of a database. Read access to documents and view can be defined in read access lists.

1.6.6.7 Public and Private Keys

Lotus Notes uses public and private keys for authentication, encryption of information, encryption of network data and for electronic signatures. It is based on the RSA algorithm. The private and the public key are mathematically related. Data encrypted with the public key can only be decrypted with the private key and vice versa.

Every client and every server has a private and a public key. The public key is stored in the public Names & Addressbook and in the ID file. It can be seen and used by everyone. The private key is only stored in the private ID file and can only be used by its owner.

If for example you want to send encrypted mail to another user, you will use the public key of that user to encrypt the mail. Only the receiving user can read your mail because he owns the private key, which is nessary to decrypt notes, encrypted with his public key.

1.6.7 Databases

Lotus Notes uses distributed, shared databases to store information and mail. A Lotus Notes database stores a collection of documents. A document holds the data, that a user entered to a form. A form is the layout of a document and consists of several fields, to which the user enters his data. The documents in a database can be organized by different views. Each view of a database shows different parts of a database. Documents in a view can be categorized and sorted.

A document can contain the following types of objects:

- Text (rich text)
- Graphics
- Sound
- Motion picture images
- Buttons (to run macros from within a document)
- Links to other documents
- File-attachments (they can be launched or detached by the reader)

1.6.7.1 Replication

Databases can be stored on multiple servers or locally on clients. Users work on their local databases or use the databases, stored on a server, which they are allowed to access. In order to exchange all the changes made to a database that is used by different servers and clients, Lotus Notes uses database replication to update the databases. Replication allows users to work on databases distributed all over the world without worrying about how the information will reach other users working on the same database stored on another server. The servers will connect at a scheduled time, to exchange new information stored in the databases. A replication ID is used to verify if a databases is a replica of a database on another server. Replication uses the principle of push and pull to exchange new information. Server-to-server replication is different than client-to-server replication. In the case of server-to-server replication each server pulls new information from the other server. In the client-to-server replication, only the client is the active part, who pulls new information from the server and pushes changes from his local database to the server.

1.6.7.2 Accessing Other Database′s Systems

By integrating Notes object store with the organization′s other databases, Notes enhances the overall value of the organization′s information assets. Lotus and its business partners have developed a variety of integration techniques and products that allow application developers to leverage the power of both Lotus Notes and relational databases (RDBMSs).

Integration products and technologies that application developers use to leverage Notes and RDBMSs include:

- Access to DBMSs from Notes. Lotus Data Access Tools and Notes @DB functions allow the application developer to look up values stored in DBMS tables and use those values to compute field values in a Notes document.
- Access to RDBMSs from Notes gives developers the opportunity to generate keyword lists, perform lookup operations, launch stored procedures and queries stored in external databases, disseminate RDBMS reports and query results, and capture and store RDBMS data in Notes databases.
- Lotus DataLens allows application developers to lookup values stored in DBMS tables. DataLense provides a driver manager and database-specific drivers that support access to these databases on the following plattforms:
  - Windows: dBase, ODBC bridgw, Paradox, DB2/2, Informix, Microsoft SQL Server, Sybase and Oracle
  - OS/2: dBase, DB2/2, Microsoft SQL Server, Sybase and Oracle
  - UNIX, Solaris 1.1: Informix, Sybase, Oracle
- Access to Notes from ODBC-compliant products. NotesSQL is the Lotus Notes ODBC driver for Windows. It enables users of ODBC-compliant desktop applications to access, query, and report on Notes-based information.
- Background/Agent Migration. Notes/RDBMS integration can selectively move data and metadata between different database systems on an event-driven or scheduled basis. Such applications transform the data en-route according to instructions that are scriptable and provide access to multiple data sources, including RDBMSs and Notes databases.
- API-Level Integration. Notes/RDBMS server integration can also be affected by uniting the Notes API with the RDBMS′s APIs in a C application program.

Developers can create triggers, general event management and remote procedure calls in the DBMS and combine them with Notes to handle real-time, single-transaction-at-a-time processing.

- Import/Export Facility. The Notes import/export facility is used for one-time or infrequent copy operations between Notes and other data sources. A user can export all or a selected range of documents from a Notes view into structured text, tabular text or spreadsheet format.

1.6.8 Application Development

Lotus Notes offers the ability to create your own applications in an easy way. A Notes application is a database with all its forms, view and access rights. Applications can be created at every client and used locally for individual purposes or stored on the Notes server for public use.

The following are the major parts of the application development:

Creating Forms Defining the layout of different documents, stored in a Notes database.

Creating Views You can define several views for different documents. Each view of a document shows only a particular part of the database.

Defining Access Right As the developer of an application, you are the manager of that database. As a manager, you are responsible to control access to your database.

Notes knows different options to develop an application. You can develop a new application the scratch, you can simply use Notes Design templates (delivered with Lotus Notes), or you can modify and customize templates for your own purpose.

- **Creating Applications from a Design Template**

  With Notes several design templates are delivered, which support the most common needs of users.

  The following are some important templates:

  - Name and Addressbook
  - Mail
  - Discussion
  - Meeting Tracking
  - Things To Do
  - News
  - Reporting and Status

  To create a new database from a design template, the new database inherits the forms, views and access right from the template. You can create as many databases from one design template for all your different needs. You also have the ability to inherit design changes to the template, which means, whenever the template changes, your database layout will change automatically.

- **Customize Design Templates**

You can change the forms, views and access rights stored in a design template. For example, you can insert new fields, change the field names or add new views to the database, that shows only the data you want to show.

- **Creating Your Own Design Templates / Applications**

  Notes supports you with several functions to create your own design templates. The use of functions and macros to create applications is easy to learn and a graphical user interface simplifies the layout of forms with text, images and data fields. Notes supports different functions for string manipulation, arithmetic, time/date, logic, statistics, database access, lists, and more. Most functions work behind a field of a form. They initialize it with default values, checks the user′s input, calculates values for other fields or look up data in other databases.

  The following are supported field types:

  – Text
  – Number
  – Time/Date
  – Keywords
  – Rich text
  – Names
  – Reader Names
  – Author Names
  – Sections

  A Notes function has the following format: @functionname(value1,value2...).

  To create a new view, the developer has to select the fields of a form that they want to show in a view. A view must not show all documents of a database. With a selection formula only specific documents can be shown. The selection formula may only show documents created with a special form or documents with certain value in one or more fields of a form.

1.6.9 Lotus Notes 4.0

The Lotus Notes Release 4.0 will better enable you to communicate with other users, collaborate in teams and coordinate key business processes. Functions from previous releases will be enhanced or improved, new features will enhance Lotus Notes 4.0. The main focus of Release 4.0 is around the task of building applications that are powerful, easy to use and maintain, secure, and mobile.

Lotus Notes 4.0 will provide the following new features or enhancements:

- The graphical user interface (GUI) will be improved and make it easier for end users to use their Lotus Notes system.
- The mobile capabilities of Notes have been enhanced and are easier to use. The back-end performance has been improved and will save time and expense for the mobile user. Notes today allows bi-directional synchronization of databases. Notes Release 4.0 builds on this model with an expanded focus on laptop tools. For example, users can preset their systems to selectively extract information for use on the road. This could include such information as key portions of Notes databases, the latest mail message, the appropriate modem dialing rules or pre-fixes.

- Lotus Notes 4.0 offers an enhanced development environment for technical, advanced and novice Notes users and developers through supporting LotusScript. Main enhancements are:
  - New macro functions
  - Programmable actions
  - Navigators
  - Point and click design
  - Agent builder
- Additional performance, administrative, scalability and security capabilities to manage Lotus Notes.
- It provides a mail-user interface, based on cc@colon.Mail, to the Notes′ client/server mail system. Notes will support industry standard ″back-end″ message transfer agents (MTAs) such as X.400 and SMTP.
- Notes users will be able to browse the World Wide Web on the Internet and seamlessly incorporate Web documents into Notes documents using the Notes Web Navigator on the client in conjunction with the Notes Web Server. All the power of Notes (security, mobility, rich text, replication, etc) can be extended to the Web.
- Lotus Notes 4.0 will be available for:
  - Mac Client for PowerPC and 68000
  - Windows 3.1 16-bit Client
  - Windows 95 32-bit Client and Server
  - WindowsNT 32-bit Server
  - OS/2 32-bit Client and Server
  - UNIX HP-UX Client and Server
  - UNIX Solaris 2.X SPARC Client and Server
  - IBM AIX Client and Server

  The Windows 16-bit Server is not supported in Release 4.0. It is replaced by the Windows95 Server.
- Protocols supported by the Notes Server:
  - NetBIOS
  - SPX/IPX
  - TCP/IP
  - Banyan Vines
  - AppleTalk

1.6.10 Additional Products for Lotus Notes

Lotus offers a lot of additional products to enhance the capabilities of your Lotus Notes system and network. Lotus also has services to connect your Notes server and clients.

1.6.10.1 Lotus NotesPump

NotesPump is a server-based data transfer engine that enables scalable, high-bandwidth exchange of data between Lotus Notes and relational database management systems (RDBMSs). Through the use of advanced database and server technology, Lotus NotesPump reaches new levels of performance, scheduling flexibility, enterprise scalability, and management capabilities. Using Lotus NotesPump, developers, database administrators and information technology professionals can schedule and execute dependable, scalable, and secure exchanges of data between Lotus Notes and a variety of RDBMSs. The advanced database and interchange capabilities in Lotus NotesPump allow IT professionals to deliver corporate data and store information to Lotus Notes users faster, easier and in a more timely manner.

1.6.10.2 Lotus Notes HiTest

Notes HiTest development tools enable rapid development of applications that expand and extend Notes. Notes tools provide the following:

- Access to the secure, replicated Notes data-store from Visual Basic and VBA.
- A high-level, object-based C language API for Lotus Notes.
- A common language for cross-application scripting in Lotus products.

Notes HiTest Tools for Visual Basic is a set of development tools that offers Notes capabilities to developers using Visual Basic. Lotus Notes HiTest consists of the Notes HiTest Visual Controls (12 Visual Basic custom controls) and the Notes HiTest BASIC API.

Notes HiTest C API is a high-level object-based C API for Lotus Notes. Developers can programmatically take advantage of familiar Notes UI objects through this powerful C interface to Notes.

LotusScript is a powerful, full-featured, object-oriented derivative of BASIC. LotusScript enables customization, automation, and integration of Lotus Products, with each other and with other OLE-enabled applications.

1.6.10.3 Lotus Phone Notes

Lotus Phone Notes allows telephone users to access, create, update and forward Notes documents, and allows developers to create interactive voice response applications that access Notes data and all of the messaging, workflow and applications development facilities of Lotus Notes. Phone Notes applications include customer support help desks and surveys, sales support systems, event registration, faxback, and order processing inquiry systems.

1.6.10.4 Lotus Phone Notes Mobile Mail

Lotus Phone Notes Mobile Mail is a complete Phone Notes application which enables remote Notes users to access and manage their Notes Mail from any touchtone telephone. Users can access, create, forward, fax and edit NotesMail documents, embed voice messages in documents, play and record voice messages, and use text-to-speech technology to play the information from NotesMail. Telephony software and voice-processing boards are included.

1.6.10.5 Lotus Notes: Document Imaging (LN:DI)

Lotus Notes: Document Imaging (LN:DI) is a family of add-on products for integrating images into Notes applications. The product family includes a Windows client (image capture, display and manipulation), an OS/2-based storage server (hierarchical storage management), and an optical character recognition (OCR) server. LN:DI also works with the Lotus fax server for both Notes and cc:Mail.

1.6.10.6 Lotus VideoNotes

Lotus VideoNotes efficiently incorporates digital video into Notes documents.

1.6.10.7 Lotus Notes Pager Gateway

The Lotus Notes Pager Gateway enables you to send urgent messages quickly and easily from Lotus Notes or Notes Express to a pager. In just minutes, the message is displayed on the recipient's pager. There's no need to buy additional desktop paging software to send pager messages. All you need is Notes or Notes Express and the Notes Pager Gateway.

1.6.10.8 Lotus NotesView

Lotus NotesView is a real-time, graphical management package that enables you to monitor and control your entire Notes enterprise. From a single management station, you can monitor and control Notes servers using industry-standard management tools and gain real-time access to Notes network information. With NotesView, complete, up-to-the-minute status of any server is possible.

NotesView automatically creates multiple map views of a your Notes network topology. For example, you can create maps of the replication paths to and from a server or of the mail routing topology. The color-coded graphical display alerts you to changes in the state of a Notes server. Or, as soon as a change occurs, NotesView can notify you via Notes Mail or even a pager message. This management application lets you respond swiftly to avert problems before they affect critical applications or users.

You can also use NotesView to collect historical data and chart the health of servers over time and under different uses. It's easy to troubleshoot, analyze performance trends and plan for enhancements to optimize your Notes environment and maintain predictable service levels for every Notes user.

NotesView makes use of industry-standard network management protocols, platforms and conventions, thereby reducing the overall cost of managing the Notes network.

1.6.10.9 InterNotes Web Publisher

InterNotes Web Publisher automates the process of publishing information to the World Wide Web (WWW), by converting Notes documents, forms, views, and attachments into HTML. InterNotes Web Publisher leverages the power of Notes to coordinate and collect Web information from many sources throughout your organization, then translates the documents and views into a series of HTML pages.

1.6.11 Services

Lotus offers network services to its customers to provide them with news, product and business information and give them the ability to communicate with other users or to access foreign databases.

1.6.11.1 LNN (Lotus Notes Network)

Up to 1.5 million Notes users have the potential to exchange information, send and receive E-mail and work together via the LNN. You can share data with Lotus business partners and other Notes users and can get a quick and easy answer to a business problem. You have the ability to receive third-party public and private databases and get proprietary information direct from Lotus in your standard Notes format. Workgroups can be created that exist on different parts of the world, and let you work together with your associates in the worldwide Lotus Notes community.

With the Lotus Notes Network, you can share information and work together, without enrollment fees, monthly minimums, long-distance charges for connect time, or the hidden telecommunications costs that are associated with many public online services.

1.6.11.2 Lotus Notes: Newsstand

Lotus Notes:Newsstand is a service being offered initially to subscribers of the Lotus Notes Network (LNN), and on other Notes-based networks in the future. Through the Newsstand, LNN will offer a growing number of publications tailored specifically for Lotus Notes.

You might think of Lotus Notes:Newsstand as an electronic corner news kiosk right on your desktop, where you can look for and subscribe to publications in the Lotus Notes format. You can browse the content of a publication, or you can use Notes′ powerful search and indexing capabilities to gather, annotate, and reuse the information (according to the agreement with the information provider).

Chapter 2. LAN Management

The purpose of this chapter is to provide a guideline for helping customers make the right choice(s) for a distributed management platform(s).

Customer systems and networks grow in size and complexity each day and there are several ways to provide the network and systems management for the enterprise. In addition to the growing complexity, there has been escalating growth of distributed systems which require a degree of distributed systems and network management capability. This chapter will hopefully give the reader some understanding of what platform and applications should be used for specific customers. It must be said that most customers will probably require more than one platform because they wish a split between distributed and centralized management or they have a wide variety of managed resources. Systems and networks have so many options now and in the future that it will be rare to see a situation where one platform and a series of applications could handle the enterprise management needs of the customer.

2.1 Systems and Network Management

The following topics will describe the basic points of systems and network management. The topics will also define terms related to management.

2.1.1 System Management Concepts

The concept of a manager/client division of work is fundamental in the distributed systems management industry. These definitions stated very simply follow:

- **Manager**

  A manager (also called managing system) is responsible for the management of other systems.

- **Client**

  A client (also called agent or managed system) is responsible for providing information about itself to the managing system.

Managing system components are:

- End-user interface or automated operator

  The manager has (optionally) a user interface to display information gathered by the management applications. If an operator is not available or not required, automation can be used to analyze the data collected and act on anticipated events. A manager could, in turn, be a managed system from another manager. Thus, information gathered at one manager could be forwarded to another in either a hierarchical or peer relationship.

- Management process application

  A manager contains some managing process. This is an application that contains the logic and commands to process the management data received from the agents.

Clients contain agents that provide a linkage between the objects to be managed and the transport to the manager.

Agents respond to commands from the manager and collect requested data concerning the managed device. Agents can respond to commands from the manager or send unsolicited information to the manager if conditions arise that dictate such an action.

Management information about a resource includes status, characteristics, and data about some specific aspect of a managed device. This information can be hardware or software information. The information is stored in a management information base (MIB). The following are some examples of information:

- Name of user for the system
- Status of software (running/not running)
- Number of jobs in the print queue
- Amount of memory on a system
- Amount of memory in use
- Names of users logged on to a server

To communicate, the agent and manager use a specific protocol, or language, called the simple network management protocol (SNMP). SNMP was created to manage the Internet network funded by the United States Government with links to networks throughout the world. The Internet is the largest network in the world with thousands of attached networks and millions of attached devices. The devices include personal computers, mainframes, servers, and network equipment such as routers and hubs.

- Transport protocol

  In addition to a management protocol (the language) there must be a protocol for communication. The transport can be in the same device (cross memory, for example), local (across a LAN or channel), or remote (across a wide area network). If the management protocol is the language for communications, then the transport protocol is the medium for communications. As we speak, the medium is the air through which sound travels. Or, the medium could be the telephone wires when we speak over the telephone.

  Ideally, the management protocol should be able to use any transport protocol that you have. That is, as long as we are speaking the same language, it should not matter whether we are speaking in a room together, over phone wires, over a LAN using IBM′s Person-to-Person product, over radio, or any other media.

- Two way

  Another key aspect to the management protocol is the requirement for it to be a two-way method of communication. The agent should be able to notify the manager of critical conditions, and the manager should be able to send commands to the agent.

A client is managed by a manager. Clients contain agents which respond to commands from the manager and send the requested management information.

2.1.2 What Is RMON?

Remote Network Monitoring (RMON) is ″An implementation of remote performance monitoring of token-ring and Ethernet LAN segments through smart agents. Each agent gathers and analyzes data from every frame passed in the segment. Agents can be remotely configured by a manager to set thresholds and report SNMP traps.″

RMON is defined by a set of MIBs defined in IETF standards RFC 1271 (which has been superceded by RFC 1757) and RFC 1513. The 1271/1757 MIBs were specifically developed for the reporting of performance on remote Ethernet segments, but there are groups with the MIBs that are relevant to LANs regardless of media type. RFC 1513 is an extension of the other 2 MIBs which adds groups that are specific to token-ring segments.

RFC 1271 defined 9 major groups of information. RFC 1757 further divided these groups into 10 groups. RFC 1513 uses some of the groups from 1271 and added others; bringing the total major groups count to 10 (or 11 if you start with 1757). The main point to all this is that by definition an ″RMON-compliant″ agent or manager only has to support a ″subgroup″ of information within one major group. Making a network management decision involving RMON agents or managers means understanding RMON in much more detail than knowing it's a ″good thing do to″.

The goals set forth by the vendors who started the RMON initiative include the following:

- Offline Operation

  An RMON agent is a non-interactive monitor sitting on a LAN segment. It reads and copies each frame on its local LAN, updating counters based on the contents of the frame. In general this information is saved at the agent until a remote managing station requests that it be sent. The managing station is not actively involved in the data collection until problem analysis is needed.

- Preemptive Monitoring

  By capturing (and filing) LAN performance across a period of time, an RMON management application can do comparisons to current traffic versus previous patterns. Using this technique a sudden change in network traffic can be detected before a problem becomes critical to operations.

- Problem Detection and Reporting

  If the agent is configured to recognize thresholds exceeded, and to generate SNMP traps when these events occur, SNMP managers can be notified quickly of problems. Additional information from the RMON MIBs can be used to further qualify the fault area within the segment.

- Value Added Data

  The RMON MIBs, especially for token-ring LANs, can carry detailed information such as NAUN order of the token-ring adapters on the segment, or the source and destination MAC addresses of the stations with the most network traffic. RMON managers can exploit this information to help isolate causes of performance problems.

- Multiple Managers

A single RMON agent can support several remote RMON managers. A table is maintained within the agent of what information (and at what intervals) information is to be sent to specific IP addresses. This is done through the ″alarm and event″ groups within RMON MIBs. Other information is routinely collected by the agent, captured in memory, and reported within Get Responses to a remote SNMP manager.

RMON is widely recognized as a multivendor supported tool for the remote monitor of LAN health and performance. RMON management applications, however, are passive managers dependent on other device management applications to provide change and control operations.

2.2 Where Do I Start?

The process of selecting a management platform can be difficult. To make this process easier, consider the following three items:

- Hardware/software platform
- Resources you want to manage
- Management protocols supported by the different platforms

2.2.1 Platforms

- S/390 - MVS/ESA
- RISC System/6000 - AIX
- Intel-based workstations - OS/2
- Intel-based workstations - Windows

2.2.2 Resource Types

- Network devices (for example, bridges, routers, hubs)
- LAN media (for example, token-ring, Ethernet, FDDI and ATM)
- Operating systems (for example, OS/2, AIX/UNIX, DOS-Windows, DEC)
- LAN Operating systems (for example, LAN Server, Novell NetWare)
- Subsystems (for example, Communications Manager, Database Manager)
- Communications protocols (for example, SNA, TCP/IP, 802.2, and IPX)

2.2.3 Management Protocols

- CMIP
- SNMP
- SNA/MS
- Token-ring
- Private, such as Novell′s NMS NLM

SNMP and CMIP are two of the most common management protocols used in LAN management. It is helpful to understand the basics of these two management protocols to assist in making a decision. A basic description of these two protocols is in Chapter 4 of *Local Area Network Concepts and Products: LAN Architecture*, SG24-4753.

2.3 MVS LAN Management

In the following sections, these IBM LAN management products for the MVS platform are discussed:

- NetView for MVS/ESA
- IBM NetView Performance Monitor
- IBM NetView MultiSystem Manager for MVS/ESA

2.4 NetView for MVS/ESA

IBM NetView for MVS/ESA is a key part of the SystemView program for managing networks and systems through automation. NetView for MVS/ESA is a comprehensive network management solution that lets you monitor your client/server devices on Transmission Control Protocol/Internet Protocol (TCP/IP) networks.

IBM NetView for MVS/ESA will benefit users that need central management capability for their entire I/T business. NetView for MVS/ESA provides the only systems management server capable of managing thousands of multivendor resources. It provides easy to use graphics and administration facilities to help you create a client/server environment that boosts productivity for your help desk and operations staff.

- Manage TCP/IP, token-ring, Novell, and LAN Management Utilities (LMU) managed workstations using MultiSystem Manager, AS/400s (using NetView ROM)
- Manage Systems Network Architecture (SNA) subarea and Advanced Peer-to-Peer Networking (APPN) resources with NetView′s connections to VTAM
- Manage your multivendor networking system with dynamically built graphical displays showing status and topology information
- Configuration, fault, and performance management functions
- Network and system management tool that provides distributed and centralized management of your entire world-wide enterprise

Some of the function and benefits derived from installation of IBM Netview for MVS/ESA might include:

- Management of heterogeneous, multivendor networks; virtually any device managed through a NetView service point
- Resources stored as objects in a high-speed data cache
- Dynamic discovery and automatic correlation of workstation protocols including TCP/IP, APPN, IPX, token-ring and NetBIOS
- Integrated performance data using NetView Performance Monitor

2.4.1 Minimum Requirements for Management System

NetView for MVS/ESA runs in a virtual storage environment on any System/370 or System/390 processor or configuration with sufficient storage that supports the corresponding system environment.

2.5 IBM NetView Performance Monitor

This integrated package of powerful facilities allows you to manage the performance and growth of VTAM-based communication networks. It monitors resources such as CPU, available RAM, hard disk usage, and more to give you an accurate view of system status.

NetView Performance Monitor (NPM) provides the necessary information associated with a customer′s communications network that is needed for performance management, network accounting and problem determination. Customers using NetView, ACF/VTAM, ACF/NCP, LAN Manager, LAN Network Manager and NetWare can realize the benefits of managing the performance of their networks using NPM.

- Real-time monitor graphics and historical analysis of session data
- Records comprehensive data about resource utilization to log files
- Alerts are sent to NetView based on thresholds set for NetWare resources being monitored

Additional functions and benefits of IBM Netview Performance Monitor would include the following:

- Extends the innovative concept in performance management of the easy-to-use NPM Desk/2 graphical user interface with the new NetWare resources data collection
- Enhances the synergy among NetView Graphic Monitor Facility (NGMF), NetView MultiSystem Manager and NPM for NetWare resources
- Supports the OEM multisession manager TPX (Terminal Productivity Executive)

2.5.1 Minimum Requirements for Management System

Hardware:

- Any processor that supports MVS/ESA (MVS/SP V.3, V.4, or V.5) for MVS/Enterprise System Architecture or VM/ESA (VM/Enterprise System Architecture) Version 1
- An IBM 3270 display with 32 rows or a 3290 terminal operating as a systems network architecture (SNA) logical unit (LU) type 0 or type 2.

Software:

- ACF/VTAM V.3 R.4 or later for MVS/ESA, or for VM/ESA
- For NetWare resource data collection: NetWare 3.11 and Netware for SAA 1.3b or NetWare Management Agent for NetView

2.6 IBM NetView MultiSystem Manager for MVS/ESA

MultiSystem Manager (MSM) is a powerful tool that simplifies the task of network management by harnessing the power of NetView for MVS/ESA to centrally manage your network resources. MultiSystem Manager is a NetView application that consists of a base feature and separately-orderable topology features for each type of network you want to manage.

The MultiSystem Manager base feature contains the following components:

- A topology manager (common services)
- Messages
- Help panels
- Installation samples
- Data model parts
- Supplemental tools and utilities

MultiSystem Manager features enable you to manage the following types of networks:

- IBM OS/2 LAN Network Manager (LNM) networks
- Novell NetWare networks
- IBM LAN NetView Management Utilities (LMU) networks
- TCP/IP networks managed by IBM NetView for AIX
- Any network supported by MultiSystem Manager open topology agents

The following five sections contain an overview of each one of the features listed above.

2.6.1 MultiSystem Manager Open Topology Interface Feature

The MultiSystem Manager open topology interface feature (hereafter referred to as the open topology feature) uses application programs, called topology agents that have been developed using the open topology application programming interface (API) to manage your networks. You can use MultiSystem Manager and the open topology feature to either create your own topology agents or use vendor-supplied topology agents.

Creating Your Own Topology Agents: You can use the MultiSystem Manager open topology feature to create your own topology agents to manage a wide range of diverse network resources; resources not managed by other MultiSystem Manager topology features. For information on how to create your own open topology agents, refer to *NetView MultiSystem Manager MVS/ESA V2R1 Open Topology Interface*, ST00-9535.

You can also create topology agents that reside on the NetView host. These agents can use REXX routines to manage their resources.

Using Vendor-Supplied Topology Agents: Vendor-supplied open topology agents work with the MultiSystem Manager open topology interface to extend your network management.

The open topology feature contains the following:

- Topology manager extensions
- Command support
- Installation samples

2.6.1.1 MultiSystem Manager/Open Topology Feature Benefits

MultiSystem Manager provides an integrated and centralized network management facility that enables you to manage your diverse network resources from a NetView Graphic Monitor Facility (NGMF) workstation.

Using the MultSystem Manager Open topology feature, Multisystem Manager enables you to directly access the NetView resource object data manager (RODM). You can store your own information into RODM, as well as, access information stored in RODM by others.

To help you manage your networks, MultiSystem Manager provides the following benefits:

- Dynamic topology and status discovery of your networks
- Instant access to graphic views of the topology and status of your networks, all from a single NGMF workstation
- Quick notification of any changes in the topology and status
- The ability to send commands to network resources simply by selecting the resource in an NGMF view and then selecting the command from a pull-down window
- The ability to integrate the management of various types of networks SNA, and non-SNA networks
- The ability to access the Information/Management database from MultiSystem Manager resources displayed in your NGMF views by means of NGMF Inventory/Problem Management functions

2.6.1.2 How MultiSystem Manager Communicates with Your Distributed Networks

Figure 7 on page 77 shows how MultiSystem Manager fits into your network environment. MultiSystem Manager uses a manager-agent relationship to manage network resources. This relationship consists of a topology manager and a topology agent. MultiSystem Manager provides a topology manager, which runs on the NetView host. You, or an agent supplier, provides a topology agent that resides in your network. This topology agent manages the resources in its network. You can design your network to have multiple topology agents, each managing a part of your network resources, or you can have a single topology agent manage all your resources.

The topology manager uses NetView RUNCMD commands over SNA sessions to communicate with the topology agents. The MultiSystem Manager Open topology feature supports LU 6.2 sessions and same-domain SSCP-PU sessions. Cross-domain SSCP-PU sessions are not supported.

Topology agents use message to operators (MTOs) and RUNCMD responses to communicate with MultiSystem Manager. MTOs are received by the NetView automation table and forwarded to MultiSystem Manager. Figure 8 on page 78 shows how MultiSystem Manager communicates with the topology agents.

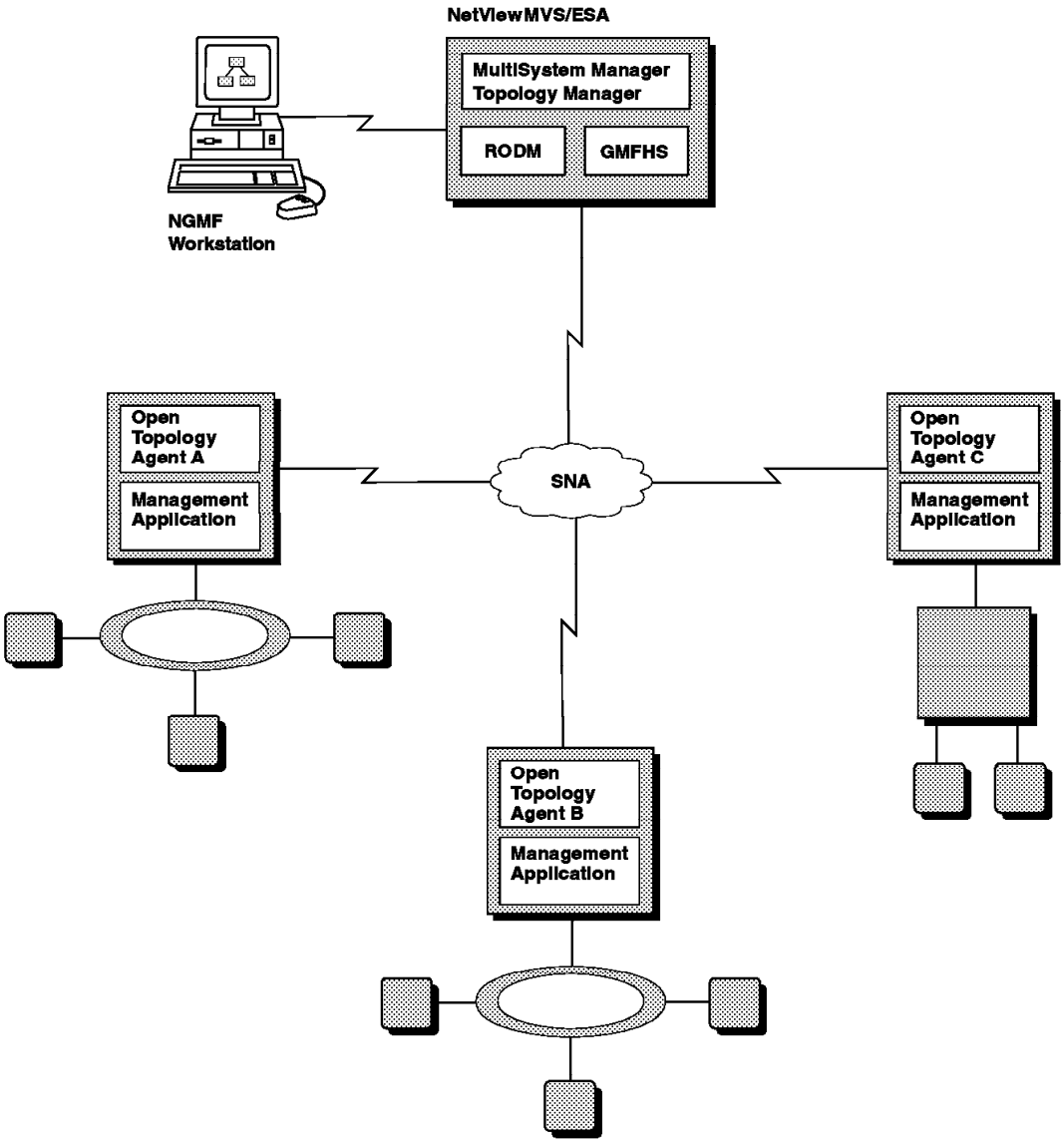


Figure 7. MultiSystem Manager Open Environment

2.6.1.3 The Role of the Topology Agents

The role of a topology agent is to manage its network resources and to dynamically communicate information about changes in network topology or resource status to the topology manager.

When the topology manager issues a command to gather topology and status, the topology agent collects the information and sends it back as part of the command's response.

When a topology agent wants to inform the topology manager of a topology or status change, the agent sends a message to operator (MTO) indicating that an event has occurred.

The topology manager updates the status of the resource in RODM and reflects this status change in your NGMF views.

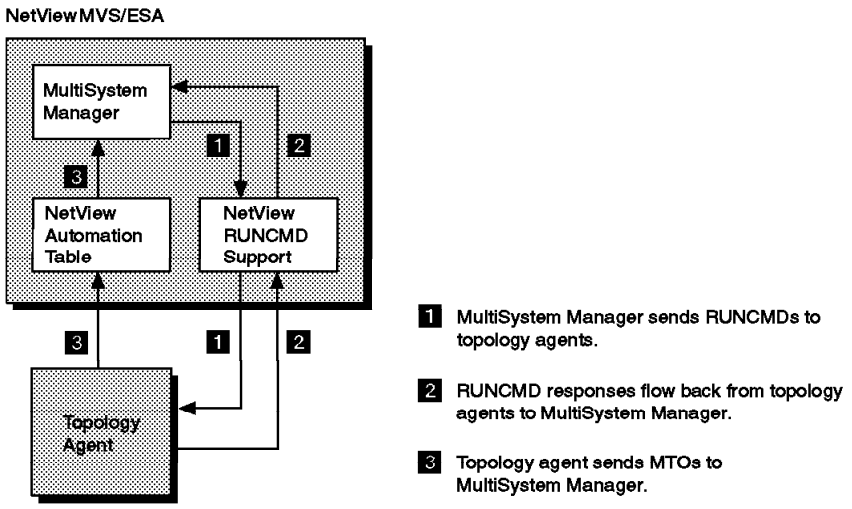


Figure 8. Communication Between MultiSystem Manager and Topology Agents

2.6.1.4 The Role of the MultiSystem Manager Topology Manager

To help monitor and manage your networks, the MultiSystem Manager topology manager performs three primary tasks:

- Dynamically discovers the topology and status of the network and stores it in RODM
- Automatically processes the topology and status updates from the topology agents
- Provides an easy-to-use command interface

2.6.1.5 Dynamic Topology Discovery

The MultiSystem Manager topology manager begins the process of managing your networks by dynamically discovering the initial topology and status of the resources in your network and then storing this information in RODM. After the information is in RODM, you can view your network resources from your NGMF workstation. Figure 9 on page 79 shows an example of the types of views you can create with MultiSystem Manager.

2.6.1.6 Automatic Topology and Status Updates

After MultiSystem Manager is initialized and the network's initial topology and status is stored in RODM, the topology manager keeps topology and status up-to-date by receiving updates from the topology agents.

2.6.1.7 Easy-to-Use Command Interface

MultiSystem Manager provides an easy-to-use command interface, called distributed manager command support (DMCS), that enables you to send commands to the topology agents. You can build your own command sets that reflect the commands issued by management applications (as shown in Figure 7 on page 77) and store these commands on the NGMF workstation. DMCS automatically retrieves RODM information that is required to send the command. You can use DMCS in an automation routine, from the NetView operator command line, or from the NGMF workstation.

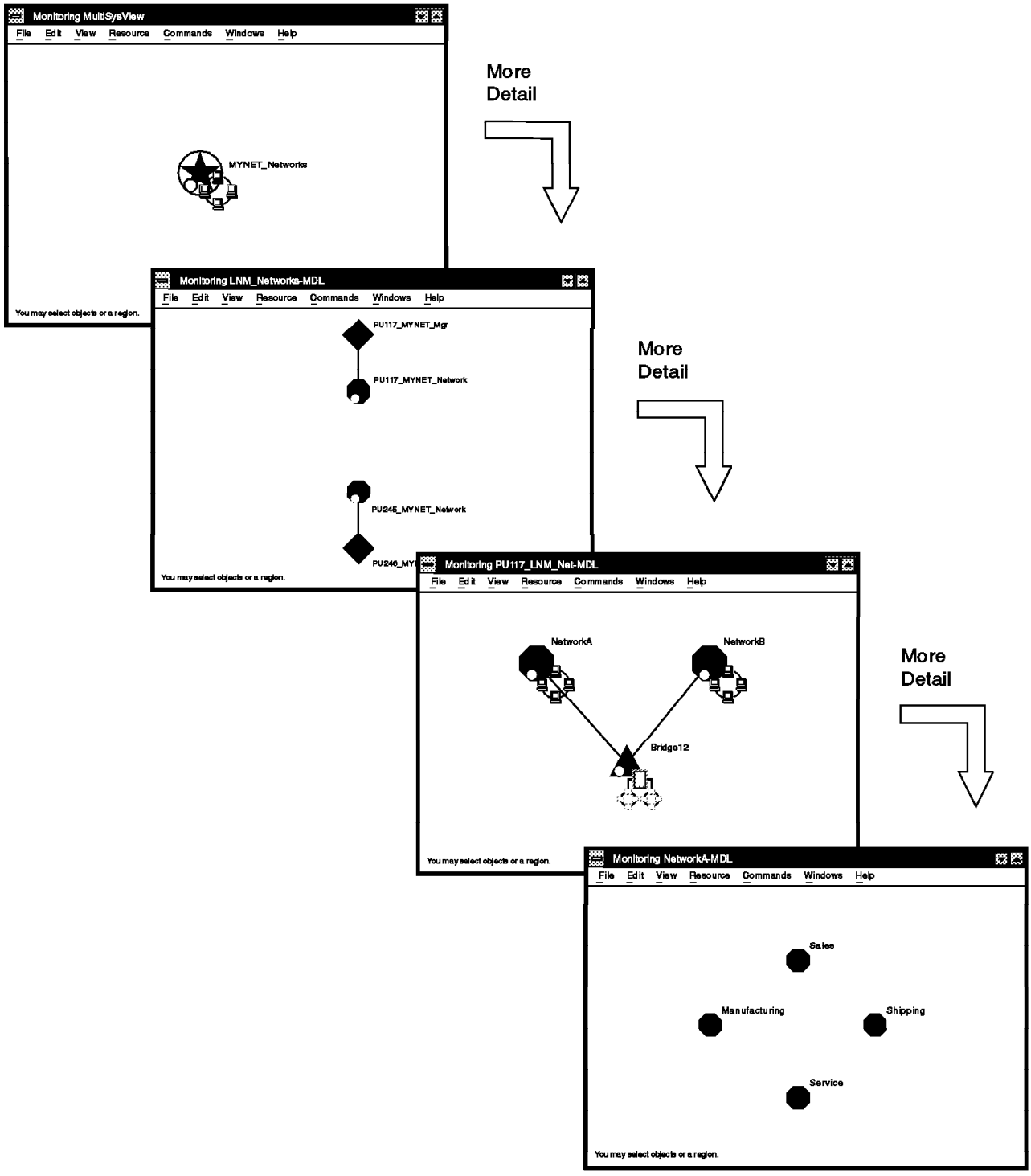


Figure 9. An Example of Open Views

2.6.1.8 Inventory/Problem Management (IPM) Support

The Inventory/Problem Management (IPM) component of NetView for MVS provides support for access to Information/Management database records from NGMF. Using the NGMF Inventory command exit, you can display inventory information stored in Information/Management. The NGMF Problem Management function allows you to list, display, update, and add problem records. MultiSystem Manager provides sample alias tables and customization files that enable the basic IPM functions for the default IPM program interface data tables (PIDTs). These samples are provided as a working example of the customization required to fully exploit IPM. You need to modify the samples so IPM will work with your existing Information/Management records. Refer to the *NetView for MVS V3R1 Graphic Monitor Facility User's Guide*, SC31-8095 and the *NetView for MVS V3R1 Customization Guide*, SC31-8052 for more information about using Inventory/Problem Management.

2.6.1.9 Creating Views

Your vendor-supplied topology agent defines the basic structure and contents of your views, but you can customize these views to better meet your specific network management needs.

You can monitor your network from a single NGMF view, or you can create multiple NGMF views, perhaps each view reflecting a different grouping of your resources.

You can also integrate your MultiSystem Manager networks with other network views. For example, if you have an SNA network view, you can add your MultiSystem Manager networks to that view.

MultiSystem Manager also provides a View Customization utility, called BLDVIEWS, which enables you to create your own views.

2.6.1.10 Resolving Network Problems

You can use NGMF menus and facilities to navigate between views and to locate failing resources. Once the failing resource is located, you can simply select the object on your view and send a command to resolve the problem.

2.6.1.11 Automating Network Management

You can use MultiSystem Manager to automate many network management procedures. In general, there are two types of automation: NetView-based automation and RODM-based automation.

2.6.1.12 NetView-Based Automation

This type of automation is based on user-written applications that react to information received by NetView from the topology agents. MultiSystem Manager adds statements to the NetView automation table to capture alerts, resolutions, and message-to-operators (MTOs) and react to them. You too can add statements to the NetView automation table thus allowing you to receive updates from the topology agents.

2.6.1.13 RODM-Based Automation

This type of automation is based on user-written applications that access information stored in RODM. RODM automation applications can process within RODM, using RODM methods, or externally using MultiSystem Manager Access or the RODM API. You can write automation applications that react to status changes made by MultiSystem Manager alert processing. You can also write applications that correlate resources reported upon by different topology managers. These applications can react to problems affecting multiple resources, which might have been reported in multiple alerts.

MultiSystem Manager uses RODM-based automation and the workstation correlate utility to dynamically correlate different managed resources to the same workstation.

2.6.2 MultiSystem Manager/IP Topology Feature

In this section the internet protocol (IP) network management is discussed.

The IP topology feature contains the following:

- Topology manager extensions
- Command support
- Installation samples
- IP topology agent

2.6.2.1 MultiSystem Manager/IP Topology Benefits

MultiSystem Manager IP topology feature provides an integrated and centralized network management facility that enables you to manage your IP networks from a NetView Graphic Monitor Facility (NGMF) workstation.

MultiSystem Manager works with: AIX SystemView NetView/6000 Version 2 or NetView for AIX Version 3 (referred to hereafter as NetView for AIX).

To help you manage your networks, MultiSystem Manager provides the following benefits:

- Dynamic topology and status discovery of your networks
- Instant access to graphic views of the topology and status of your networks, all from a single NGMF workstation
- Quick notification of any changes in the topology and status of your networks, such as:
  - A node went down.
  - A node joined the network.
- The ability to send commands to network resources simply by selecting the resource in an NGMF view and then selecting the command from a pull-down window
- The ability to integrate the management of your IP, SNA, and non-SNA networks
- The ability to access the Information/Management database from MultiSystem Manager resources displayed in your NGMF views by means of NGMF Inventory/Problem Management functions

2.6.2.2 How MultiSystem Manager Communicates with Your IP Networks

Figure 10 on page 83 shows how MultiSystem Manager fits into your network environment. MultiSystem Manager uses a manager-agent relationship to manage IP resources. This relationship consists of a topology manager and a topology agent. MultiSystem Manager provides a topology manager that runs on the NetView host. The MultiSystem Manager IP topology feature supplies an application to run with each NetView for AIX program in your network. This application acts as the topology agent for all the resources managed by that NetView for AIX.

The topology manager uses NetView RUNCMD commands over SNA sessions to communicate with the topology agents. The MultiSystem Manager Internet Protocol topology feature supports only LU 6.2 sessions. SSCP-PU sessions are not supported.

Topology agents use alerts and RUNCMD responses to communicate with MultiSystem Manager. Alerts are received by the NetView automation table and forwarded to MultiSystem Manager. Figure 11 on page 84 shows how MultiSystem Manager communicates with the topology agents.

2.6.2.3 The Role of the Topology Agents

The role of a topology agent is to manage its IP resources and to dynamically communicate information about changes in network topology or resource status to the topology manager.

When the topology manager issues a command to gather topology and status, the topology agent collects the information and sends it back as part of the command's response.

When a topology agent wants to inform the topology manager of a topology or status change, the agent sends an alert indicating that some event has occurred and some action might need to take place as the result of that event.

The topology manager updates the status of the resource in RODM and reflects this status change in your NGMF views. Alerts are then stored in the resource's alert history and can be displayed on your NGMF workstation.

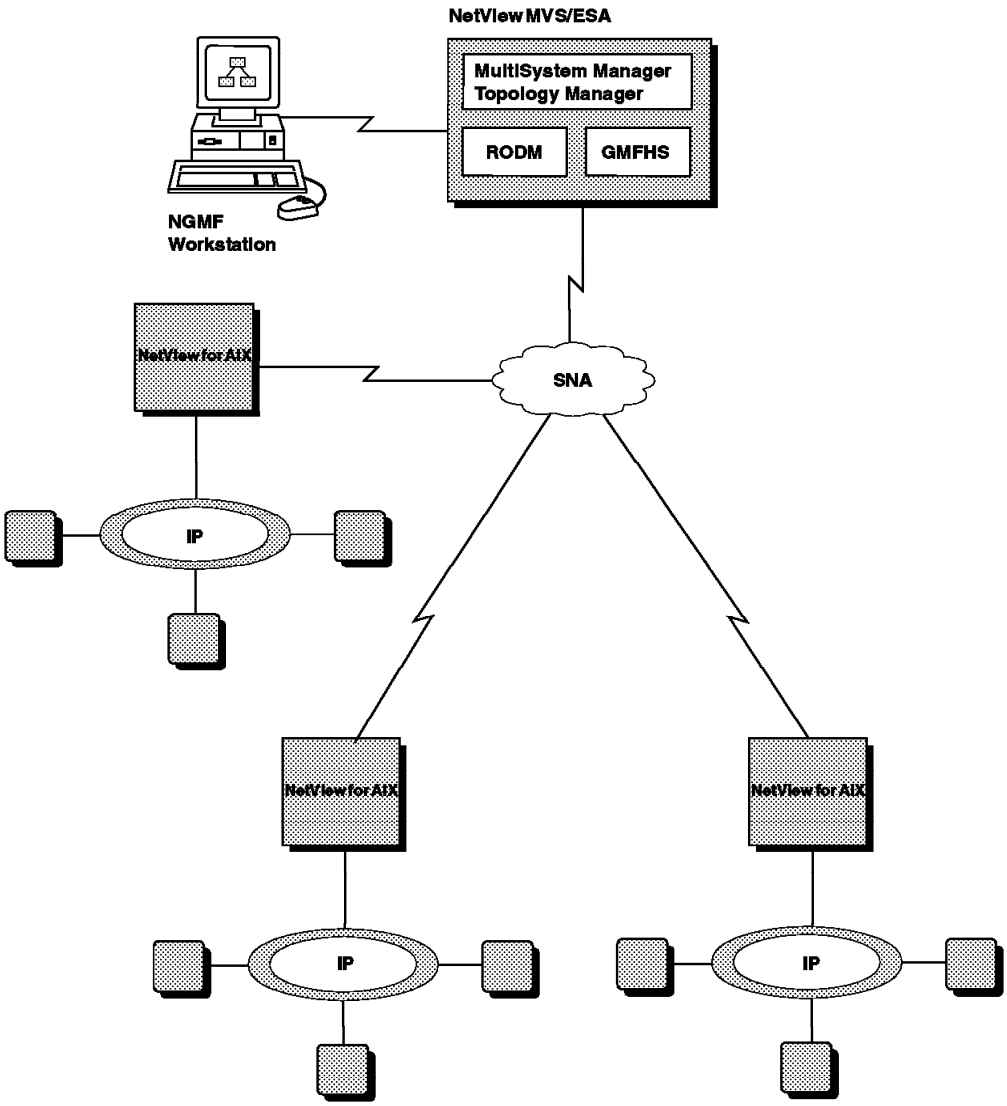


Figure 10. MultiSystem IP Environment

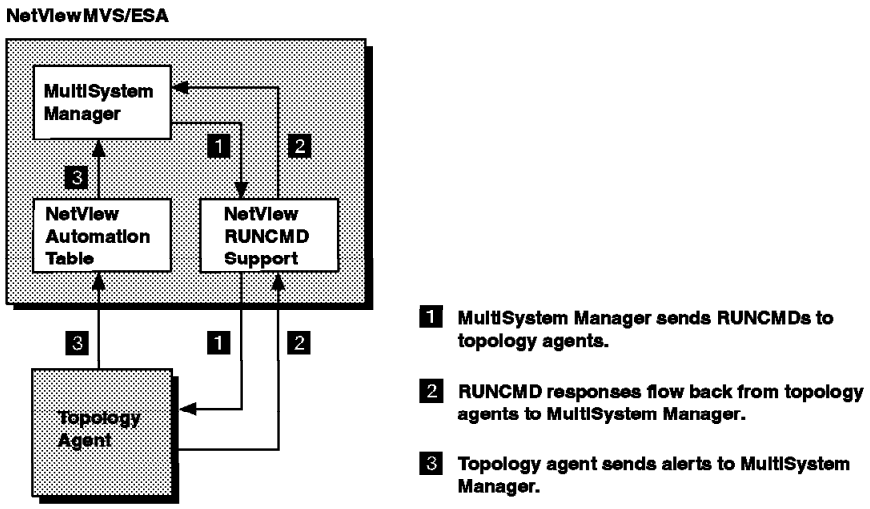


Figure 11. Communication between MSM and Topology Agents

2.6.2.4 The Role of the MultiSystem Manager Topology Manager

To help monitor and manage your networks, the MultiSystem Manager topology manager performs three primary tasks:

- Dynamically discovers the topology and status of the network and stores it in RODM.
- Automatically processes the topology and status updates from the topology agents.
- Provides an easy-to-use command interface.

2.6.2.5 Dynamic Topology Discovery

The MultiSystem Manager topology manager begins the process of managing your networks by dynamically discovering the initial topology and status of the resources in your network and then storing this information in RODM. After the information is in RODM, you can view your network resources from your NGMF workstation. Figure 12 on page 86 shows an example of the types of views created by MultiSystem Manager.

2.6.2.6 Automatic Topology and Status Updates

After MultiSystem Manager is initialized and the network's initial topology and status is stored in RODM, the topology manager keeps topology and status up-to-date by receiving updates from the topology agents. The status changes are reflected in your views and the alerts are stored in the GMFHS alert history file.

2.6.2.7 Easy-to-Use Command Interface

MultiSystem Manager provides an easy-to-use command interface, called distributed manager command support (DMCS), that enables you to send commands to the topology agents. DMCS allows you to issue IP commands from your NGMF workstation. DMCS automatically retrieves RODM information that is required to send the command. You can use DMCS in an automation routine, from the NetView operator command line, or from the NGMF

workstation. Figure 13 on page 87 shows how MultiSystem Manager presents a list of commands on your NGMF workstation.

2.6.2.8 Inventory/Problem Management (IPM) Support

The Inventory/Problem Management (IPM) component of NetView for MVS provides support for access to Information/Management database records from NGMF. Using the NGMF Inventory command exit, you can display inventory information stored in Information/Management. The NGMF Problem Management function allows you to list, display, update, and add problem records.

MultiSystem Manager provides sample alias tables and customization files that enable the basic IPM functions for the default IPM program interface data tables (PIDTs). These samples are provided as a working example of the customization required to fully exploit IPM. You need to modify the samples so IPM will work with your existing Information/Management records. Refer to *NetView for MVS V3R1 Graphic Monitor Facility User's Guide*, SC31-8095 and the *NetView for MVS V3R1 Customization Guide*, SC31-8052 for more information about using Inventory/Problem Management.

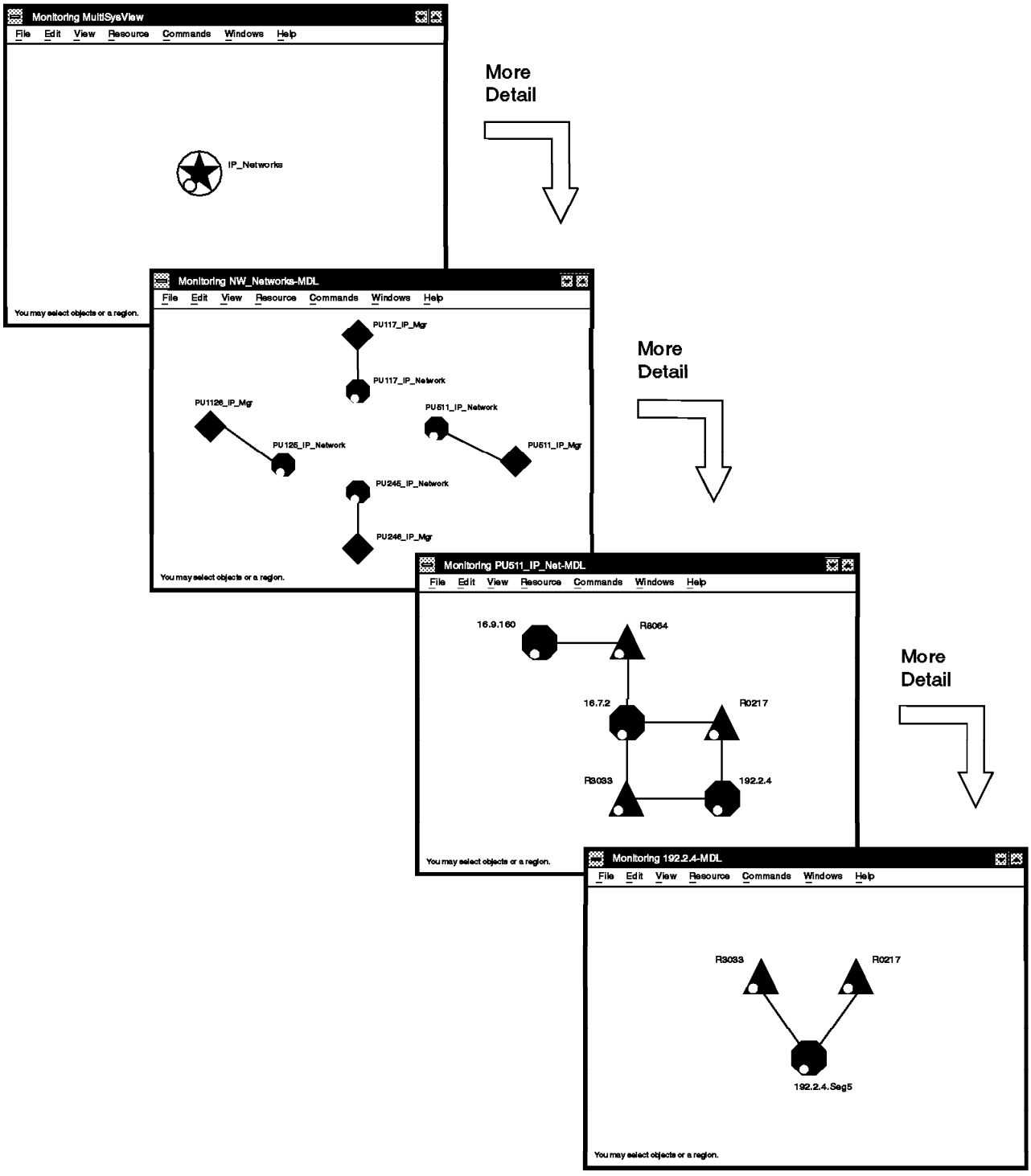


Figure 12. An Example of IP Views

2.6.2.9 Creating Views

MultiSystem Manager dynamically builds views that meet the majority of your network management needs, but you might also want to create unique views.

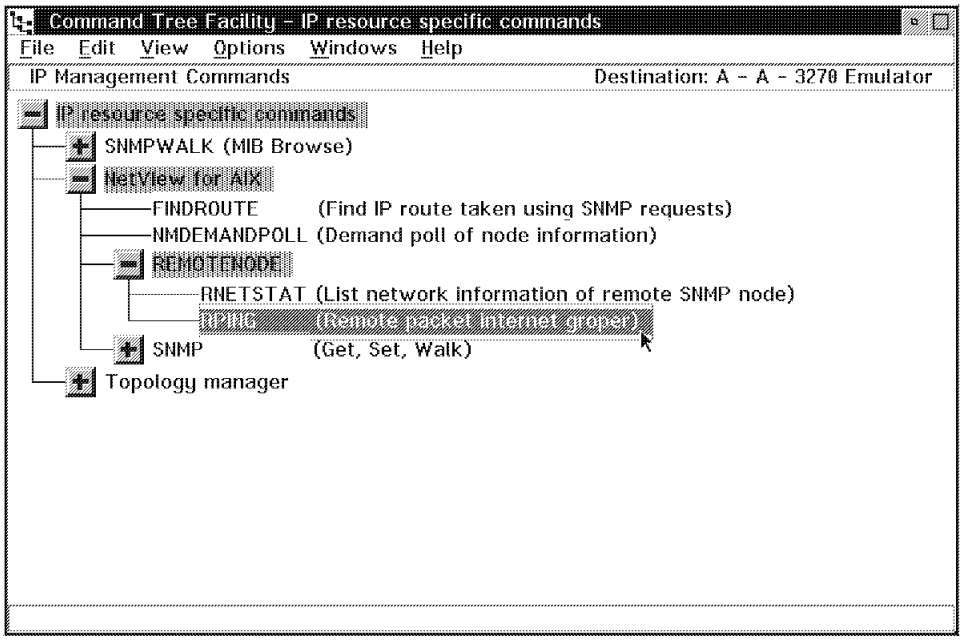


Figure 13. A MultiSystem Manager Command Menu Example

You can monitor your network from a single NGMF view, or you can create multiple NGMF views, perhaps each view reflecting a different grouping of your resources.

You can also integrate your MultiSystem Manager networks with other network views. For example, if you have an SNA network view, you can add your MultiSystem Manager networks to that view.

MultiSystem Manager also provides a View Customization utility, called BLDVIEWS, which enables you to create your own views.

2.6.2.10 Resolving Network Problems

You can use NGMF menus and facilities to navigate between views and to locate failing resources. Once the failing resource is located, you can simply select the object on your view and send a command to resolve the problem.

2.6.2.11 Automating Network Management

You can use MultiSystem Manager to automate many network management procedures. In general, there are two types of automation: NetView-based automation and RODM-based automation.

2.6.2.12 NetView-Based Automation

This type of automation is based on user-written applications that react to information received by NetView from the topology agents. MultiSystem Manager adds statements to the NetView automation table to capture alerts and react to them. The NetView automation table makes this information available to user-written programs. You too can add statements to the NetView automation table thus allowing you to receive updates from the topology agents.

2.6.2.13 RODM-Based Automation

This type of automation is based on user-written applications that access information stored in RODM. RODM automation applications can process within RODM, using RODM methods, or externally using MultiSystem Manager Access or the RODM API. You can write automation applications that react to status changes made by MultiSystem Manager alert processing. You can also write applications that correlate resources reported upon by different topology managers. These applications can react to problems affecting multiple resources, which might have been reported in multiple alerts.

MultiSystem Manager uses RODM-based automation and the workstation correlate utility to dynamically correlate different managed resources to the same workstation.

2.6.3 MultiSystem Manager/Novell NetWare Topology Feature

MultiSystem Manager works with Novell NetWare and NetWare for SAA.

The Novell NetWare topology feature contains the following:

- Topology manager extensions
- Command support
- Installation samples
- NetWare topology agent
- Supplemental tools and utilities

2.6.3.1 MultiSystem Manager/Novell NetWare Topology Benefits

MultiSystem Manager provides an integrated and centralized network management facility that enables you to manage your NetWare networks from a NetView Graphic Monitor Facility (NGMF) workstation.

To help you manage your networks, MultiSystem Manager provides the following benefits:

- Dynamic topology and status discovery of your networks
- Instant access to graphic views of the topology and status of your networks, all from a single NGMF workstation
- Quick notification of any changes in the topology and status of your networks, such as:
  - A file server joins or leaves the network.
  - A requester logs into or out of a file server.
  - A file server's CPU utilization exceeds a user-defined threshold.
  - Free space on a file server volume falls below a user-defined threshold.
- The ability to send commands to network resources simply by selecting the resource in an NGMF view and then selecting the command from a pull-down window
- The ability to integrate the management of your NetWare, SNA, and non-SNA networks
- The ability to access the Information/Management database from MultiSystem Manager resources displayed in your NGMF views by means of NGMF Inventory/Problem Management functions

2.6.3.2 How MultiSystem Manager Communicates with Your NetWare Networks

Figure 14 on page 90 shows how MultiSystem Manager fits into your network environment.

MultiSystem Manager uses a manager-agent relationship to manage LANs. This relationship consists of a topology manager and a topology agent. MultiSystem Manager provides a topology manager, which runs on the NetView host. The MultiSystem Manager NetWare topology feature supplies two NetWare loadable modules (NLMs) that reside on each file server in your network. These NLMs (named FLCFNETV.NLM and FLCEAGNT.NLM) work together to act as the topology agent for all of the resources in that file server's domain. These two NLMs comprise the service point application IBMFLC.

MultiSystem Manager requires that you configure one file server in each of your NetWare networks as a collection-point file server. Topology agents that reside in collection-point file servers are referred to as collection-point topology agents. The collection-point topology agent monitors the other file servers, referred to as end-point file servers, throughout the network.

The topology manager uses NetView RUNCMD and RMTCMD commands over SNA sessions to communicate with the topology agents. The MultiSystem Manager NetWare topology feature supports both LU 6.2 and SSCP-PU sessions.

Topology agents use alerts, resolutions, and RUNCMD responses to communicate with MultiSystem Manager. Alerts and resolutions are received by the NetView automation table and forwarded to MultiSystem Manager. Figure 15 on page 91 shows how NetView communicates with the collection-point topology agents. The collection-point file server, in turn, communicates with the other file servers in the network.

2.6.3.3 The Role of the Topology Agents

The role of a topology agent is to monitor the file server's network and to dynamically communicate information about changes in network topology or resource status to the topology manager. Each file server running a topology agent monitors itself and optionally, its requesters.

The topology agent in the collection-point file server has an additional role. The agent notifies the topology manager whenever a new file server enters or leaves

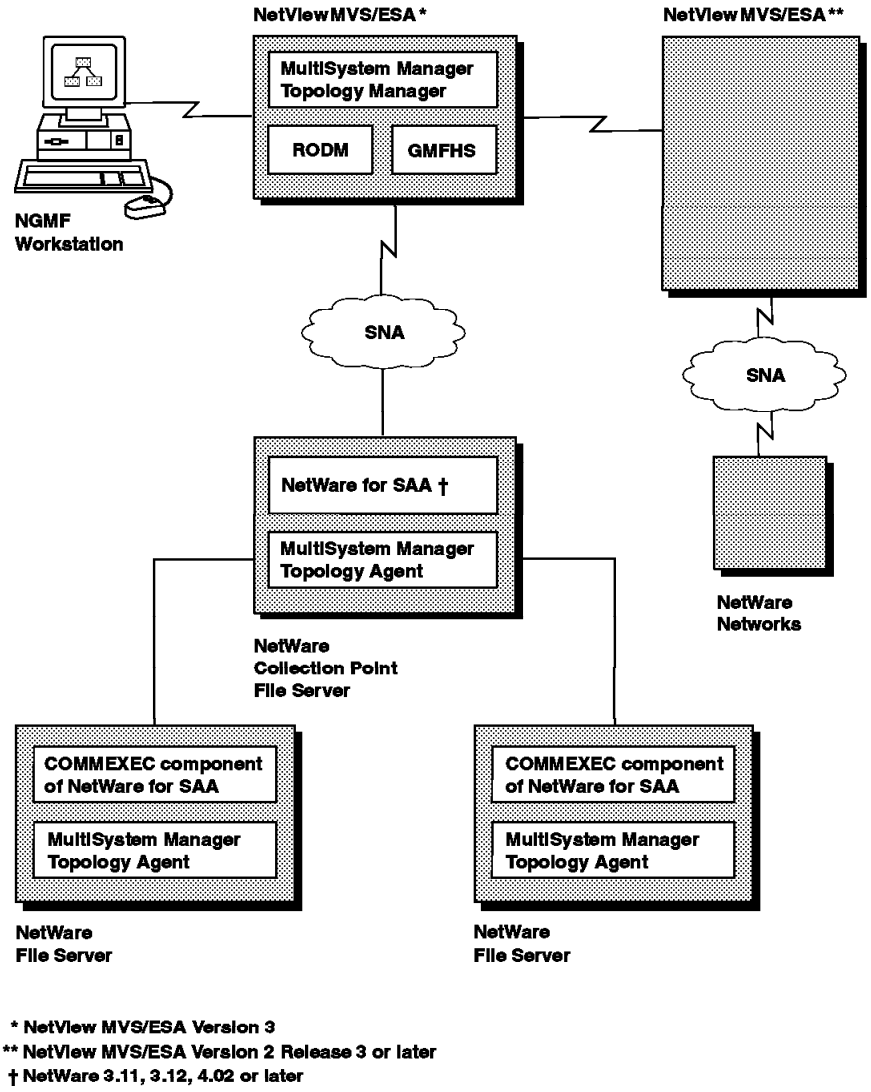


Figure 14. MultiSystem Manager NetWare Environment

the network. It informs the topology managers whenever a file server comes online or goes offline.

When the topology manager issues a command to gather topology and status, the topology agent collects the information and sends it back as part of the command's response.

When a topology agent wants to inform the topology manager of a topology or status change, the agent sends an alert or resolution indicating that some event has occurred and some action might need to take place as the result of that event.

The topology manager updates the status of the resource in RODM and reflects this status change in your NGMF views. Alerts and resolutions are then stored in the resource's alert history and can be displayed on your NGMF workstation.

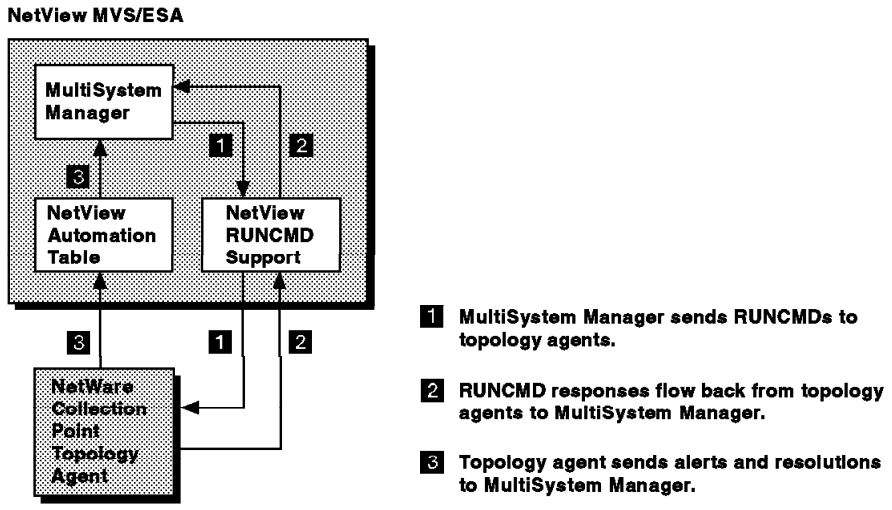


Figure 15. Communication between MultiSystem Manager and Topology Agents

2.6.3.4 The Role of the MultiSystem Manager Topology Manager

To help monitor and manage your networks, the MultiSystem Manager topology manager performs three primary tasks:

- Dynamically discovers the topology and status of the network and stores it in RODM. Automatically processes the topology and status updates from the topology agents
- Provides an easy-to-use command interface

2.6.3.5 Dynamic Topology Discovery

The MultiSystem Manager topology manager begins the process of managing your networks by dynamically discovering the initial topology and status of the resources in your network and then storing this information in RODM. After the information is in RODM, you can view your network resources from your NGMF workstation. Figure 16 on page 92 shows an example of the types of views created by MultiSystem Manager.

2.6.3.6 Automatic Topology and Status Updates

After MultiSystem Manager is initialized and the network′s initial topology and status is stored in RODM, the topology manager keeps topology and status up-to-date by receiving updates from the topology agents. For example, when a collection-point topology agent informs the topology manager that a new file server topology agent has come online, the topology manager automatically issues a command to the new topology agent to get topology and status of the new file server. When the new agent returns this information, the topology manager adds this information to RODM and the new file server appears in your network views.

The topology agents also send additional alerts to the topology manager indicating problems such as, server login disabled or CPU usage exceeded threshold. When all of the problems known to the MultiSystem Manager topology agent on a server are resolved, the topology agent sends a resolution indicating that the file server is fully operational.

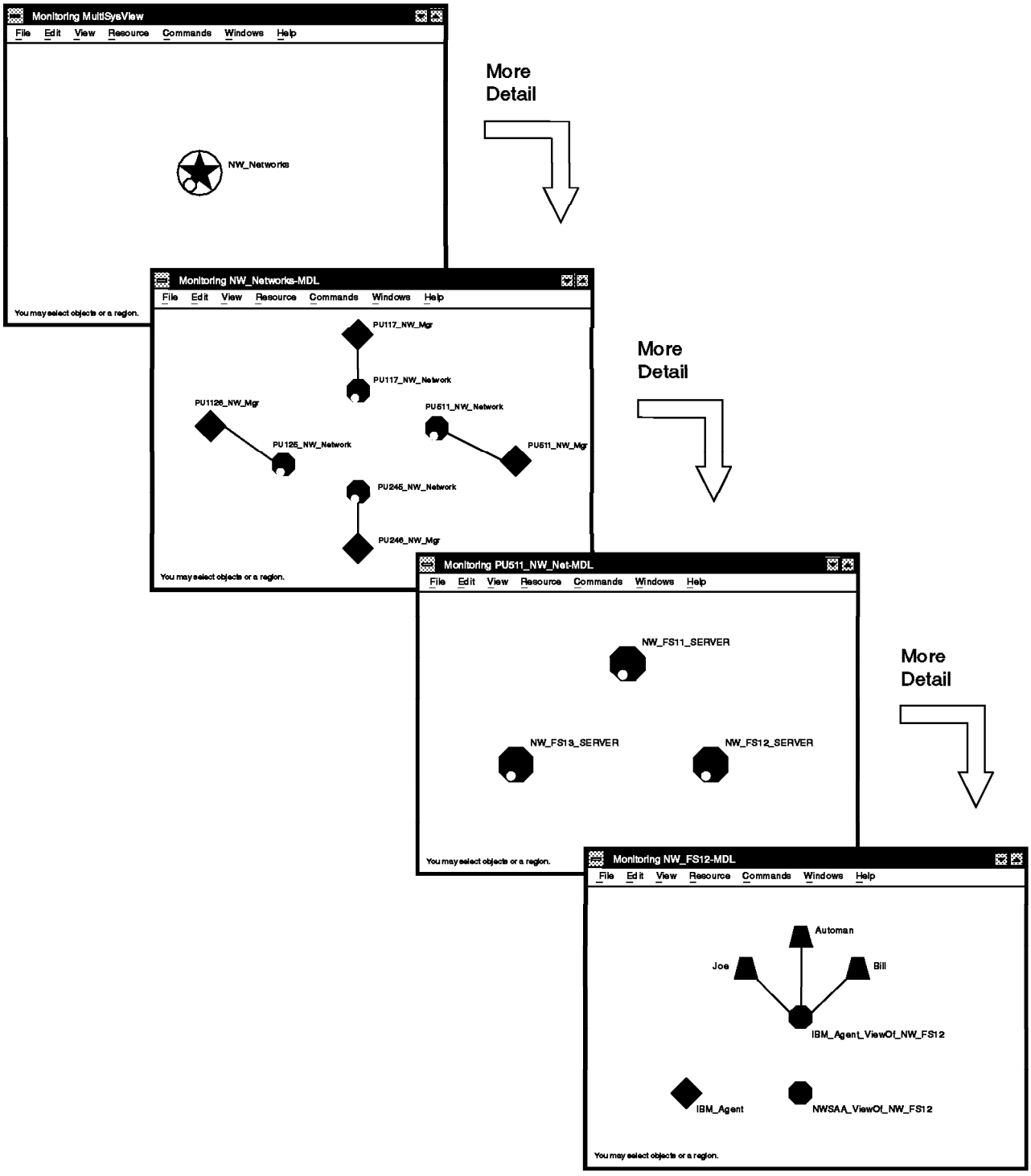


Figure 16. An Example of NetWare Views

Unlike the MultiSystem Manager topology agent, NetWare for SAA does not send a resolution indicating that file server problems have been corrected. You can, however, use the NetWare agent alert monitoring feature available on NetWare 4.x servers in conjunction with the LIST ALERTS, RESOLVE ALERTS, and SET MONITOR THRESHOLD commands to more closely monitor the status of your NetWare networks.

The topology manager receives status updates from both the MultiSystem Manager topology agents and the NetWare application programs (NetWare for SAA) running in the file servers. Updates from both the topology agents and the NetWare applications update your views, but only the updates from the topology agents are stored in the GMFHS alert history file.

2.6.3.7 Easy-to-Use Command Interface

MultiSystem Manager provides an easy-to-use command interface, called distributed manager command support (DMCS), that enables you to send commands to the topology agents. DMCS allows you to issue NetWare commands from your NGMF workstation. DMCS automatically retrieves RODM information that is required to send the command. You can use DMCS in an automation routine, from the NetView operator command line, or from the NGMF workstation. Figure 17 on page 94 shows how MultiSystem Manager presents a list of commands on your NGMF workstation.

2.6.3.8 Inventory/Problem Management (IPM) Support

The Inventory/Problem Management (IPM) component of NetView for MVS provides support for access to Information/Management database records from NGMF. Using the NGMF Inventory command exit, you can display inventory information stored in Information/Management. The NGMF Problem Management function allows you to list, display, update, and add problem records. MultiSystem Manager provides sample alias tables and customization files that enable the basic IPM functions for the default IPM program interface data tables (PIDTs). These samples are provided as a working example of the customization required to fully exploit IPM. You need to modify the samples so IPM will work with your existing Information/Management records. Refer to *NetView for MVS V3R1 Graphic Monitor Facility User's Guide*, SC31-8095 and the *NetView for MVS V3R1 Customization Guide*, SC31-8052 for more information about using Inventory/Problem Management.

2.6.3.9 Creating Views

MultiSystem Manager dynamically builds views that meet the majority of your network management needs, but you might also want to create unique views.

You can monitor your network from a single NGMF view, or you can create multiple NGMF views, perhaps each view reflecting a different grouping of your resources.

You can also integrate your MultiSystem Manager networks with other network views. For example, if you have an SNA network view, you can add your MultiSystem Manager networks to that view.

MultiSystem Manager also provides a View Customization utility, called BLDVIEWS, which enables you to create your own views.

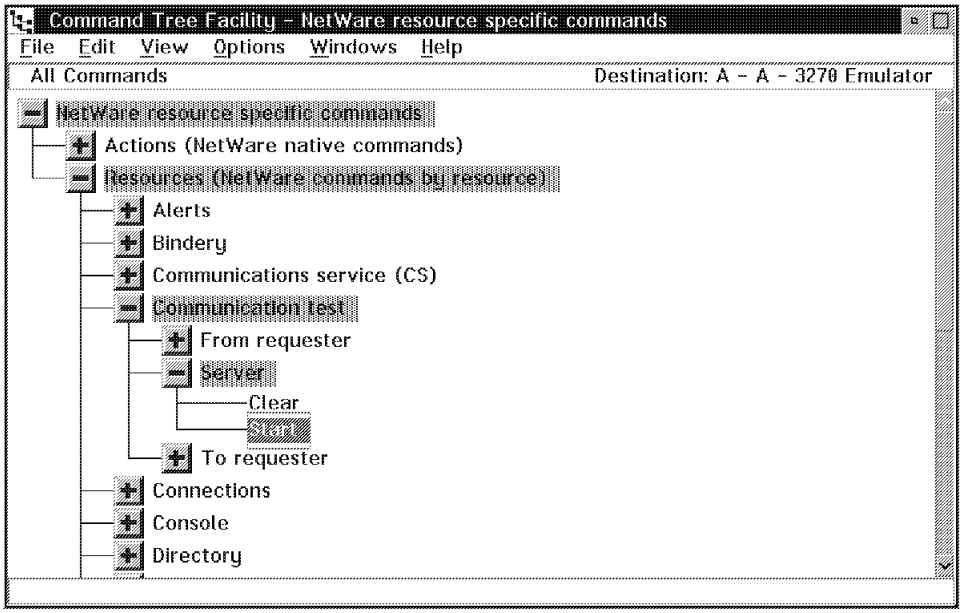


Figure 17. A MultiSystem Manager Command Menu Example

2.6.3.10 Resolving Network Problems

You can use NGMF menus and facilities to navigate between views and to locate failing resources. Once the failing resource is located, you can simply select the object on your view and send a command to resolve the problem.

2.6.3.11 Automating Network Management

You can use MultiSystem Manager to automate many network management procedures. In general, there are two types of automation: NetView-based automation and RODM-based automation.

2.6.3.12 NetView-Based Automation

This type of automation is based on user-written applications that react to information received by NetView from the topology agents. MultiSystem Manager adds statements to the NetView automation table to capture alerts and resolutions and to react to them. The NetView automation table makes this information available to user-written programs. You too can add statements to the NetView automation table thus allowing you to receive updates from the topology agents.

2.6.3.13 RODM-Based Automation

This type of automation is based on user-written applications that access information stored in RODM. RODM automation applications can process within RODM, using RODM methods, or externally using MultiSystem Manager Access or the RODM API. You can write automation applications that react to status changes made by MultiSystem Manager alert processing. You can also write applications that correlate resources reported upon by different topology managers. These applications can react to problems affecting multiple resources, which might have been reported in multiple alerts. MultiSystem Manager uses RODM-based automation and the workstation correlate utility to dynamically correlate different managed resources to the same workstation.

2.6.4 MultiSystem Manager / OS/2 LNM Topology Feature

The OS/2 LNM topology feature contains the following:

- Topology manager extensions
- Command support
- Installation samples

The OS/2 LNM topology feature works with:

- OS/2 LAN Network Manager 1.1 and 2.0 (referred to hereafter as LNM)

2.6.4.1 MultiSystem Manager / OS/2 LNM Topology Feature Benefits

MultiSystem Manager provides an integrated and centralized network management facility that enables you to manage your LAN Network Manager (LNM) networks from a NetView Graphic Monitor Facility (NGMF) workstation.

To help you manage your networks, MultiSystem Manager provides the following benefits:

- Dynamic topology and status discovery of your networks
- Instant access to graphic views of the topology and status of your networks, all from a single NGMF workstation
- Quick notification of any changes in the topology and status of your networks such as:
  - A token-ring has excessive errors.
  - A bridge went offline.
  - A monitored adapter is not responding.
- The ability to send commands to network resources simply by selecting the resource in an NGMF view and then selecting the command from a pull-down window
- The ability to integrate the management of your LNM, SNA, and non-SNA networks
- The ability to access the Information/Management database from MultiSystem Manager resources displayed in your NGMF views by means of NGMF Inventory/Problem Management functions

2.6.4.2 How MultiSystem Manager Communicates with Your LNM Networks

Figure 18 on page 97 shows how MultiSystem Manager fits into your network environment.

MultiSystem Manager uses a manager-agent relationship to manage LANs. This relationship consists of a topology manager and a topology agent. MultiSystem Manager provides a topology manager, which runs on the NetView host. Each LAN Network Manager (LNM) acts as the topology agent for the network and resources controlled by that LNM.

The topology manager uses NetView RUNCMD and RMTCMD commands over SNA sessions to communicate with the topology agents. The MultiSystem Manager LNM topology feature supports both LU 6.2 and SSCP-PU sessions.

Topology agents use alerts, resolutions, and RUNCMD responses to communicate with MultiSystem Manager. Alerts and resolutions are received by the NetView automation table and forwarded to MultiSystem Manager. Figure 19 on page 98 shows how MultiSystem Manager communicates with the topology agents.

2.6.4.3 The Role of the Topology Agents

The role of a topology agent is to monitor the network in which it resides and to dynamically communicate information about changes in network topology or resource status to the topology manager.

When the topology manager issues a command to gather topology and status, the topology agent collects the information and sends it back as part of the command's response.

When a topology agent wants to inform the topology manager of a topology or status change, the agent sends an alert or resolution indicating that some event has occurred and some action might need to take place as the result of that event.

The topology manager updates the status of the resource in RODM and reflects this status change in your NGMF views. Alerts and resolutions are then stored in the resource's alert history and can be displayed on your NGMF workstation.

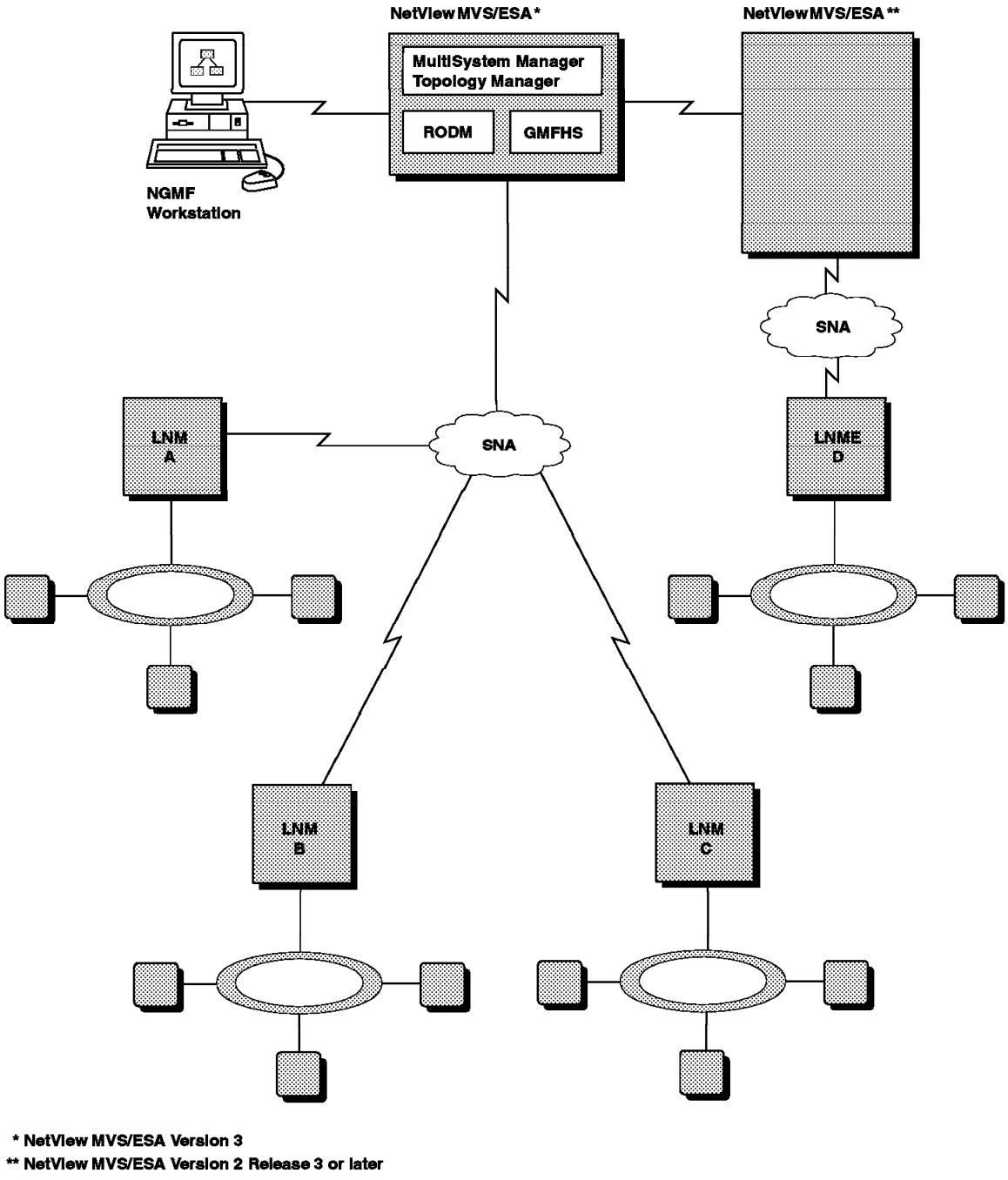


Figure 18. MultiSystem Manager LNM Environment

2.6.4.4 The Role of the MultiSystem Manager Topology Manager

To help monitor and manage your networks, the MultiSystem Manager topology manager performs three primary tasks:

- Dynamically discovers the topology and status of the network and stores it in RODM
- Automatically processes the topology and status updates from the topology agents

- Provides an easy-to-use command interface

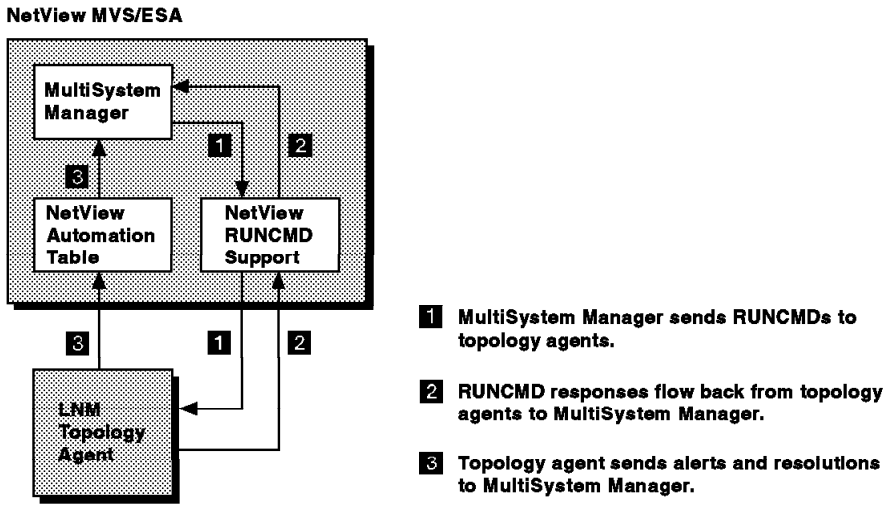


Figure 19. Communication Between MultiSystem Manager and Topology Agents

2.6.4.5 Dynamic Topology Discovery

The MultiSystem Manager topology manager begins the process of managing your networks by dynamically discovering the initial topology and status of the resources in your network and then storing this information in RODM. After the information is in RODM, you can view your network resources from your NGMF workstation. Figure 20 on page 99 shows an example of the types of views created by MultiSystem Manager.

2.6.4.6 Automatic Topology and Status Updates

After MultiSystem Manager is initialized and the network's initial topology and status is stored in RODM, the topology manager keeps topology and status up-to-date by receiving updates from the topology agents. For example, when an LNM becomes active, the LNM sends an alert to the topology manager. If the service point has been defined to MultiSystem Manager, the topology manager automatically issues a series of RUNCMDs to the new LNM to get topology and status of its currently monitored resources.

The LNMs also send additional alerts to the topology manager indicating problems, for example, adapter congested, or token-ring inoperative. When the problems are resolved, the LNM sends resolutions to the topology manager, for example, adapter no longer congested or token-ring recovered. The status changes are stored in RODM and are reflected on your views and the alerts and resolutions are stored in the GMFHS alert history file.

2.6.4.7 Easy-to-Use Command Interface

MultiSystem Manager provides an easy-to-use command interface, called distributed manager command support (DMCS), that enables you to send commands to the topology agents. DMCS allows you to issue LNM commands from your NGMF workstation. DMCS automatically retrieves RODM information that is required to send the command. You can use DMCS in an automation routine, from the NetView operator command line, or from the NGMF

workstation. Figure 21 on page 100 shows how MultiSystem Manager presents a list of commands on your NGMF workstation.

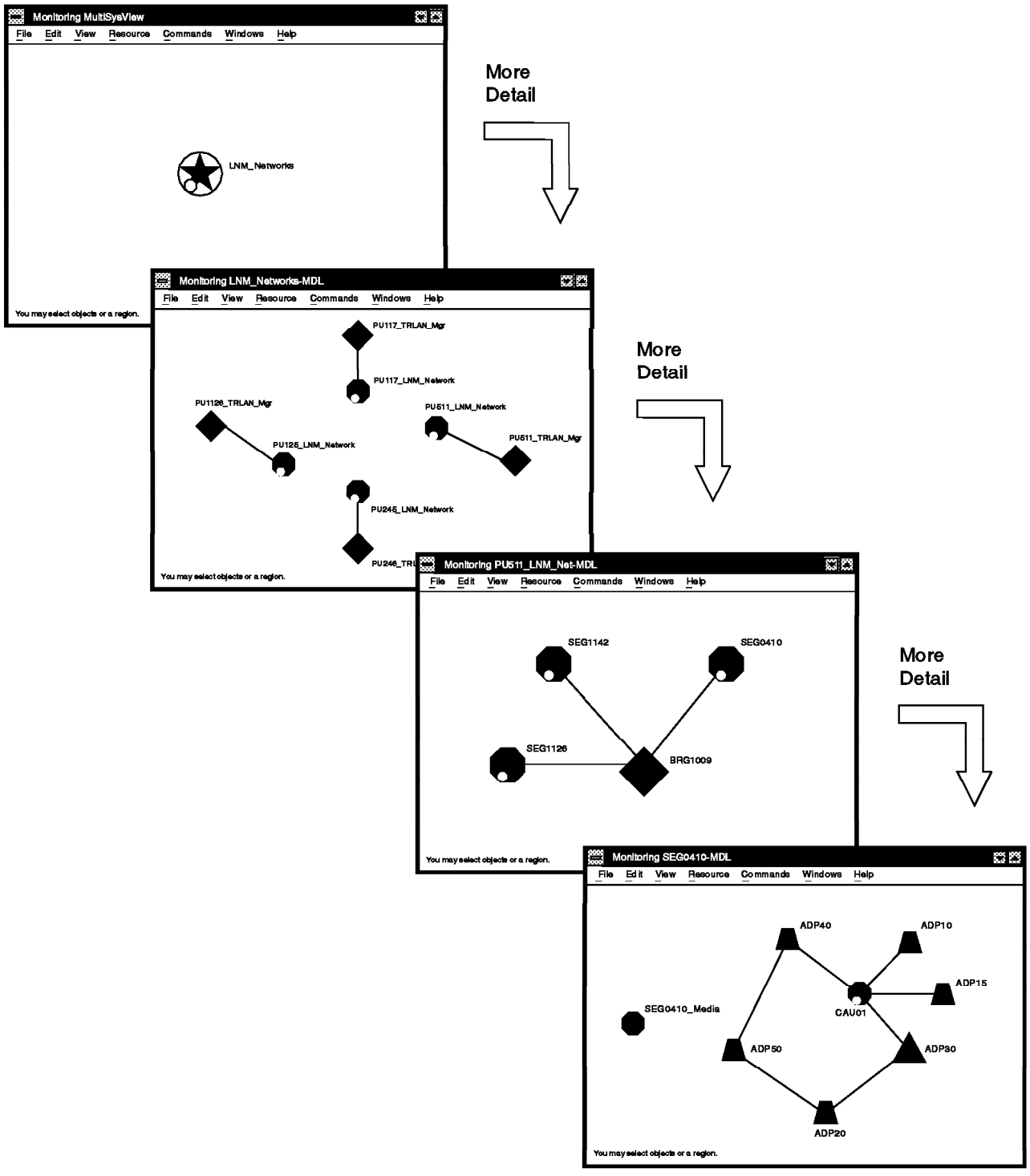


Figure 20. An Example of LNM Views

2.6.4.8 Inventory/Problem Management (IPM) Support

The Inventory/Problem Management (IPM) component of NetView for MVS provides support for access to Information/Management database records from NGMF. Using the NGMF Inventory command exit, you can display inventory information stored in Information/Management. The NGMF Problem Management function allows you to list, display, update, and add problem records.

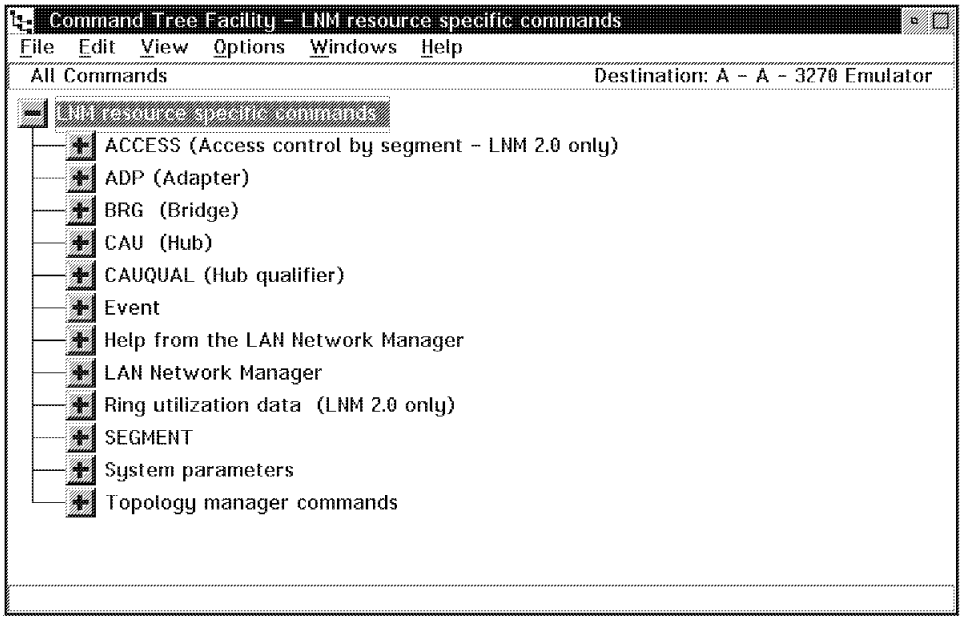


Figure 21. A MultiSystem Manager Command Menu Example

MultiSystem Manager provides sample alias tables and customization files that enable the basic IPM functions for the default IPM program interface data tables (PIDTs). These samples are provided as a working example of the customization required to fully exploit IPM. You need to modify the samples so IPM will work with your existing Information/Management records. Refer to the NetView for MVS NGMF User's Guide and the NetView for MVS Customization Guide for more information about using Inventory/Problem Management.

2.6.4.9 Creating Views

MultiSystem Manager dynamically builds views that meet the majority of your network management needs, but you might also want to create unique views.

You can monitor your network from a single NGMF view, or you can create multiple NGMF views, perhaps each view reflecting a different grouping of your resources.

You can also integrate your MultiSystem Manager networks with other network views. For example, if you have an SNA network view, you can add your MultiSystem Manager networks to that view.

MultiSystem Manager also provides a View Customization utility, called BLDVIEWS, which enables you to create your own views.

2.6.4.10 Resolving Network Problems

You can use NGMF menus and facilities to navigate between views and to locate failing resources. Once the failing resource is located, you can simply select the object on your view and send a command to resolve the problem.

2.6.4.11 Automating Network Management

You can use MultiSystem Manager to automate many network management procedures. In general, there are two types of automation: NetView-based automation and RODM-based automation.

2.6.4.12 NetView-Based Automation

This type of automation is based on user-written applications that react to information received by NetView from the topology agents. MultiSystem Manager adds statements to the NetView automation table to capture alerts and resolutions and to react to them. The NetView automation table makes this information available to user-written programs. You too can add statements to the NetView automation table thus allowing you to receive updates from the topology agents.

2.6.4.13 RODM-Based Automation

This type of automation is based on user-written applications that access information stored in RODM. RODM automation applications can process within RODM, using RODM methods, or externally using MultiSystem Manager Access or the RODM API. You can write automation applications that react to status changes made by MultiSystem Manager alert processing. You can also write applications that correlate resources reported upon by different topology managers. These applications can react to problems affecting multiple resources, which might have been reported in multiple alerts.

MultiSystem Manager uses RODM-based automation and the workstation correlate utility to dynamically correlate different managed resources to the same workstation.

2.6.5 MultiSystem Manager / LMU Topology Feature

MultiSystem Manager works with LAN NetView Management Utilities (LMU) Version 1.1.

The LMU topology feature contains the following:

- Topology manager extensions
- Command support
- Installation samples

2.6.5.1 LMU Terms and Concepts

The following is a list of LMU terms:

- **Administrator System**

  The administrator system issues commands to managed systems. The administrator system must reside on the service point workstation.

- **Database System (Optional)**

  The database system is a managing system that maintains an LMU database. LMU applications send database records to the database system. If used, the database system must reside on the service point workstation.

- **Fault Manager**

  The fault manager system receives alerts from fault reporters and responds by forwarding alerts to MultiSystem Manager. The fault reporter is a managed system that receives alerts from management applications and sends them to the fault manager.

- **Managed System**

  The managed system is monitored by the managing system. The managed system sends heartbeats (″I am here″ messages) to the managing system. The managed system receives commmands from the administrator system.

- **Managing System**

  The managing system monitors the network for managed system heartbeats. It is aware of the status of all its managed systems. A managing system must be either a service point workstation or a workstation that is directly managed by a service point workstation.

- **Service Point Workstation**

  For each LMU network, one workstation acts as the SNA service point for all systems (both managed and managing) in the network. The service point workstation must be the administrators system and must run Communication Manager/2 with the following applications:

  – Service Point Application Router (SPAR)
  – Remote Operations Support (ROPS)

  MultiSystem Manager requires that the service point workstation be defined as the fault manager, and the LMU database, if used, must reside on the service point workstation.

2.6.5.2 MultiSystem Manager / LMU Topology Feature Benefits

MultiSystem Manager provides an integrated and centralized network management facility that enables you to manage your LMU networks from a NetView Graphic Monitor Facility (NGMF) workstation.

To help you manage your networks, MultiSystem Manager provides the following benefits:

- Dynamic topology and status discovery of your networks
- Instant access to graphic views of the topology and status of your networks, all from a single NGMF workstation
- Access to LMU workstation information, such as serial numbers, component list, and installed memory
- The ability to send commands to network resources simply by selecting the resource in an NGMF view and then selecting the command from a pull-down window
- The ability to integrate the management of your LMU, SNA, and non-SNA networks
- The ability to access the Information/Management database from MultiSystem Manager resources displayed in your NGMF views by means of NGMF Inventory/Problem Management functions

2.6.5.3 How MultiSystem Manager Communicates with Your LMU Networks

Figure 22 on page 104 shows the relationship between workstations across LMU networks. MultiSystem Manager uses a manager-agent relationship to manage LMU network resources. This relationship consists of a topology manager and a topology agent. MultiSystem Manager provides a topology manager, which runs on the NetView host. The LMU service point workstation acts as the MultiSystem Manager topology agent. LMU A, LMU C, and LMU D are LMU service point workstations. Service point workstations can manage other managing workstations. For example, LMU E manages LMU F and LMU G. Note that LMU F or LMU G cannot be managing workstations because they are not managed by an LMU service point workstation. For more information about LMU terms and concepts, refer to the *LAN NetView Management Utilities for OS/2 User's Guide*, SC30-3555.

The topology manager uses NetView RUNCMD and RMTCMD commands over SNA sessions to communicate with the topology agents. The MultiSystem Manager LMU topology feature supports both LU 6.2 and SSCP-PU sessions.

Topology agents use alerts and RUNCMD responses to communicate with MultiSystem Manager. Alerts are received by the NetView automation table and forwarded to MultiSystem Manager. Figure 24 on page 106 shows how MultiSystem Manager communicates with the topology agents.

2.6.5.4 The Role of the Topology Agents

The role of a topology agent is to monitor the network in which it resides and to dynamically communicate information about changes in network topology or resource status to the topology manager.

When the topology manager issues a command to gather topology and status, the topology agent collects the information and sends it back as part of the command's response.

When a topology agent wants to inform the topology manager of a topology or status change, the agent sends an alert indicating that some event has occurred and some action might need to take place as the result of that event.

The topology manager updates the status of the resource in RODM and reflects this status change in your NGMF views. Alerts are then stored in the resource's alert history and can be displayed on your NGMF workstation.

2.6.5.5 The Role of the MultiSystem Manager Topology Manager

To help monitor and manage your networks, the MultiSystem Manager topology manager performs three primary tasks:

- Dynamically discovers the topology and status of the network and stores it in RODM
- Automatically processes the topology and status updates from the topology agents
- Provides an easy-to-use command interface

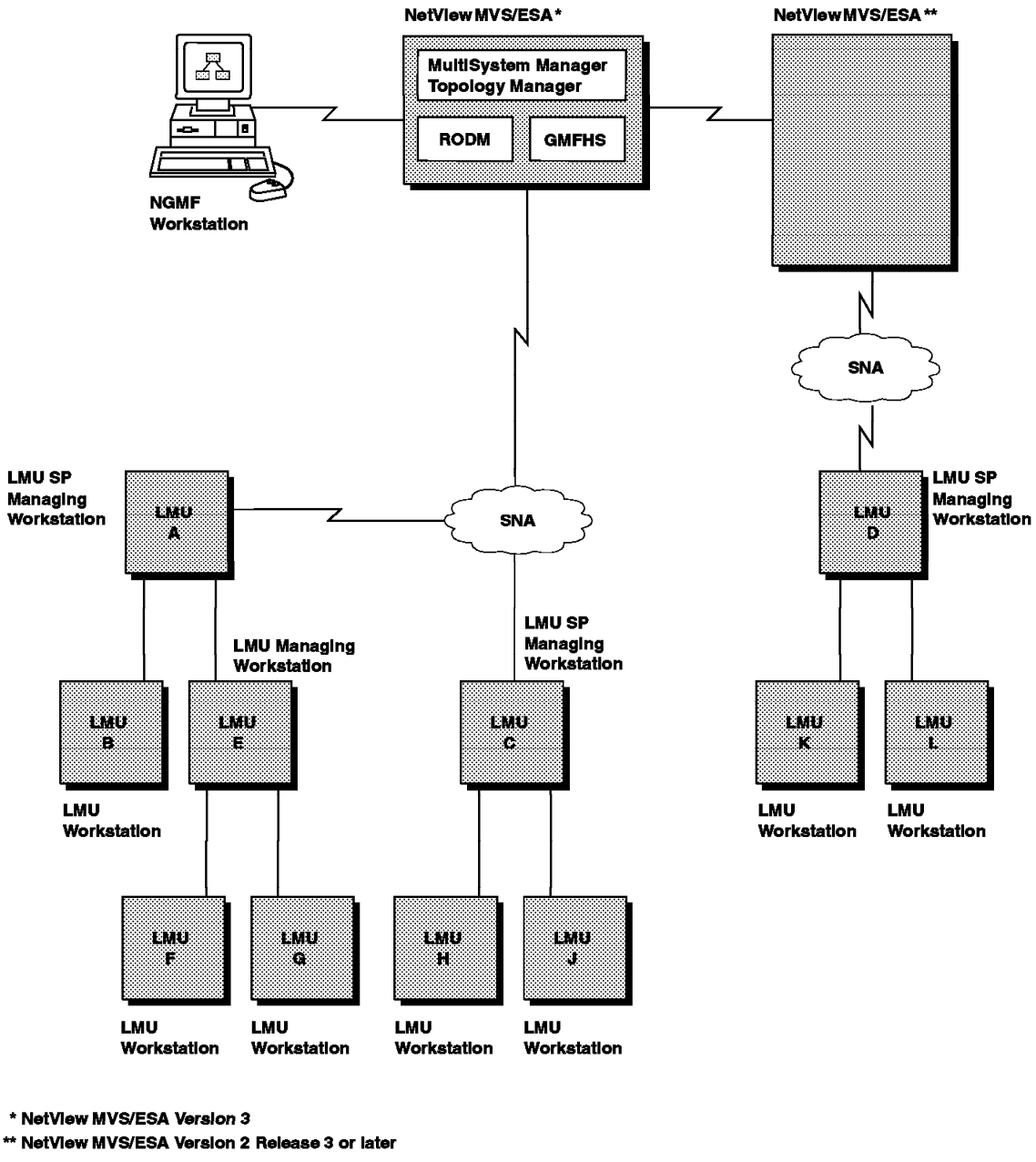


Figure 22. MultiSystem Manager LMU Environment

2.6.5.6 Dynamic Topology Discovery

The MultiSystem Manager topology manager begins the process of managing your networks by dynamically discovering the initial topology and status of the resources in your network and then storing this information in RODM. After the information is in RODM, you can view your network resources from your NGMF workstation. Figure 23 on page 105 shows an example of the types of views created by MultiSystem Manager.

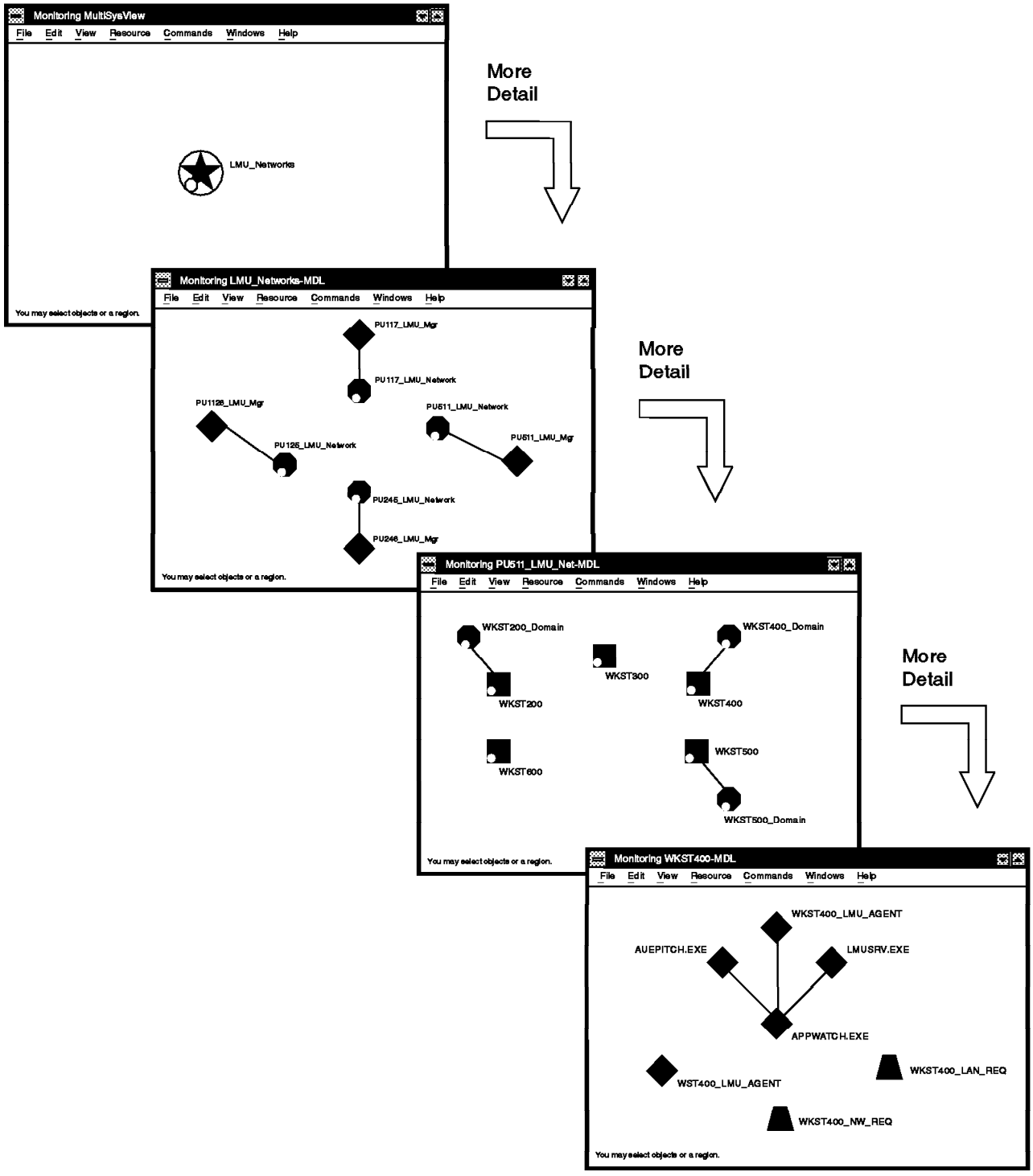


Figure 23. An Example of LMU Views

2.6.5.7 Automatic Topology and Status Updates

After MultiSystem Manager is initialized and the network's initial topology and status is stored in RODM, the topology manager keeps topology and status up-to-date by receiving updates from the topology agents. For example, when a managed workstation becomes active, the workstation notifies the topology agent in the LMU service point. The topology agent sends an alert to the topology manager indicating that a new managed workstation is now active in

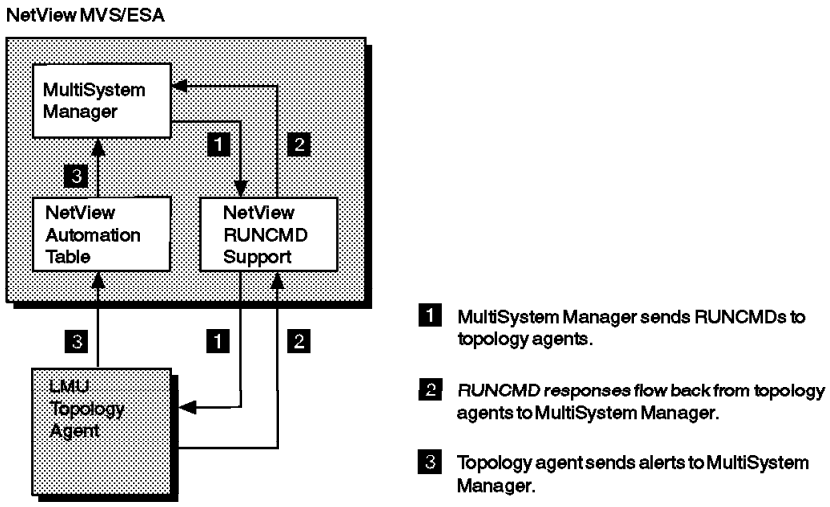


Figure 24. Communication Between MultiSystem Manager and Topology Agents

the network. The topology manager gathers the new workstation's topology and status and displays the workstation in your NGMF views. Alerts received from the topology agents are stored in the alert history file and can be displayed on your NGMF workstation.

2.6.5.8 Easy-to-Use Command Interface

MultiSystem Manager provides an easy-to-use command interface, called distributed manager command support (DMCS), that enables you to send commands to the topology agents. DMCS allows you to issue LMU commands from your NGMF workstation. DMCS automatically retrieves RODM information that is required to send the command. You can use DMCS in an automation routine, from the NetView operator command line, or from the NGMF workstation. Figure 25 on page 107 shows how MultiSystem Manager presents a list of commands on your NGMF workstation.

2.6.5.9 Inventory/Problem Management (IPM) Support

The Inventory/Problem Management (IPM) component of NetView for MVS provides support for access to Information/Management database records from NGMF. Using the NGMF Inventory command exit, you can display inventory information stored in Information/Management. The NGMF Problem Management function allows you to list, display, update, and add problem records.

MultiSystem Manager provides sample alias tables and customization files that enable the basic IPM functions for the default IPM program interface data tables

(PIDTs). These samples are provided as a working example of the customization required to fully exploit IPM. You need to modify the samples so IPM will work with your existing Information/Management records. Refer to *NetView for MVS V3R1 Graphic Monitor Facility User's Guide*, SC31-8095 and the *NetView for MVS V3R1 Customization Guide*, SC31-8052 for more information about using Inventory/Problem Management.

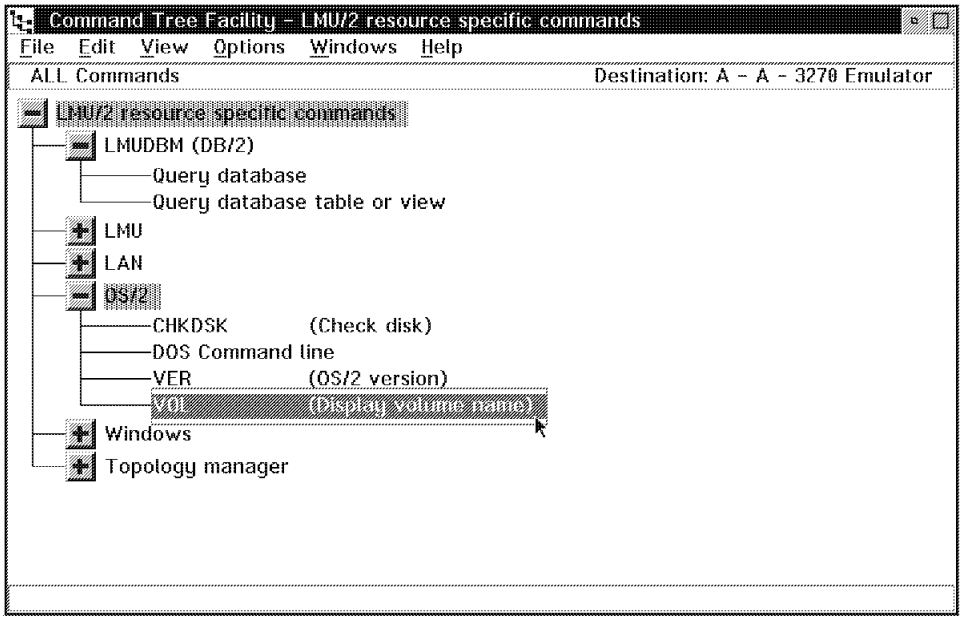


Figure 25. A MultiSystem Manager Command Menu Example

2.6.5.10 Creating Views

MultiSystem Manager dynamically builds views that meet the majority of your network management needs, but you might also want to create unique views.

You can monitor your network from a single NGMF view, or you can create multiple NGMF views, perhaps each view reflecting a different grouping of your resources.

You can also integrate your MultiSystem Manager networks with other network views. For example, if you have an SNA network view, you can add your MultiSystem Manager networks to that view.

MultiSystem Manager also provides a View Customization utility, called BLDVIEWS, which enables you to create your own views.

2.6.5.11 Resolving Network Problems

You can use NGMF menus and facilities to navigate between views and to locate failing resources. Once the failing resource is located, you can simply select the object on your view and send a command to resolve the problem.

2.6.5.12 Automating Network Management

You can use MultiSystem Manager to automate many network management procedures. In general, there are two types of automation: NetView-based automation and RODM-based automation.

2.6.5.13 NetView-Based Automation

This type of automation is based on user-written applications that react to information received by NetView from the topology agents. MultiSystem Manager adds statements to the NetView automation table to capture alerts and resolutions and to react to them. The NetView automation table makes this information available to user-written programs. You too can add statements to the NetView automation table thus allowing you to receive updates from the topology agents.

2.6.5.14 RODM-Based Automation

This type of automation is based on user-written applications that access information stored in RODM. RODM automation applications can process within RODM, using RODM methods, or externally using MultiSystem Manager Access or the RODM API. You can write automation applications that react to status changes made by MultiSystem Manager alert processing. You can also write applications that correlate resources reported upon by different topology managers. These applications can react to problems affecting multiple resources, which might have been reported in multiple alerts.

MultiSystem Manager uses RODM-based automation and the workstation correlate utility to dynamically correlate different managed resources to the same workstation.

2.6.6 Online Help

MultiSystem Manager provides online help for commands and messages. This help is available on your NGMF workstation and from your NetView command line.

You can obtain contextual help for MultiSystem Manager supported commands and the MultiSystem Manager messages from the Command Tree/2 help facility. You can obtain help for the topology commands and all MultiSystem Manager messages at your NetView session by entering the NetView HELP command. You can also obtain help from the BookManager copy of this book if it is installed on your NGMF workstation or NetView host.

2.6.7 Software Requirements

MultiSystem Manager requires NetView Version 3 for MVS/ESA (5655-007), with the NetView Graphic Monitor Facility host subsystem feature. Previous versions of NetView are not supported by MultiSystem Manager Version 2 Release 2. NetView must be at the service level required by the MultiSystem Manager program directory, The software requirements for NetView are listed in the *NetView for MVS V3R1 Installation and Administration Guide*, SC31-8043.

2.6.8 Hardware Requirements

MultiSystem Manager runs in a virtual storage environment on any System/370 or System/390 processor (or configuration) with sufficient storage that supports NetView Version 3 for MVS/ESA.

2.6.9 Related Publications

A guide to install, customize and operate MultiSystem Manager as well a detailed hardware and software requirements are contained in the following books:

- *NetView Multisystem Manager Internet Protocol Networks*, SC31-8131-01
- *NetView Multisystem Manager Open Topology Interface*, SC31-8144-01
- *NetView Multisystem Manager LAN NetView Management*, Utilities SC31-8112-01
- *NetView Multisystem Manager Novell NetWare Networks*, SC31-8129-01
- *NetView Multisystem Manager OS/2 LAN Network Manager*, SC31-8130-01

2.7 AIX LAN Management

In the following sections, these IBM LAN management products for the AIX platform are discussed:

- NetView for AIX
- Nways Campus Manager ReMon for AIX/HP
- Nways Campus Manager LAN for AIX
- Nways Campus Manager ATM for AIX
- Nways Campus Manager ATM for AIX
- LAN Network Manager for AIX
- LAN NetView Management Utilities for AIX (LMU)

2.8 NetView for AIX

NetView for AIX and NetView Entry for AIX provide a comprehensive network management solution for heterogeneous, multivendor devices and open networks requiring SNMP. They facilitate network management in a multivendor Transmission Control Protocol/Internet Protocol (TCP/IP) network, and provide management of TCP/IP devices that include simple network management protocol (SNMP) agents, and monitor all IP-addressable devices.

NetView for AIX uses a graphical, object-oriented user interface built on OSF/Motif, which allows the network to be displayed on top of meaningful pictures, such as maps, buildings, or devices. It also uses dynamic network discovery to maintain a current view of the network topology.

NetView for AIX extends management to non-SNMP devices using its General Topology Manager (GTM). Resources are stored in the GTM database along with their MAC (media access control) addresses. This allows correlation of multiple protocols running on the same resource. Figure 26 on page 110 shows the NetView for AIX topology screen with icons for the integrated management of

TCP/IP, hubs, token-rings and LMU managed resources, such as OS/2, NetWare, DOS and DOS/Windows.

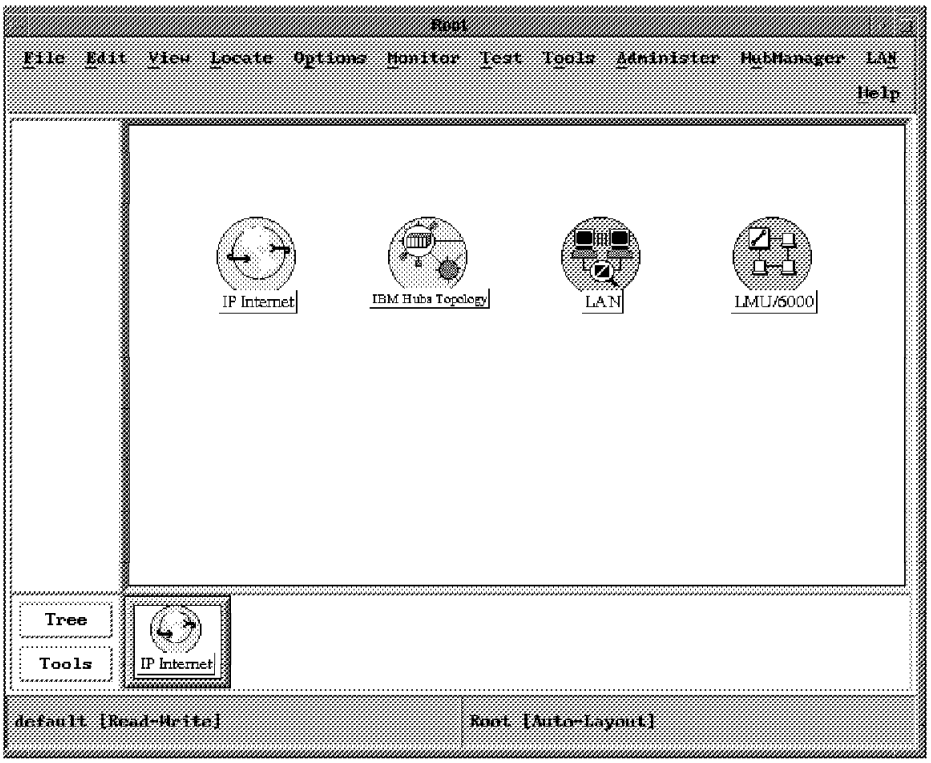


Figure 26. NetView for AIX with Hub Manager for AIX, LNM for AIX and LMU/6000

Figure 27 shows an example of the NetView for AIX screen for switching between the different protocol views for a device.

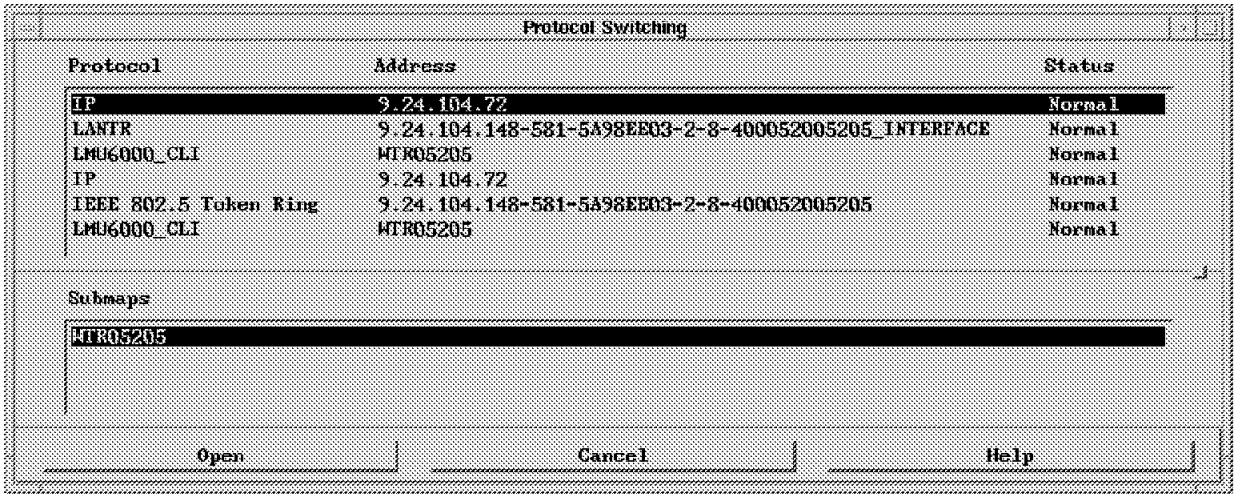


Figure 27. NetView for AIX Protocol Switching Screen

NetView for AIX provides the ability to store and retrieve IP topology, SNMP Management Information Base (MIB) data collected by NetView for AIX's snmpCollect daemon, traps sent to NetView for AIX and vendor-provided applications, in conjunction with the following relational databases:

- IBM DB2/6000 Version 2

- Informix Relational Database
- Ingres Relational Database
- ORACLE Relational Database
- Sybase Relational Database

IBM NetView Entry for AIX is identical in function to IBM NetView for AIX, with the limitation of 32 managed nodes and no relational database support.

NetView for AIX is an open network management platform that enables the integration of SNMP and CMIP applications for managing IP and other networks, such as LAN media, from a single management platform. A complete set of industry-standard open APIs is shipped with NetView for AIX, enabling seamless integration of vendor and customer applications with the base platforms.

Several samples of application code are shipped with NetView for AIX. The following table summarizes the applications available from IBM for NetView for AIX, along with the functionality provided. Many other applications, such as Synoptics Optivity and Wellfleet Site Manager are detailed in the *NetView Association Catalog from IBM and Digital* and are available from the respective vendors.

Table 1. Applications Available from IBM for NetView for AIX		
This *NetView for AIX* Application	**Uses...**	**To Provide...**
ATMC Manager	IBM 8260 ATM nodes and IBM 8282 ATM Concentrators MIBs	ATM Campus physical and logical resource management
Intelligent Hub Manager for AIX and Intelligent Hub Manager for AIX Entry	IBM 8250/IBM 8260/Chipcom MIBs	Graphical hub management and integration with LNM, RABM/6000 and ATMV Manager
LAN Management Utilities for AIX	LMU for OS/2	Vital product data and management for OS/2, DOS/Windows, DOS, NetWare, and Macintosh workstations running on NetBIOS or IPX networks
LNM for AIX	SNMP agents which implement MIB II and RFC1286 or MIB II and RFC1525 and RFC1493(bridge), Ring Station Groups of RFC1513(RMON), AWP7607(token-ring surrogate), IBM 8230 MIB, IBM FDDI agent, and LNM for OS/2 V2	FDDI logical topology, token-ring topology, bridge topology, bridge traffoc loads, bridge errors, adapters status monitoring, ring soft errors reporting and MAC level statistics
RMONitor for AIX	RMON agents which are compliant with RFC 1513 (token-ring) or RFC 1271 (Ethernet)	RMON data such as Top N hosts and threshold monitoring
Router and Bridge Manager/6000	IBM: 6611, 2210, 8229, 8250/8260 router blades, Cisco 8.X/9.X, Wellfleet, or other SNMP MIB-II routers or bridges	Router and bridge statistics by protocol, APPN, DLSw and threshold monitoring
SNA Manager/6000	S/390 NetView	Graphical SNA network topology with status; NetView command interface
Systems Monitor for AIX	Systems Monitor Information Agent MIB	Systems management information such as machine type/model, file system utilization, paging space utilization, users, processes, etc.
Systems Monitor for AIX	Systems Monitor Mid-Level Manager	Distributed polling, thresholding and trap filtering
Trouble Ticket for AIX	AIX, SunOS, HP-UX, or DOS/Windows clients	Problem and change management

2.8.1 Technical Description

NetView for AIX components work together to create a comprehensive network management product that provides service for open networks. Three of these components are application functions that benefit your network. They are fault, configuration, and performance management.

2.8.1.1 Fault Management

One of the most requested network management applications is fault management, or the ability to detect if something in the network is not functioning.

Verifying Connectivity: NetView for AIX automatically and continually verifies that devices are connected. Operators can see the results on a network map that shows by color code the status of devices. Topology changes such as the addition or deletion of network interfaces are also reflected in the map.

Setting Thresholds: Network operators can determine what thresholds are critical for their networks and set NetView for AIX to poll (or check) nodes for these thresholds. If a threshold is exceeded, NetView for AIX generates an event which is displayed as an event card and can be used to initiate automation.

Specifying Trap Formats and Actions: When SNMP devices send SNMP traps that are specific to that device, the network operator can customize the message that is logged, as well as the action to be taken when a given trap is received. The operator also has the capability to define filtering and thresholding parameters affecting the information sent to the them, events sent to an application and alerts sent to host NetView. The trap can be customized in the following ways:

- Specify the text and MIB variables of the message to be logged
- Specify a program or a shell script to be executed when the SNMP trap arrives

Trap Generator: NetView for AIX enhances the error log management of RISC System/6000 AIX workstations through the trap generator function of its distributed subagent `trapgend`. This function takes the RISC System/6000 AIX workstation alertable error log information and converts it to traps that are sent to NetView for AIX. The following could be examples for such errors:

- Hardware errors, like problems accessing a tape
- Software problems, like a core dump from an application

Additionally, a user can customize both the predefined AIX system errors and user-defined errors to be alertable, which causes the trapgend daemon to send a trap to NetView for AIX. NetView for AIX can then manage these traps and can also convert these traps to SNA alerts if mainframe management is desired.

The trapgend subagent is software that comes with NetView for AIX and may be distributed to AIX workstations. Trapgend also extends the SNMP MIB to include information on the file systems (size and space available) and CPU utilization.

Diagnosing Problems: Network administrators can test problem devices in a remote location. Tools to simplify troubleshooting have been integrated into the network map. Customers can select a problem node with the mouse, and quickly perform the following tests:

- Use the IP PING to verify physical connectivity.
- Perform a TCP connection test.
- Check a node to determine whether it has an SNMP agent running.

Getting Network Information: To quickly resolve problems, operators select the appropriate event card where relevant information, such as problem description, location, user contact, and failing device information, is provided. If more information is needed, the operator can select nodes from a map and choose menu items for access to pertinent information.

Saving a Map Snapshot: You can save the current map to compare with later maps. The changes that are apparent when you compare maps are often helpful in solving problems.

Determining Packet Routes: Using the traceroute function, text and graphics are displayed to show the real and actual route a packet takes between nodes of a network even if there are routers and bridges involved.

Filtering: Filtering criteria can be applied to event information that is displayed on the NetView for AIX screen, as well as filtering of the alert information that is sent to host NetView. Multiple dynamic events displays are supported and each can use a different set of filters.

2.8.1.2 Configuration Management

Another desirable application is configuration management. The NetView for AIX configuration application reduces human intervention and continually provides up-to-date network topologies.

Automatic Network Discovery: NetView for AIX automatically discovers IP addressable nodes and places them on a map in their correct relationship. NetView for AIX continues to find new devices as they are added to the network and determines whether devices should be deleted from the network. This continual discovery ensures that the user has a current map of the network topology. This discovery provides for up to 2000 interfaces per node.

Keeping Records Electronically: NetView for AIX automatically generates and continually updates the network map and associated databases.

Event Configuration: NetView for AIX provides a graphical user interface for the event configurator function to define what actions to take when it receives a standard or enterprise-specific SNMP trap. In addition, NetView for AIX provides user-configurable status changes that allow a user to specify the meaning of status events for specific traps. One enterprise-specific trap might indicate that a node is down. After the operator takes action, or an automated action is taken, another trap could indicate that a node is up. The status changes are reflected dynamically in the network topology display as a color change.

Editing the Network Map: To tailor the map to suit the operator′s needs, NetView for AIX provides functions like cut, paste, copy, hide, add, delete, reposition, and create object/containers. Map editing is done with a mouse using select, drag and drop.

Browsing the Management Information Base (MIB): By using the mouse, customers can select object values from the MIB. NetView for AIX supports MIB-II, and enterprise-specific MIBs. With this function, one or more object values can be retrieved, numerical objects can be graphed in real time, and settable objects can be set through the dialog box.

Loading an MIB: NetView for AIX ships a large number of vendor-specific MIBs, including the IBM HACMP/6000, IBM 8250, IBM 6611, Synoptics, Cisco, Wellfleet, and many others. These MIBs are tested and can be compiled and loaded using the point-and-click MIB Loader. Vendor specific MIBs that conform to ASN.1 syntax that were not shipped with NetView for AIX can also be easily complied and loaded into NetView for AIX. This makes management of these devices possible for NetView for AIX. The latest NetView Association catalog, which provides a list of vendors providing MIBs, can be obtained from your local IBM office.

Listing Remote Network Services: Customers have access to information about TCP/IP services that are available from a remote node.

Getting Node Descriptions: You can edit node descriptions, providing a contact name and network location beyond what is provided in the MIB definition. Subsequently, network operators can access this and other MIB data using the mouse.

Locating Map Objects: Customers can locate objects in large networks or for inventory control by using various attributes. The attributes that are available to be searched include the host name, link address, IP address, object type, vendor and network configuration.

2.8.1.3 Performance Management

Still another often requested network management task is performance management. Being able to find trends and pinpoint problems quickly is the basis of NetView for AIX′s performance management application.

The systems performance monitoring tool provides background monitoring of the NetView for AIX workstation status and automated commands to correct problems that affect performance.

Monitoring the Network: NetView for AIX makes it possible for customers to monitor network statistics in a real-time, graphical form. The information, provided in peaks and averages, identifies trends and aids in problem tracking. In addition, the data may be viewed in several presentation styles. Data collected for managed SNMP objects may be displayed as a form, table or a graph.

MIB Application Builder: The MIB Application Builder provides the operator a point-and-click interface to build graphs or tables which dynamically display MIB variable values for whichever device is currently selected. These applications are easily integrated into NetView for AIX′s tool palette.

Gathering Historical Data: Network administrators can gather historical information about Management Information Base (MIB) variables of SNMP devices using the NetView for AIX′s MIB data collector. The data can be stored in flat files or in a relational database such as DB2/6000, Informix, Ingres, ORACLE, or Sybase. The information can then be accessed directly, printed, or saved in an ASCII format or exported in a spreadsheet format for future network planning and troubleshooting. The Xnmgraph utility that comes with NetView for AIX can also be used to display data from applications.

Defining Thresholds in the MIB: Network operators can determine what thresholds are critical for their networks and set the NetView for AIX program to poll or check for these thresholds. If a threshold is exceeded, NetView for AIX

will indicate that this event has occurred. This function provides network administrators the information they need to understand their network for planning purposes and troubleshooting.

2.8.2 End-User Interface

NetView for AIX's object-oriented graphical user interface as seen in Figure 28, is built on the OSF/Motif standard, and provides the ability to do the following:

- Invoke network configuration, fault, and performance management functions
- View and modify network maps
- Add customized or "canned" background maps
- Customize icons and colors
- Manage MIB information
- Monitor and graph network performance statistics
- View problems and changes in the network as they occur
- Access documentation online

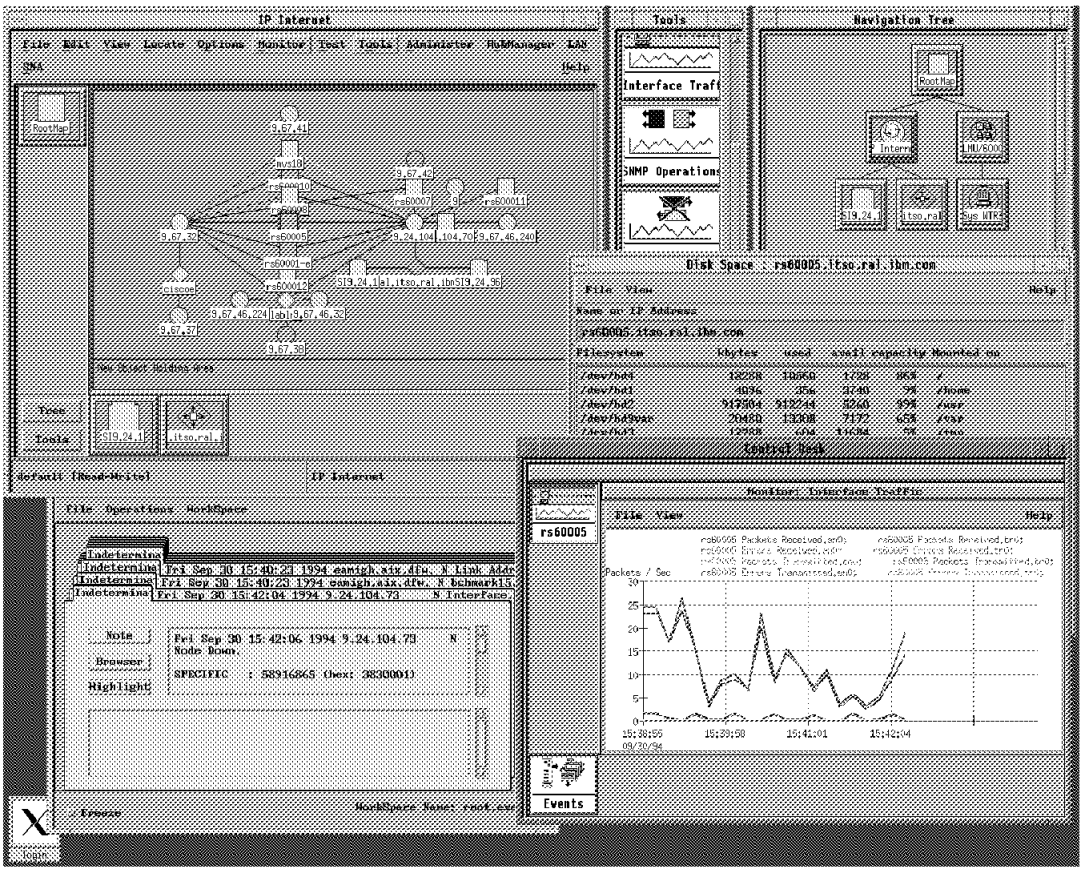


Figure 28. The Graphical User Interface of NetView for AIX

Highlights include the following:

Single Active Map Window - The network is depicted through hierarchies of submaps which include graphical representations of your network. The user can drill up and down through these submaps, including internet, network, segment, and node levels. Additional levels can easily be added. An icon

bar on the left displays parent icons from which the current view was derived, and child icons which were products of drilling through the visible submap are depicted in an icon bar below the active window. Additional submap windows can be opened at any time so that multiple windows can be viewed side by side. Submaps may be customized to represent only a certain group of objects, which may have been copied from other submaps. More than one protocol topology, each with its own submap hierarchy, can easily be displayed. Each user can have access to his own customized set of maps.

Navigation Tree - The Navigation Tree shows the hierarchy of submaps the user has drilled through. Using the icons on the Navigation Tree, the user can return to a previously opened submap by dragging that icon back to the active view window, without having to search a number of cascaded windows.

Control Desk - The Control Desk provides a place to run and group applications. Multiple applications can be running within the Control Desk simultaneously and the user can toggle between each application using the icons in the icon bar. Multiple control desks can be opened, and other applications can easily be started by dragging icons from the Tool Palette.

Tool Palette - NetView for AIX provides an iconized palette of common tools and applications for network managers. By dropping icons into a Control Desk, a user can quickly start applications.

2.8.2.1 Manager Takeover Function

This function enables the customer to define a backup NetView for AIX which will assume management responsibility for a user-defined subset of network devices, called a container. You may choose to use this when the primary NetView for AIX has failed, or when control is passed due to work shifts or time zones. The container is user-defined and can cover any subset of defined nodes.

2.8.2.2 NetView for AIX APIs

NetView for AIX APIs give the customer the ability to manage the open environment network. The following APIs are provided:

- GTM API - Allows applications that use the GTM
- XMP API - Provides SNMP and CMIP over TCP/IP (CMOT) application support based on the OSF Distributed Management Environment (DME) technology
- End-user interface API - Enables integration of vendor and customer applications with NetView for AIX′s graphical interface
- SNMP API (based on Carnegie-Mellon SNMP API) - Provides SNMP application support
- Event filtering API - Provides filter definitions and thresholding of event information sent to the events display, the NetView program, NetView for AIX applications, or your registered applications

2.8.2.3 NetView Connection

NetView for AIX, in cooperation with AIX NetView Service Point and SNA Server/6000, provides complementary network management support via an LU 6.2 interface with host NetView. Traps received from TCP/IP SNMP agents are filtered and converted to SNA alerts by NetView for AIX and then sent to host NetView via AIX NetView Service Point. NetView for AIX can then accept and execute commands from host NetView (such as the RUNCMD) and send responses back. A host NetView RUNCMD can be sent to the NetView for AIX

management station, either by an operator or through the automation table invoked programs to make use of full automation capabilities of host NetView. SNMP network management commands can be sent or shell scripts can be created and executed, to perform remote unattended operations from a central host NetView using this connection. Using the alert editor function, the user can customize the alert codepoint information and send it to host NetView.

Additionally or alternatively, NetView for AIX can manage the SNA network known to host NetView via SNA Manager/6000, a separately licensed product. SNA Manager/6000 provides a graphical view of SNA resources such as PUs, LUs, and major applications. The icon colors change as the resource status changes. Host NetView commands, such as `act` and `inact`, can be sent from the NetView for AIX end-user interface via SNA Manager/6000.

2.8.2.4 Additional Functions in NetView for AIX Version 3

Key enhancements in Version 3 are as follows:

1. Helps customers to utilize their existing relational database product for Internet Protocol (IP) topology data, SNMP collected data and logged trap data, while taking advantage of the client/server capability of the individual relational database products. The following are the databases supported in NetView for AIX:

   - IBM DB2/6000 Version 2
   - Informix Relational Database
   - Ingres Relational Database
   - ORACLE Relational Database
   - Sybase Relational Database

   The customer has the option of selecting the database support at installation.

2. Enables the customer to define a backup NetView for AIX which will assume management responsibility for any user-defined subset of network devices.

3. Provides extensive systems management with the IBM Systems Monitor System Information Agent feature.

4. Distributes network management tasks such as discovery and polling using the IBM Systems Monitor Mid-Level Manager feature, thereby reducing network traffic.

5. Provides a Systems Performance Monitoring tool for monitoring the NetView for AIX workstation resource status and provides automated commands to correct performance problems.

6. Provides full-function management of the local area network (LAN) resources with the IBM LAN Network Manager for AIX.

7. Supports the IBM Trouble Ticket for AIX V3 product which provides enhanced trouble ticketing, problem and change management, system inventory, and notification (replaces features previously available on IBM NetView for AIX and IBM NetView for AIX Entry).

8. Through a joint effort by Novell and IBM, network mapping integration, (the ability for a map of the network gathered by Novell′s NetWare Management System to be integrated with and managed by IBM′s NetView for AIX product) Novell is offering an enhancement to NMS 2.0 that exposes to NetView for AIX all discovered, mapped and user-defined information in the NMS database, including all IP, IPX, AppleTalk and DECnet nodes. IBM is

offering an enhancement to NetView for AIX that acquires and integrates NMS topology information and displays it on the NetView console.

2.8.3 Prerequisites

Hardware Requirements: The NetView for AIX licensed program runs on the RISC System/6000 POWERstations and POWERservers (including those with PowerPC card).

NetView for AIX is designed to execute with AIX/6000 on a properly configured RISC System/6000 system. It requires a TCP/IP connection and the following hardware requirements:

- Minimum 64 MB memory
- 200 MB disk space
- Color display supporting AIXwindows System Version 11 Release 5 and OSF/Motif Version 1 Release 2

  The display must support:

  – Minimum of 256 colors
  – Depth, 8 planes
  – Bits in color, 8 bits
  – Dimensions, 1280x1024 pixels

Additional hardware may be needed if connecting to NetView (see Software Announcement for details).

Software Requirements: NetView for AIX requires the following software:

- IBM AIX Version 3.2.5 for RISC System/6000
- AIXwindows Environment/6000 X-Window 11.5 and Motif 1.2

If a host NetView connection is desired, IBM AIX NetView Service Point Version 1 Release 2 and SNA Server/6000 are required.

The customer has the option of selecting any one of the following databases at installation:

- IBM DB2/6000 Version 2
- Informix Relational Database
- Ingres Relational Database
- ORACLE Relational Database
- Sybase Relational Database

2.8.4 NetView for AIX Version 4

NetView for AIX is the Network Operations Management feature of SystemView for AIX. NetView for AIX is primarily an SNMP-based management application. However it also provides platform functions that are used by many other management applications. The platform facilities that NetView for AIX provides may be summarized as follows:

Network mapping NetView for AIX provides an extensive set of APIs to allow other applications to use its topology display capabilities.

Menu registration Applications can add functions to the NetView for AIX menus. Such applications do not necessarily make use of the network mapping APIs (although many do).

Event handling NetView for AIX provides a standardized facility for processing and displaying event messages, based on SNMP traps.

Non-IP topology The open topology API simplifies the integration of other network topologies along with the IP views.

Communications Applications can also gain access to SNMP and CMOT protocols using APIs provided by NetView for AIX.

In Version 4, many enhancements have been made to NetView for AIX, affecting almost every aspect of its capabilities and use. In this section we describe examples which illustrate or exploit some of these enhancements, developed during projects at the ITSO-Raleigh center. The time available precluded us from covering all of the new features in equal depth. In this section, therefore, we will briefly introduce the enhancements before going on describe the detailed examples.

2.8.5 What′s New in NetView for AIX Version 4?

The following sections summarize the new features in NetView for AIX Version 4.

2.8.5.1 General

NetView for AIX Version 4 runs on either AIX Version 3.2.5 or 4.1.3 (or higher). When running on a Version 4.1.3 system it is compatible with the Common Desktop Environment (CDE).

NetView for AIX Version 4 is fully National Language Support (NLS) and double-byte character set (DBCS)-enabled. It is available translated into a number of languages, including Japanese and simplified Chinese.

2.8.5.2 Client/Server

The client/server support as implemented in NetView for AIX Version 4 provides the ability to distribute the graphical user interface (GUI) and the processes that support it to other RISC System/6000 AIX systems.

This has the effect of reducing load and resource demand on the server system and on the network between the server and the GUI. Where possible, application programming interfaces (APIs) are unchanged by the client/server implementation, but there may be some impact on applications, because previously they only had to be concerned with running on a single system. Such applications can run exactly as before, but it may be better to redesign them to take full advantage of the client/server environment.

2.8.5.3 GUI Improvements

The graphical user interface (GUI) of NetView for AIX Version 4 retains the same general appearance as the previous releases. However, there have been several small enhancements made to improve usability, as follows:

Navigation Tree and View Stack Enhancement: The NetView for AIX network mapping capability differs from many other similar products in that it attempts to minimize the number of windows displayed at any one time. It does this by overlaying the existing subnet display when you double-click on a symbol to

open the lower-level submap. This means that you may have many submaps open, but only have one or two of them displayed. The navigation tree and view stack are tools that allow you to easily move between open submaps. The navigation tree shows you all the open submaps and the parent-child relationships between them. The view stack shows you the parentage of the submap you are currently viewing.

Logically, each submap has one parent object. That is, when you double-click on a symbol that represents an object, the child submap of that object is opened. However, prior to Version 4, the parent of a submap was not its parent object, but the *symbol* representing that object. This had an unfortunate effect if an object had symbols on multiple submaps, since it meant that when you double-clicked on the symbol, the submap containing the parent of the new submap that you saw would not necessarily be the submap that you had just come from. In Version 4 the navigational relationships are preserved correctly.

Enhancements to Context Menus and Tool Palette: Three new functions allow an application to dynamically add menu entries to the object menu for a specific object, or to the tool palette. The function calls are OVwAddObjMenuItem, OVwAddObjMenuItemFunction and OVwAddToolPalItem. This new capability is used by the MIB Application Builder to dynamically add new monitoring applications to context menus.

There is also a new flag for tool palette registration entries that allows you to specify the order in which items appear.

Print Tool Enhancement: The print tool gives you the ability to print an image of a selected window. This tool can now be used with a color postscript printer, if you wish.

2.8.5.4 Manager Takeover Improvements

Manager takeover is a NetView for AIX function that allows you to subdivide management of the network among two or more systems. Manager takeover is not a full peer-to-peer communication system between managers, but rather a way of allowing one NetView for AIX to provide backup for another. Network container objects (such as IP subnetworks and segments) are associated with a primary and a fallback NetView for AIX. Both the primary and the fallback system have to discover the complete network, but the fallback system will have the objects in an *unmanaged* state. That is, it will not poll them. The fallback system also polls the primary system to check that it is available and, if it is not, NetView for AIX asks the user whether to manage the primary manager′s resources.

In NetView for AIX Version 4, several enhancements have been made to the way in which this process is implemented, as follows:

- Instead of monitoring to see if the whole of the system on which the primary manager is running is up, NetView for AIX now monitors an SNMP MIB table, which reports the status of the NetView for AIX daemons. There is a new SNMP subagent daemon, mgragentd, which provides this MIB table.
- There is a new submap that shows the NetView for AIX managers discovered in the network and shows their status.
- When the fallback NetView for AIX detects that the primary NetView for AIX has failed, it pops up a message asking whether the user wants to manage all the affected nodes. If the user clicks on **OK**, Version 3 would open

submaps for all the affected nodes. With Version 4 the nodes are managed without opening submaps.

- When the primary NetView for AIX returns, another pop-up asks whether the resources should be unmanaged again. In Version 3 the user had to close all submaps to achieve this, but in Version 4, click on the **Close All** button to make this more convenient.

We do not cover manager takeover in more detail in this section, but you will find a full description of the Version 3 function in *Examples Using NetView for AIX*, GG24-4327.

2.8.5.5 Security Implementation

NetView for AIX Version 4 provides new security features that enable the network administrator to keep under control who is going to use the product and the capabilities of each user.

The facilities provided include the following:

- User authentication
- Controlled access to all NetView for AIX Version 4 items:
  - Menu bar
  - Context menu
  - Tool palette
  - Command line commands
- Auditing
- Customization
- Integration of user-written programs

2.8.5.6 Event Rulesets

The processing of events in NetView for AIX is completely changed in Version 4, by the introduction of event rulesets. These provide the following capabilities:

- Correlation between different events, or the ability to treat two related events as one trigger
- Read and write access to additional information, external to the event stream itself (for example, the object database, MIB data and global variables)
- An override capability so that event severity and node status may be dynamically modified
- For all of these features, the ability to trigger on and have access to any of the information carried within the event

2.8.5.7 Event Display Enhancements

There are several changes to the event display application, nvevents, in NetView for AIX Version 4, as follows:

- Integration of event rulesets. Correlation and filtering can now be done using ruleset processing. The filtering capability of Version 3 is still supported, but it has been functionally superseded by rulesets.
- Support for the client/server implementation. The event display application, nvevents, can now run on distributed client systems. This is achieved by means of a new daemon, nvserverd, with which each copy of nvevents

establishes a socket connection. The nvserverd daemon is then responsible for distributing events as they arrive.

- Synchronization between different users. Prior to Version 4, any actions that a user made against events in an nvevents workspace were not seen by other users. Specifically this applied to adding notes or clearing events from the display. With Version 4 these changes can be broadcasted to all other NetView for AIX users. In addition, a user can make a severity or category change to an event, and it will also be reflected in all users′ displays.
- Color-coded card tabs. The card format event display now has a colored tab on the top of which indicates the severity of the event. The mapping of colors to severity is controlled by X-Windows resources. At the time of writing, the list format of the event display did not have color coding, but it was a planned enhancement.

2.8.5.8 Object Collection Facility

The object collection facility as implemented in NetView for AIX Version 4 provides important enhancements to the organization of network management. Collections can be created of nodes with similar characteristics, such as hardware, network address or object database information.

There are two tools provided with the object collection facility: the graphical user interface (GUI) and the collection APIs. The first supports all functions needed by the user to create, test, modify, and delete any collection. The second one is helpful in implementing applications that use collections features.

2.8.5.9 Agent Policy Manager

The agent policy manager is a new feature of NetView for AIX Version 4 which simplifies the configuration and management of Systems Monitor agents.

2.8.5.10 Intention to Support SNMP Version 2

As part of the announcement of NetView for AIX Version 4, a statement of direction was made that SNMPv2 will be supported in the near future. The main reason for the delay of this support is the unfortunate confusion over the security aspects of the new SNMP Version 2 standards.

NetView for AIX Version 4 will use a dual stack approach, providing a WINSNMP API implementation to allow applications to have transparent access to SNMP Version 1 and Version 2 agents, while at the same time preserving the current OVSNMP API.

2.9 Nways Campus Manager ReMon for AIX/HP

The Nways Campus Manager ReMon for AIX/HP provides full RMON management support for RMON-compliant agents for medium-to-large customers who use a UNIX-based management platform to manage their network devices. Similarly, the Nways Campus Manager ReMon Advance for AIX/HP package is also targeted for medium-to-large customers with UNIX-based management systems. The advance package offers added stress testing and collecting additional LAN statistics in addition to full RMON support.

RMON is designed for remote or distributed LAN performance monitoring. RMON probes and managers are supposed to be the one-stop alternative giving

network managers a way to keep a weather eye on their networks from the data center.

The Nways Campus Manager ReMon advance for AIX/HP package includes the base offerings plus a TTMM and an ECAM that can be downloaded to remote probes in the network. The advance package also includes the TTMM and ECAM client software.

The TTMM module helps managers identify causes of problems by generating particular types of packets or sequences of packets onto remote LANs or recreating problems that occurred between particular communication pairs. The ECAM module is used for monitoring protocols and applications. The TTMM and ECAM clients provides the graphical software that runs on your AIX or HP workstation.

This program should be considered by customers with medium to large campus networks with large branch offices, such as banks or insurance companies, as a standards-based client/server solution for remote monitoring of Ethernet and token-ring LANs. Nways Campus Manager ReMon for AIX and the advance package not only perform all of the functions of a protocol analyzer, it's also a standards-based tool set that can be extended to perform other LAN management tasks over time.

The Nways Campus Manager Remote provides the following generic functions:

- Full RMON support for token-ring and Ethernet LANs
- Summary screen gives you a high-level view of the entire LAN segment or ring
- Rapid fault discovery and response for identifying and solving network faults
- Graphical software for analyzing data and packets collected by remote probes

2.9.1 Supported Standards

The Nways Campus Manager Remote supports the following:

- SNMP (RFC 1155, RFC 1157, RFC 1212, RFC 1213)
- IETF RMON 1 Working Group RFC 1757 (formerly 1271) and 1513

2.9.2 Product Positioning

This program is applicable for campus network environments and to companies that occupy several buildings in a campus environment.

If you have campus networks and want the advantages of being able to troubleshoot all LANs from one central workstation, Nways Campus Manager Remote Monitor lets experts work on several problems at once or troubleshoot a problem at more than one location.

2.9.3 Technical Information

2.9.3.1 Hardware Requirements

- RISC System/6000
- Base Package -- 70 MB
- Advance Package -- Base + 23 MB

2.9.3.2 Software Requirements

- AIX 3.2.5, or later
- Motif 1.2
- NetView for AIX 3.0, or later

2.9.4 Publications

The following hardcopy publications will be delivered with the product:

- *Nways Campus Manager Remote Monitor Installation and User's Guide (LAN ReMon AIX/HP only)*, SA33-0367.
- *Nways Campus Manager Remote Monitor Traffic Transmission Management Module User's Guide*, SA33-0369.
- *Nways Campus Manager Remote Monitor Enterprise Communication Analysis Module User's Guide*, SA33-0368.

2.10 Nways Campus Manager LAN for AIX

Nways Campus Manager LAN for AIX is an advanced package of integrated network management applications that provides optimal and extensible management of your traditional campus network.

Nways Campus Manager LAN enables complete management of your Ethernet, token-ring, or FDDI-based campus network composed of hubs, LAN switches, bridges, and concentrators. Nways Campus Manager LAN also provides complete management of IBM (and selected non-IBM) routers.

Nways Campus Manager LAN package of integrated applications includes the following proven network management applications:

- Intelligent Hub Management V2 program for managing 8250 and 8260 hubs
- Router and Bridge Management V1R2 program for managing 6611 and 2210 routers, as well as other non-IBM routers
- Device-specific applications that support 8224, 8230, 8271 (Models 001/108), 8272, 8238 and 8281

Nways Campus Manager LAN package features the following:

- Seamless navigation between Nways Campus Manager LAN for AIX and SystemView for AIX
- Device management functions for creating device-specific topology maps
- Member of the SystemView Family, fully integrated with NetView for AIX (V3 or V4) feature of SystemView for AIX

Nways Campus Manager LAN should be considered by customers who need to manage medium to large campus networks (containing one or more of the

aforementioned campus hubs, routers, or switches) using the high-end NetView for AIX (V3 or V4) feature of SystemView for AIX.

2.10.1 Product Overview

The Nways Campus Manager LAN provides device configuration and network topology views that enable administrators to quickly determine the state of the network and its components. Performance and fault management allow control and monitoring at the port and device level. The integrated router management also provides control and monitoring for routed protocols (SNA-APPN, IP, IPX, AppleTalk, and Banyan Vines). Nways Campus Manger LAN, combined with the NetView for AIX (V3 or V4) feature of SystemView for AIX, allows you to manage your campus environments from a single operator console on your AIX workstation.

2.10.1.1 Continuous Monitoring

Campus devices (for example, hubs, LAN switches, concentrators, and routers) are automatically discovered, mapped, and monitored. When the network changes, the discovery capability indicates the changes and updates your network map.

2.10.1.2 Improved Reliability

System reliability is increased through cooperative management with NetView for AIX feature of SystemView for AIX. Nways Campus Manager LAN interoperates with the NetView for AIX feature of SystemView for AIX for the quick recognition of network management information from different sources. The results are improved response time for error conditions, resulting in improved network availability.

2.10.1.3 User Productivity

Nways Campus Manager LAN takes advantage of the NetView for AIX feature of SystemView for AIX open systems computing environment in some of the following ways by:

- Integrating its topology into the NetView for AIX feature of SystemView for AIX topology displays
- Providing a common format for graphical interface panels
- Supplying the NetView for AIX feature of SystemView for AIX event log and other event-monitoring applications with device-specific alarm information

2.10.1.4 Resource Monitoring

Nways Campus Manager LAN enables you to easily monitor the following network resources:

- Devices (hubs, switches, concentrators, routers)
- Concentration modules
- Ports
- Routed protocols

The graphical topology display and other resource views use specific colors to represent the status of resources displayed in submaps. If a resource becomes inactive or its operation becomes impaired, you receive notification. The submap or the view is updated to reflect the change in status of the resource by a change in the resource′s color.

2.10.1.5 Performance Information

Nways Campus Manager LAN enables you to select key performance counters and to track their variations over time for the three LAN protocols (FDDI, Ethernet, and token-ring) on any segments, for routed protocols (SNA-APPN, IP, IPX, Banyan Vines, and AppleTalk), and for source routed and transparent bridges. This data may be stored and displayed in various graphical forms across a selected time interval. The availability of performance information from Nways Campus Manager LAN also enhances the network by facilitating performance refinements and network tuning.

2.10.1.6 Performance Information

Nways Campus Manager LAN provides extensive control over campus devices (hubs, switches, concentrators, bridges, and routers). The Nways Campus Manager LAN provides easy access to various submap levels (network, device, module, and port), allowing users to set and change device, module, or port configurations.

2.10.1.7 Change Management

Nways Campus Manager LAN provides a quick way to download code upgrades in the campus devices through the network itself, and then allow easy problem fixes or function migration on specific devices.

2.10.1.8 Fault Management

Nways Campus Manager LAN provides a complete set of messages, traps, and event notifications. The integration of this information into the NetView for AIX feature of SystemView for AIX Event Log enables retrieval and more efficient problem determination, especially in a multiprotocol environment. You can customize the events to reduce the amount of information and to manage large networks efficiently.

2.10.2 Supported Standards

Nways Campus Manager LAN supports the following industry standards, as understood and interpreted by IBM as of September 1994.

- RFC854 - Telnet protocol
- RFC1084 - BOOTP
- RFC1350 - Trivial file transfer protocol (TFTP)
- SNMP:
  - RFC1155 - Structure and Identification of Management Information (SMI) for TCP/IP-based Internet
  - RFC1157 - Simple Network Management Protocol (SNMP)
  - RFC1213 - Management Information Base (MIB) for Network Management of TCP/IP-based Internets (MIB-II)
- FDDI:
  - RFC1285 - FDDI MIB updated by RFC1512
  - RFC1512 - FDDI MIB
  - SMT 7.3
- Token-Ring:
  - RFC1231 (1239) - IEEE 802.5 Token-Ring MIB
- Bridges

  - RFC1286 - Definitions of managed objects for bridges
  - RFC1398 (former RFC1284) - Definitions of managed objects for Ethernet-like interfaces
- Routed Protocols
  - RFC 1234 - AppleTalk MIB
  - RFC 1289 - DECnet Phase IV MIB extensions

Nways Campus Manager LAN demonstrates IBM′s commitment to provide standards-driven products that satisfy customer requirements for developing consistency with Distributed Management Environment (DME) OSF/Motif-based user interface X-Window.

2.10.3 Product Positioning

Nways Campus Manager LAN is an integrated package of network management applications (including Intelligent Hub Manager for AIX V2, Route and Bridge Manager/6000, and IBM-specific campus device management) and is intended to replace individual, stand-alone, applications that manage traditional (Ethernet, token-ring, and FDDI) campus networks.

Nways Campus Manager LAN manages the following hardware:

- 8260 Release 1 (all modules)
- 8260 Release 3.5:
  - Ethernet Monitor card
  - DMM Release 2.2/2.3
- 8250 Release 1 to 9 (all modules)
- 6611 Network Processor Models 120, 125, 145, 175
- 2210 Nways Multiprotocol Router Models 121-128
- 8224 Ethernet Stackable Hub Models 001, 002
- 8230 Token-Ring Concentrator Models 003, 013, 213, 004A, 004P
- 8271 EtherStreamer Switch Models 001, 108
- 8272 LANStreamer Switch Model 108
- 8238 Nways Token-Ring Stackable Hub
- 8281 ATM LAN Bridge

Nways Campus Manager LAN covers the high-end AIX segment of the campus network management market, while Nways Manager for Windows covers the low-end Windows segment for the same network environment.

A key benefit of Nways Campus Manager LAN is the NetView for AIX (V3 or V4) feature of SystemView for AIX integration which leverages the platform functions mainly for topology, fault/event monitoring, and EUI consistency.

As a member of the SystemView Family, this product is fully integrated with the NetView for AIX feature of SystemView for AIX.

2.11 Nways Campus Manager ATM for AIX

Nways Campus Manager ATM for AIX is a state-of-the-art network management application package to manage your campus ATM network and provides the following:

- ATM Campus Manager for AIX
- Device management for 8281 and 8282
- Seamless navigation between ATM Campus Manager and device management applications
- ATM device management and graphical ATM connection tracking
- Member of the SystemView Family, fully integrated with NetView for AIX (V3 or V4) feature of SystemView for AIX

Nways Campus Manager ATM integrates ATM Campus Manager with device management applications that supports various ATM devices including:

- 8282 ATM Workgroup Concentrator

Complete 8260 device management is available when Nways Campus Manager ATM is installed with Nways Campus Manager LAN.

New ATM management functions provided with Nways Campus Manager ATM include the graphical display of ATM connections within an ATM switch allowing connection tracking to be performed. Nways Campus Manager ATM contains integrated network management support including:

- Nways ATM Campus Manager for AIX V1R1
- Device-specific applications that support 8281 and 8282

Nways Campus Manager ATM should be marketed to customers who need to manage medium to large campus ATM networks (containing one or more of the mentioned campus chassis hubs, bridges, or concentrators) using the high-end NetView for AIX (V3 or V4) feature of SystemView for AIX.

Nways Campus Manager ATM contains additional function over ATM Campus Manager and maintains a competitive price.

Nways Campus Manager ATM should be considered by customers who need to manage medium-to-large campus ATM networks (containing one or more of the mentioned campus chassis hubs, bridges, or concentrators) using the high-end NetView for AIX (V3 or V4) feature of SystemView for AIX.

Nways Campus Manager ATM contains additional function over ATM Campus Manager.

2.11.1 Product Overview

Nways Campus Manager ATM provides device configuration and ATM network topology views that enable administrators to quickly determine the state of the network and its components. Performance and fault management, also provided by Nways Campus Manager ATM, allow control and monitoring at the port and device level. Combined with the NetView for AIX (V3 or V4) feature of SystemView for AIX, Nways Campus Manager ATM allows you to manage your

campus ATM environments from a single operator console on your AIX workstation.

2.11.1.1 Continuous Monitoring

With the Nways Campus Manager ATM discovery function, campus devices (for example, hubs, concentrators, and bridges) are automatically discovered, mapped, and monitored. When the network changes, the discovery capability indicates the changes and updates your network map.

2.11.1.2 Improved Reliability

System reliability is increased through cooperative management with NetView for AIX feature of SystemView for AIX. Nways Campus Manager ATM interoperates with NetView for AIX feature of SystemView for AIX, which allows for the quick recognition of network management information from different sources. Improved response time for error conditions results in improved network availability.

2.11.1.3 User Productivity

Managing your campus network from a central point saves time and money. Nways Campus Manager ATM also improves productivity by its integration as a single package.

Nways Campus Manager ATM takes advantage of NetView for AIX feature of SystemView for AIX open systems computing environment in some of the following ways by:

- Integrating ATM topology into the NetView for AIX feature of SystemView for AIX topology displays
- Providing a common format for graphical interface panels
- Supplying the NetView for AIX feature of SystemView for AIX event log and other event-monitoring applications with hub-specific alarm information

2.11.1.4 Resource Monitoring

The graphical topology display and other resource views use specific colors to represent the status of resources displayed in submaps. If a resource becomes inactive or its operation becomes impaired, you receive notification. The submap or the view is updated to reflect the change in status of the resource by a change in resource's color.

2.11.1.5 Performance Information

Nways Campus Manager ATM enables you to select key performance counters and to track their variations over time for campus ATM networks. This data may be stored and displayed in various graphical forms across a selected time interval. The availability of performance information from Nways Campus Manager ATM also enhances the network by facilitating performance refinements and network tuning.

2.11.1.6 Configuration Information

Nways Campus Manager ATM provides extensive control over campus ATM devices. The Nways Campus Manager ATM applications provide easy access to various submap levels (ATM network, device, module, and port), allowing users to set and change device configuration, module configuration, or port configuration.

2.11.1.7 Change Management

Nways Campus Manager ATM applications provide a quick way to download code upgrades in the campus devices through the network itself and then allow easy problem fixes or function migration on specific devices.

2.11.1.8 Fault Information

Nways Campus Manager ATM applications provide a complete set of messages, traps, and event notifications. The integration of this information into the NetView for AIX feature of SystemView for AIX program enables retrieval and more efficient problem determination, especially in a multiprotocol environment. You can customize the events to reduce the amount of information and to manage large networks efficiently.

2.11.2 Supported Standards

Nways Campus Manager ATM applications support the following industry standards, as understood and interpreted by IBM as of September 1994.

- RFC854 - Telnet protocol
- RFC1084 - BOOTP
- RFC1350 - Trivial file transfer protocol (TFTP)
- SNMP:
  - RFC1155 - SMI for TCP/IP-based Internet
  - RFC1157 - SNMP
  - RFC1213 - MIB for Network Management of TCP/IP-based Internets (MIB-II)
- ATM
  - RFC 1695 ATM MIB
  - ATM UNI 3.1 for ILMI from ATM Forum

Nways Campus Manager ATM demonstrates IBM′s commitment to provide standards-driven products that satisfy customer requirements for developing consistency with DME OSF/Motif-based user interface X-Window.

2.11.3 Product Positioning

Nways Campus Manager ATM is an integrated package of network management applications (including ATM Campus Manager and campus ATM device management) and is intended to replace individual, stand-alone, applications that manage ATM campus network.

Nways Campus Manager ATM allows management of the following hardware:

- 8260 Models A10, A17
  Complete device management of the 8260 (including power supply and temperature) requires Nways Campus Manager LAN to be installed with Nways Campus Manager ATM. Nways Campus Manager ATM is focused on management of the 8260s ATM components.
- 8281 ATM LAN Bridge Model 001
- 8282 ATM WorkGroup Concentrator Model 001

Nways Campus Manager ATM covers the high-end AIX segment of the campus ATM network management market, while Nways Manager for Windows covers the low-end Windows segment for the same network environment.

A key benefit of Nways Campus Manager ATM is the NetView for AIX (V3 or V4) feature of SystemView for AIX integration which leverages the platform functions mainly for topology, fault/event monitoring, and EUI consistency.

As a member of the SystemView Family, this product is fully integrated with the NetView for AIX feature of SystemView for AIX.

2.12 Nways Campus Manager Suite for AIX

Nways Campus Manager Suite for AIX is a powerhouse suite that combines all the applications needed to manage your traditional and ATM campus networks, and includes a remote networking monitoring (RMON) application. This suite contains:

- Nways Campus Manager Remote Monitor
- Nways Campus Manager LAN
- Nways Campus Manager ATM

Nways Campus Manager Suite should be considered by customers who need to manage medium to large campus networks containing both traditional and ATM networks, using the high-end NetView for AIX (V3 or V4) feature of SystemView for AIX.

2.12.1 Product Overview

Nways Remote Monitor Advanced provides complete RMON management of Ethernet and token-ring networks (13 token-ring and 9 Ethernet groups). In addition, network layer protocols management and traffic generation tools are provided.

2.12.2 Supported Standards

Nways Campus Manger Suite applications support the same industry standards, as described under the Nways Campus Manager ReMon , Nways Campus Manager LAN and Nways Campus Manager ATM sections.

Nways Campus Manager Suite demonstrates IBM′s commitment to provide standards-driven products that satisfy customer requirements for developing consistency with DME OSF/Motif-based user interface X-Window.

2.12.3 Product Positioning

Nways Campus Manager Suite is a suite of network management applications (including Nways Campus Manager LAN, Nways Campus Manager ATM, and Nways Campus Manager Remote Monitor Advance) for traditional and ATM campus networks and is intended to bundle together all the network management applications into one comprehensive package for ease of ordering.

Nways Campus Manager Suite covers the high-end AIX segment of the campus network management market, while Nways Manager for Windows covers the low-end Windows segment for the same network environment.

2.12.4 Technical Information

The following text details the hardware and software requirements for Nways Campus Manager Suite for AIX.

2.12.4.1 Hardware Requirements

Nways Campus Manager LAN, Nways Campus Manager ATM, and Nways Campus Manager Suite run on the RISC System/6000 POWERstations and POWERservers.

They are designed to execute with the NetView AIX (V3 or V4) feature of SystemView for AIX on a properly configured RISC System/6000 system. It requires a TCP/IP connection and the following hardware requirements:

- An IBM-compatible mouse
- Additional minimum 64 MB memory
- Minimum 33 MHz processor speed (50 MHz recommended)
- A 256-color (8-bit planes) display device supporting a compatible X-Window System V11 R5 compliant interface. (Must support 8-bit planes, or more, if you want to use geographic maps with NetView for AIX.)
- Free disk space
  - Nways Campus Manager LAN minimum 90 MB
  - Nways Campus Manager ATM minimum 30 MB
  - Nways Campus Manager Suite minimum 203 MB

2.12.4.2 Software Requirements

The Nways Campus Manager LAN and Nways Campus Manager ATM require the following:

- SystemView for AIX: NetView 3.1 for AIX feature or NetView 4.1 for AIX feature. Refer to Software Announcement 295-395, dated July 25, 1995.
- AIX V3.2.5 or V4.1 for RISC System/6000. Refer to Software Announcement 295-355, dated July 25, 1995.
- AIXwindows Environment/6000 (5601-257) with the then current release at the planned availability date.
- X-Window System V11 R5.
- Motif 1.2.
- SystemView NetView for AIX feature, V3 PTF U438566 or for V4, PTF U439028 for Management Application Transport (MAT) function.

The Nways Campus Manager Suite requires the following:

- SystemView for AIX: NetView 3.1 for AIX feature or NetView 4.1 for AIX feature. Refer to Software Announcement 295-395, dated July 25, 1995.
- AIX V3.2.5 or V4.1 for RISC System/6000. Refer to Software Announcement 295-355, dated July 25, 1995.
- AIXwindows Environment/6000 (5601-257) with the then current release at the planned availability date.

- X-Window System V11 R5.
- Motif 1.2.

2.12.4.3 Compatibility

These products use only existing external interfaces.

2.12.4.4 Performance Considerations

For optimum performance, 128 MB free disk space is recommended for a swapping requirement.

2.12.4.5 Planning Information

Nways Campus Manager LAN, Nways Campus Manager ATM, and Nways Campus Manager Suite installation procedures are supplied to be run from a System Management Interface Tool (SMIT) menu to provide quick and easy installation.

Nways Campus Manager LAN, Nways Campus Manager ATM, and Nways Campus Manager Suite can be installed while the NetView for AIX feature of SystemView for AIX program remains running. This program can be started or halted without affecting the NetView for AIX feature of SystemView for AIX operations.

2.12.5 Summary

The Nways Campus Manager LAN, Nways Campus Manager ATM, and Nways Campus Manager Suite are software packages of network management applications that remotely control and monitor traditional campus networks (for example, Ethernet, token-ring, FDDI) and campus ATM networks.

2.12.6 Publications

Nways Campus Manager LAN and Nways Campus Manager ATM contain softcopy documentation.

Nways Campus Manager Suite contains the following hardcopy documentation:

- *Nways Campus Manager Remote Monitor Installation and User's Guide (LAN ReMon AIX/HP only)*, SA33-0367.
- *Nways Campus Manager Remote Monitor Traffic Transmission Management Module User's Guide*, SA33-0369.
- *Nways Campus Manager Remote Monitor Enterprise Communication Analysis Module User's Guide*, SA33-0368.

2.13 LAN Network Manager for AIX

LAN Network Manager (LNM) for AIX is integrated with the NetView for AIX program to enable you to effectively manage the LAN resources of your network. Figure 29 on page 135 shows an integrated view of the LNM for AIX LAN topology. This enables you to extend the reach of NetView for AIX to include SNMP bridge, SNMP token-ring, FDDI and non-SNMP token-ring environments.

The LNM for AIX program in conjunction with agents provides views of a physical topology of the LAN, using the NetView for AIX GTM APIs to integrate the physical LAN topology with IP topology. This integration enables the

protocol switching function of NetView for AIX. Protocol switching provides a fast path among domains represented. The LNM for AIX program also provides configuration, fault and performance information for your LAN resources.

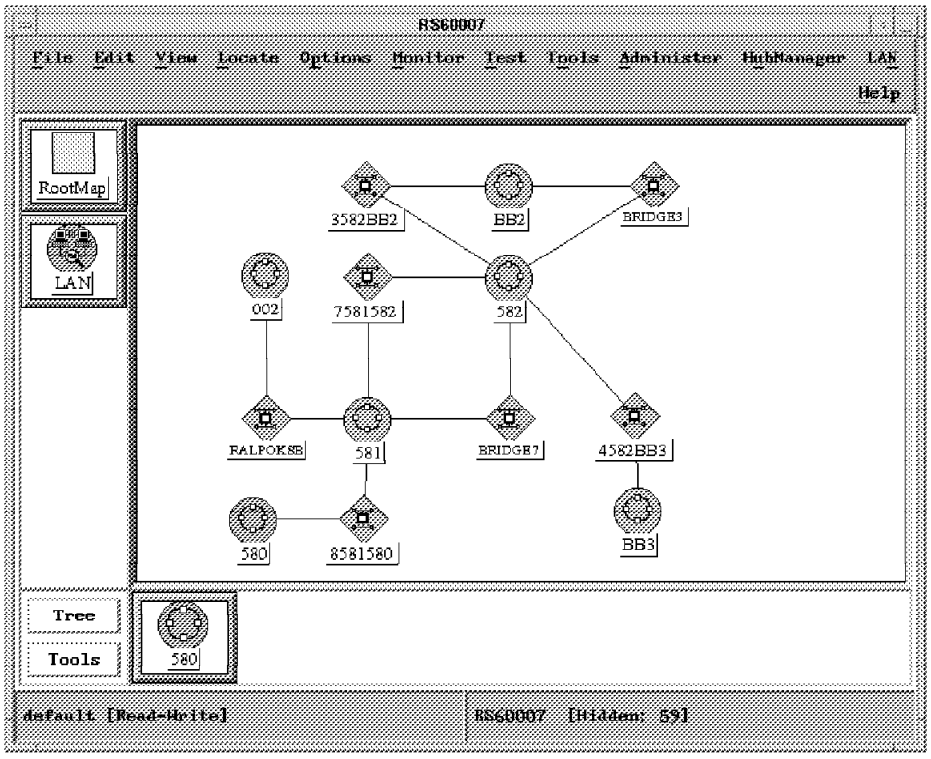


Figure 29. LNM for AIX LAN Topology Display

2.13.1 Technical Description

With LNM for AIX, you can view FDDI, token-ring and Ethernet LAN segments interconnected by bridges using X.25, Frame Relay, DS1, RS-232, token-ring, or Ethernet. Each of these views is called a subnet. A subnet consists of related symbols that are displayed in a single window. Multiple subnets are displayed in a submap.

As with any NetView for AIX application, LNM for AIX events are displayed as event cards in the Control Desk and can thus open incidents in Trouble Ticket for AIX. These can also be converted to alerts and forwarded to host NetView, if desired.

LNM for AIX comprises several applications to manage the physical layer of token-ring environments.

In addition, you can view the topology of FDDI and token-ring segments, manage devices such as the IBM 8230 Token-Ring Concentrator, IBM 8244 Workstation Group Concentrator, and manage the IBM 8250 and IBM 8260 Intelligent Hubs when coupled with IBM Intelligent Hub Manager for AIX.

2.13.1.1 SNMP LAN Segment Management

LAN Network Manager for AIX will graphically display the physical interconnection of bridges and LANs and analyze the MIB information to determine the status and media type of the LAN segment. Unique icons for FDDI, Ethernet and token-ring LANs are shown along with the bridge icons that connect them. If the FDDI or token-ring segments are managed by LNM for AIX using the FDDI application of LNM for AIX or the SNMP token-ring application of LNM for AIX, the subnet view will indicate the status of the segment based on all the devices within that segment. Otherwise, if the SNMP bridge agent supports RFC 1231, the status of the segment will be reflected based on the information from RFC 1231. Icons will change color according to:

- SNMP traps indicating a resource has become inactive
- Return of the resource to the network
- Resources that cannot be managed because of inadequate SNMP MIB support in the agent

From the LAN subnet view the user can open a token-ring or FDDI LAN segment submap. Provided that the required IP-address definitions had been made, LNM for AIX will automatically discover certain SNMP agents, including SNMP proxy agents for FDDI concentrators, IBM 8250 and 8260 hubs, RMON agents, and the SNMP-managed IBM 8230 Models 3 and 013 Controlled Access Unit (CAU). Concentrators and hubs are indicated with a unique icon. Color-coding of the icons within the segment view represents the operational status of these devices.

2.13.1.2 SNMP Bridge Management

Another feature of LNM for AIX is its bridge management application. This application enables you to manage source routed and/or transparent bridges that support MIB II and RFC 1286 (or RFC 1525 and RFC 1493) including IBM bridges such as:

- The Ethernet and token-ring bridge modules of the 8250 and 8260 Intelligent Hubs
- The 8229 Token-Ring to Token-Ring or Token-Ring to Ethernet Bridge
- The 6611 Network Processor in bridging mode
- IBM 2210
- IBM 8271
- OEM bridges

In addition, LNM for AIX will provide interface information if the bridge supports any of the following MIBs:

- RFC 1284 - Ethernet
- RFC 1231 - Token-Ring
- RFC 1315 - Frame Relay
- RFC 1232 - DS1
- RFC 1317 - RS232
- RFC 1381 - X.25 LAPB
- RFC 1382 - X.25 Packet

You can display a submap showing a graphical representation of a bridge, and display profile, configuration, fault, and performance information for bridges and bridge ports. You can display and change specific information about the SNMP bridges as well as modify values for the spanning trees. Performance information includes frames transmitted and received, the total number of frames and the frame ratio, as well as source routing traffic analysis for specific routing paths. Bridge fault information displays the number of discarded frames for the selected bridge, categorized by the reason the frames were discarded, and the ratio of discarded frames to total traffic.

2.13.1.3 FDDI LAN Management

Using LNM for AIX you can monitor and manage FDDI resources in your network. Management is offered for devices that support levels 6.2 and 7.3 of the FDDI station management (SMT) standard that is defined by the American National Standards Institute (ANSI). You can manage both single and dual-attached stations, as well as concentrators or hubs that support SMT 6.2 or 7.3. The IBM FDDI SNMP proxy agent on the FDDI LAN is required to accept the instructions from LAN Network Manager for AIX and to obtain status and change information pertaining to the FDDI resources. The FDDI proxy agent also converts status reporting frames (SRFs) from the FDDI segment into SNMP traps and passes them on to the LNM for AIX application. LNM for AIX allows you to:

- Concurrently manage multiple FDDI segments
- Manage FDDI stations that support parameter management frames
- Manage concentrators/hubs that support SMT 6.2 and 7.3.

LNM for AIX provides bit maps for the IBM 8240 FDDI Concentrator, IBM 8244 FDDI Workstation Group Concentrator, and a generic FDDI concentrator bit map for OEM FDDI concentrators.

2.13.1.4 Management of SNMP Token-Ring Resources

LAN Network Manager for AIX also provides management of token-ring segments, down to the adapter level, for the following SNMP agents:

- IBM Token-Ring Surrogate Agents implemented through IBM′s Architecture Working Paper 7607 (AWP7607), available with the IBM 8229 Bridge and IBM 8260 Intelligent Hub
- Remote Monitor (RMON) agents that implement the ring station groups defined in RFC 1513 (as provided by the IBM RMON agent in the IBM 8260 Intelligent Hub)
- The IBM 8230 Model 3 CAU′s vendor-specific MIB

Included in the token-ring LAN segment management feature of LNM for AIX are the following functions:

- Display of network devices in NAUN order indicating in color the resource status.
- Display of segment profile, configuration, fault and performance information.
- Critical resource monitoring of SNMP agents and/or MIB variables.
- Time-of-day access control at the adapter level.
- Graphical box management of token-ring concentrators such as the IBM 8230 Model 3 (including fault, configuration, and Remote Program Load support).

- Protocol switching to another NetView for AIX-enabled application that offers additional management views of a network resource through a different view (such as the IP node view).

2.13.1.5 Management of Non-SNMP Token-Ring Resources

Before SNMP, IBM′s token-ring devices used their own management flows. They take advantage of the management intelligence inherent in the token-ring architecture along with logical link control flows and proprietary management such as is offered with IBM′s LAN Network Manager product that runs on an OS/2 workstation. This management protocol can be found in the following IBM products:

- 8230 Models 1 and 2 Controlled Access Units (see Figure 30)
- Token-ring networking DOS bridges
- 8209/8229 Token-Ring to Token-Ring and Token-Ring to Ethernet bridge.
- Token-ring adapter cards

Included in the LAN Network Manager for AIX product is support for the proxy agent included in IBM′s LAN Network Manager for OS/2 V2. By carrying some of management intelligence of LNM across a TCP/IP network, LNM for AIX will be able to isolate much of the management traffic overhead to the remote LAN and provide centralized control of these LANs through the same application that supports the SNMP managed agents. An LNM for OS/2 managed domain will appear as one IP node to NetView for AIX, representing the OS/2 workstation running LAN Network Manager.

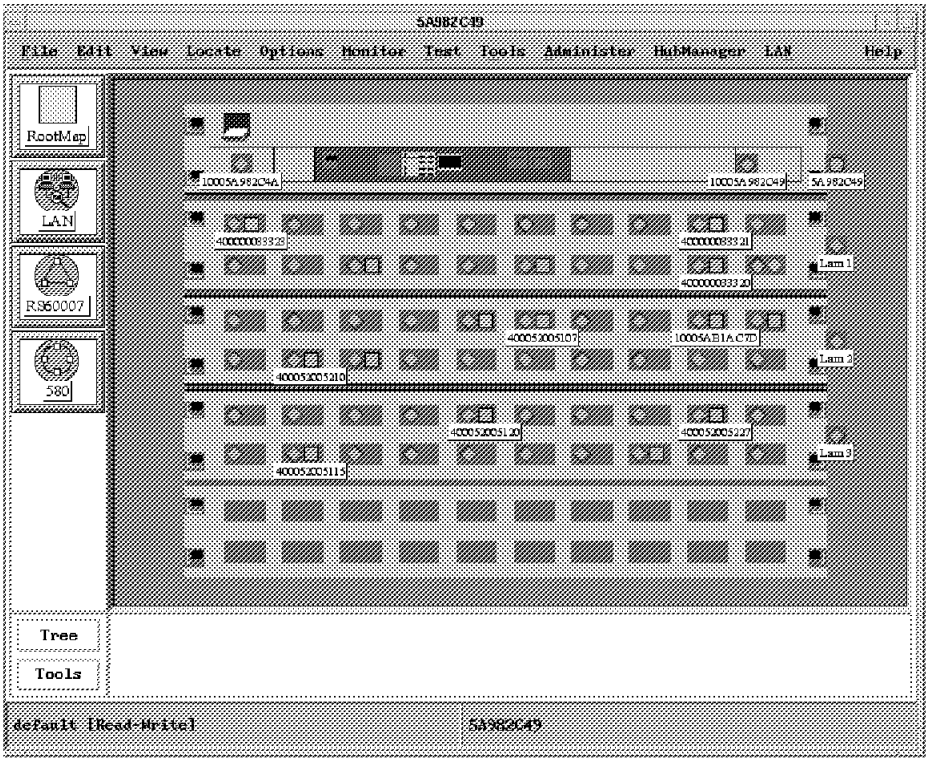


Figure 30. LNM for AIX Display of an 8230 Model 1

2.13.2 Prerequisites

The following are the hardware and software requirements for LAN Network Manager for AIX:

Hardware Requirements: The LNM for AIX licensed program product runs on the RISC System/6000 POWERstations and POWERservers. LNM for AIX is designed to execute with NetView for AIX on a properly configured RISC System/6000 system. It requires the following hardware:

- A minimum of 128 MB of available memory is recommended for NetView for AIX and LNM for AIX together to manage a medium size non-IP network with only NetView for AIX and LNM installed. Additionally, paging space three times real memory is recommended.
- The display device must support 8-bit planes or more if using LNM for AIX for geographic maps.
- 96 MB minimum of disk space. It is recommended that this be a separate logical volume for LNM for AIX. After the install, most of the data will actually be in files under the /usr/OV directory since LNM integrates into the ovw database, receives and logs trap traffic (/usr/OV/log/trapd.log), and nettl logs (/usr/OV/log).

  The actual amount for free disk space and RAM required depend on the size of the network you are managing, the number of other applications and XStations you are supporting, the NetView for AIX tuning options you are using, and the number of LNM for AIX applications you are using. 16 MB of real memory is the minimum RAM requirement for the LNM for AIX program itself. If you are using more than one LNM for AIX management application, this requirement will increase.

Software Requirements: LNM for AIX requires the following software:

- IBM AIX Version 3 Release 2.5
- AIX NetView/6000 Version 2 or higher with the latest PTFs

  Note: If LNM for AIX is purchased within IBM SystemView for AIX, then NetView for AIX Version 3.1 is required.
- AIXwindows Environment
- Motif 1.1 or higher

2.13.3 Related Publications

In addition to the list of publications that is provided in the preface section of this book, this list is made available to point out some additional publications that are available for a more detailed discussion of LNM for AIX:

- ITSO Redbooks
  - *LAN Management Using LNM for OS/2 V2.0 and LNM for AIX*, SG24-2504
- Product publications
  - *Installing LAN Network Manager for AIX*, GC31-7114
  - *Getting Started with LNM for AIX*, SC31-7109
  - *Using LNM for AIX*, SC31-7110
  - *LNM for AIX Reference*, SC31-7111

2.14 LAN Management Utilities/6000 (LMU/6000)

As networks grow in both size and variety and with the number of suppliers and networking protocols increasing at a rapid pace, LMU/6000 helps to manage your heterogeneous environments from a single NetView for AIX management station. LMU/6000 expands the management capability you get from NetView for AIX by providing support for clients and servers on your Novell and IBM PC LAN networks.

Resource savings can be realized through LMU/6000 because management resources and skills can be concentrated at a single location instead of spreading them out throughout the network.

LMU/6000 gives you control over the LMU-managed resources in your network. LMU/6000 is fully integrated with NetView for AIX and thus benefits from the NetView features. Figure 31 shows the integration of LMU/6000 into NetView for AIX. System status displays graphically; easy-to-identify icons represent your network and color indicates status. The extensive functions and available tools from NetView for AIX give you complete control of your network.

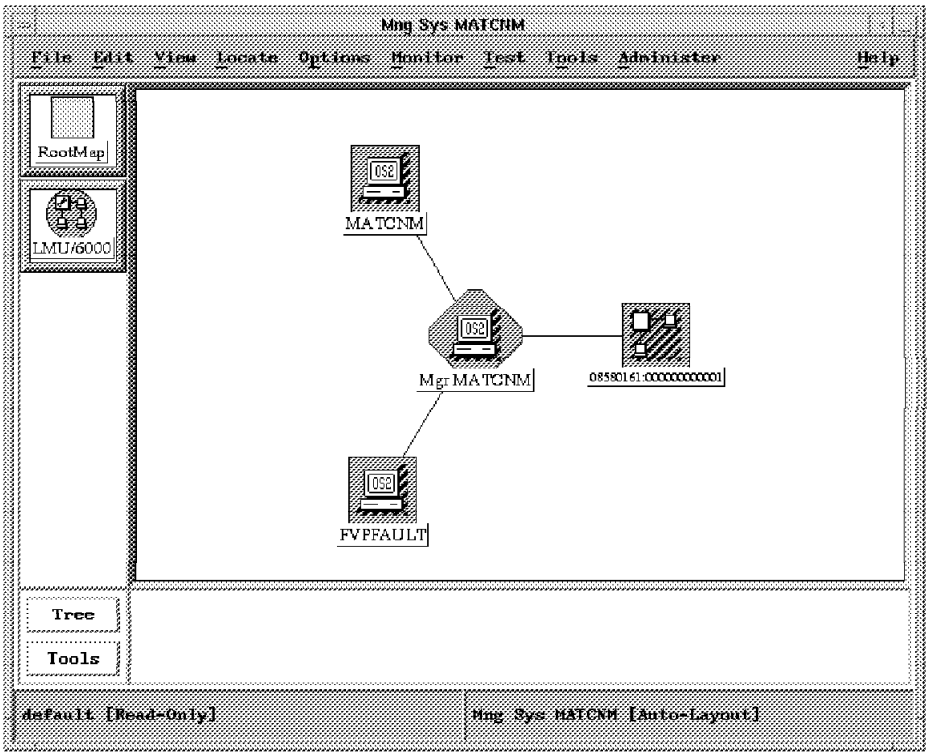


Figure 31. A NetWare Server and Some LAN and NetWare Requesters As Displayed by LMU/6000

2.14.1 Technical Description

LMU/6000 allows you to manage OS/2 LAN servers and Novell NetWare servers, and OS/2, DOS Windows, DOS and Apple MacIntosh clients on IBM NetBIOS and NetWare IPX networks.

Integrating LMU/6000 with NetView for AIX gives you the flexibility to choose to distribute the management of your NetBIOS and Novell IPX environments within

your network through the LAN NetView Management Utilities for OS/2 (LMU) program, or to consolidate your management skills and resources in one location and manage centrally from NetView for AIX.

LMU/6000 provides an easy way to retrieve configuration, performance, and fault information on the managed nodes. For example, system configuration data such as CPU type, machine type, fixed disk size, operating system characteristics, and universal LAN addresses can be retrieved. Performance data that can be monitored includes processor utilization, memory, disk activity, and server statistics. LMU and NetView for AIX management functions are integrated and interface to common applications such as event handling and trouble ticketing. LMU/6000 provides a complete set of messages, traps and event notifications.

The LMU/6000 network topology is fully integrated with the NetView for AIX topology. The LMU domains, stations, and their status are displayed and continuously updated using the NetView for AIX graphical end-user interface. The LMU/6000 browse function, which allows you to display configuration and performance data, is Motif-compliant and can be accessed directly from the NetView for AIX screen.

A dialog box is also provided for easy remote command execution. This allows you to remotely execute a program or procedure at a managed OS/2 workstation or NetWare server station.

2.14.1.1 LMU Components

The LMU/6000 program comprises the following two components:

- LMU/6000 Application

  The LMU/6000 Application is responsible for managing interactions between NetView for AIX and LMU for AIX to accomplish tasks selected from the NetView for AIX menu bar or context menu. This is the application that provides the graphical interface allowing you to perform system management functions on the LANs.

- Topology Daemon (lmuTopod)

  The lmuTopod daemon retrieves and maintains topology information of the managed nodes. It interacts directly with the LMU subagents on OS/2 systems to retrieve topology information and send it to the gtmd daemon of NetView for AIX. The gtmd daemon stores it in both the generic topology manager (GTM) and OVW databases. The lmuTopod daemon continually monitors the subagents and updates the topology as necessary. The xxmap application retrieves the information from the GTM database for display on the NetView for AIX graphical interface.

2.14.1.2 Supported Protocols and Platforms

LMU/6000 communicates with the LMU/2 proxy subagent contained in the OS/2-based LAN NetView Management Utilities. The relationship is depicted in Figure 32 on page 142. That means, to manage your LAN with LMU/6000, you need to have the following:

- A managing workstation running OS/2 with LMU/2 installed. This workstation has to be connected via token-ring or Ethernet to the LAN that is to be managed.
- LMU agents on the workstations that are to be managed.

Alerts flow to NetView for AIX from LMU the same way as they would flow from any SNMP device via the event log. Configuration, operations, fault, and performance management are provided in either an Ethernet or token-ring environment for the following:

- Novell NetWare and OS/2 LAN Servers on NetBIOS or IPX
- DOS, DOS/Windows, and OS/2 clients on NetWare IPX and IBM NetBIOS networks
- Apple MacIntosh clients on NetWare IPX networks

The management protocol between the subagents and LMU/6000 is SNMP. The transport protocol between the subagents and the managed node depends on the network operating systems being managed. NetBIOS is used between the subagents and IBM LAN Server servers and requesters. IPX is used between the subagents and NetWare.

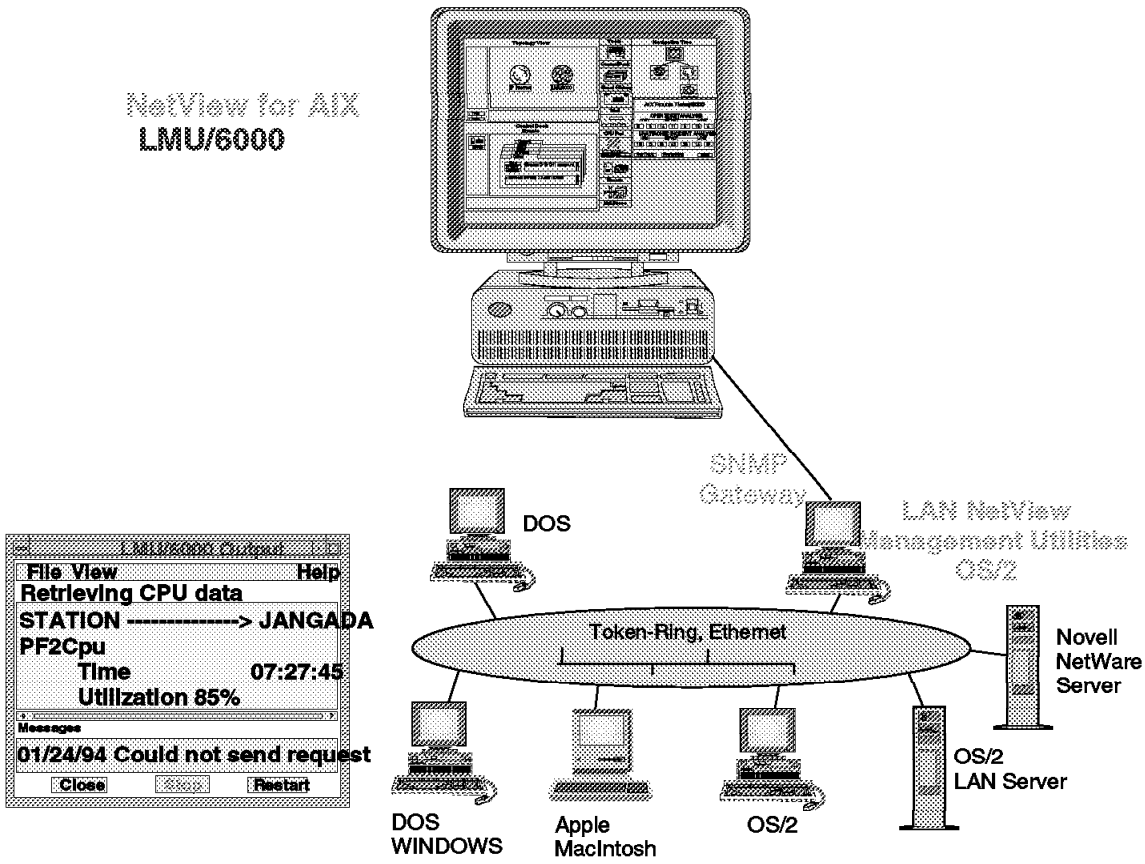


Figure 32. Relationship of LMU/6000, LMU OS/2 (LMU/2) and LMU Agents

2.14.1.3 LMU Operations Support

The LMU/6000 program will allow the following:

- Monitoring network status.

  Resource status is represented by specific colors on the NetView for AIX graphical interface for easy monitoring of your LMU-managed LAN network.

- Monitoring MIB attributes on a node.

Using the LMU/6000 application, you can view configuration and performance data defined in the LMU MIB for any node in your LMU-managed LAN network. This MIB extension is shipped with LMU/6000.

- Managing selected LAN servers and requesters.

  LMU/6000 provides the capability to select which nodes you want to manage; that is, you can dynamically define your administrative domain. LMU will continue to collect data for unmanaged nodes. This allows you to retrieve configuration and performance data for those nodes even though you are not monitoring or managing them. Selecting insignificant nodes to be unmanaged also reduces network traffic.

- Dialog box and scheduler for easy remote command execution. See Figure 33 on page 144.

  The remote command provides the capability to remotely execute a program or procedure at a managed OS/2, Windows, Macintosh workstation or NetWare server station, either immediately or at a later time. A dialog box is provided to ease this operation by enabling you to execute previously built commands or you can use the command line option contained in the dialog box for a one-time execution. LMU/6000 allows the execution of a command immediately or to schedule it for a later time. A common use of this remote operations capability is to execute a remote shutdown of a client workstation or server. A server, for example, could then be scheduled to automatically reboot after a period of time.

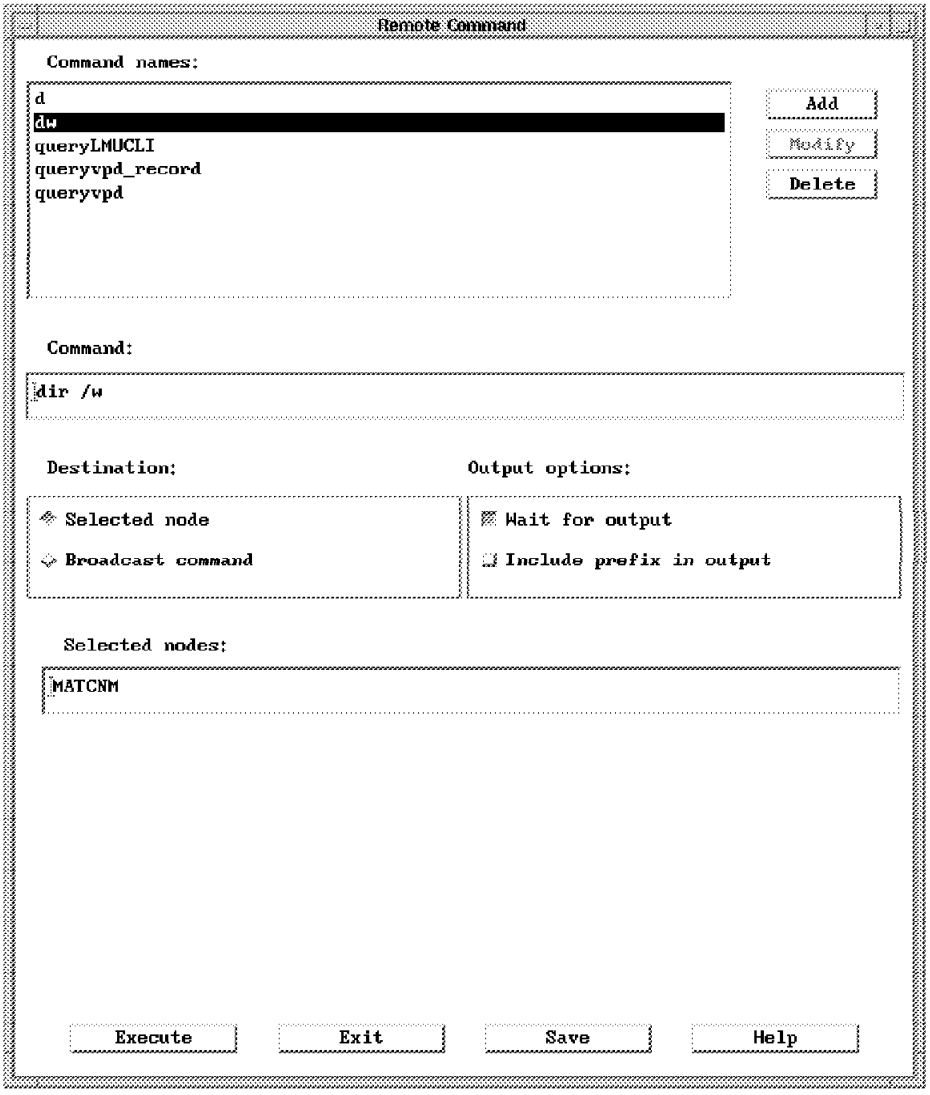


Figure 33. LMU/6000 Panel For Executing Remote Commands

2.14.1.4 LMU Configuration Information

LMU collects product information about the DOS, DOS/Windows, OS/2, NetWare or Macintosh server workstation in which it is executing and stores this data in a central OS/2 relational database. In a DOS machine, this is done with an executable which runs at boot time. On a DOS/Windows machine, this is implemented as a DLL, not a TSR. One vital product data image per workstation is kept in the database so if there have been any changes to the user's workstation since the last query, LMU will write those changes to a change log. This provides a running chronology of configuration changes and alterations for these workstations. An alert can be generated whenever a configuration change is detected. This is particularly helpful in maintaining hardware asset security. Critical files, such as CONFIG.SYS, can be monitored for changes.

The following information can be viewed via LMU/6000. See Figure 34 on page 145.

- Machine type
- CPU type

- Keyboard type
- Video adapter and display type
- Fixed disk type and size
- Diskette type and size
- Logical drive characteristics
- Installed Micro Channel adapter types and slot number
- Local and Universal LAN addresses
- Operating system
- SYSLEVEL information for installed software (OS/2)
- Date, time, and size of user-specified files
- User-customizable data

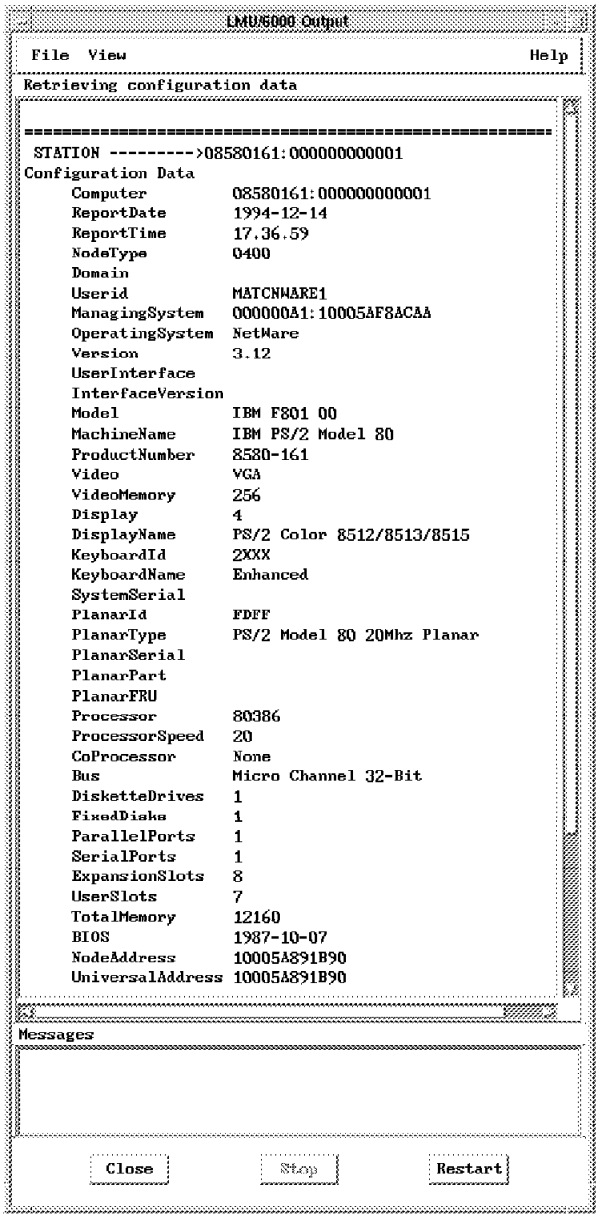


Figure 34. LMU/6000 Display of Some of the Configuration Data Retrieved from a NetWare Server

2.14.1.5 LMU Fault Management

The fault management function of LMU lets the LAN administrator automate the reaction to and recovery from common error conditions on the LAN and at the client workstation. Every NetWare server and OS/2 client or server can be set up to send heartbeats to the managing system at some regular interval. Missed heartbeats indicate a system-down condition, and LMU can generate alerts, page the LAN Administrator, and so on. Additional functions include the following:

- Ability to notify a pager if a fault is detected
- Alerts based on performance thresholds and critical applications
- Alert filtering
- Automated program execution on the client workstation if a fault is detected
- Capability to create software LAN alerts from C or REXX language programs, and batch files on DOS
- Ability to generate a ″virus alert″ from DOS, DOS/Windows or OS/2 when a virus-detection program detects a problem
- Automated recovery for software LAN alerts, including alerts generated by LMU
- Generation of a Presentation Manager Message Box as an alert action or from the OS/2 command line

2.14.1.6 LMU Performance Management

LMU collects performance data, provided by Novell′s SS.NLM for NetWare servers and by IBM Systems Performance Monitor/2 for OS/2 systems, and stores relevant data in an OS/2 relational database. The information is then available for analysis and manipulation or forwarding to a mainframe database for use at the corporate level. Statistics can also be used to generate events when user-defined thresholds are reached as well as for trending and capacity planning. Statistics that are available include the following:

- NetWare and OS/2 Server statistics
  - Average response time
  - Request buffer failures
  - Big buffer failures
  - Volume information
  - Available/total/purgeable block space
  - Available/total directory space
  - CPU utilization
  - Workstation memory
  - Physical disk activity
  - Swap activity
  - File opens/creates/renames/deletes
  - File reads/writes
  - Packets received/transmitted
  - Bytes received/transmitted
  - Logical I/O (reads, writes, opens, and closes)
  - Number of NCBs
  - Number of NetBIOS sessions
  - Number of transmission errors or aborted transmissions
  - Number of users logged on
- Network statistics
  - Novell′s IPX and SPX Network Statistics
  - IPX Layer Statistics

2.14.2 Prerequisites

The following lists the hardware and software requirements for LAN Management Utilities/6000:

Hardware Requirements: The following hardware components are required for LMU/6000:

- RISC System/6000 POWERstation or POWERserver
- 8 MB of memory minimum, 10 MB recommended
- 30 MB of free disk space (minimum) on the manager system and 10 MB of disk space on the remote node for the subagent
- Color display supporting AIXwindows System Version 11 Release 4 or later and OSF/Motif Version 1 Release 1 or later
- Connection to your TCP/IP network

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

- AIX NetView/6000 Version 2 Release 1, or later.
- AIX Version 3 Release 2.5 for RISC System/6000 with AIXwindows Environment/6000 1.2.5, which will build an X11R5 and Motif 1.1.4 compliant product.
- TCP/IP option of above AIX Version 3 Release 2.5 must be installed.
- LAN NetView Management Utilities for OS/2 installed in the network that you want to manage.

Please note that NetView for AIX requires some PTFs to run LMU/6000 as an application. To learn more about what PTFs are required to run a certain version of LMU, please consult the documentation for LMU/6000 and NetView for AIX.

2.14.3 Related Publications

In addition to the list of publications that is provided in the preface section of this book, for additional information on LMU/6000, please refer to *AIX LAN Management Utilities/6000 User's Guide*, SC31-7154.

2.15 OS/2 LAN Management

In the following sections, these IBM LAN management products for the OS/2 platform are discussed:

- NetView for OS/2

  NetView for OS/2 is an SNMP (Simple Network Management Protocol) systems management platform for PC LANs in environments that may have a centralized MVS, AIX or OS/2 management platform. NetView for OS/2 is an open management platform because it offers SNMP APIs for development and integration of third-party applications.

- LNM (LAN Network Manager)

  LNM is an OS/2 program, which manages the resources of a network more effectively. Stations, bridges and hub devices can be defined on the network

and events that occur on the LAN segments and the attached devices can be monitored. The program also assists in problem determination and error recovery for a LAN.

- LMU (LAN NetView Management Utilities)

  LMU is a systems management product for PC LANs in enterprise environments with a centralized MVS or AIX management platform. The LMU manager runs on OS/2 and manages OS/2, DOS, Windows and Macintosh clients and OS/2 LAN Server and NetWare servers.

- NetFinity

  NetFinity is a very easy-to-use systems management product for PC LANs in workgroup and distributed environments. NetFinity is shipped with IBM PC hardware, including IBM PC Servers, IBM commercial desktops and some IBM ThinkPads. This provides PC systems management support at no extra charge to customers who buy IBM PCs. The NetFinity manager runs on multiple operating systems (OS/2, Windows, Windows 95 and soon NT) and it manages OS/2, Windows and Windows 95 clients and OS/2 LAN Server and NetWare servers (and soon NT).

Figure 35 on page 149 shows a sample LAN management environment.

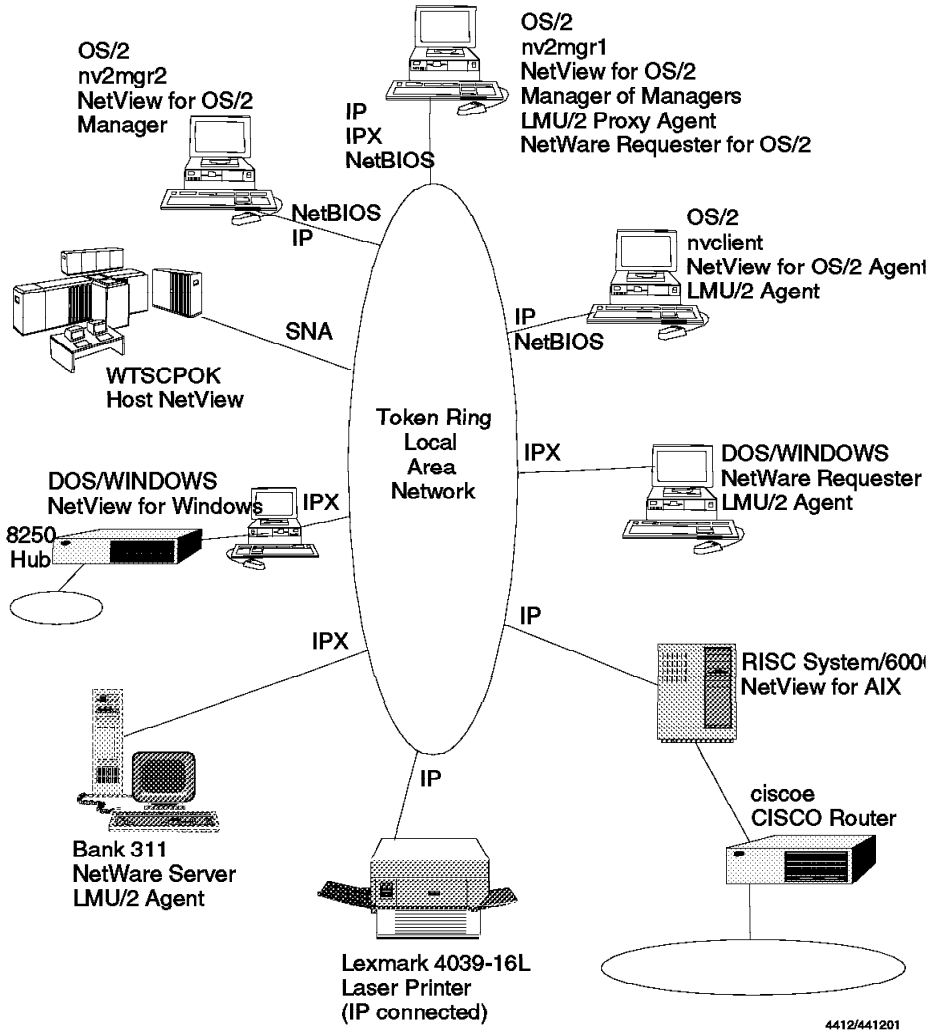


Figure 35. LAN Management Environment

2.16 NetView for OS/2

Local area network (LAN) and wide area network (WAN) administrators require comprehensive and readily available information to keep user productivity high and to efficiently manage the resources on their networks. LANs are becoming increasingly widespread, and end users rely on their networked PCs for critical business applications.

LAN administrators are responsible for ensuring that users have maximum access to network resources and minimum interruption in service, whether a problem is involved, or whether a planned change is required to respond to the needs of the business. LAN administrators are also challenged to control costs; not only hardware and software costs, but the increasing costs of supporting a network.

IBM NetView for OS/2 specifically addresses these requirements:

- Increasing the ability to efficiently use network resources
- Increasing productivity on the LAN
- Increasing control of hardware, software, and support costs

For administrators, IBM NetView for OS/2 is an industry-standards-based managing system platform for creating and running systems management applications. Standard applications and agents are included so you can immediately begin managing your environment.

NetView for OS/2 is a comprehensive network management solution that lets you keep accurate track of all systems resources. It is designed for management of systems and networks. NetView for OS/2 provides improved productivity to both the administrator by providing a powerful, easy-to-use management facility and the ultimate end user by improving network and resource availability. It gives a single, integrated view on one display of all LAN resources, such as clients, servers, and network devices. NetView automatically looks for trouble in your network and dynamically displays any denigrated or offline systems. It also allows remote system management for configuration and performance tracking and increases the control of hardware, software, and support costs for greater network efficiency.

LAN Server, NetWare, OS/2, IBM DOS, MS-DOS, Windows, and Microsoft NT are all supported right out of the box. Other critical network devices such as hubs, routers, database servers, communications servers, and simple network management protocol (SNMP) devices are supported.

The common user interface for NetView for OS/2 is provided by the Management Desk component, which presents system and network resources as graphical objects on the display. This provides a convenient, object-oriented method for performing operations. Clicking on the icon brings up a menu of applications that can be performed against the resource.

The benefits of NetView for OS/2 are improved availability of network resources, greater efficiency for administrators, reduced costs over the running life of the LAN, and better service for all network users.

2.16.1.1 Functions

IBM NetView for OS/2 provides the following:

- A comprehensive, integrated set of systems management programs from IBM and other vendors for both local and remote LANs
- A common, graphical user interface that integrates IBM and non-IBM applications
- Topology display for different perspectives of the network, with automatic discovery and monitoring of resources
- IBM resource manager agents for OS/2, NetWare, DOS, DB2/2, and CM/2
- Fault, performance, configuration, and operations applications to support these and other agents
- Host connection, allowing two way communications with NetView and other SNMP management platforms, such as NetView for OS/2 or NetView for AIX
- An extendible product for future support of other platforms in addition to the current platforms

- Products written to a standardized, and an object interface that allows applications to support data collection on other platforms
- A set of programmer tools that enables vendors and customers to write their own systems management applications

The following text describes the significant features and benefits of NetView for OS/2.

2.16.1.2 Management Desk

- Graphical user interface
- Integrates both IBM and non-IBM applications under a common user interface
- Enhances administrator productivity
- Allows execution of all functions with a common look and feel

2.16.1.3 Agents (Operating Systems and Subsystems)

- Supports IBM DOS, MS-DOS, Windows, OS/2 clients
- Supports IBM LAN Server, and NetWare servers/requesters
- Supports database servers and communications servers, such as IBM DATABASE 2 OS/2 (DB2/2)

2.16.1.4 Topology/Discovery Service

- Automatically discovers resources on a network and displays them
- Provides an up-to-date picture of the network devices and system resources
- Discovers clients, servers, and network devices
- Makes network resources available to applications
- Allows you to control discovery by filtering
- Helps you keep accurate track of all devices and systems resources by monitoring all additions and deletions
- Reduces administrative costs associated with asset management
- Reduces unnecessary capital expenditures on equipment

2.16.1.5 Remote Command Line Interface

- Allows entry of a command at the manager workstation for execution on remote OS/2 and Windows workstations
- Allows remote LAN Management
- Improves administrator productivity

2.16.1.6 MIB Loader/Browser

- Provides access to functions in remote SNMP agent
- Allows dynamic loading of agent description so management applications can begin working with remote systems
- Allows requests to set or query agent values
- Improves administrator productivity by centralizing management

2.16.1.7 Data Collector

- Collects performance information for reporting or displaying to use for making business decisions about upgrading systems
- Thresholding of performance information alerts the user about critical events

2.16.1.8 Application Builder

- Application Generator allows users, without programming knowledge, to create custom applications which retrieve real-time information from an agent
- Generated applications automatically placed in a folder, and optionally on pulldown menus for fast operation

2.16.1.9 Event Disk

- Filtering of display so users only see important events
- Historic information for tracking of problems
- Link to MIB browser application for retrieval of more detailed information

2.16.1.10 Event Automation

- Ability to automate responses to error conditions
- Support for pop-up displays, pagers, forwarding to other management systems, and user's exits

2.16.1.11 Host Connection

- Translates error messages to host NetView format for centralized trouble monitoring
- Runs programs as specified by host NetView operators

2.16.1.12 Development Platform with Programmer Tools

- Provides an application development platform for creating systems management applications and agents
- Provides interfaces for user interface integration and access to platform functions
- Allows vendors and customers to implement their own systems and network management applications and integrate them into NetView for OS/2
- Enables a more robust management system

2.17 LNM for OS/2

With the LAN Network Manager for OS/2 program, you can manage the resources of your network more effectively. You can define the stations, bridges, and hub devices on your network, and monitor events that occur on the local area network (LAN) segments and attached devices. You can control adapter access to the LAN and enable password protection for the LAN Network Manager for OS/2 program. The program also assists you in problem determination and error recovery for a LAN.

The LAN Network Manager for OS/2 program provides:

- Management and monitoring of a LAN

- NetView or NetView for AIX communication
- Alert filtering
- A database interface
- A graphical user interface
- An OS/2 command line interface

2.17.1.1 Network Management

The LAN Network Manager for OS/2 program manages up to 256 segments, depending on your network needs.

The LAN Network Manager for OS/2 Version 2.0 program consists of three tiers. The tier level of the program you are using dictates the number of segments that the LAN Network Manager for OS/2 program can manage:

Tier Level	Manages
Entry Tier 1	2 segments
Enhanced Entry Tier 1	9 segments
Full Capacity Tier 1	256 segments

All LAN Network Manager for OS/2 tiers provide the option of enabling or disabling a graphical interface at startup. If you have more than 256 segments in your LAN, install more than one LAN Network Manager for OS/2 program to manage the LAN.

To manage your assets more effectively, you can install the LAN Station Manager program on all the workstations on the managed LANs. Operating the LAN Station Manager program in the LAN Network Manager for OS/2 station and in each workstation enhances network management by enabling ring utilization. You can also obtain more information about the workstation, its adapters, and attached devices than would otherwise be possible. You can use this information to inventory workstation assets.

Figure 36 on page 154 shows a sample LNM managed environment.

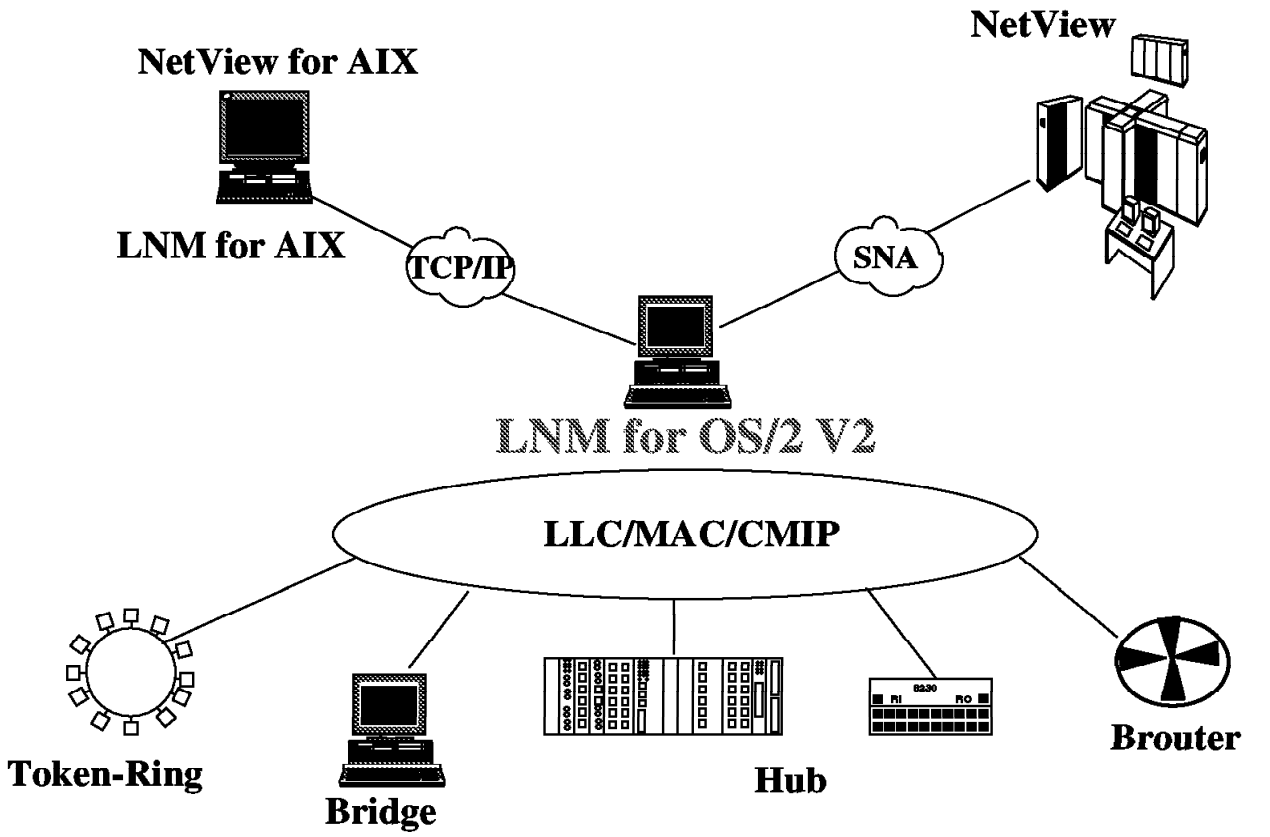


Figure 36. LNM for OS/2 Managed Environment

To aid in network management, the LAN Network Manager for OS/2 program:

- Manages both the LAN segment to which the LAN Network Manager for OS/2 adapter is attached and the remote LAN segments to which the LAN Network Manager for OS/2 adapter is linked by bridges (the managed domain).
- Receives error reports about the local segment, as well as segments other than the local segment from the linked bridges on those LAN segments, and reports errors it detects on the remote LAN segments.
- Enables you to monitor network traffic loads by providing:
  - Ring utilization information for a specified segment that has a station on it that is running the LAN Station Manager program, expressed as a percentage of the total data-transmission capacity of the segment
  - Bridge performance notification data, which you can use to monitor traffic between segments
- Maintains logs and configuration information using the DB2/2 program. You can analyze this information using the OS/2 Query Manager program.
- Provides a configuration monitor (CM) function, which:
  - Maintains a configuration table of adapters in the network, by LAN segment, and station-identifying information.
  - Maintains a location table for stations attached to hubs that contains hub attachment information.

  - Updates these tables when notifications of adapter insertions and removals are received. This includes active upstream neighbor (NAUN) changes and hub lobe status changes.
  - Resynchronizes the LAN Network Manager for OS/2 program's understanding of the network (determines which adapters are currently inserted into the ring) one segment at a time, after a user-specified interval has expired.
  - Performs an immediate resynchronization of a single segment at your request.
  - If access control is active, verifies access control information for each station, when it enters the network and during resynchronization.
  - Deletes an inactive adapter from the tables, at your request or after the adapter has been inactive for a user-specified interval.
- Provides the following support for stations:
  - Locates a defined workstation in the network by its LAN adapter.
  - Configures workstations by adding new station definitions or by changing or deleting existing definitions.
  - Displays its profile, which includes information about the workstation, its LAN adapter, and its attached peripheral devices, if the LAN Station Manager program is installed in the workstation.
  - Defines LAN Station Manager information from the LAN Network Manager for OS/2 program, if the LAN Station Manager program is installed in the workstation.
- Provides the following support for bridges:
  - An automatic link option in which the LAN Network Manager for OS/2 program attempts to link to specified bridges at startup and attempts to reestablish a link to bridges with which it has lost communication
  - Automatic relinking to activate changed bridge parameters
  - A link-status report
  - Logging of successful linking and unlinking activity
  - Logging performance-counter notifications
  - Linking different bridges that are managed by the same LAN Network Manager for OS/2 in both controlling and observing mode
  - Support for the IBM 8209/8229 Local Area Network Bridge
  - Support for the IBM 6611 Network Processor
  - Support for the IBM RouteXpander/2 Bridge with Multiport Support
  - Support for the 3174 Establishment Controller with Peer Communication bridge (3174 peer communication), which connects a token-ring segment to a 3174 peer communication segment
  - Support for all other original equipment manufacturer (OEM) bridges that have been certified as LAN Network Manager for OS/2 compatible.
- Provides the following support for hubs:
  - Microcode updates
  - Processing requests for hub information and status

  - Enabling directed reconfiguration of a hub
  - Processing requests to reset a hub
  - Handling unsolicited events from a hub
  - Support for the IBM 8230 Models 1 and 2 Controlled Access Unit
  - Support for all other OEM hubs that have been certified as LAN Network Manager for OS/2 compatible
- Supports functions for:
  - Viewing a list of events that is updated dynamically (as events are received by the LAN Network Manager for OS/2 program) or statically
  - Access control, which provides the detection and removal of unauthorized adapters
  - Asset management, which captures location information about adapters and sends a notification if an adapter is moved

For more information about network management options, refer to *Using LAN Network Manager for OS/2 Version 2.0,* SC31-7105.

2.17.1.2 NetView Communication

The LAN Network Manager for OS/2 program can communicate with NetView as a system network architecture (SNA) service point, or it can communicate with NetView for AIX as a simple network management protocol (SNMP) proxy agent. From the Network Level View System pull-down menu, you can select to communicate with NetView, NetView for AIX, NetView and NetView for AIX, or none of them.

NetView Communication: If you establish communications with NetView, the LAN Network Manager for OS/2 program can forward alerts to the NetView program. The alerts can be LAN alerts or alerts that are generated by application programs on the network and notify the NetView operator of problems, or potential problems on the network.

A command list sends the operator′s commands to the LAN Network Manager for OS/2 program and displays the responses at the operator′s console. You can issue all of the LAN Network Manager for OS/2 commands, that you issue from an OS/2 command line, from NetView.

The LAN Network Manager for OS/2 program generates and sends messages to NetView in response to the command lists. The NetView operator views these messages at NetView in the same way the operator can view a message generated by the NetView program.

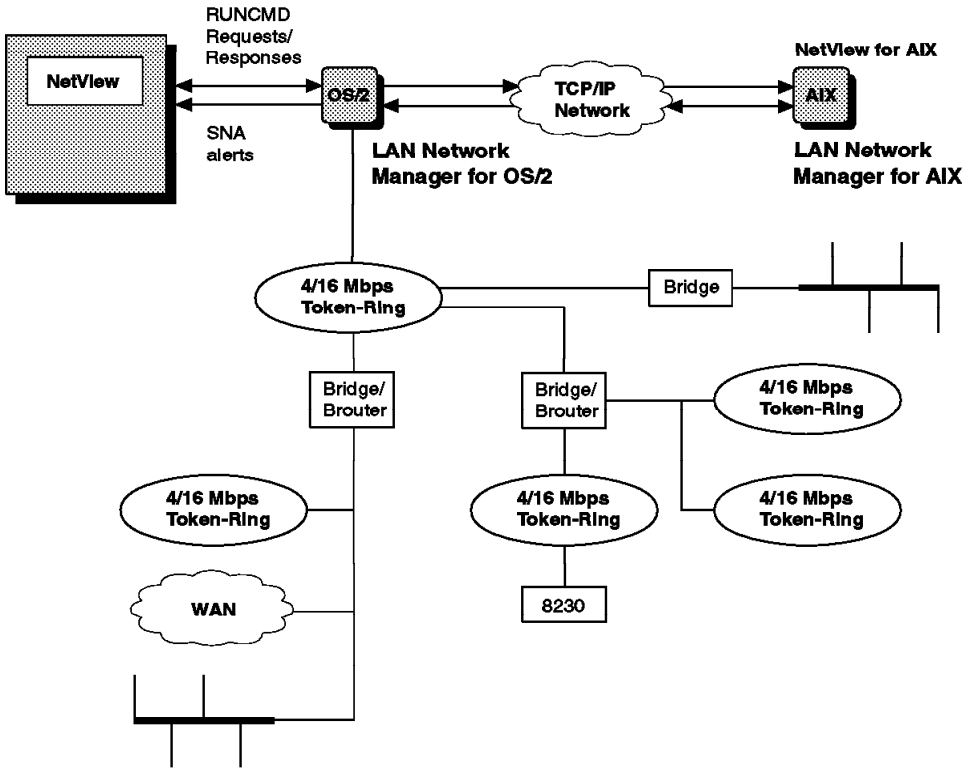


Figure 37. NetView or NetView for AIX Communication

NetView for AIX Communication: The LAN Network Manager for OS/2 program contains an SNMP agent that enables it to communicate with NetView for AIX in two ways. If you establish communication with NetView for AIX, the LAN Network Manager for OS/2 program can receive commands from, and send responses to an SNMP client (the LAN Network Manager for AIX program) and then on to the NetView for AIX program. It can also send unsolicited notifications to NetView for AIX in the form of an SNMP trap travelling through a TCP/IP socket interface. The SNMP trap contains management information from the LAN Network Manager for OS/2 program to enable the NetView for AIX operator to better manage the LAN Network Manager for OS/2 token-ring network.

2.17.1.3 Alerts

With the LAN Network Manager for OS/2 program, you can define filters or specify a user-written program to filter alerts that are sent to the NetView program. If you specify a user-written program, alerts are passed to the program before they are forwarded. The return code from the program determines whether or not the alert is forwarded to NetView. If you do not have an active NetView connection, no program is called and no alerts are filtered. You can also filter alerts that are recorded in the event log by defining an event log filter.

2.17.1.4 Database Interface

The LAN Network Manager for OS/2 program uses DB2/2 to store its data. Database tables include the following:

- Station, port, bridge, and hub definitions
- Alert and event filters
- Station locations
- The event log
- Ring utilization
- A list of all adapters that are known to LAN Network Manager for OS/2

You can query, print, or export these tables for use in other applications (such as spreadsheet programs) by using the OS/2 Query Manager or a user program.

2.17.1.5 Graphical Interface

You have the choice of using the LAN Network Manager for OS/2 program with either the graphical user interface or a command line interface. If you choose the graphical user interface, you can display and manage your network at the following view levels:

- Network level

  The network level view displays the entire LAN, showing all the managed segments, bridges, and the ports that connect them.

- Segment level

  Each segment level view of this type displays an entire segment, including bridge adapters and hubs, and the stations on a segment attached to a hub.

- Segment level-aggregated

  Each segment level-aggregated view displays an entire segment, showing the bridge adapters and devices that are directly attached to the segment. Hubs attached to the segment are displayed, but stations connected to the hubs are not.

- Device level

  Each device level view displays a hub with all attached devices.

Status of network objects is indicated by color, so you can recognize an area of the network that is experiencing trouble. You can then navigate from the network view to the device that is causing the problem.

You can customize all views. For example, you can do the following:

- Move objects in views
- Hide or display object labels
- Add your own text to views
- Add backdrops behind views (except hub level views)
- Display active adapters only or both active and inactive adapters from a segment level view

2.17.1.6 OS/2 Command Line Interface

In addition to using the graphical user interface, you can also monitor and manage your network only from an OS/2 command line, or from both the graphical user interface and an OS/2 command line simultaneously. From the command line interface, you can:

- Obtain the current status of adapters, bridges, and hubs.
- Remove an adapter from the network.
- Display the event log, query details of event messages, and clear the event log.
- Access help for various LAN commands and messages.
- Display and set options to control which soft error changes are reported.
- Query profiles for adapters, bridges, and hubs.
- Add, change, and delete definitions for adapters, bridges, and hubs.
- List the current configuration of active adapters, linked bridges, and hubs.
- Obtain the current status of adapters, bridges, and hubs.
- Request that the LAN Network Manager for OS/2 program link to or unlink from a bridge.
- Query the current status of all monitored LAN segments.
- Establish event log filters.
- Query ring utilization information for segments.
- Restart the LAN Network Manager for OS/2 program to activate configuration changes.
- Exit the LAN Network Manager for OS/2 program.

You can automate LAN management tasks by creating a file that contains one or more LAN Network Manager for OS/2 commands. When you execute the file, all of the commands contained within it are issued one at a time to the LAN Network Manager for OS/2 program. You can also choose to direct the LAN Network Manager for OS/2 program′s responses to your commands to a file.

2.17.1.7 Understanding the Managed Domain

The LAN Network Manager for OS/2 program manages the network according to the concept of the management mode, which indicates the extent of the management function available to a particular LAN Network Manager for OS/2. The following are two management modes that LAN Network Manager for OS/2 can use to create a flexible and effective management environment:

Controlling This mode gives you the ability to perform all network management functions, including tasks that are restricted to the controlling mode, such as changing bridge passwords, enabling or disabling bridge functions, and enforcing access control functions.

Observing In this mode you can perform all network management functions except those that are restricted to the controlling mode. Examples include monitoring traffic across bridges, tracking adapter

insertions and deinsertions on a segment, and monitoring the status of your network resources.

You can combine these two management modes in different ways to provide more complete coverage of your network resources. For example, you can actively manage the resources on one segment in controlling mode, while at the same time monitoring the activity of resources on another segment in observing mode.

Bridges in the Managed Domain: The management mode of the bridge is dictated by the reporting link mode that is used when the bridge is linked. With LAN Network Manager for OS/2 you can specify a controlling link mode or an observing link mode for the bridge.

Instead of using a specific reporting link when linking to a bridge, you can also use a default link mode. The default link mode assigns the same reporting link value to all bridges that are defined to use the default link mode. This enables you to change the reporting link value of more than one bridge at the same time. For example, if you change the default link mode to reporting link Observing 3, all bridges that are defined to use the default link mode are updated to use the new reporting link. Any changes to the default link mode do not affect those bridges that have been defined to use a specific reporting link.

Segments in the Managed Domain: The management mode of the segment to which the LAN Network Manager for OS/2 program is attached (the local segment) is determined by the default link mode for LAN Network Manager for OS/2. For example, if the default reporting link is Observing 1, the management mode of the local segment is observing, even if you link to a bridge attached to the local segment in controlling mode. The only exception to this occurs if you include the number of the local segment in the hub qualifiers list. In this case, LAN Network Manager for OS/2 attempts to register with hubs on the local segment, regardless of the default link mode.

If the LAN Network Manager for OS/2 program is linked to more than one bridge attached to the same segment, the management mode of the segment is determined by the reporting link mode of the bridges. If one of the bridges is using the controlling reporting link, the management mode of the segment is considered controlling, unless the linking LAN Network Manager for OS/2 is running on that segment. If no controlling link exists, the management mode of the segment is observing.

The LAN Network Manager for OS/2 program uses its segment table to keep track of the number of segments that it currently knows about. When a bridge is linked, the segments that the bridge connects are added to the segment table. When the total number of segments in the table is exhausted, no more segments can be added. In some situations, the bridge may link to a type of segment that LAN Network Manager for OS/2 does not actively manage, such as frame relay, X.25, or SNA. Although such segment types are not managed, LAN Network Manager for OS/2 nonetheless includes them in the segment table. If your network contains a number of bridges that connect to these unmanageable segment types, a portion of the segment table can be occupied by these segments, limiting the number of segments that LAN Network Manager for OS/2 can actively manage. This effect can be especially pronounced if you are using multiport bridges in your network.

You can allow for unmanageable segments by adding extra entries to the segment table when you start the LAN Network Manager for OS/2 program. Both manageable and unmanageable segments are added to the expanded segment table as LAN Network Manager for OS/2 runs, but the program can distinguish between the manageable segments and the unmanageable segments. This enables LAN Network Manager for OS/2 to enforce the limits of the program′s tier level. If you exceed the limit of the program′s tier level (linking 20 bridges with the Enhanced Entry Tier program, for example), the segments that cannot be managed due to the tier restriction are still displayed on the network level view but with a status of Unknown. The unmanaged segments are not displayed in the segments list unless you increase the number of non-manageable segments when you start the LAN Network Manager for OS/2 program. You cannot perform segment-related functions, such as soft error logging or ring utilization, on these segments.

Hubs in the Managed Domain: A qualifier is a segment number that represents a segment which contains a concentrator but that may not be connected to the LAN Network Manager for OS/2 program by a linked bridge. The LAN Network Manager for OS/2 program can use a list of hub qualifiers to determine which hubs to register with when it does not have a controlling management link to the appropriate segments. If you are running the Entry Tier or Enhanced Entry Tier level of the LAN Network Manager for OS/2 program, you can use hub qualifiers to extend your network management beyond that provided through your linked bridges.

2.17.1.8 Managing Networks

From the LAN Network Manager for OS/2 main window, you can perform most of the tasks and view status messages necessary to monitor and manage your network. This window shows a graphical representation of the segments, bridges and ports that make up your network.

From this view you can use the LAN Network Manager for OS/2 program to determine the status of the following:

- LAN Network Manager for OS/2 adapter and the local segment
- Alerts that have been logged since you last displayed the event log
- Graphical view (whether the LAN Network Manager for OS/2 program is refreshing the view or updating configuration)

From this view, navigate to a segment level view by double-clicking on the segment symbol, or display data for devices on your network by double-clicking on that device.

2.17.1.9 Managing Segments

Segment management is important in maintaining control of your network from a central location. The LAN Network Manager for OS/2 program provides such control by allowing you to maintain current configuration information for the managed segments and to test these segments for data transfer capability.

You can also use the program to manage segments by doing the following:

- Displaying the status of all segments in your managed domain
- Displaying a list of adapters on each LAN segment
- Displaying details about the status of a segment

- Setting options for soft-error reporting
- Displaying ring utilization information for a segment

2.17.1.10 Defining and Managing Stations

To efficiently manage stations on the network, you can use the LAN Network Manager for OS/2 program to assign symbolic names for each adapter. You can also specify which adapters you want to monitor, and control each adapter′s access to the network.

In addition, you can use the LAN Station Manager program with the LAN Network Manager for OS/2 program to access more information about the workstation, its adapters, and its attached devices than is otherwise possible. By installing the LAN Station Manager program in the workstations and in the LAN Network Manager for OS/2 station, you can use the LAN Network Manager for OS/2 program to inventory workstation assets and provide ring utilization for the segment.

You can also use the LAN Network Manager for OS/2 program to manage stations by:

- Displaying a list of stations on a segment
- Locating a specific adapter
- Displaying the profile of a selected station
- Removing a specific adapter
- Adding, changing, or deleting station definitions
- Querying the management information base (MIB) of the LAN Station Manager program for information about workstation assets, such as hardware, operating system, and type of communication
- Specifying the dates and times during which an adapter can access the network

2.17.1.11 Defining and Managing Bridges

When you use the LAN Network Manager for OS/2 program to manage linked bridges, you can monitor and manage other segments in addition to the segment to which the LAN Network Manager for OS/2 station is physically attached. You can display and change the bridge configuration parameters and reporting link parameters for linked bridges.

You can also manage bridges by:

- Linking to and unlinking from a bridge
- Linking different bridges that are managed by the same LAN Network Manager for OS/2 program in both controlling and observing mode
- Displaying a list of bridges
- Locating a specific bridge in a list or in a graphical view
- Adding, changing, or deleting a bridge definition
- Displaying the profile of a selected bridge
- Displaying or changing configuration parameters
- Displaying or changing port definitions

- Displaying and logging bridge performance data

2.17.1.12 Defining and Managing Hubs

When you use the LAN Network Manager for OS/2 program to manage hubs, you can control network access for the adapters attached to it. When you use LAN Network Manager for OS/2 to register with a hub, you can:

- Enable and disable lobe receptacles and attachment modules
- Set the hub's internal parameters and password
- Change its wrap state

You can also manage hubs by:

- Enabling or disabling ports on a hub
- Displaying a list of hubs
- Locating a specific hub in a list or in a graphical view
- Adding, changing, or deleting hub definitions
- Displaying the profile of a hub
- Updating the microcode in a hub
- Displaying a picture of a hub
- Registering and deregistering with a hub
- Resetting a hub
- Flexible hub management

When the workstations are attached to a hub, you can have the LAN Network Manager for OS/2 program automatically disable the port to which an adapter is attached if the access control parameters that you specify are violated and if you have activated access control.

2.17.1.13 Working with the Event Log

The LAN Network Manager for OS/2 program maintains a history of network events by recording them in a database with the date and time the event was logged. You can view a list of events that is updated dynamically, as the LAN Network Manager for OS/2 program receives notification of the alerts and configuration changes, or you can view them statically.

You can also use the LAN Network Manager for OS/2 program to do the following:

- Display events or alerts that are logged by the program
- Display a dynamic list of events
- Display events for a particular device
- Use event log filters to control the types of events that are logged by the program
- Diagnose network problems and take recommended actions by displaying the details of individual events and alerts
- Print event details
- Delete events from the event log

2.17.1.14 Solving LAN Problems

When there are problems in the network, you can use the LAN Network Manager for OS/2 program to troubleshoot these problems. By using the status information and the alerts and events that the LAN Network Manager for OS/2 program reports, you can determine which actions to take to resolve network difficulties. Other LAN Network Manager for OS/2 functions, such as the event log, allow you to display event details and to obtain suggestions for isolating and solving problems.

2.17.1.15 Measuring Bridge Performance

The LAN Network Manager for OS/2 program provides data that enables you to evaluate the performance of the bridges in your network. You can measure bridge performance by doing the following:

- Receiving an alert whenever the percentage of lost frames at a bridge exceeds a threshold.
- Starting a periodic measurement of a bridge′s performance and have the results accumulate in the bridge performance table. You can view, print, or export the results to a spreadsheet program.
- Displaying performance data in the LAN Network Manager for OS/2 program′s Performance Data page of the Profile/Change Bridge Definition notebook, either for the entire time the bridge has been linked or for an interval you can control.

2.17.1.16 Establishing Password Security

You can use the LAN Network Manager for OS/2 program to limit access to LAN Network Manager for OS/2 through the secure system option.

With secure system, you can enable password security for the LAN Network Manager for OS/2 program. You can use password security to ensure that only authorized users have access to the functions and the configuration data of the program.

2.17.1.17 Measuring Event Severity

You can use the graphical user interface to monitor the status of resources in your network. The LAN Network Manager for OS/2 program updates the graphical views to show that an event affecting a resource has occurred. When an event is logged in the event log, the object representing the resource involved in that event is hatched (shaded with diagonal, parallel lines). If that event results in a status change, the LAN Network Manager for OS/2 program also updates the color of the involved object, or objects, to show the severity level of the event.

2.18 LMU for OS/2

LAN Netview Management Utilities for OS/2 is a comprehensive network management solution that lets you keep accurate track of all systems resources. It provides easy network management and system administration. LMU helps to manage small OS/2-based networks efficiently and productively by collecting information about OS/2, DOS, DOS with Windows, and Macintosh workstations and NetWare servers, and sending it to a database.

It allows a designated workstation to manage both servers and requesters in IBM LAN Server and Novell NetWare networks by providing the following systems management functions:

- Operations management
- Configuration management
- Performance management
- Fault and problem management

LMU consists of a graphical display of the local area network (LAN), command and data transport, and management applications (configuration, performance, operation, and fault), and it can collect asset information into an OS/2 database. User-written applications can supplement those supplied by IBM. LMU can run as a stand-alone application or be seamlessly integrated into the NetView for OS/2 framework.

The following are among the facilities offered by the IBM supplied utilities:

2.18.1.1 Configuration Management

- Collects vital product information about the OS/2, DOS, Microsoft Windows 3.1, and Macintosh workstations, as well as the NetWare servers and IBM LAN Servers being managed. This data is either displayed on the managing station screen or placed in a central OS/2 database.
- Maintains a change log in the managing station, and optionally generates an alert when a managed station′s configuration changes.
- Monitors the number of instances of specific OS/2 application programs in an OS/2 workstation and sends generic alerts to the Fault Management system when user-specified thresholds are reached.

2.18.1.2 Operation Management

- Provides the capability to remotely run a program or procedure at a managed OS/2 workstation, Windows workstation, or NetWare server station. OS/2 and Windows console text output can be optionally redirected to the administrator workstation or to IBM NetView. Some LMU functions can be remotely run on a Macintosh system.
- Provides the ability to shut down in an orderly manner all functions in a managed OS/2 system or NetWare server, and to optionally reboot the system.
- Schedules program execution on one or more OS/2 workstations, Windows workstations, Macintosh workstations, or NetWare server workstations on a timed basis.

2.18.1.3 Performance Management

- Collects OS/2 workstation performance data from the IBM System Performance Monitor/2 (SPM/2) product, sends the collected information to a central OS/2 database, and optionally generates generic alerts when user-specified thresholds are reached.
- Monitors the set of workstations (adapters) logged on to a specified OS/2 LAN server for IBM NetBIOS status, and generates generic alerts when specific conditions occur.

- Collects OS/2 LAN server statistics and generates generic alerts when thresholds are reached.
- Monitors network statistics for Novell′s IPX and SPX layers for OS/2 and DOS workstations attached to a NetWare file server, and generates generic alerts when user-specified thresholds are reached.
- Collects NetWare server volume information, sends the collected information to a central OS/2 database, and optionally generates alerts when user-specified thresholds are reached.
- Collects NetWare server performance data, sends the collected information to a central OS/2 database, and optionally generates alerts when user-specified thresholds are reached. (This function requires Novell NetWare′s SS.NLM module.)

2.18.1.4 Fault Management

- Provides software LAN alerts from IBM LAN NetView Management Utilities applications
- Creates software LAN alerts (generic alerts) from C or REXX language programs in OS/2, and from batch files on DOS
- Provides alert thresholding and filtering
- Enables automated recovery for software LAN alerts, including alerts generated by IBM LAN NetView Management Utilities functions
- Forwards alerts directly to LAN Network Manager or NetView/390
- Converts alerts into SNMP traps for use with SNMP management platforms, such as LAN NetView and NetView/6000
- Serves as an alert automation exit routine for LAN Network Manager

2.18.1.5 Miscellaneous Functions

- Heartbeat: Allows the managed station to signal ″This station is alive and well″ status to the managing system at specified intervals. If the managing system does not receive the heartbeat status within the required time, a generic alert is generated and sent to the fault management system.
- Profile Services: Supplies programs that allow the customer to:
  - Convert OS2.INI files, such as OS2SYS.INI, into a readable ASCII format
  - Convert a readable ASCII file of the appropriate format into the OS/2.INI format
- Simple Network Management Protocol: Provides an industry standard SNMP gateway to communicate between SNMP-compatible network management consoles and LMU managing systems to integrate the PC LAN management into the overall enterprise network management.

IBM LAN NetView Management Utilities consists of a graphical display of the LAN, command/data transport, management applications (configuration, performance and fault), and an OS/2 database for data collection. User-written applications can supplement those supplied by IBM.

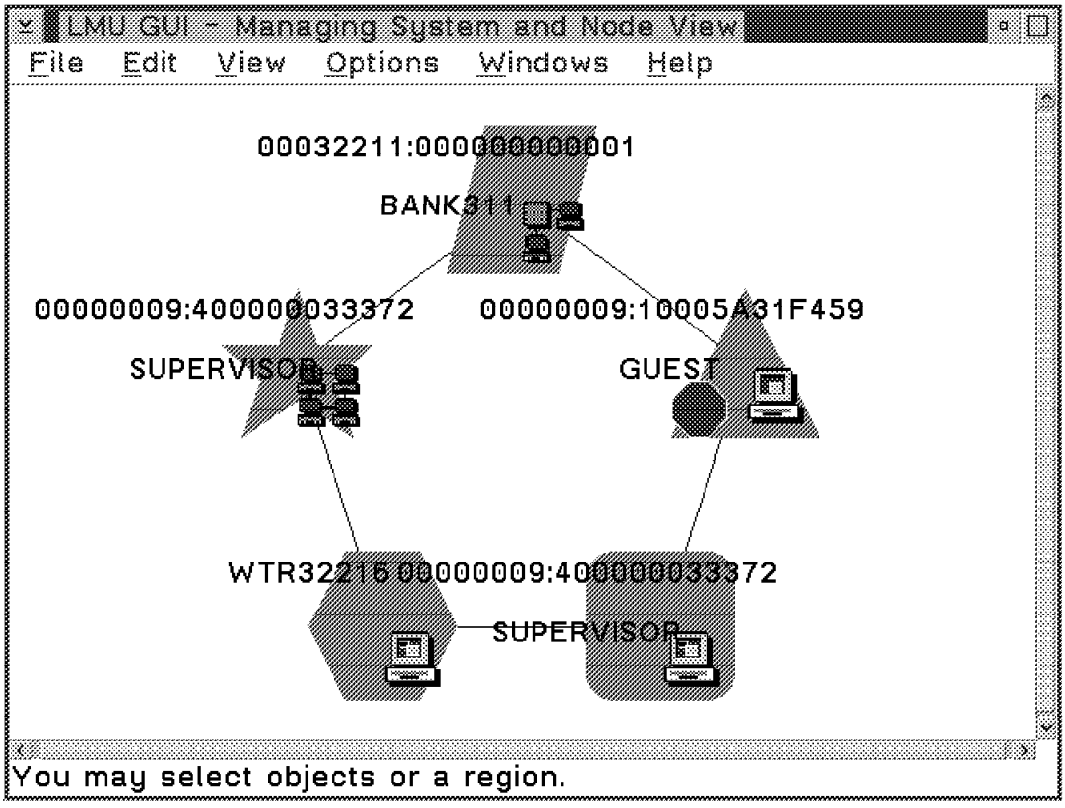


Figure 38. LMU Graphical User Interface

2.18.1.6 Product Positioning

1. LMU provides a robust set of systems management services across the LAN to address the disciplines of performance, operations, fault, and configuration/asset management. While its primary focus is systems management of the LAN-attached servers and workstation systems, it can also provide support of the LAN media and transports when coupled with the LAN Network Manager via the user exit interface.
2. LMU provides these services in the mode appropriate to the customer environment. This includes independent PC LAN management, cooperative application processing and as an element of the larger enterprise network management framework.
   a. LMU enables remote/local management of LAN-attached OS/2, DOS, Windows, Macintosh and NetWare systems.
   b. It complements the capabilities of LAN Network Manager when present. LMU adds additional LAN Network Manager alert filtering and an automation capability.
   c. It communicates with the IBM NetView platform products to integrate PC LAN management information into the overall enterprise network management framework as a cooperative application set.
   d. Managing systems may be operated independently, may be run on the LAN NetView framework or can be remotely managed by LAN NetView or NetView/6000 via SNMP.
3. LMU includes both the OS/2 managing system code and code that runs on the OS/2, DOS, Windows, and Macintosh managed systems. Also provided

are NetWare loadable modules (NLM) to support NetWare as a managed system. LMU's OS/2 performance data is provided by IBM's SPM/2 product.

4. LMU capability is limited only by the capacity of the managing system and operational characteristics of the managed systems:
   a. Management capacity of a single LMU managing system is dependent upon the size of the processor and the amount of data being gathered and processed.
   b. LMU allows management information to be forwarded to a NetView host system, designated user systems on the LAN, SNMP-compatible network management consoles, or combinations of the host, SNMP, and LAN.
   c. One LMU managing system may manage other LMU managing systems.
   d. LMU management services may be distributed across the LAN. LMU only requires LAN access to an OS/2 DBM, OS/2 Communications Manager for NetView support if needed, and either OS/2 LAN Server or Novell Server as an application server. Coupling with LAN Network Manager requires both LMU and LAN Network Manager to run on the same OS/2 system. SNMP management connection to the LMU managing workstation requires TCP/IP on that PC.
5. LMU allows customer flexibility in the placement of the overall management focus. Whether a customer requires a centralized, host-oriented solution, a localized solution, or a combination of the two, LMU offers the flexibility in its implementation to satisfy these needs.
6. While LMU is not limited, it is particularly suitable for entry PC LAN environments from a function and cost standpoint. From small stand-alone segments with low cost requirements this PC LAN management solution can grow with the enterprise. From primary management of a single segment to cooperative management with other systems management platforms of worldwide networks, LMU preserves the customer's investment and supports their growth.
7. This product is appropriate for the following:
   a. Customers who are entering into management of small LANs but want an investment that can grow with them and that offers an application set that can cooperate with other systems management products, with future growth of either the customer's business or LAN management requirements.
   b. Customers engaged in large rollouts of distributed LANs, require remote unattended management, and require a package of existing applications due to time or cost constraints that prohibit application development.
   c. Customers with OS/2, DOS, Windows, Macintosh and Novell servers who are looking for a single product solution to manage their LAN environment.
   d. Customers looking for a local automation platform for their LAN systems.

2.19 NetFinity for OS/2

NetFinity is a low cost, highly flexible hardware management program with general system management functions. NetFinity on its own provides a full set of easy-to-use hardware management services, and allows LAN administrators to view, initiate and exploit management services. It compliments and enhances both NetView for OS/2 and LAN Management Utilities for OS/2. NetFinity Manager is composed of three components: NetFinity Manager, Netfinity Services for OS/2, and Netfinity Services for NetWare. It requires NETBIOS, TCP/IP, or IPX and allows for the use of the following:

- Hardware and software configuration details
- Resource monitoring and alerting
- Security management
- Customizable system profile

Functions:

- Can be used in conjunction with LAN Management Utilities for OS/2 as a complementary product that provides hardware management services in addition to the features of LMU
- Critical File Monitoring for critical system files or data files as defined by the system operator
- Configuration/Installation/Distribution (CID) enabled
- Remote Dial-in Support to any remote NetFinity Services or NetFinity Manager system
- Process Manager allows a remote administrator to view active processes, terminate rogue processes and initiate new processes
- DMI-enabled: supports the industry standard Desktop Management Interface (DMI)
- Delivers a broad range of system management services

There are two components of NetFinity software: NetFinity Services and NetFinity Manager. NetFinity Services are applications that reside on each connected system, providing the means for participating in NetFinity systems management. NetFinity Manager resides on the LAN administrator′s systems, allowing remote initiation and control of NetFinity functions.

2.19.1.1 NetFinity Services

- System Information Tool

  Detects and reports detailed information on a wide variety of systems, including adapters, SCSI configuration and devices, disk drives, PCMCIA devices, memory, I/O devices, and much more.

- System Profile

  A fully customizable user and system information facility. Comes complete with a customizable template to get you started.

- System Monitoring

  Displays line graphs and real-time monitors for a variety of system resources, including microprocessors, disks, and memory. Alerts the user or network manager when user-defined thresholds are exceeded.

- Security Manager

  Prevents unauthorized access to your NetFinity services.

- Alert Manager

  Receives and processes application-generated alerts. You can examine, edit, and print reports from the alert log and customization actions (including logging alerts, notifying remote users, displaying pop-up messages, and starting programs) in response to received alerts.

- ECC Memory Setup

  Enables you to control ECC memory features on many IBM personal computers.

- System Partition Access

  A powerful access tool for IBM systems that have built-in System Partitions. It updates, backups, and even deletes your System Partition without using your Reference Diskette.

2.19.1.2 NetFinity Manager

- Remote System Manager

  Enables you to access and control all NetFinity Services installed on remote systems within your network. Systems are organized into logical system groups for simplified management. Remote System Manager also features a Discovery process that automatically recognizes NetFinity systems and places them in a group.

- Power-On Error Detect

  Immediately warns you when a remote system has startup problems, letting you minimize downtime.

- Remote Session

  Enables you to establish a fully active remote session with a remote system.

- File Transfer

  Enables you to easily send, receive, or delete files and directories locally and remotely.

- Screen View

  Takes a snapshot of a remote system′s current screen display. Screens can be saved as bit maps and loaded for viewing later.

  The object-oriented design of NetFinity allows new services and protocol support to be added without any impact to the base product.

  NetFinity can operate in the absence of any requestor or server software. Only one of the supported protocols is required.

2.19.1.3 Management Functions

IBM NetFinity provides local and remote system management functions with the emphasis on hardware. The hardware management functions are:

- Exploitation of system partitions (PS/2 systems)
- Exploitation of C2 security
- Exploitation of Micro Channel, EISA and PCMCIA buses
- ECC configuration management (PS/2 systems with ECC memory)

- Collects detailed hardware configuration information:
  - Model and processor
  - Memory subsystem
  - Video subsystem
  - Disk subsystem
  - SCSI subsystem
  - Power management information
  - Peripheral devices (keyboards, mouse and I/O ports)
  - Security features
  - Vital product data (VPD) information
  - RAID subsystem

The following general systems management functions provided are:

- File transfer
- Remote screen snapshots
- Resource and performance monitoring
- Built-in multilevel security
- Built-in alert generation and logging
- Collects software configuration information
- Operating system (level and settings)
- Application versions
- CONFIG.SYS analysis
- Current TASK lists

Systems Management - Managing Multiple Systems: NetFinity provides balanced systems management for both workstations and servers. The balance is achieved through NetFinity hardware management services. The system with more hardware features will benefit more from the hardware services. All systems retain basic system management functions.

Growth Enablement - Centralized Control Improvements: A system administrator using NetFinity has the ability to perform key management functions on remote workstations. The program has built-in features to expand with the growth of a customer's network while maintaining the centralized controls.

2.20 Summary

LMU and NetFinity are systems management applications, while NetView for OS/2 is an open SNMP systems management platform, with APIs for developing and integrating multivendor management applications.

LMU and NetFinity for OS/2 manage PC desktops and servers, but do not manage networking devices. NetView for OS/2 manages not only PCs, but also any network device that has an SNMP agent. NetFinity for OS/2 are significantly easier to set up than LMU or NetView for OS/2.

NetFinity for OS/2 provide a Manager pass-through feature that differentiates them from LMU and NetView for OS/2. The Manager pass-through feature allows one NetFinity for OS/2 Manager to access a remote NetFinity Manager and manage its managed PCs. The connection between the two NetFinity Managers can use a different network protocol than the one used to connect the remote NetFinity Manager to its managed PCs. This feature provides a lot of flexibility for deploying systems management functions across a distributed network environment.

A significant feature that differentiates NetFinity is its platform independence. NetFinity Manager runs on OS/2, Windows and Windows 95 (and soon NT). LMU and NetView for OS/2 managers run only on OS/2.

A significant feature that differentiates LMU is that it offers command line interfaces for every function, which is key for automation (via REXX routines). Automation is essential to support high availability, and without command line interfaces; customers cannot write REXX automation routines. Another important feature is that LMU interoperates well with NetView for MVS and NetView for AIX, while NetFinity for OS/2 can only send alerts to these platforms. Finally, LMU is the only product that can manage DOS and Macintosh systems.

NetView for OS/2 is an integration platform for LMU and NetFinity for OS/2, as explained below:

- The LMU SNMP Proxy agent integrates LMU-managed systems into the NetView for OS/2 user interface. A NetView for OS/2 manager can manage multiple downstream LMU managers and their managed PCs.
- NetFinity for OS/2 can be integrated with the NetView for OS/2 user interface. Once you launch NetFinity Manager from NetView for OS/2, you can use it to manage PCs that have NetFinity Services installed. Using the Manager Pass-through feature, you can access other remote NetFinity Managers and manage their managed PCs, even if they were not discovered by NetView for OS/2.

These are some key LMU features that differentiate it from NetFinity for OS/2, and make it more appropriate for enterprise environments:

- Two-way communication with NetView for MVS (SNA alerts and commands)
- Support by the NetView Multisystem Manager
- SNMP proxy agent for interoperability with SNMP managers (NetView for OS/2 and NetView for AIX)
- Command line interface to all functions (excellent automation support via REXX programs)
- Virus alert
- Alert thresholding and filtering for forwarding to other systems
- Support for FFST alerts from multiple OS/2 products
- Extensive performance threshold monitoring and alerting for:
  - OS/2 performance (PERFCAP2)
  - NetBIOS adapter performance (OSRWATCH)
  - IPX/SPX statistics
- Configuration change log
- DOS and Macintosh support

These are some key NetFinity for OS/2 features that differentiate them from LMU and make them more appropriate for workgroup and distributed environments:

- Better user interface

- Easier to set up and use
- Ability to create groups of systems instead of displaying all managed systems in the managing system′s console
- Better multiprotocol support for LAN environments (NetBIOS, IPX/SPX, TCP/IP and Serial Dial-up)
- Manager pass-through feature for accessing remote managers across a distributed network environment and managing their managed PCs
- Lotus Notes database
- Launch of NetFinity from Novell NMS
- DMTF (Desktop Management Task Force) DMI instrumentation (Desktop Management Interface)
- Software Inventory Service
- Alert information sent via E-mail (cc:Mail, Lotus Notes and TCP/IP Sendmail)
- Better PC hardware management features:
  - More detailed hardware configuration information
  - Power-On Error Detect
  - Predictive Failure Analysis
  - ECC Memory Setup
  - System Partition Access
  - Remote RAID Array management
- Very granular security options
- NetFinity for OS/2 clients do not require LAN Requester software
- APIs for development and integration of third-party extensions

These are some key NetView for OS/2 features that differentiate it from LMU and NetFinity for OS/2:

- SNMP systems and network management platform; it can manage any resource with an SNMP agent (for example, UNIX, Lotus Notes, hubs, etc.)
- SNMP subagents for managing LAN Server/LAN Requester, Communications Manager/2 and DB2/2
- SNMP management APIs for development and integration of third-party systems management applications
- Consistent graphical user interface for integration of multiple systems management applications
- More sophisticated discovery mechanisms (seed and mask files) for a wider variety of devices
- SNMP tools for fault, operations and performance management:
  - Data Collector
  - Application Builder
  - MIB Loader
  - MIB Browser
- Flexible grouping of devices on a logical basis that allows LAN administrators to display only the systems they need to manage
- Application Builder for easy creation of SNMP MIB tools without requiring any programming

2.21 DOS/Windows LAN Management

In the following sections, these IBM LAN management products for the DOS/Windows platform are discussed:

- NetView for Windows
- Nways Manager for Windows

- IBM Nways LAN Remote Monitor for Windows
- IBM Intelligent Hub Management Porgram/DOS entry

2.22 IBM NetView for Windows Version 2.0

NetView for Windows Version 2.0 provides low-cost simple network management protocol (SNMP) device management in the Windows environment. It includes fault, performance, and configuration monitoring, and manages all SNMP devices, including workstations, hubs, routers, bridges, and switches.

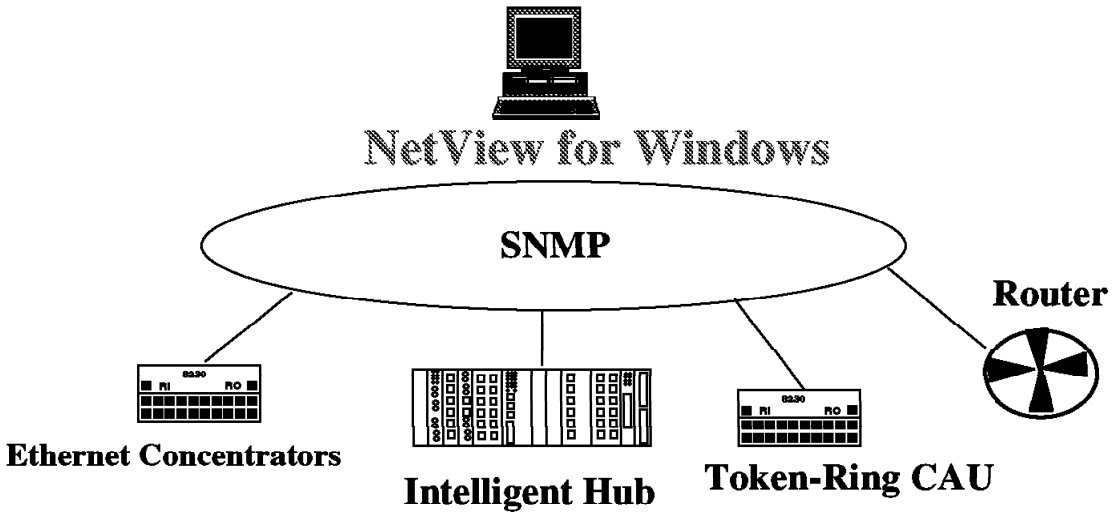


Figure 39. NetView for Windows

NetView for Windows Version 2.0 continues to provide trouble ticketing, File Transfer Protocol, Telnet capabilities, TCP/IP communications, an integrated object-oriented database, and the following:

- Supports auto-discovery of Internet Protocol (IP) resources
- Supports enhanced multivendor fault management
- Provides an improved MIB browser with a MIB compiler included
- Offers enhanced graphics for real-time statistics display
- Provides support for the industry-standard Windows Socket API

Product-specific modules (PSMs) are available for device-specific SNMP management of a number of IBM and non-IBM hardware devices. NetView for Windows Version 2.0 continues support for device-specific applications such as the IBM 8230 Model 3 Controlled Access Unit, the IBM 8224 Ethernet Stackable Hub, and the 8271 EtherStreamer (TM) Switch, supported in NetView for Windows Version 1.0.

NetView for Windows Version 2.0 works seamlessly with the Nways Manager for Windows Version 1.0, an integrated suite of network management applications

that can remotely monitor and control IBM networking devices. Some examples of PSMs included in the Nways Manager for Windows Version 1.0 are the following:

- 8224 Ethernet Stackable Hub
- 8230 Token-Ring Concentrator
- 8250 Multiprotocol Intelligent Hub
- 8271 EtherStreamer Switch
- 8281 LAN ATM Bridge
- 8282 ATM Workgroup Concentrator
- 6611 Network Processor
- 2210 Nways Multiprotocol Router
- 8260 Multiprotocol Intelligent Switching Hub
- 8238 Token-Ring Stackable Hub

2.22.1 Description

IBM NetView for Windows Version 2.0 is a low-cost Simple Network Management Protocol (SNMP) management platform on Microsoft Windows 3.1. It offers an object-oriented structure centered around an integrated database and provides a MIB browser and application program interface for device management.

Version 2.0 supports two levels of applications. Product Integration Modules (PIM) provide dialog box management information or static views about SNMP devices. Dialog boxes are available under the NetView for Windows management pull-downs. Product Specific Modules are full-function applications that provide device-specific management using an interactive graphic picture and the NetView for Windows pull-down menu.

You can layer and customize the topology network views to monitor network devices for presence, fault data, and traps. Traps, PING, and threshold status are integrated into a hierarchical database to provide fault record graphs and trouble tickets.

Performance information is provided for devices that support MIB II, and for bridges and routers. You are made aware of performance limitations through threshold alarm notifications. Performance data is maintained to provide historical tracking data so you can identify trends. This data can be presented in graph form in either real-time or historical mode.

NetView for Windows Version 2.0 adds new function including IP auto-discovery. This function is completely customizable. You can cut and paste information, and enable and disable this function as needed.

NetView for Windows Version 2.0 also adds enhanced fault management that allows you to see fault conditions reported via enterprise-specific traps with a meaningful text description of each trap. In addition, you can associate each trap with the desired level of severity that should be reported.

2.22.1.1 Usability

NetView for Windows Version 2.0 offers an intuitive, easy-to-use, and improved graphical user interface for simple navigation through the display panels for both the new and experienced user.

This ease of use allows you to become quickly productive. A Trouble Ticket feature allows for easy problem tracking. Now IP devices can be automatically discovered and displayed by way of a map function, significantly improving ease of operation. New trap management is provided to receive and interpret SNMP traps from generic network devices.

2.22.1.2 Serviceability

NetView for Windows Version 2.0 provides continuous monitoring of your network to assist in problem determination and error recovery. Failing stations can be quickly identified for problem isolation. The Trouble Ticket feature enhances the serviceability of this product.

2.22.1.3 Interoperability

NetView for Windows Version 2.0 manages IBM and non-IBM hardware devices through associated PIMs or PSMs. These applications can be developed at any time, and for IBM devices, the PIM and PSM applications will be shipped separately from the NetView for Windows Version 2.0 platform. Consult specific hardware announcements for packaging and pricing information.

2.22.1.4 Installability

NetView for Windows Version 2.0 provides an install routine to assist with the ease of installation of this program.

2.22.1.5 Open Enterprise

NetView for Windows Version 2.0 demonstrates IBM′s commitment to provide standards-based products that satisfy customer requirements for a low-end management solution.

2.22.2 Publications

For more information, the following publications are available :

- *Using NetView for Windows V2.0*, SC31-8195
- *NetView for Windows Quick Installation*, SX75-0111

Displayable softcopy publications: Only the Using NetView for Windows publication is offered in displayable softcopy form. This displayable manual is part of the basic machine-readable material. The files are shipped on the same media type as the basic machine-readable material.

2.22.3 Technical Information

The following text details the hardware and software requirements for NetView for Windows V2.0.

2.22.3.1 Hardware requirements

- 80486 DX at a minimum 33 MHz
- SVGA high resolution monitor (1,024 x 764)
- Any mouse supported by the installed operating system
- An SVGA adapter is required only if SVGA support is not built in the motherboard. Most machines will not require an SVGA adapter.
- 16 MB RAM (24 MB for large networks)
- 125 MB minimum hard disk; 240 MB recommended
- 1 MB to 2 MB video memory recommended for better performance but not required
- Network card with NDIS driver such as IBM Token-Ring Adapter 4 or 16/4 Mbps cards or the IBM Ethernet cards. Some examples of token-ring cards are the following:

  – LANStreamer (TM) MC 32 Adapter
  – LANStreamer MC 16 Adapter
  – Auto LANStreamer MC 32 Adapter
  – Auto LANStreamer PCI Adapter
  – Auto 16/4 Token-Ring ISA Adapter
  – Token-Ring Network 16/4 Adapter/A
  – Token-Ring Network 16/4 Adapter
  – Token-Ring Network 16/4 Adapter II
  – 16/4 ISA-16 Adapter

  Some examples of Ethernet cards are the following:

  – IBM LAN Adapter for Ethernet
  – IBM LAN Adapter for Ethernet TP
  – IBM LAN Adapter for Ethernet CX
  – IBM LAN Adapter/A for Ethernet
  – IBM EtherStreamer MC 32 Adapter
  – IBM Credit Card Adapter for Ethernet
  – IBM EISA Ethernet Adapter

  Other supported devices include the following:

  – IBM 8230 Token-Ring Controlled Access Unit Models 3, 4, and 13
  – IBM 8224 Stackable Ethernet Hub Model 2
  – IBM 8271 EtherStreamer Switch
  – IBM 8250 Multiprotocol Intelligent Hub
  – IBM 8281 ATM LAN Bridge
  – IBM 8282 Workgroup Concentrator
  – One 3.5-inch diskette drive

2.22.3.2 Software Requirements

- Windows 3.1, or later
- DOS 5.0, or later
- TCP/IP (included in the NetView for Windows package)
- Requires 2 MB RAM (additional to base requirement)
- Requires 8 MB free hard disk (additional to base requirement)

Compatibility: All product-specific modules supported by the previous NetView for Windows Version 1.0 product operate without change with the new IBM NetView for Windows Version 2.0.

2.22.3.3 Security, Auditability and Control

The NetView for Windows Version 2.0 provides security through password access control for two levels of users. The system administrator has full access while the operator is limited to certain operations.

User management is responsible for the evaluation, selection, and implementation of security features, administrative procedures, and appropriate controls in application systems and communication facilities.

2.23 Nways Manager for Windows Version 1

The Nways Manager for Windows program provides integrated and easy-to-use graphical interfaces for configuration, fault, and performance management of one or more IBM 8224, 8230, 8271, 8281, 8282, 8250, 2210, and 6611 networking devices.

Nways Manager for Windows Version 1 is a competitively priced integrated suite of network management applications that work seamlessly with the NetView for Windows management platform to remotely control and monitor IBM networking devices.

2.23.1 Description

Nways Manager for Windows and NetView for Windows provides the following functions:

- Remote control and monitoring of IBM networking subsystems
- Thresholding
- MIB browser
- Trouble ticketing, to gather information about network problems and following up on the problem until resolution

2.23.1.1 Integration

With applications similar to the Nways Manager for Windows program, you can manage a growing set of networking products from a single, low-cost, NetView for Windows management platform starting with management applications for the following:

- IBM 8250 Multiprotocol Intelligent Hub
- IBM 8271 EtherStreamer Switch Model 001
- IBM 8224 Ethernet Stackable Hub
- IBM 8230 Model 003 Controlled Access Unit

The suite of available IBM NetView for Windows integrated applications will be expanded over time to include other IBM and non-IBM products.

2.23.1.2 Improved Systems Availability

Nways Manager for Windows, together with NetView for Windows, enables a network operator to quickly identify and resolve network problems. Global network availability is improved; down time is reduced.

2.23.1.3 Open Enterprise

Nways Manager for Windows supports the following:

- SNMP (RFC 1155, RFC 1157, RFC 1212, RFC 1213)
- FTP
- Telnet 786
- IETF MIB II interface group

2.23.2 Product Positioning

Nways Manager for Windows is a new member in the IBM family of campus network management programs. Nways Manager for Windows integrates several existing applications for the management of the following:

- 8224 Ethernet Hub
- 8230 Model 003 Token-Ring Concentrator
- 8250 Intelligent Hub
- 8271 EtherStreamer Switch Model 001

Along with new integrated applications for:

- 8230 (Model 3/13, 213, 4A/4P) Token-Ring Concentrator
- 8281 LAN ATM Bridge
- 8282 ATM Workgroup Concentrator
- 2210 Multiprotocol Router
- 6611 Network Processor

This program provides the benefit of integrated, and easy-to-use graphical interfaces, consistent online documentation, and a simple installation process.

This program is applicable to a small campus network environment, typically small businesses or branch offices, and to medium-sized companies that occupy several buildings in a campus-like environment.

Nways Manager for Windows is the recommended management program for customers with small to medium-size campus networks or multiple SNMP devices, who want to centralize the management of various devices on a single Windows-based management platform.

2.23.3 Technical Information

The following text details the hardware and software requirements for Nways Manager for Windows Version 1.

2.23.3.1 Hardware Requirements

- 80486 DX at a minimum 33 MHz
- SVGA high-resolution workstation monitor (1024 x 764)
- 16 MB RAM
- 14 MB free hard disk space
- Network card with NDIS driver, such as IBM Token-Ring Adapter, 4 or 16/4 Mbps adapters, or IBM Ethernet Adapters
- One 3.5-inch diskette drive
- Any mouse supported by Windows 3.1

2.23.3.2 Software Requirements

- DOS 5.0, or later
- Windows 3.1, or later

Compatibility: This product is using only existing external interfaces offered by NetView for Windows.

2.23.3.3 Security, Auditability and Control

Nways Manager for Windows uses the security features of NetView for Windows. NetView for Windows provides security through password access control for two levels of users. The system administrator has full access, while the normal user is limited to certain operations.

User management is responsible for evaluation, selection, and implementation of security features, administrative procedures, and appropriate controls in application systems and communication facilities.

2.24 IBM Nways LAN Remote Monitor for Windows

The Nways LAN Remote Monitor for Windows provides management support for RMON (remote monitor) compliant agents over token-ring or Ethernet LANs. You can access real-time, statistical information on remote devices attached to your LAN. A GUI, designed specifically to hide the complexity of the RMON standard, displays activity levels and alarm locations across the network and drills down to individual workstations. You can view all activity on a LAN segment and drill down to see how specific hosts and pairs of hosts are impacting it. You can also set up LAN-specific tables, alarms, and filters on remote probes.

The Nways LAN Remote Monitor for Windows features:

- A full range of RMON-compliant functions for Ethernet and token-ring LANs
- Easy-to-use software lets you analyze real-time and historical information and troubleshoot faults
- Simple, straightforward installation
- Enabled to run with or without a network management platform
- Full RMON support for customers with Nways Manager for Windows

The Nways LAN ReMon for Windows package provides:

- Stand-alone support for very small customers who do not use a management platform

- RMON management support for customers who have invested in the Nways Manager for Windows

The Nways LAN Remote Monitor for Windows runs both in stand-alone Windows and with Nways Manager for Windows.

In summary, the LAN Remote Monitor for Windows is a standards-based client/server LAN management solution that fits flexibly into the network environment. The LAN Remote Monitor for Windows is designed to grow as industry-standards evolve.

2.24.1 Description

The LAN Remote Monitor for Windows program offers a standards-based client/server solution that fits flexibly into your network. LAN Remote Monitor for Windows can collect data for any RMON-compliant management application and can direct any RMON-compliant probe.

LAN Remote Monitor for Windows provides the following functions:

- Full RMON support for token-ring and Ethernet LANs
- Summary screen gives you a high-level view of the entire LAN segment or ring
- Rapid fault discovery and response for identifying and solving network faults
- Graphical software for analyzing data and packets collected by remote probes

2.24.1.1 Open Enterprise

LAN Remote Monitor for Windows supports the following:

- SNMP (RFC 1155, RFC 1157, RFC 1212, RFC 1213)
- IETF RMON 1 Working Group RFC 1757 (formerly 1271) and 1513

2.24.2 Product Positioning

This program is applicable for campus network environments and to companies that occupy several buildings in a campus environment.

If you have campus networks and want the advantages of being able to troubleshoot all LANs from one central workstation, LAN Remote Monitor for Windows lets experts work on several problems at once or troubleshoot a problem at more than one location.

2.24.3 Technical Information

The following text details the hardware and software requirements for LAN Remote Monitor for Windows.

2.24.3.1 Hardware Requirements

- 80486 DX at a minimum 33 MHz
- SVGA high-resolution monitor (1024 x 764)
- 8 MB of RAM
- 15 MB of free hard disk space

2.24.3.2 Software Requirements

- DOS 5.0, or later
- Microsoft Windows 3.1, or later
- TCP/IP stack (required to run stand-alone)
- NetView for Windows V2 included in Nways Manager for Windows

2.24.3.3 Security, Auditability and Control

NetView for Windows provides security through password access control for two levels of users. The system administrator has full access, while the normal user is limited to certain operations.

User management is responsible for evaluation, selection, and implementation of security features, administrative procedures, and appropriate controls in application systems and communication facilities.

2.25 IBM Intelligent Hub Management Program/DOS Entry Version 2

IHMP/DOS Entry is a licensed program which facilitates and expands the management of LANs built with IBM 8250 and IBM 8260 Multiprotocol Intelligent Hubs, and the new family of IBM 8238 Nways Token-Ring Stackable Hubs. As a result, operating environments with small to medium size networks and multiple Simple Network Management Protocol (SNMP) devices can be managed on a single PS/2-based platform.

The IBM Intelligent Hub Management Program/DOS Entry Version 2 features the following:

- Provides an easy-to-use, graphical network management interface to one or more selected IBM hubs.
- Allows you to view or change the configuration of your IBM hub.
- Supports four RMON groups: statistics, host, alarms, and events.
- Provides system status at a glance, with color codes and real-time problem detection.
- Allows you to select specific IBM hub components to manage via point-and-click selection.

IHMP/DOS Entry Version 2 supports the following IBM hubs:

- IBM 8250 Model 017/017LS
- IBM 8250 Model 006/06S/6HC/06PS
- IBM 8260 Model 10/17
- IBM 8238 Model PB1/PS1/PG1/AB1/AS1/AG1

By providing full graphical support of network devices, IHMP/DOS Version 2 brings an effective network management solution for networks that use SNMP. In addition, IHMP/DOS also brings RMON statistics support to your desktop.

With IHMP/DOS Entry Version 2, you get an easy-to-use, intuitive graphical network management interface to one or more IBM hubs (8238, 8250, 8260).

2.25.1 Description

The IHMP/DOS Entry Version 2 program offers an easy-to-use, graphical interface to manage your IBM 8238,8250, and 8260 hubs.

With IHMP/DOS Entry Version 2, network administrators can:

- View or change the configuration of the IBM hubs via point-and-click operation on a realistic, graphical, and dynamic representation of these hubs:
  - At hub level
  - At module level
  - At port level
- Detect and locate faults in the network.
- Display (graphically) and store real-time and historical statistics (faults, traffic).
- Take advantage of the RMON standard for the following groups: statistics, host, events, and alarms.
- Gather and display comprehensive statistics at network and port level (real-time and historical).
- Provide system status at a glance, with color codes, and real-time problem detection.
- Deliver real-time event monitoring, including a time-stamped alarm log.
- Enable you to download microcode to the hub agents.

2.25.1.1 Improved Worker Productivity

Easy access to statistics from the hub icon display screen space reduces time and skill for the operators controlling the network and online help is supplied with the program.

The program is supplied with online help.

2.25.1.2 Improved Systems Availability

Because of this easy access to performance data, time is reduced for problem detection and anticipation of future problems; this will significantly reduce system down time.

2.25.1.3 Centralized Control Improvements

With IHMP/DOS Entry Version 2 installed on the PS workstation, the operator has a global view of the hub network through the hubs control panel.

2.25.1.4 Open enterprise:

IHMP/DOS Entry Version 2 supports:

- SNMP (RFC 1155, RFC 1157, RFC 1212, RFC 1213)
- FTP
- Telnet 786
- IETF MIB II interface group
- RMON RFCs (Ethernet and token-ring)

2.25.2 Product Positioning

IHMP/DOS Entry is the recommended management program for networks with a small number of hubs. The high range program for IBM 8250/8260 hub management is Hub Manager for AIX, operating with NetView for AIX network management platform.

IHMP/DOS Entry addresses the needs of customers who prefer PS/2 workstation-based management over a UNIX implementation and who want to protect their investments in PS/2 stations.

With IHMP/DOS Entry operating on a portable PS/2, the station becomes the installation or maintenance station, replacing the dumb terminal connected to the hub.

This product is positioned at the very low end of our Hub Management program family as an entry solution optimized for small and medium size networks. The Nways Manager for Windows being announced today, or the previous Hub Manager for Windows (8250 only), brings more functions such as platform integration, fault/event monitoring, topology, auto discovery, or Trouble Ticket. The Nways Manager for Windows is a medium-range solution for customers with many more SNMP network devices to manage, therefore needing an SNMP platform such as Netview for Windows.

2.25.3 Technical Information

The following text details the hardware and software requirements for IHMP/DOS Entry Version 2.

2.25.3.1 Hardware Requirements

- 80486 DX at a minimum 33 MHz
- SVGA high resolution monitor (800 x 600) or better
- An SVGA adapter only if SVGA support is not built in the motherboard (most machines do not require an SVGA adapter)
- 8 MB RAM, 16 MB RAM (recommended)
- A swap space of twice the memory installed (minimum of 16MB is required)
- 40 MB free hard disk space
- Network card with NDIS driver, such as IBM Token-Ring Adapter, 4 or 16/4 Mbps adapters, or IBM Ethernet adapters
- One 3.5-inch diskette drive
- Any mouse supported by the installed operating system

2.25.3.2 Software Requirements

- DOS 5.0, or greater
- Windows 3.1, or greater
- TCP/IP stack Chameleon from NetManage
  - This software is bundled with the IHMP/DOS Entry package.

Compatibility: The IHMP/DOS Entry package includes the SNMP stack. This stack is specific to the application; we recommend having no other network application operating in the PS/2 (such as an IBM TCP/IP stack-based application).

IHMP/DOS Entry Version 2 does not operate with DOS Windows in OS/2 compatibility mode.

This product uses only existing external interfaces.

2.25.3.3 Performance Considerations

Performances is dependent upon the processor speed and disk access time. A 486 DX or faster processor is recommended.

Maximum performance is obtained with up to 100 hubs managed by IHMP/DOS Entry Version 2.

Appendix A. Special Notices

This publication is intended to help customers, systems engineers, services specialists, and marketing specialists understand LANs and IBM LAN solutions and architectures for planning and support purposes. The information in this publication is not intended as the specification of any programming interfaces that are provided by the products mentioned in this book. See the PUBLICATIONS section of the IBM Programming Announcement for IBM LAN products 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.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

ACF/VTAM	ADSTAR
Advanced Peer-to-Peer Networking	AIX
AIX/6000	AIXwindows
AnyNet	APPN
AS/400	BookManager
DATABASE 2	DatagLANce
DB2	DB2/2
DB2/6000	DFSMS
ES/9000	ES/9370
ESCON	EtherStreamer
FFST	FFST/2
First Failure Support Technology/2	HACMP/6000
IBM	LAN Distance
LANStreamer	MVS/ESA

MVS/SP	NetFinity
NetView	Nways
Operating System/2	OS/2
Person to Person	PowerPC
POWERstation	POWERserver
Predictive Failure Analysis	Presentation Manager
Print Services Facility	PS/2
PSF	RISC System/6000
RMONitor	S/370
S/390	SAA
SystemView	System/390
System/370	Trouble Ticket
VM/ESA	VTAM
WIN-OS/2	Workplace
Workplace Shell	400

The following terms are trademarks of other companies:

C-bus is a trademark of Corollary, Inc.

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.

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

Advantis	Advantis
Apple, Macintosh, AppleTalk, TokenTalk, EtherTalk, LocalTalk, Mac	Apple Computer, Incorporated
ARCnet	Datapoint Corporation
AT&T	American Telephone and Telegraph Company
Attachmate	Attachmate Corporation
Banyan	Banyan Systems, Incorporated
cc:Mail	cc:Mail, Incorporated
Cisco	Cisco Systems, Incorporated
Compaq	Compaq Computer Corporation
DECnet, DEC, Digital, VAX, VMS	Digital Equipment Corporation
Designer	Micrografx, Incorporated
Dialog	American Telephone and Telegraph Company
EtherLink, NDIS, 3Com	3Com Corporation
Hewlett-Packard, HP, OpenView	Hewlett-Packard Company
HYPERchannel	Network Systems Corporation
IDNX	Network Equipment Technologies, Incorporated
Intel, Pentium, SX, 386, 486	Intel Corporation
IPX, LANalyzer, NetWare, NetWare MHS, Novell	Novell, Incorporated
LANtastic	Artisoft, Incorporated
Lotus, Lotus Notes	Lotus Development Corporation
Motif	Open Software Foundation, Incorporated
MS, MS-DOS, NDIS, Visual Basic	Microsoft Corporation
Network File System, NFS, Solaris, Sun, SunOS	Sun Microsystems, Incorporated
Open Server	The Santa Cruz Operation, Incorporated
Oracle	Oracle Corporation
Motif, OSF, OSF/Motif	Open Software Foundation, Incorporated

Paradox	Borland International, Incorporated
PostScript	Adobe Systems Incorporated
Proteon	Proteon, Incorporated
Qualitas	Qualitas
Quarterdeck	Quarterdeck Corporation
SCO	The Santa Cruz Operation, Incorporated
SCSI	Security Control Systems, Incorporated
Sniffer Network Analyzer	Network General Corporation
SPARCstation	SPARC International, Incorporated
Sybase	Sybase, Incorporated
SynOptics	SynOptics Communication Incorporated
Toshiba	Toshiba Corporation
Wellfleet	Wellfleet Communications, Incorporated
X-Windows	Massachusetts Institute of Technology
X/Open	X/Open Company Limited
Xerox	Xerox Corporation
386MAX	Qualitas, Incorporated

Other trademarks are trademarks of their respective companies.

Appendix B. Related Publications

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

B.1 International Technical Support Organization Publications

For information on ordering these ITSO publications see “How To Get ITSO Redbooks” on page 193.

- *LAN Management Using LNM for OS/2 V2.0 and LNM for AIX*, SG24-2504
- *Local Area Network Concepts and Products: LAN Adapters, Hubs an ATM*, SG24-4754
- *IBM 8250 Intelligent Hub and IBM Hub Management Program/6000*, GG24-4033-00
- *The IBM 6611 Network Processor as an IP Router*, GG24-4064-00 (available on CD-ROM, SK2T-6022)
- *High-Speed Networking Technology: An Introductory Survey*, GG24-3816-01 (available on CD-ROM, SK2T-6022)
- *IBM Workgroup Hubs and Switches*, GG24-2528-00
- *8260 Multiprotocol Intelligent Switching Hub*, GG24-4370-00
- *IBM 2220 Nways BroadBand Switch: Concepts and Products*, GG24-4307-00
- *Asynchronous Transfer Mode (ATM) Technical Overview*, SG24-4625-00

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

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

B.2 Other Publications

These publications are also relevant as further information sources:

- *Local Area Network Concepts and Products: LAN Architecture*, SG24-4753
- *NetView MultiSystem Manager MVS/ESA V2R1 Open Topology Interface*, ST00-9535
- *NetView for MVS V3R1 Graphic Monitor Facility User's Guide*, SC31-8095
- *NetView for MVS V3R1 Customization Guide*, SC31-8052
- *LAN NetView Management Utilities for OS/2 User's Guide*, SC30-3555
- *NetView for MVS V3R1 Installation and Administration Guide* SC31-8043
- *NetView Multisystem Manager Internet Protocol Networks*, SC31-8131-01
- *NetView Multisystem Manager Open Topology Interface*, SC31-8144-01
- *NetView Multisystem Manager LAN NetView Management*, Utilities, SC31-8112-01
- *NetView Multisystem Manager Novell NetWare Networks*, SC31-8129-01

- *NetView Multisystem Manager OS/2 LAN Network Manager*, SC31-8130-01
- *Examples Using NetView for AIX*, GG24-4327
- *Nways Campus Manager Remote Monitor Installation and User's Guide (LAN ReMon AIX/HP only)*, SA33-0367
- *Nways Campus Manager Remote Monitor Traffic Transmission Management Module User's Guide*, SA33-0369
- *Nways Campus Manager Remote Monitor Enterprise Communication Analysis Module User's Guide*, SA33-0368
- *Installing LAN Network Manager for AIX*, GC31-7114
- *Getting Started with LNM for AIX*, SC31-7109
- *Using LNM for AIX*, SC31-7110
- *LNM for AIX Reference*, SC31-7111
- *AIX LAN Management Utilities/6000 User's Guide*, SC31-7154
- *Using LAN Network Manager for OS/2 Version 2.0,*, SC31-7105
- *Using NetView for Windows V2.0*, SC31-8195
- *NetView for Windows Quick Installation*, SX75-0111
- *IBM OS/2 LAN Server Version 4.0 Commands and Utilities*, S10H-9686
- *OS/2 LAN Server Network Admin Ref Vol 3: Network Administrator Tasks*, S10H-9682
- *IBM Multiprotocol Network Program: User's Guide*, SC30-3559
- *Internetworking with TCP/IP Volume I: Principles, Protocols, and Architecture*, SC31-6144

How To Get ITSO Redbooks

This section explains how both customers and IBM employees can find out about ITSO redbooks, CD-ROMs, workshops, and residencies. A form for ordering books and CD-ROMs is also provided.

This information was current at the time of publication, but is continually subject to change. The latest information may be found at URL http://www.redbooks.ibm.com/redbooks.

How IBM Employees Can Get ITSO Redbooks

Employees may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **PUBORDER** — to order hardcopies in United States
- **GOPHER link to the Internet**

  Type GOPHER.WTSCPOK.ITSO.IBM.COM
- **Tools disks**

  To get LIST3820s of redbooks, type one of the following commands:

  ```
  TOOLS SENDTO EHONE4 TOOLS2 REDPRINT GET SG24xxxx PACKAGE
  TOOLS SENDTO CANVM2 TOOLS REDPRINT GET SG24xxxx PACKAGE (Canadian users only)
  ```

  To get lists of redbooks:

  ```
  TOOLS SENDTO WTSCPOK TOOLS REDBOOKS GET REDBOOKS CATALOG
  TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET ITSOCAT TXT
  TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET LISTSERV PACKAGE
  ```

  To register for information on workshops, residencies, and redbooks:

  ```
  TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ITSOREGI 1996
  ```

  For a list of product area specialists in the ITSO:

  ```
  TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ORGCARD PACKAGE
  ```
- **Redbooks Home Page on the World Wide Web**

  http://w3.itso.ibm.com/redbooks/redbooks.html
- **IBM Direct Publications Catalog on the World Wide Web**

  http://www.elink.ibmlink.ibm.com/pbl/pbl

  IBM employees may obtain LIST3820s of redbooks from this page.
- **ITSO4USA category on INEWS**
- **IBM Bookshop** — send orders to:

  USIB6FPL at IBMMAIL or DKIBMBSH at IBMMAIL
- **Internet Listserver**

  With an Internet E-mail address, anyone can subscribe to an IBM Announcement Listserver. To initiate the service, send an E-mail note to announce@webster.ibmlink.ibm.com with the keyword subscribe in the body of the note (leave the subject line blank). A category form and detailed instructions will be sent to you.

How Customers Can Get ITSO Redbooks

Customers may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **IBMLINK**

  Registered customers have access to PUBORDER to order hardcopy, to REDPRINT to obtain BookManager BOOKs

- **IBM Bookshop** — send orders to:

  usib6fpl@ibmmail.com (United States)
  bookshop@dk.ibm.com (Outside United States)

- **Telephone orders**

1-800-879-2755	Toll free, United States only
(45) 4810-1500	Long-distance charge to Denmark, answered in English
(45) 4810-1200	Long-distance charge to Denmark, answered in French
(45) 4810-1000	Long-distance charge to Denmark, answered in German
(45) 4810-1600	Long-distance charge to Denmark, answered in Italian
(45) 4810-1100	Long-distance charge to Denmark, answered in Spanish

- **Mail Orders** — send orders to:

IBM Publications	IBM Direct Services
P.O. Box 9046	Sortemosevej 21
Boulder, CO 80301-9191	DK-3450 Allerød
USA	Denmark

- **Fax** — send orders to:

1-800-445-9269	Toll-free, United States only
45-4814-2207	Long distance to Denmark

- **1-800-IBM-4FAX (United States only)** — ask for:

  Index # 4421 Abstracts of new redbooks
  Index # 4422 IBM redbooks
  Index # 4420 Redbooks for last six months

- **Direct Services**

  Send note to softwareshop@vnet.ibm.com

- **Redbooks Home Page on the World Wide Web**

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

- **IBM Direct Publications Catalog on the World Wide Web**

  http://www.elink.ibmlink.ibm.com/pbl/pbl

- **Internet Listserver**

  With an Internet E-mail address, anyone can subscribe to an IBM Announcement Listserver. To initiate the service, send an E-mail note to announce@webster.ibmlink.ibm.com with the keyword subscribe in the body of the note (leave the subject line blank). A category form and detailed instructions will be sent to you.

IBM Redbook Order Form

Please send me the following:

Title	Order Number	Quantity

- **Please put me on the mailing list for updated versions of the IBM Redbook Catalog.**

First name Last name

Company

Address

City Postal code Country

Telephone number Telefax number VAT number

- Invoice to customer number _____
- Credit card number _____

Credit card expiration date Card issued to Signature

We accept American Express, Diners, Eurocard, Master Card, and Visa. Payment by credit card not available in all countries. Signature mandatory for credit card payment.

DO NOT SEND CREDIT CARD NUMBERS OVER THE INTERNET.

Index

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

Printed in U.S.A.