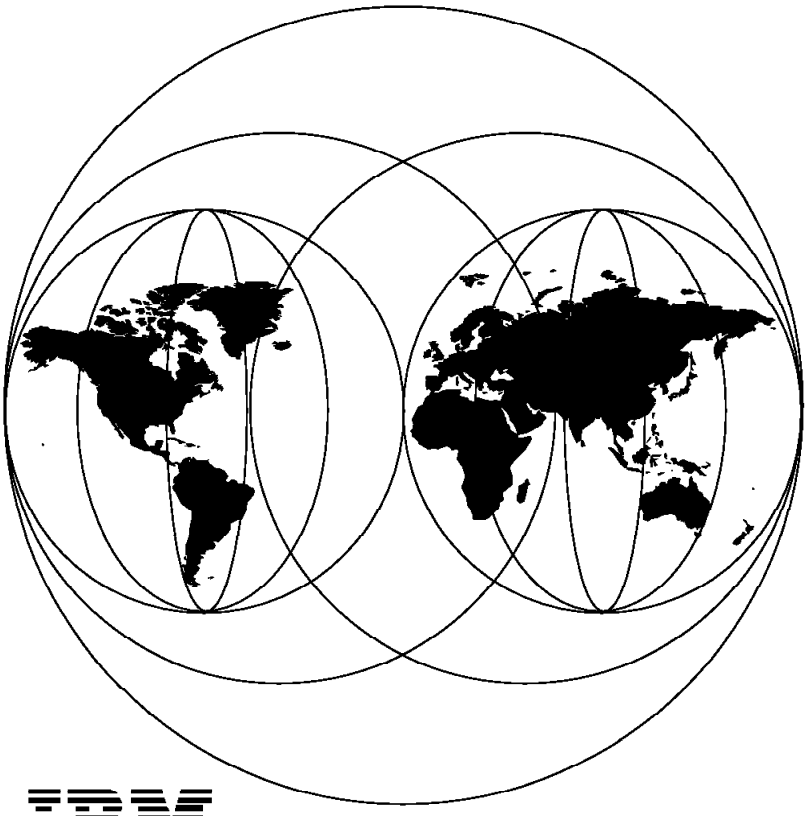
International Technical Support Organization

GG24-4337-00

Managing IP Networks Using NetView MultiSystem Manager R2

December 1994



IBM

International Technical Support Organization
Raleigh Center

International Technical Support Organization

GG24-4337-00

Managing IP Networks Using NetView MultiSystem Manager R2

December 1994

Take Note!

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

First Edition (December 1994)

This edition applies to Version 1, Release Number 2 of IBM NetView MultiSystem Manager MVS/ESA, Program Number 5655-044.

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

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

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

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

Abstract

This document describes how to centrally manage IP environments using IBM NetView MultiSystem Manager (MSM).

It shows how to set up MSM and NetView for AIX to make management as simple and effective as possible. It includes many customized samples and demonstrates some uses of the optional MSM tools.

The document shows how to create your own customized NGMF views and exception views and includes automation samples which show how to keep these views current.

The managed resources include IP hosts, routers, bridges and hubs.

This document is intended for people who plan to install, customize, and operate MSM Release 2. Some knowledge of NetView GMF is assumed as well as some NetView for AIX and TCP/IP skills.

(276 pages)

Contents

Figures

Tables

Special Notices

This publication is intended to provide information on how to centrally manage IP environments using the IBM NetView MultiSystem Manger (MSM). The information in this publication is not intended as the specification of any programming interfaces that are provided by IBM NetView MultiSystem Manager MVS/ESA. See the PUBLICATIONS section of the IBM Programming Announcement for IBM NetView MultiSystem Manager MVS/ESA 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 Commercial Relations, 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 document contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples contain the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

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

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

ACF/VTAM	Advanced Peer-to-Peer Networking
AIX	AIX/6000
APPN	CT/2
IBM	MVS/ESA
NetView	OS/2
POWERstation	Presentation Manager
PS/2	RACF
RISC System/6000	RS/6000
SystemView	VTAM

The following terms are trademarks of other companies:

INFORMIX	Informix Software, Incorporated
Oracle	Oracle Corporation
OSF and OSF/Motif	Open Software Foundation, Inc.
Novell	Novell, Incorporated
NetWare	Novell, Incorporated
X-Windows	Massachusetts Institute of Technology

Other trademarks are trademarks of their respective companies.

Preface

This document is intended for network analysts, system programmers, operators and planners using the IBM NetView MultiSystem Manager MVS/ESA or planning for its installation. It contains information on both the installation and operation of MSM for managing IP networks.

How This Document Is Organized

The document is organized as follows:

- Chapter 1, “Product Positioning”

  This chapter describes the integration of MultiSystem Manager in the network management area.

- Chapter 2, “Overview”

  This chapter provides a brief overview of MultiSystem Manager and how to manage your LAN, NetWare and IP networks from a central point.

- Chapter 3, “The MSM IP Tower”

  This chapter describes the functions provided by the IP tower in MultiSystem Manager. The chapter is organized as indicated below:

  – General information

  – Sample IP views in NGMF

  – NetView for AIX to MSM communication

  – Installation of the IP agent code

  – IP agent functions

  – Monitoring resources

  – Managing resources

- Chapter 4, “Sample IBM NetView MultiSystem Manager Scenarios”

  This chapter describes scenarios that show how to use MultiSystem Manager to manage networks including IP and LAN resources.

- Chapter 5, “Installation and Customization”

  This chapter describes:

  – NetView MSM host installation

  – NetView MSM workstation installation

  – NetView MSM informal documentation installation

- Chapter 6, “MSM Data Models and Usage for IP”

  This chapter describes the MSM data model. You need to understand how the MSM data model is organized if you plan to develop your own automation procedures or applications which use the information provided by MultiSystem Manager (using the MSM data model).

  A brief introduction to SystemView data definition concepts has also been included in this chapter.

- Chapter 7, “IBM NetView MultiSystem Manager Tools”

  This chapter describes some tools that can be used to customize NetView MSM.

Related Publications

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

- *IBM Local Area Network Host Information*, GC30-3479
- *SNA Management Service Reference*, SC30-3346
- *RODM Programming Guide SC31-6130*
- *IBM NetView MultiSystem Manager MVS/ESA for Novell NetWare Networks, SC31-7068*
- *IBM NetView MultiSystem Manager MVS/ESA for OS/2 LAN Network Manager Networks, SC31-6157*
- *NetView MultiSystem Manager MVS/ESA: NetView for AIX Networks Release 2, SC31-8041*
- *NetView Samples (MVS), SC31-6126*
- *NetView Customization Guide, SC31-7091*
- *NetView Graphic Monitor Facility User's Guide, SC31-7089*
- *NetView Tuning Guide, SC31-7079*
- *NetView for AIX Administrator's Guide, SC31-7192*
- *AIX Installation, Operation and Programming Guide, SC31-6120*

International Technical Support Organization Publications

- *Centralized Management of LNM and NetWare Networks Using NetView MultiSystem Manager MVS/ESA, GG24-4181*
- *NPM Version 2.1 Experiences Using The New GUI and VTAM Statistics, GG24-4156*
- *Overview of IBM NetView Resource Object Data Manager (RODM) and Data Models, GG24-3956*
- *RODMTool/2: Advanced Use Of NetView Graphic Monitor Facility, GG24-4292*
- *NetView V2R4 APPNTAM Feature Experiences, GG24-4203*
- *Examples of Using NetView for AIX, GG24-4327*
- *Applied Use of IBM NetView RODM and Automation, GG24-4018*

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

International Technical Support Organization Bibliography, GG24-3070.

Acknowledgments

The advisors for this project were:

Rob Macgregor
Trygve Skibeli
George Steinborn
Fergus Stewart
International Technical Support Organization, Raleigh

The authors of this document are:

Rita Steffes-Hollaender
IBM Germany

Karl Wozabal
IBM Austria

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

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

Lee Bumgarner
Joost Fonville
Vikki Hamann
Ken Howey
Eamon Murphy
Barry Nusbaum
Carla Sadtler
Dave Shogren
Shawn Walsh
Gail Wojton
International Technical Support Organization, Raleigh

Chris Mason
Technical Education
IBM IEC La Hulpe

Gary A. Forghetti
Mark L. Wright
NS Field Support
IBM RTP

David L. Schmidt
NS System Test
IBM RTP

Chapter 1. Product Positioning

The IBM* NetView MultiSystem Manager (MSM) Release 2 brings NetView* one step closer to overall enterprise-wide systems management using object-oriented and international standards. This release of MSM provides an integrated network management facility that enables centralized management of IP Networks, LAN Network Manager and Novell** NetWare** networks from a NetView Graphic Monitor Facility (NGMF) workstation.

The IBM NetView MultiSystem Manager provides dynamic topology and status discovery to simplify the task of monitoring and managing your LNM, Novell and IP networks.

1.1 IBM NetView MultiSystem Manager Components

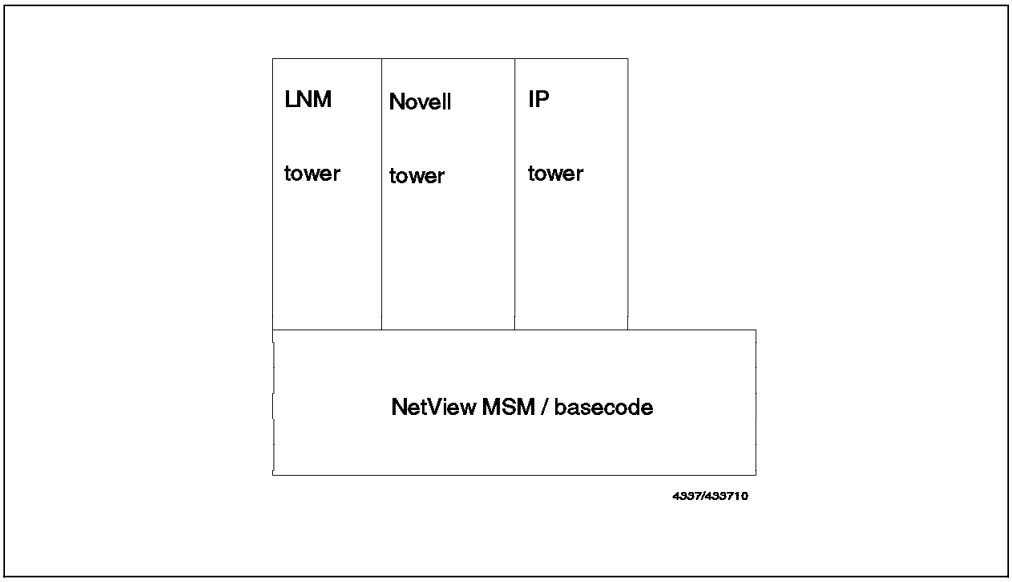


Figure 1. Component Parts of IBM NetView MultiSystem Manager

The IBM NetView MultiSystem Manager consists of a base feature and separate topology features for each environment you want to manage. With the MultiSystem Manager base code and the three available towers, you can perform centralized, dynamic and graphical management of IP, LNM and NetWare resources.

These manageable resources are:

- IP Networks
- IP Segments
- IP Routers
- IP Hosts
- IP Hubs
- LAN Adapters
- LAN Bridges

- Controlled Access Units (CAUs)
- LAN Segments
- NetWare Servers
- NetWare Requesters

1.2 Object-Oriented Technology

MultiSystem Manager is designed to provide management functions for a variety of different network environments. Different networks, represented through different network feature codes, use the same topology manager code to manage the network configuration information as illustrated in Figure 1 on page 1. The topology manager uses NetView′s high-speed data cache, the Resource Object Data Manager (RODM), for storing and retrieving topology and status information.

The definitions of the managed resources in this data cache are represented in a data model structure using an object-oriented approach.

MultiSystem Manager uses three models, or in object-oriented terminology, three domains, in the data cache:

- A service point domain. In this domain you define the protocols and the data flow that is used between the manager and its agents.

  This domain is common to all service point applications and is defined in the GMFHS data model.

- A presentation domain. This domain defines the views and the presentation rules for the resources.

  The real resources are aggregated into homogeneous groups and they can be displayed in views with other heterogeneous resources. These views can be customized for different management tasks. The presentation domain is part of the GMFHS data model.

- A management domain. This domain represents the management rules of the managed resources.

  This domain is the representation of real network resources and determines how those resources are managed.

Under the object-oriented paradigm, the behavior of a single resource is hidden in the object definition. For management purposes operators do not need to know which command syntax they have to use. The behavior of an object can be defined at a higher class level and will be inherited down to the object level. MultiSystem Manager has implemented this object-oriented technique and the concepts of the SystemView data model structure and is, therefore, a SystemView-conforming product.

Chapter 2. Overview

This chapter provides an overview of MultiSystem Manager and will help you understand what MultiSystem Manager is, what it can manage, and how you can use it.

MultiSystem Manager uses a manager-agent relationship to manage LAN and IP workgroups. This relationship consists of a managing system, from now on referred to as the topology manager, and managed systems, from now on referred to as topology agents. The MSM environment is illustrated in Figure 2.

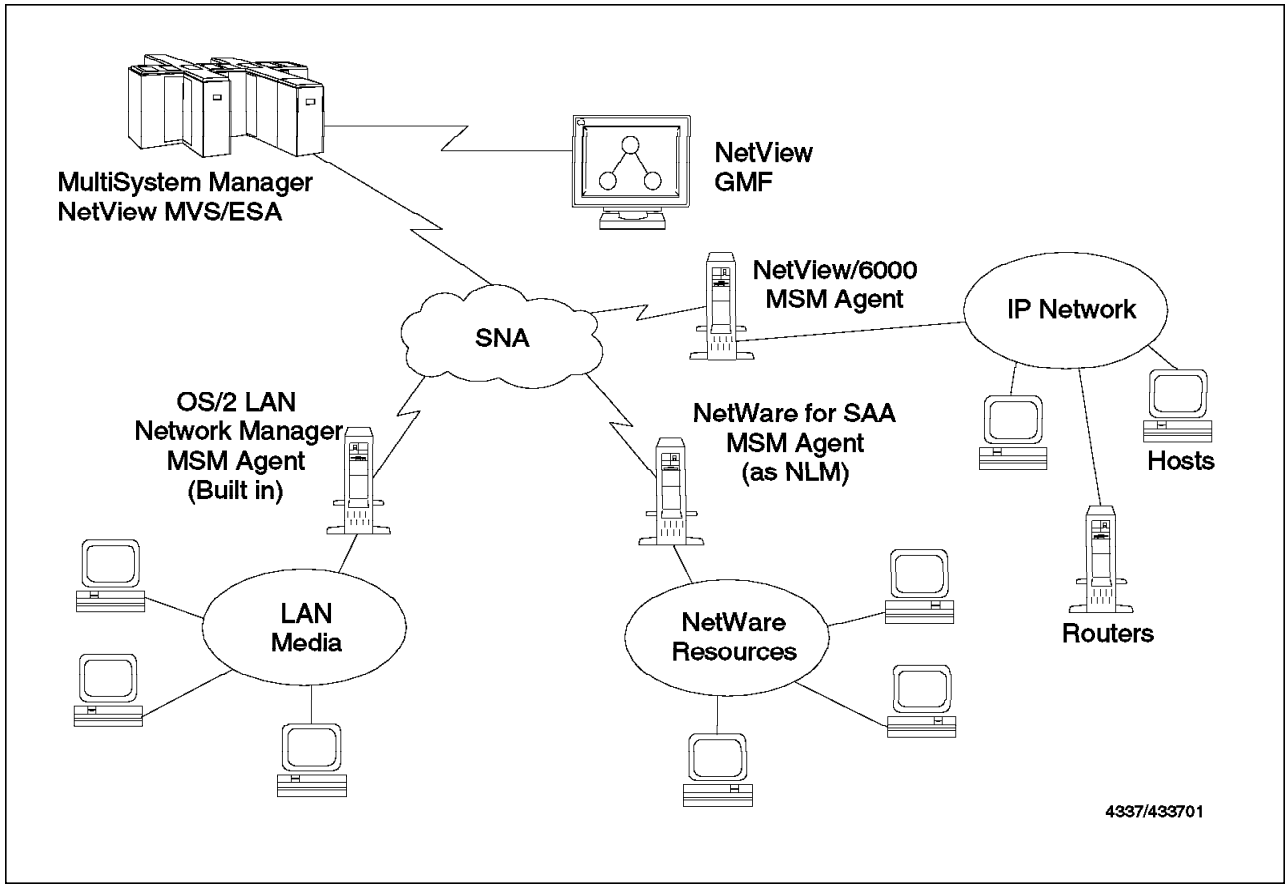


Figure 2. IBM NetView MultiSystem Manager Overview

2.1 Managed Systems

MultiSystem Manager Release 1 provides management of the following resources:

- LAN media
  - Adapters
  - Bridges
  - Controlled Access Units (CAUs)
  - Segments

- Novell NetWare networks:
  - NetWare Servers
  - NetWare Requesters

Additionally, MSM Release 2 enables management of the following IP network resources:

- Networks
- Locations
- Subnets
- Segments
- Routers
- Hosts
- Bridges
- Hubs
- Interfaces

The MSM topology agents are supported for the following software platforms:

- NetView/6000
- NetView for AIX*
- LAN Network Manager Entry
- LAN Network Manager
- Novell NetWare

Note: For both LAN Network Manager Entry and LAN Network Manager, the topology agent is included in the product. For Novell NetWare the topology agent is shipped as two NetWare loadable modules (NLMs). For NetView/6000 and NetView for AIX the topology agent is shipped as three AIX files.

The role of the topology agents is to monitor all of the resources controlled by the workstation in which the agent resides and to dynamically communicate any changes in resource status to the topology manager. The NetView/6000 agent only retrieves topology information from the NetView/6000 database when requested by MSM. Resource status changes are sent to MSM by NetView/6000.

2.2 Managing System

As briefly mentioned in Chapter 1, “Product Positioning” on page 1, MSM consists of a base component and features for the different environments. Figure 3 on page 5 provides more detail showing the components of the MSM base code.

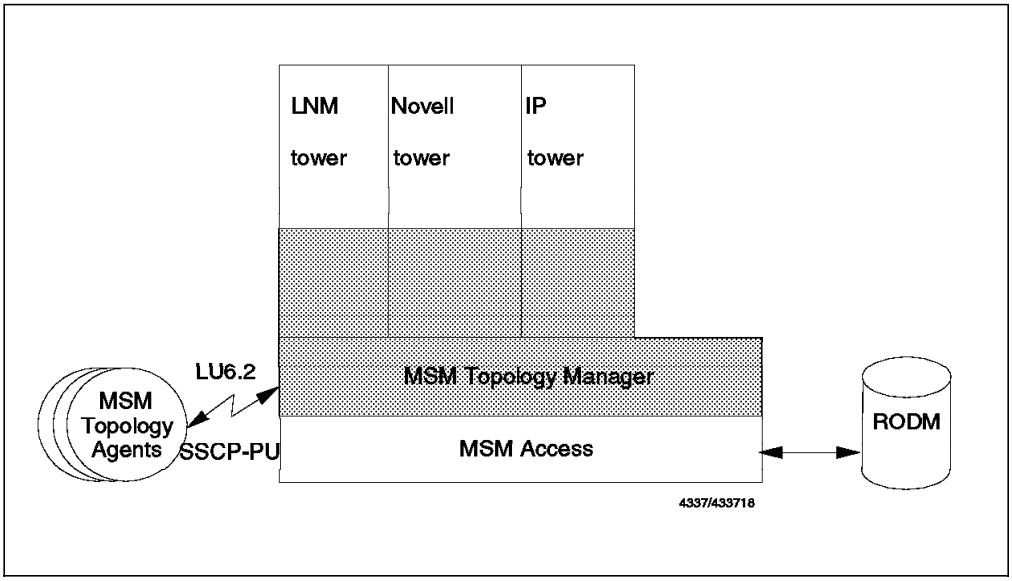


Figure 3. Detail of IBM NetView MultiSystem Manager Component Parts

MSM consists of the following components:

- NetView REXX command lists with a REXX alternate library

  Note: With SAA* REXX/370 installed, the command lists run compiled. Without the SAA REXX/370 installed, the command lists will run with the alternate library.

- NetView command processors
- NetView panels
- Load files for the MSM data model

The command lists and command processors can run in one or several NetView autotasks (for load balancing).

The MSM topology manager performs the following tasks:

- Dynamically discovers the topology and status of the network.
- Stores this information in the NetView Resource Object Data Manager (RODM).
- Automatically processes topology and status updates from the topology agents.

Centralized and integrated LAN and IP management can be achieved, because status information about your networks and all LAN and IP resources is stored in RODM. The information in RODM relates to the information received from your topology agents. In addition MSM allows graphical management of LAN and IP resources by displaying the information on the NetView Graphic Monitor Facility (NGMF) workstation. Figure 4 on page 6 shows you how MSM works in the NetView environment.

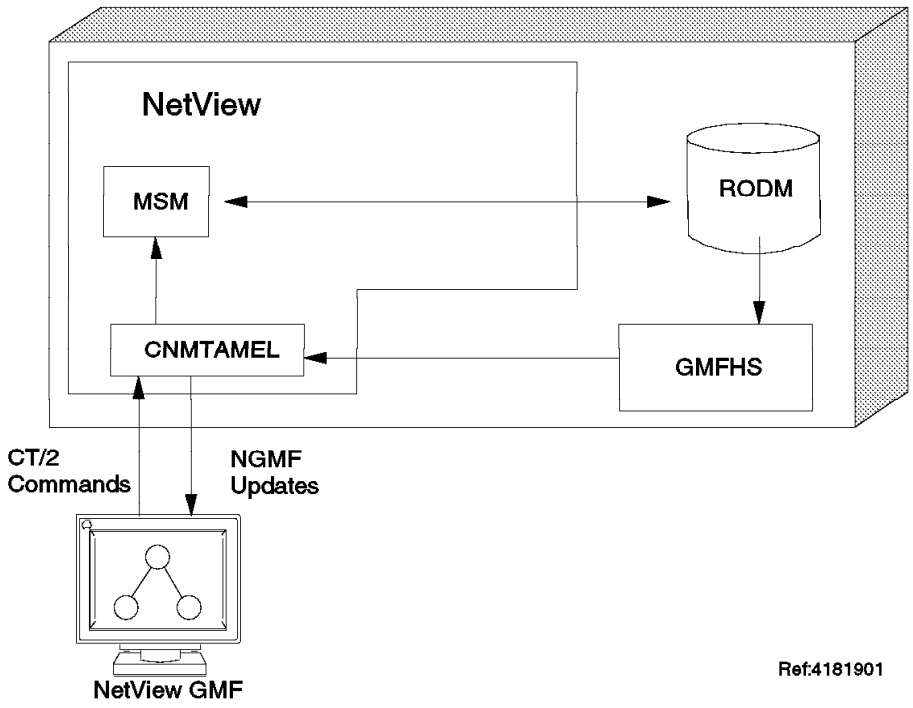


Figure 4. IBM NetView MultiSystem Manager and NetView

2.2.1 IBM NetView MultiSystem Manager Presentation Services

Using NGMF you can navigate through the views of your networks. Figure 5 on page 7 gives you an example of the IP views created by MultiSystem Manager.

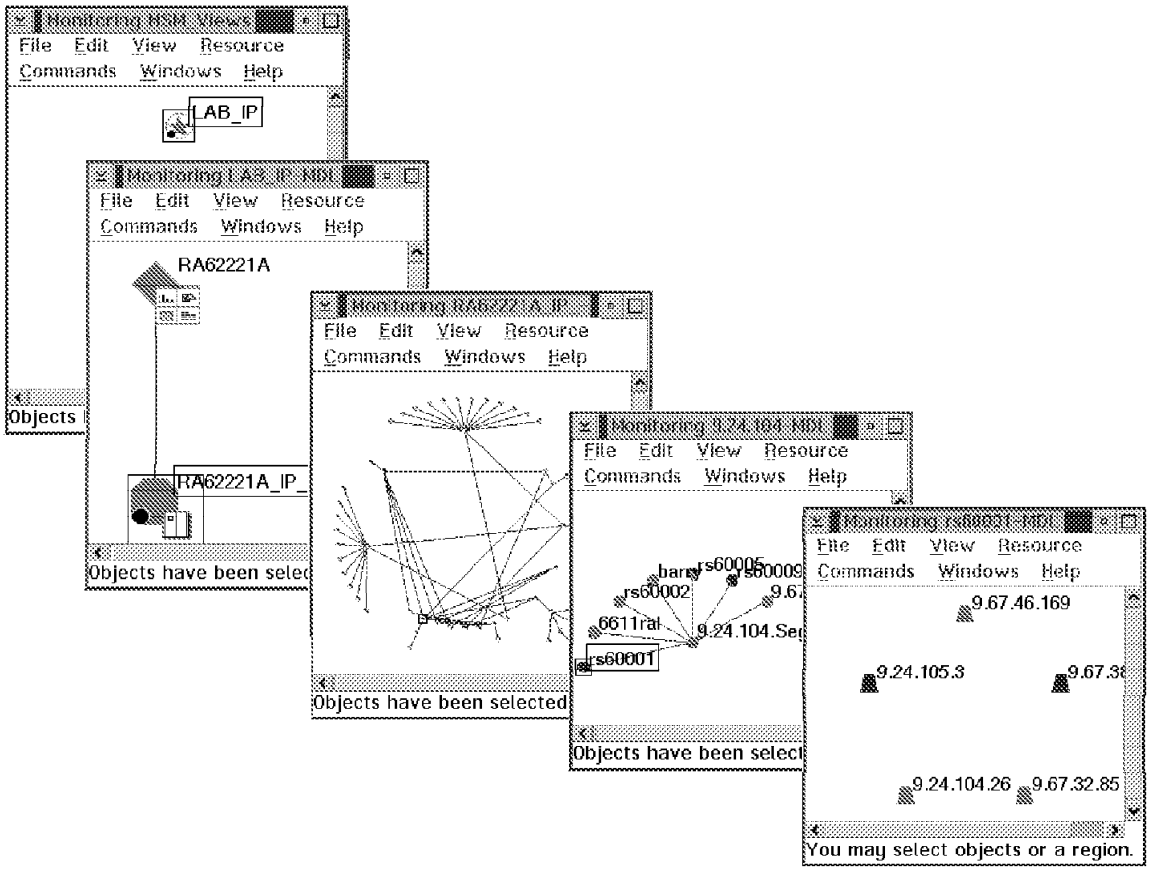


Figure 5. IBM NetView MultiSystem Manager Views

As a result of the object-oriented approach used in the data repository (RODM), the IP objects/views created by MSM can easily be integrated with other types of objects/views in RODM (for example LAN adapter, NetWare requester or SNA shadow objects). See Chapter 7, “IBM NetView MultiSystem Manager Tools” on page 149 for a description of how MSM-supplied tools can be used to achieve this integration.

2.3 Manager-to-Agent Communication

The MSM topology manager communicates with the topology agents by means of NetView RUNCMD commands across SNA sessions. Topology agents communicate with MSM through RUNCMD responses, alerts and resolutions.

2.3.1 RUNCMD

RUNCMD commands are SNA Network Management Vector Transports (NMVTs) that you send from NetView to a service point application. The workstation topology agent translates each NetView RUNCMD command into the specific workstation command. Command response NMVTs contain information about the workstation or about the result of a workstation command. After the workstation processes a command from NetView, the topology agent builds a command response, imbeds it in an SNA/MS NMVT and sends it to NetView.

2.3.2 Alerts and Resolutions

Alerts in this context are SNA/MS NMVTs sent from service point applications to NetView. The alerts from the service points will appear in the hardware monitor component of NetView.

The topology agent sends an alert when it wants to notify the topology manager of a topology or status change. When all of the problems associated with a resource are corrected, the topology agent sends a resolution notification to the topology manager indicating that the resource has now returned to a satisfactory status.

2.4 Monitoring Resources

Once the initial status for the managed resources is stored in RODM, the MSM agents can notify NetView of topology or status changes by sending alerts to NetView.

The NetView Automation Table routes the alerts to the topology manager and the GMFHS event manager. The topology manager queries RODM for the topology resources. If the resources that caused the topology change alert are not found in RODM, the topology manager will create them.

In addition, the GMFHS event manager processes these alerts and forwards them to the MSM AlertProc DUIFECMV. This AlertProc provides the code required for locating and changing status for the associated MSM object in RODM. GMFHS will also store these alerts in the Alert History Database.

Figure 6 on page 9 shows how the alerts flow through MSM.

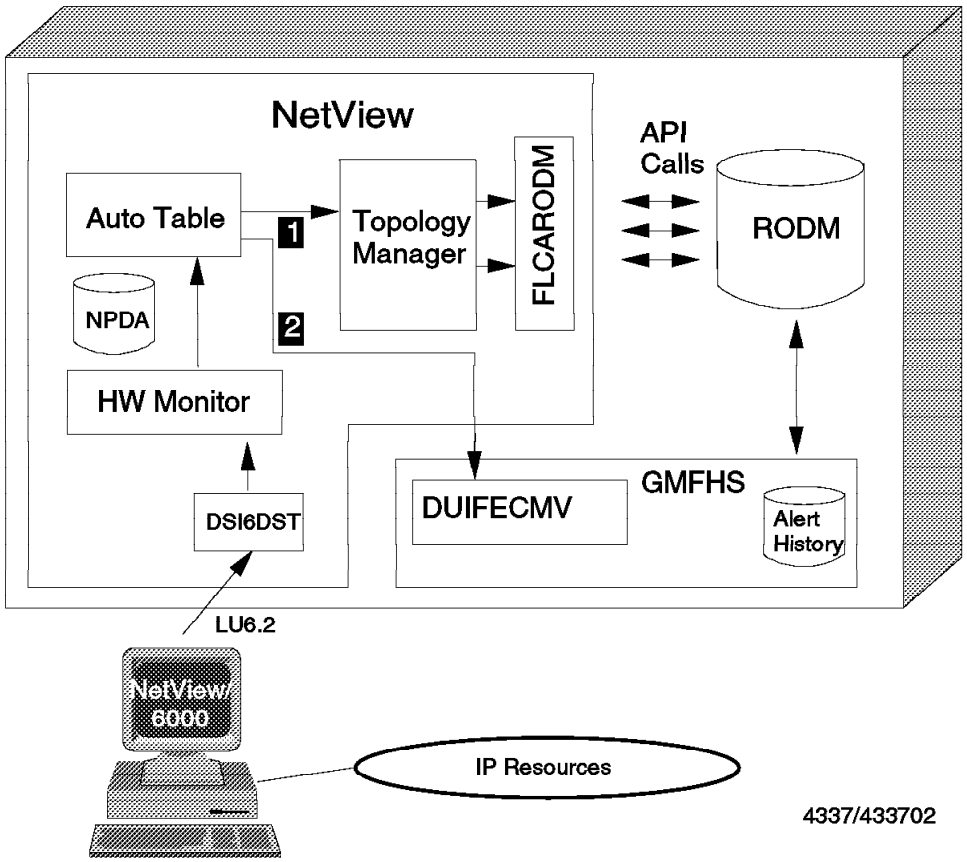


Figure 6. Alert Flow

Key Explanation:

1 The NetView Automation Table routes the alerts to the topology manager, which in turn queries RODM and creates the instance (resource) when necessary.

2 The NetView Automation Table also routes the alerts to the GMFHS Event Manager (DUIFECMV) which is used to map the alerts to RODM objects.

2.5 Managing Resources

In addition to the RUNCMDs sent from the NetView MSM topology manager, operators can send commands to the MSM agents in the following ways:

- NGMF Commands pull-down menu
  - Generic commands
  - NetView command line
  - Non-SNA command line
  - Remote console
  - Build commands with use of Command Tree/2
- Native Command Tree/2 from the NetView icon view

The Build commands function in NGMF is a user-friendly and powerful way of issuing commands to the service points. You can manage resources in the following manner:

1. Select the **Commands** pull-down and select **Resource specific commands**.
   - The Command Tree/2 panel will be displayed.
   - Select a command from the command tree.
   - An appropriate DMCS command will be built and sent to NetView.

   Note

   The DMCS command list is a high-level command list that simplifies the way to send commands to the service points. It retrieves data from the selected object in RODM, filling in the resource name and other values for you. This flow of information is illustrated in Figure 7.

2. DMCS converts the command to an appropriate RUNCMD.
3. The RUNCMD is sent to the MSM agent.
4. The RUNCMD response will appear in the NetView Command Response window.

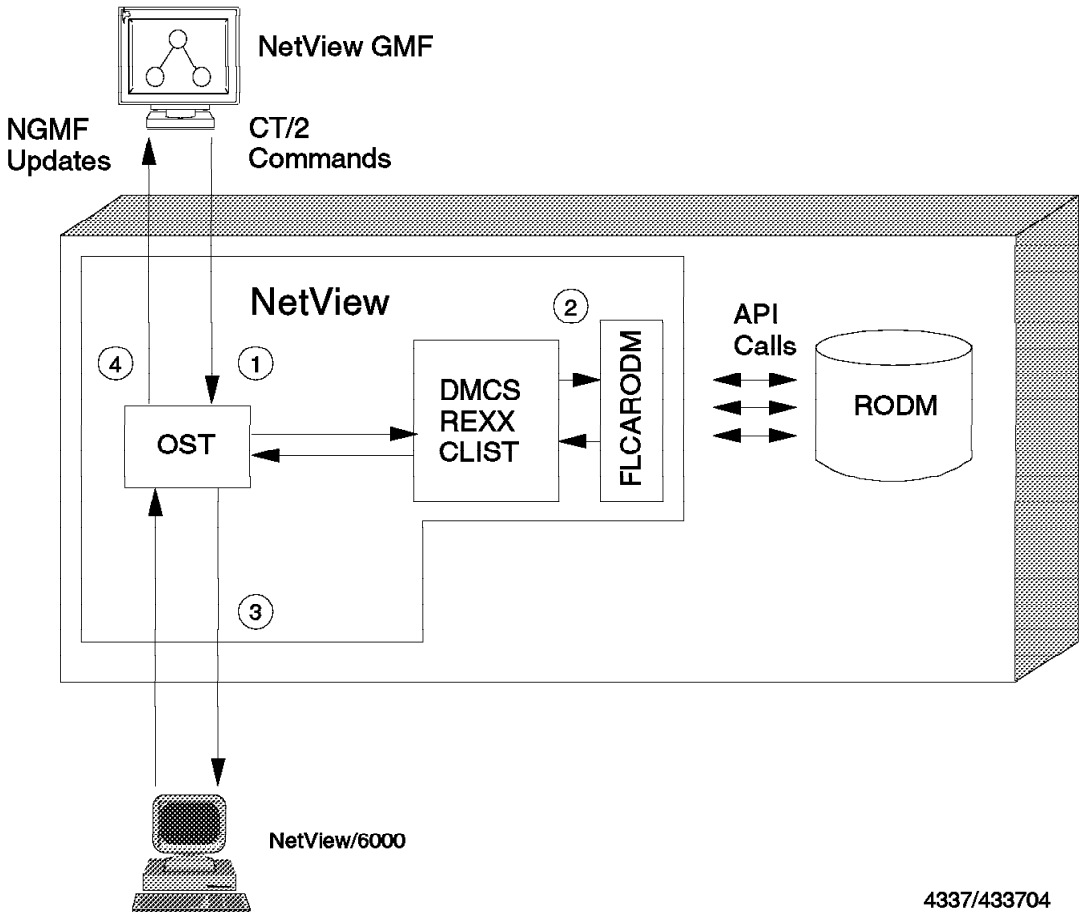


Figure 7. Managing with DMCS CLISTs

Chapter 3. The MSM IP Tower

This chapter describes the functions provided by the IP tower in MultiSystem Manager managed networks. The chapter is organized as indicated below:

- General information
- Overview of the available NGMF views
- NetView for AIX to MultiSystem Manager communication
- Installation of the MSM agent code
- Overview of IP agent functions
- Customizing the IP Views
- Monitoring IP Resources
- Managing IP Resources

3.1 General Information

As the importance of IP networks grows in an organization and resources become more heterogeneous, it becomes apparent that these networks should be managed from a central point. This may be because they are installed in remote geographies where support personnel are not always on hand or because it is necessary to have a 24-hour-per-day operation at a single point of contact. There are different platforms you can use to achieve this. NetView for AIX offers capabilities to manage LAN and SNA environments in addition to IP networks. MultiSystem Manager allows you to manage your IP networks with other environments such as LANs and SNA on a single workstation or on multiple workstations running OS/2. Included below is an illustration of this scenario.

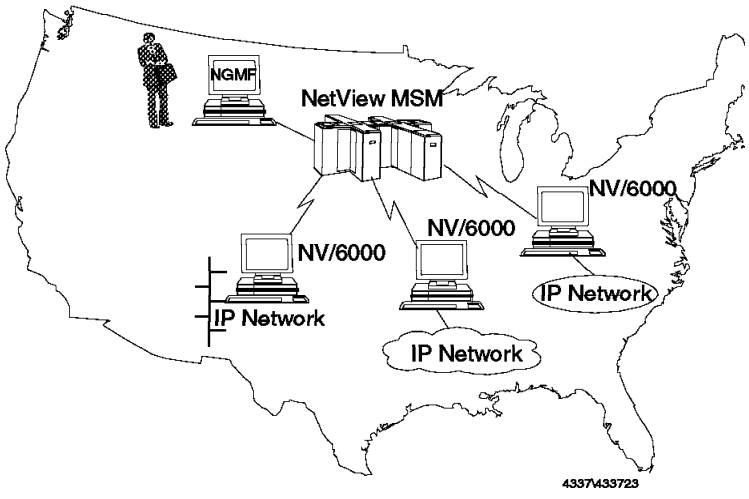


Figure 8. Management of IP Networks Using NetView for AIX Agents and IBM NetView MultiSystem Manager

MSM utilizes functions of the following products to enable centralized management of IP network environments:

- AIX NetView Service Point V1.2 or V1.2.1 (referred to hereafter as Service Point)
- AIX SystemView NetView/6000 V2.1 (referred to hereafter as NetView/6000) or NetView for AIX V3 (referred to hereafter as NetView for AIX)

MSM uses a *manager-agent* relationship to manage IP networks. This relationship consists of a *managing system*, referred to as the *topology manager* and a *managed system*, referred to as the *topology agent*. MSM provides the topology manager that runs on the NetView for MVS management platform. Each NetView for AIX includes a topology agent that reports on all of the resources controlled by that IP manager.

The data collected by MultiSystem Manager from the managed NetView for AIX systems is stored in a single high-speed data cache called the Resource Object Data Manager (RODM) and is presented on the NGMF workstation in graphical form. You still need to run NetView for AIX on one or multiple workstations, all of them managing their own resources.

NetView/6000 is a comprehensive management tool for distributed heterogeneous, multivendor devices on TCP/IP networks. It provides an open network management platform that enables the integration of Simple Network Management Protocol (SNMP) and Common Management Information Protocol (CMIP) applications.

Most common is SNMP, which is a TCP/IP recommended standard that enables managers to ask agents to retrieve and change information about network objects. Those objects make up a collection called the Management Information Base (MIB). The MIB is not an actual database residing somewhere on the network: the individual pieces of information, called MIB objects, reside on the agent system, where they can be accessed (GET-command) and changed (SET-command) at the manager's request. This is how NetView/6000 manages network objects.

NetView/6000 is an AIX application; some of the functions it provides are listed below:

- Dynamic discovery and management of IP resources
  - Networks
  - Segments
  - Routers
  - Hubs
  - Bridges
  - Hosts
  - Adapters
- Configuration, fault and performance management
- Threshold monitoring and automation facility
- Host communications with NetView for MVS using Service Point
- Alert filtering

- Interface with Ingres** database
- Graphical user interface using OSF/Motif** and X-Windows System** standards
- SNMP and NetView/6000 linemode commands

NetView for AIX adds the following functions:

- Enhanced database support to manage trap, topology and collected SNMP data using, additionally:
  - DB2/6000
  - Informix**
  - Oracle**
  - Sybase
- Enhanced event handling including trap-forwarding, multiple dynamic workspaces and operator-less event automation
- Integrated System Resource Monitoring Tool
- Distributed discovery and management using Systems Monitor V2
- Enhanced APIs
- Backup Manager function

Note

For further information on NetView for AIX please refer to the NetView for AIX manuals you will find listed in the related publications section of this document.

3.2 IP Views in NGMF

This chapter shows how IP views look in NGMF.

3.2.1 The View Hierarchy

Included below is a simple scenario in which the NGMF operator navigates “down” by double clicking on resources to display IP Internet views. Details on the views are explained in the next chapter.

An overview of the view hierarchy is provided in Figure 9 on page 14 to illustrate how to “click” your way down to the IP Internet view.

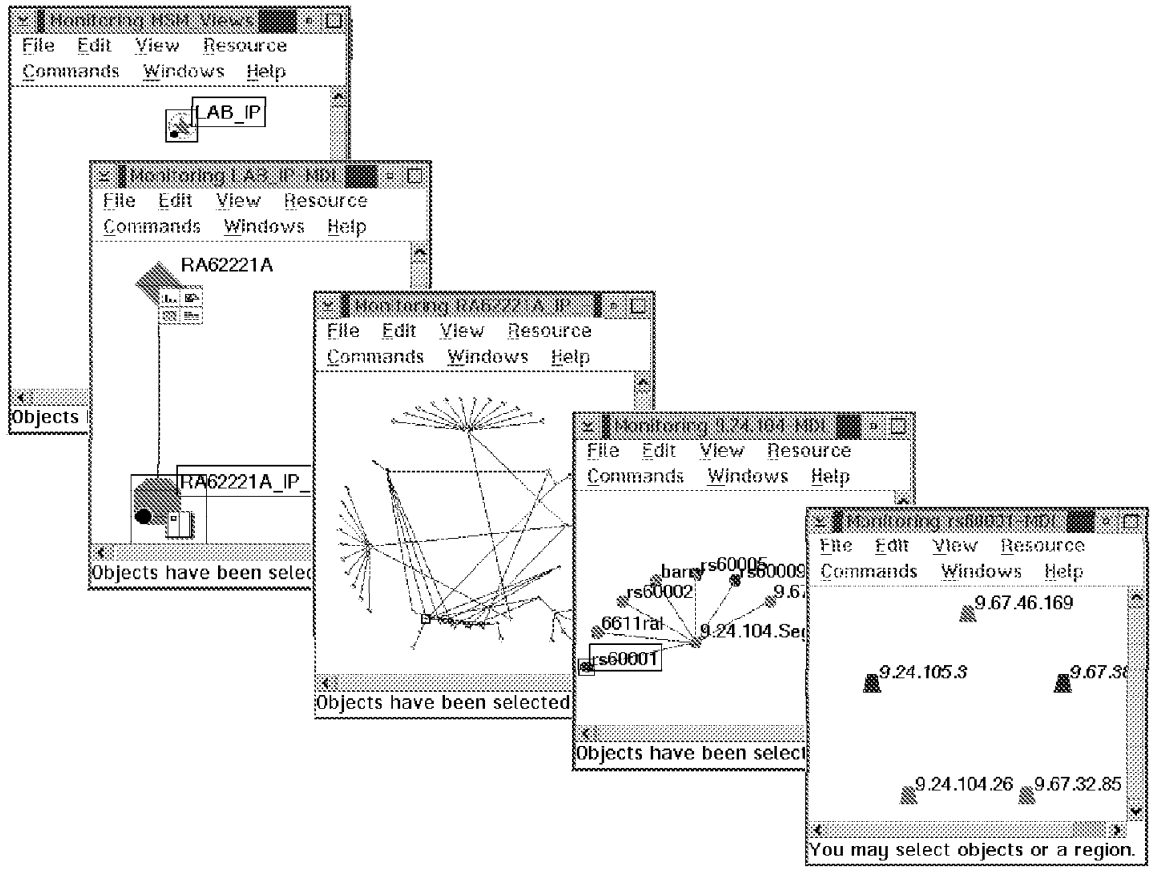


Figure 9. The MSM/IP Views at a Glance

3.2.2 Monitoring the IP Network in NGMF Views

During INITTOPO processing, which initializes MSM, we created a network view called MSM_Views that contained one aggregate for each of the managed environments (IP, LNM and Novell NetWare networks). We therefore start this scenario by opening the network view MSM_Views from the NGMF main menu as shown in Figure 10.

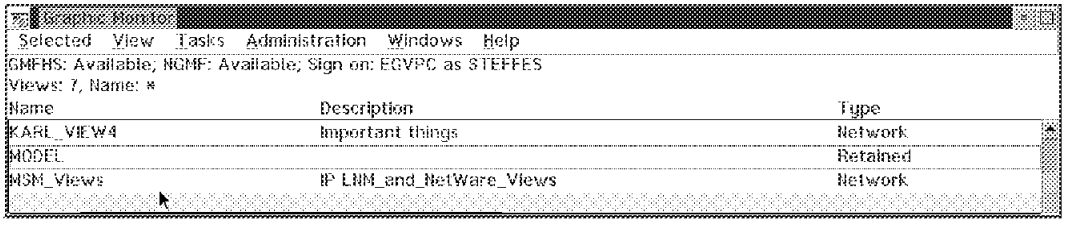


Figure 10. The NGMF Main Menu

Figure 11 on page 15 shows aggregate objects for the IP network, two LNM managed LANs and the NetWare network. These aggregates appear after double-clicking on the **MSM_Views** network view in NGMF's main menu as shown above.

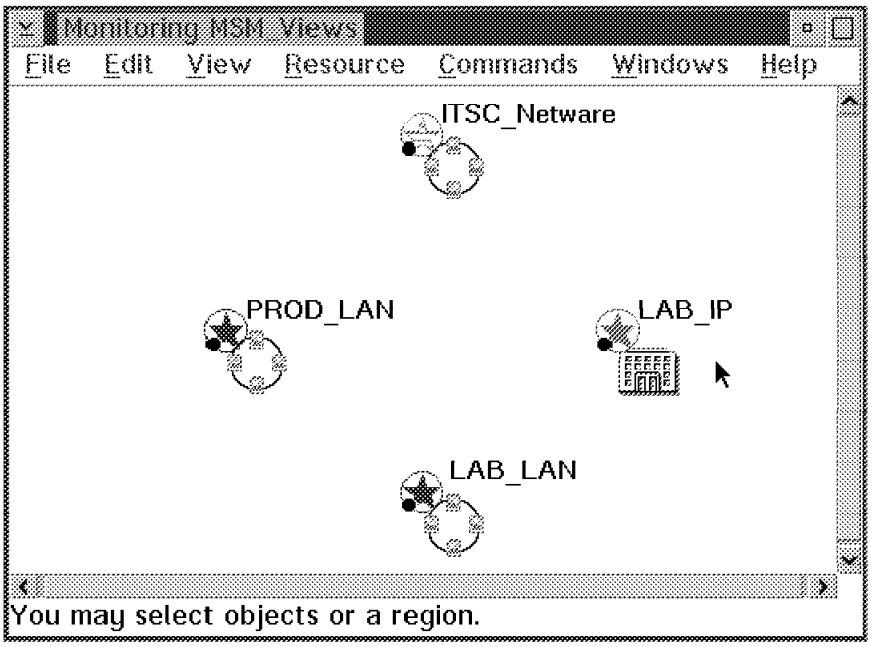


Figure 11. IP and LAN Network Aggregation Objects

LAB_IP is the name of the aggregate object for the IP network.

If you have more than one NetView for AIX, you can access each network through a separate service point. The service point represents the connection between NetView for MVS and the IP environment. By double-clicking on the object **LAB_IP**, NGMF presents a view showing the service point object for our defined IP network as illustrated in Figure 12.

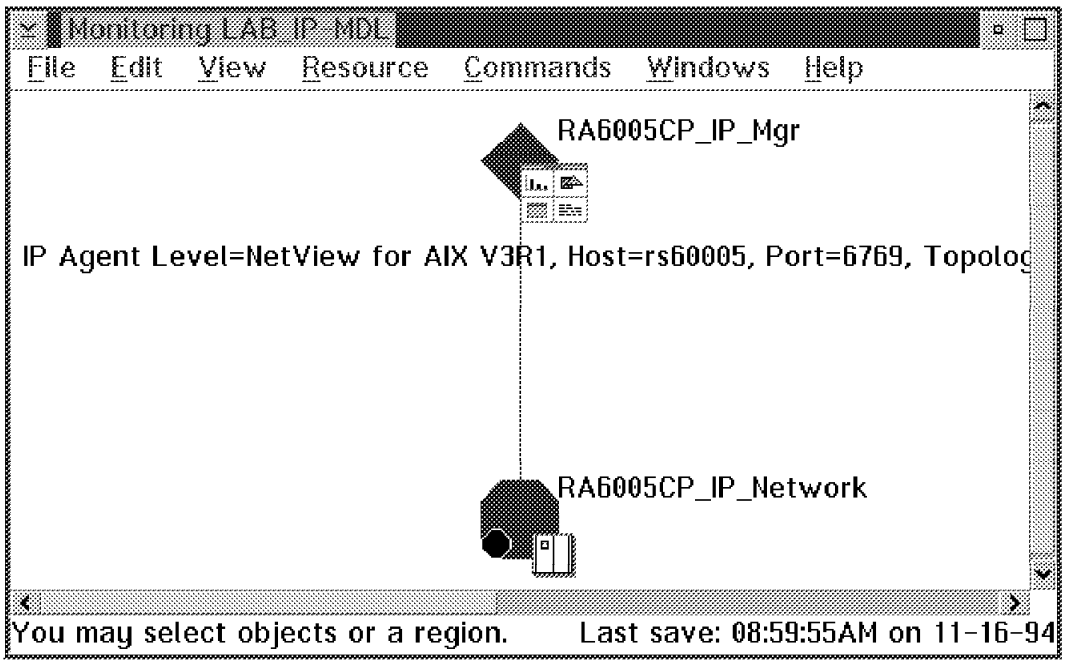


Figure 12. Domain Manager and IP Network Aggregation Object

In this example the managed IP network has a service point called RA6005CP. This is the CP name of our service point machine and has to be used in the

RUNCMD, as shown later, if LU 6.2 is used for transport. This view includes also the IP network aggregate object (RA6005CP_IP_Network) and some helpful information about the domain manager including its IP agent level, hostname and topology level (so called ″other data″), which is optional.

Aggregate objects can be recognized by an octagon being displayed in the lower left corner of the icon. The network domain aggregate shown in the figure above is the only object in the view that supports a More Detail view request (opened by the menu item ″Resource --> More detail″ or by double clicking on with MB1 on that object).

Now we are at the IP network view, called RA6005CP_IP_-MDL. It contains networks and routers - all of them represented by aggregate objects.

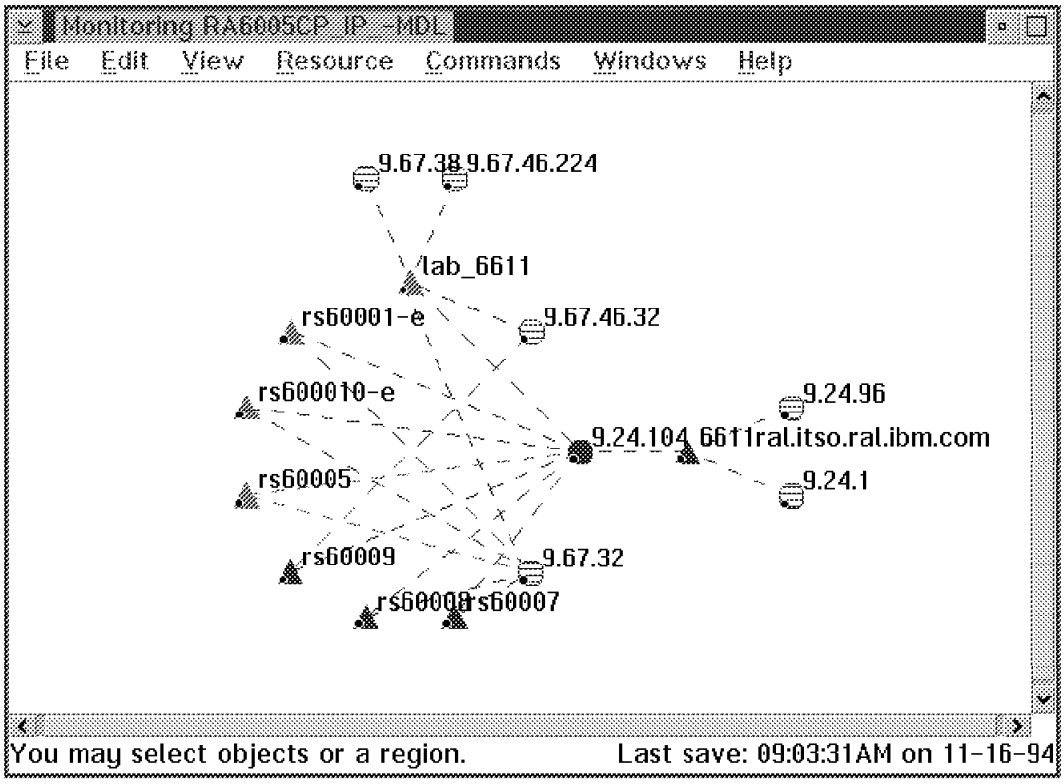


Figure 13. The IP Internet View RA6005CP_IP_-MDL in NGMF

Note

When the view opens, you may see some objects hashed. The reason is that MSM uses default aggregation threshold values, and these values may need to be customized for your environment. The hashing means there is a status inconsistency. We adjusted the status aggregation with a tool called *Buildviews*. See Chapter 7 for information on how to adjust aggregation thresholds for aggregate objects. The hashed objects you see in Figure 13 are those *unmanaged* by NetView for AIX.

By double clicking on the network aggregate **9.24.104**, which is our local IP network, we get a view containing the network with all attached routers. This view hierarchy corresponds to the view hierarchy NetView for AIX uses.

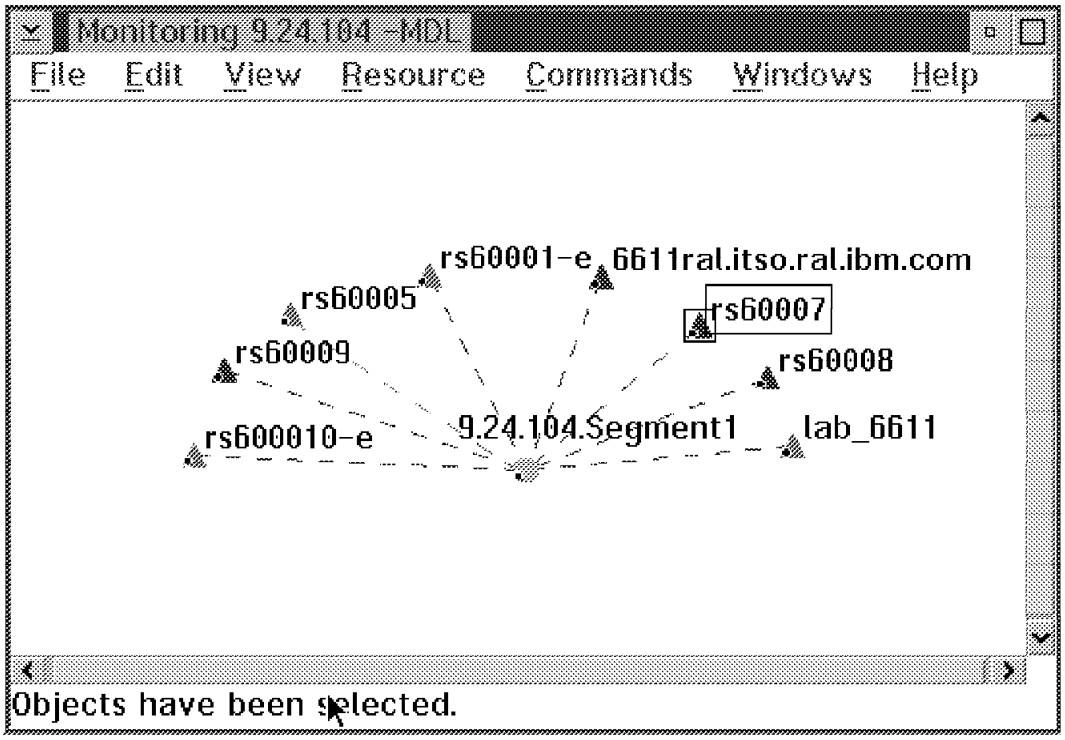


Figure 14. Display of Segment

Clicking on the aggregate network object **9.24.104.Segment1** shows you all the resources found in this IP network as illustrated in Figure 15 on page 18.

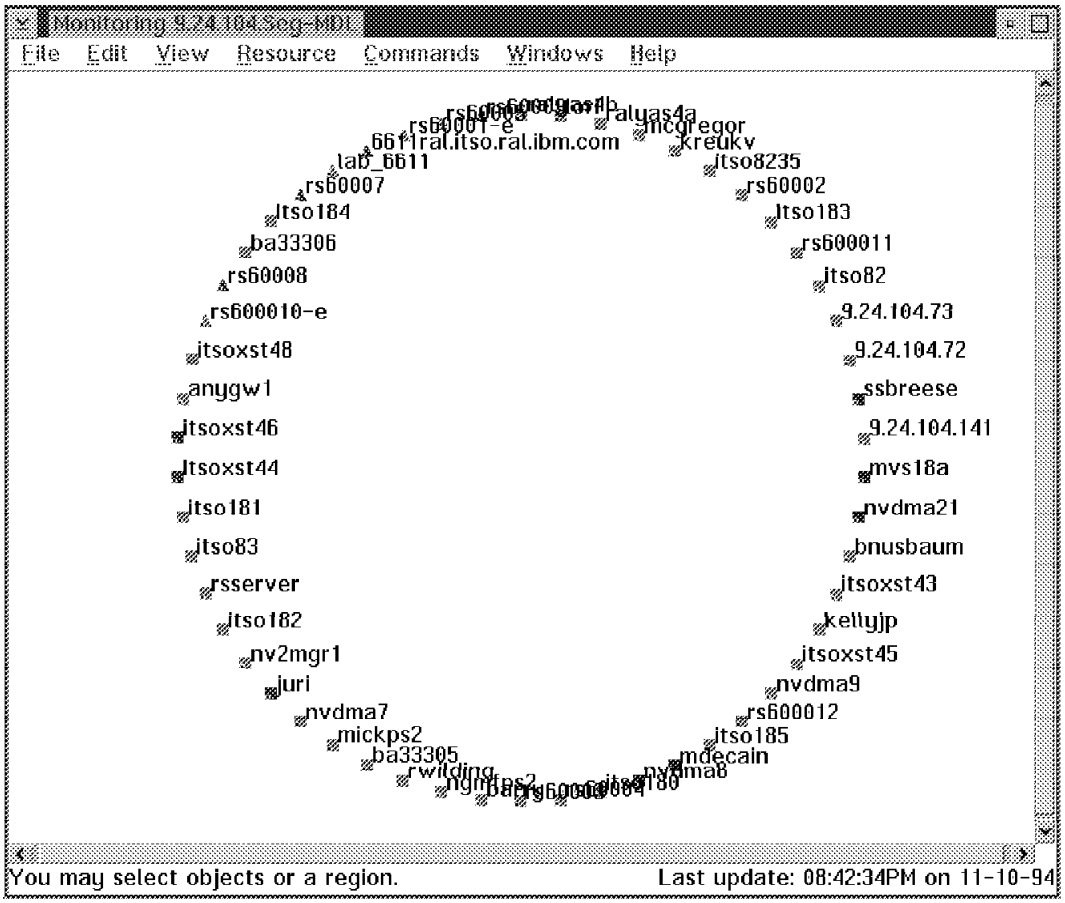


Figure 15. Display of Segment with Hosts

If you select one of the routers in Figure 14 on page 17 and request more details, you get a view containing its interfaces. Those are *real objects*, not *aggregate objects*. Figure 16 on page 19 shows the view presented by NGMF when we clicked on the router lab_6611.

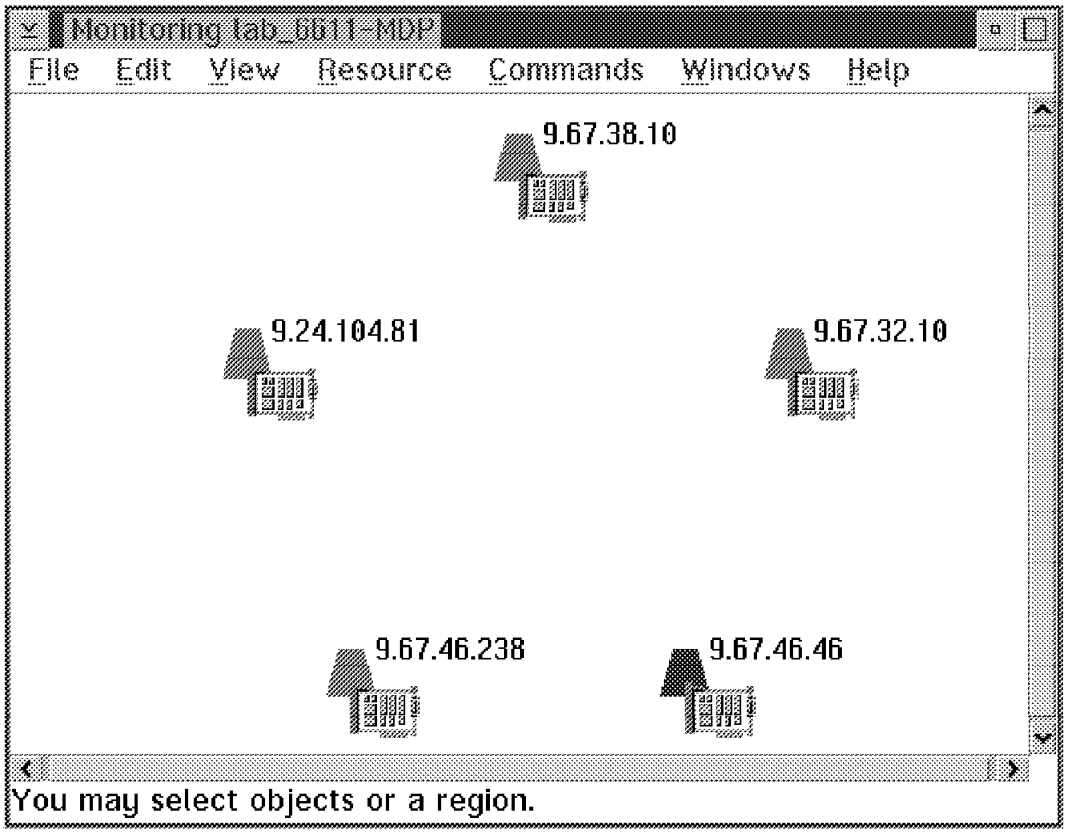


Figure 16. Display of the Interfaces of a Router

3.2.3 Additional NGMF Views

In this section two types of additional NGMF views will be described:

- Resource configuration views
- Location views

More views will be described in Chapter 7, “IBM NetView MultiSystem Manager Tools” on page 149.

In the above described scenario, double-clicking with mouse button 1 (MB1) on aggregate objects helped us get More Detail views. These types of views, however, are some of the many types of views available in NGMF for the IP resources. Except for the Configuration Peers view and the Network View, the other Non-SNA views are not specifically defined anywhere - they are dynamically created based on defined links in RODM as described below.

When a view is requested by an NGMF operator, the view request gets passed over to GMFHS **1** in Figure 17. The view manager in GMFHS queries RODM for the information required to build the view (objects and defined links **2**, **3**), and then the formatted view is passed over to the NGMF workstation **4**. This view creation process is illustrated by steps 1 to 5 in Figure 17.

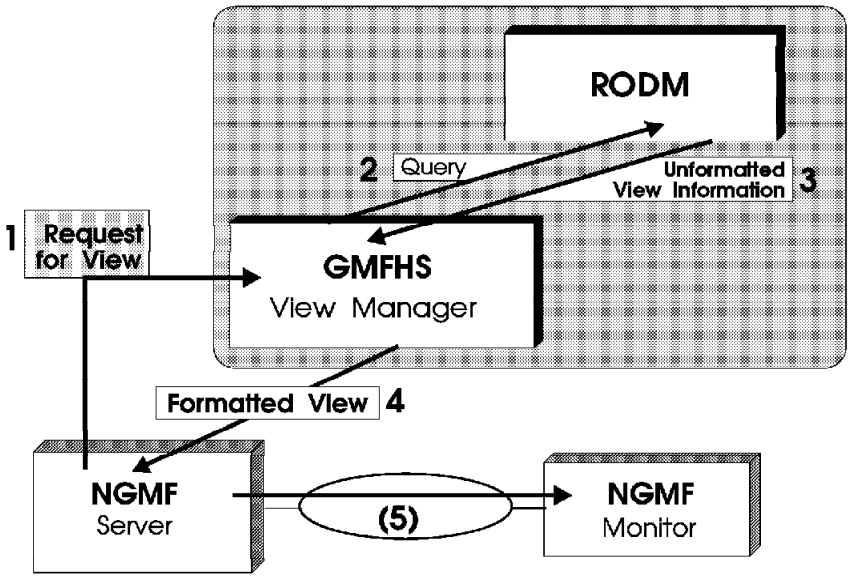


Figure 17. GMFHS View Generation

3.2.3.1 Resource Configuration Views

The link types that are being used for creating views can be found by clicking on the Resource pull-down and selecting the **Configuration** option. The resulting pull-down menu will present the following view types:

- Configuration parents view
- Configuration children view
- Configuration peers view

- Configuration logical and physical view
- Configuration logical-only view
- Configuration physical-only view

Note

All of these view types may not be available for all resources, but as described above, these views are created dynamically and NGMF will not know whether it's possible to build a view until a request has been sent to GMFHS. This is the reason why none of these view types have been grayed out in the pull-down menu (even though the links required for creating some of these views may not have been defined in RODM).

The following scenario describes some of the additional configuration views that are available for IP resources. To get access to these views, select the Resource/Configuration pull-down menu and choose one of the available options. These *Resource/Configuration* views are created based on the links defined in RODM for the selected object; if for example the selected object has links of type *PhysicalConnPP* defined in RODM, a request for a Configuration view will be successful.

There are only two types of Configuration views that we found useful with the MSM IP tower:

- Parent/Child views
- Configuration Peers views

The Configuration Peers views are only available after having used the correlation utility that ships with MSM (or your own customization). These views are described in 7.2, "CORRELATE" on page 158.

Thus, only parent/child relationships will be discussed here.

In this example we selected the Configuration/Parents option for an adapter to show how it is connected to the rest of the IP world. As all the views showing the adapter of any node are very similar, this may be very helpful. An example is shown in Figure 18 on page 22.

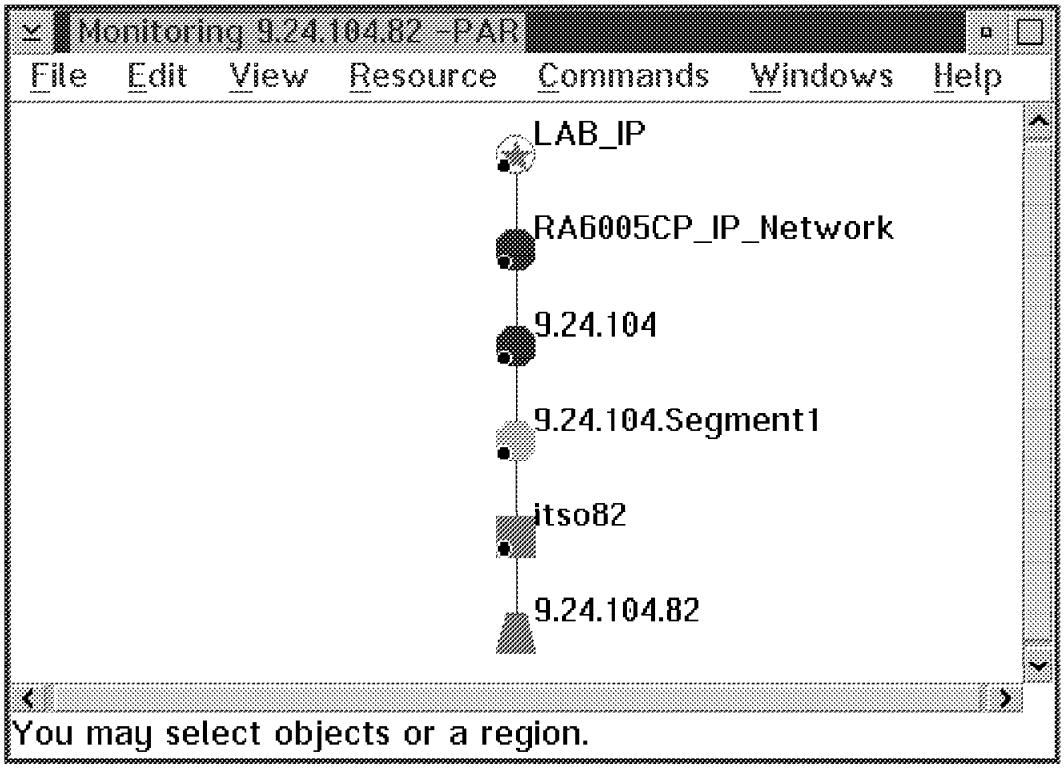


Figure 18. An Adapter and Its Parents

Figure 19 on page 23 shows the parents of a router called rs600010-e. This router has one interface connected to our Ethernet (9.67.32) and a token ring interface (network 9.24.104). Because the router is child of segments, networks and the Internet, there are five connections shown, illustrating the structure of views.

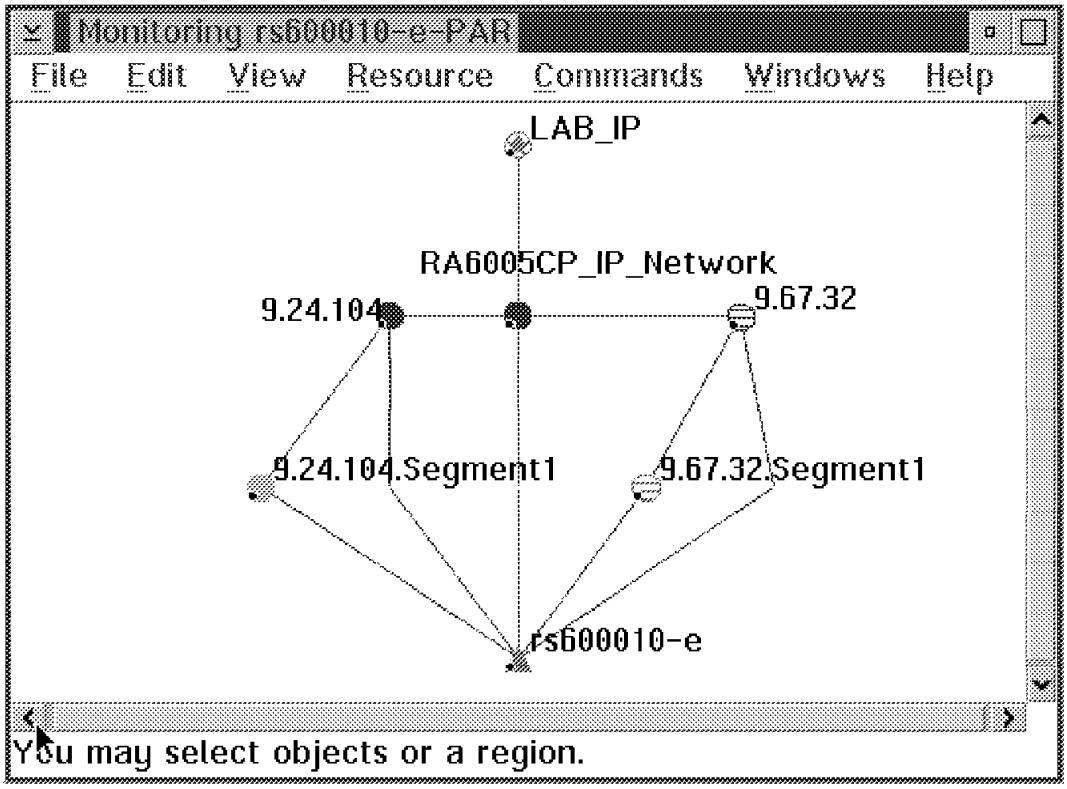


Figure 19. A Router and Its Parents

Figure 20 on page 24 shows the Configuration/Children view of the LAB_IP network. Although you can't read the labels in the lower levels, this may help you to understand the structure of your views.

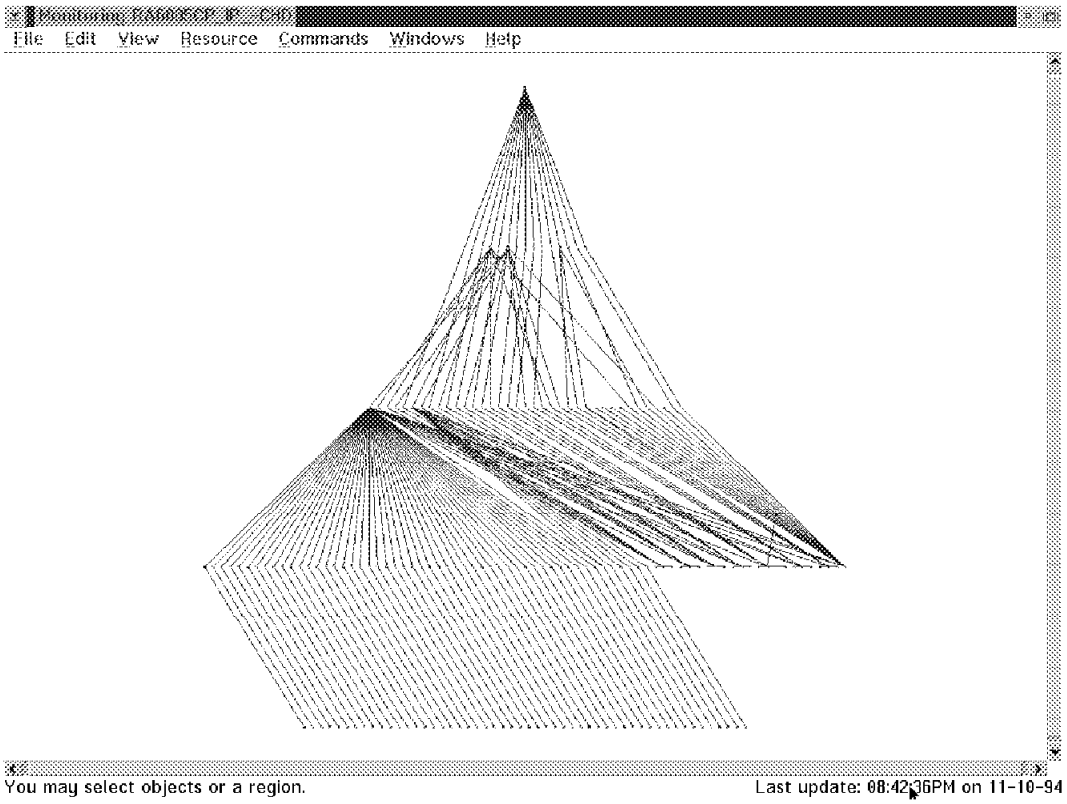


Figure 20. A Complex IP Network and Its Children

We will not discuss the picture in detail. Either you like it or you don't. However, this does show the relationship exactly as it is in NetView for AIX. Although it is confusing at first sight, it's correct, so don't be disturbed. Another example is shown in Figure 21 on page 25. This is a children view of a network, 9.67.46.32. You see one segment and two routers, rs60009 and lab_6611.

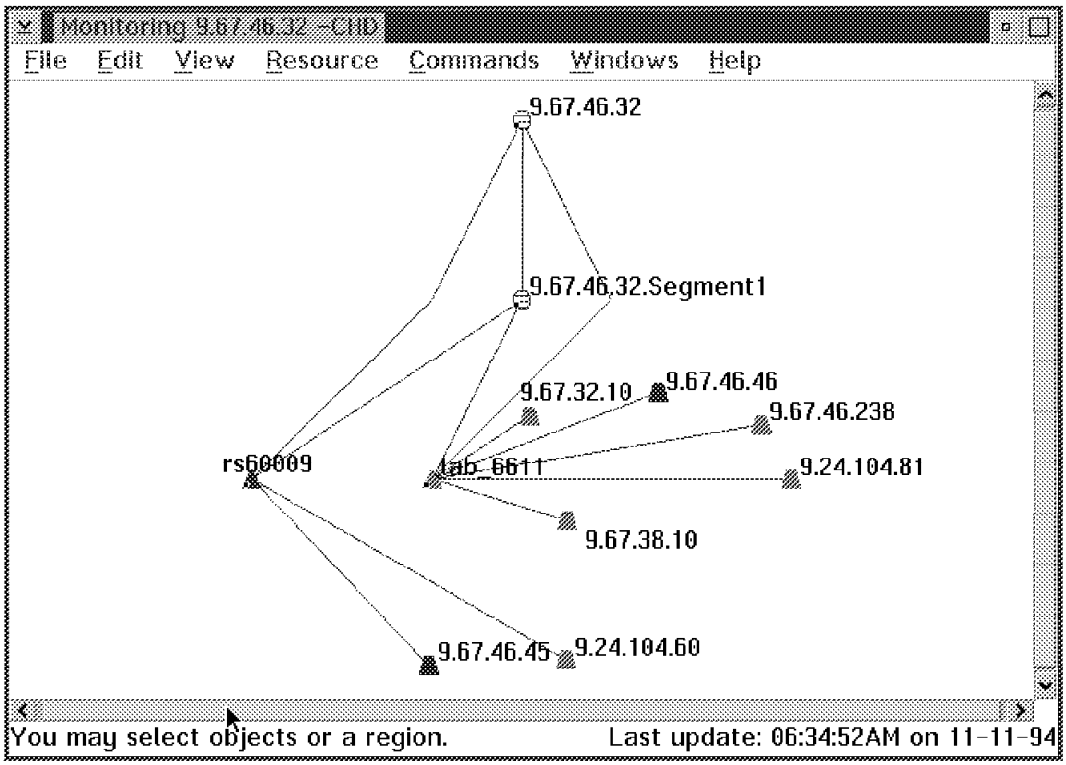


Figure 21. A Simpler IP Network and Its Children

3.2.3.2 MSM and NetView for AIX Location Views

In NetView/6000 you can group resources into so-called location views.

Note

Make sure you follow the cutting and pasting rules. If you edit your map without following the rules, the objects will be displayed in the *user plane*. You can see this by the shadow. No connections are created automatically by NetView for AIX. If you re-do the change to correct the mistake and copy the objects back where they belong, they still are not reintegrated. So be careful with cutting and pasting! If the connections are lost, this is not a problem for NGMF, as RODM adds the connections properly. See *NetView for AIX Administrator's Guide, SC31 7192*, for further details.

As locations are NetView for AIX objects in the NetView for AIX database, the information is retrieved by the GETTOPO command. Locations can be created on different views; we created a location called Malibu, containing a remote IP network. This location was created on NetView for AIXs IP Internet. It is shown connected to the Internet via 6611RAL as you see below. Malibu is at the bottom of the screen.

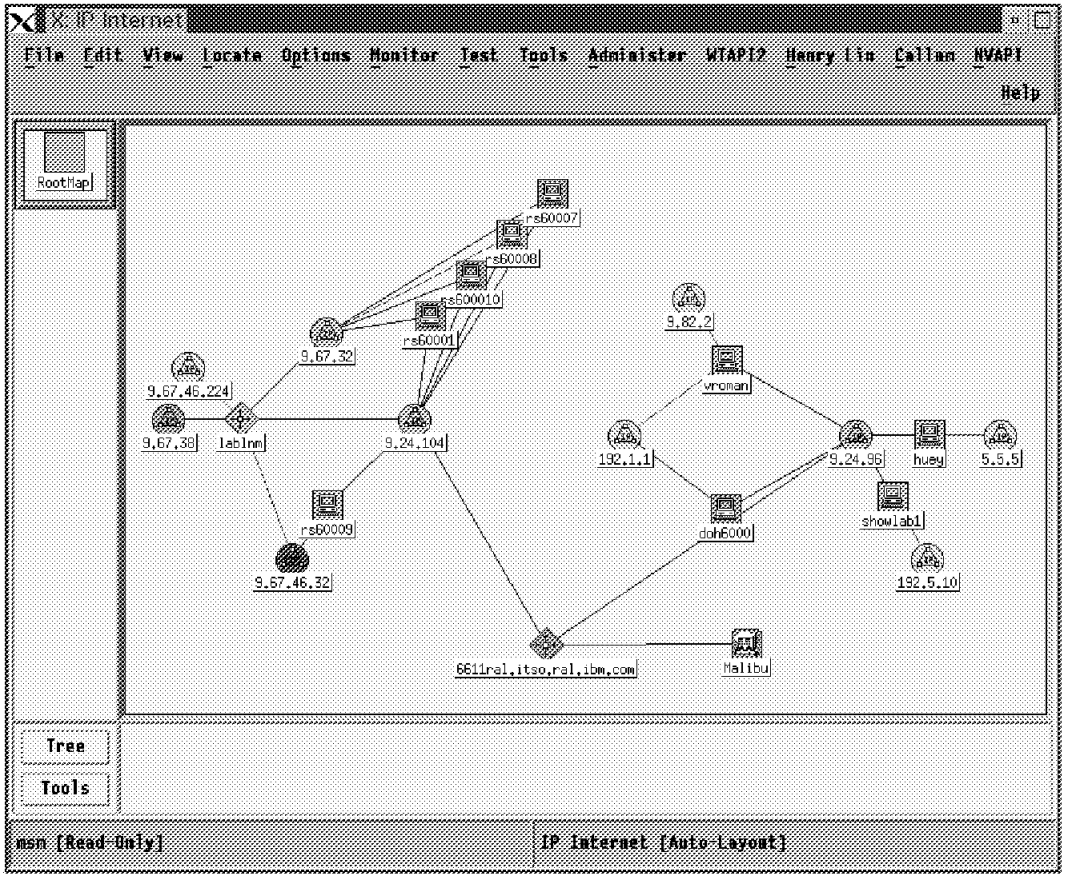


Figure 22. The IP Internet Containing Location Malibu

Note

If you change the *symbol type* of an object in NetView/6000, for example from *host* to *location*, the location flag is set for this object to true in the NetView/6000 database. To change it you have to delete the object from the entire NetView/6000, which means from all submaps in all maps and let it be completely rediscovered. It is then created as a new object in the NetView for AIX object database with proper attributes. This is not a severe problem for NetView/6000, as those attributes are only used for the selection rules; that means certain applications may or may not become active when this object is selected. But if you issue an GETTOPO with the wrong symbol type information in the NetView/6000 database then MSM puts the resource into that specific RODM class. This may produce misleading object aggregation in NGMF. It's only possible to remove that confusing and wrong information and presentation if the aggregate object does not contain any active real objects (by using the REMVOBJS command). So be careful when using the *change symbol type* option in NetView/6000.

In NetView for AIX this problem has been fixed. The flags are changed back according to your customization.

This was the content of the location Malibu, as defined in NetView for AIX:

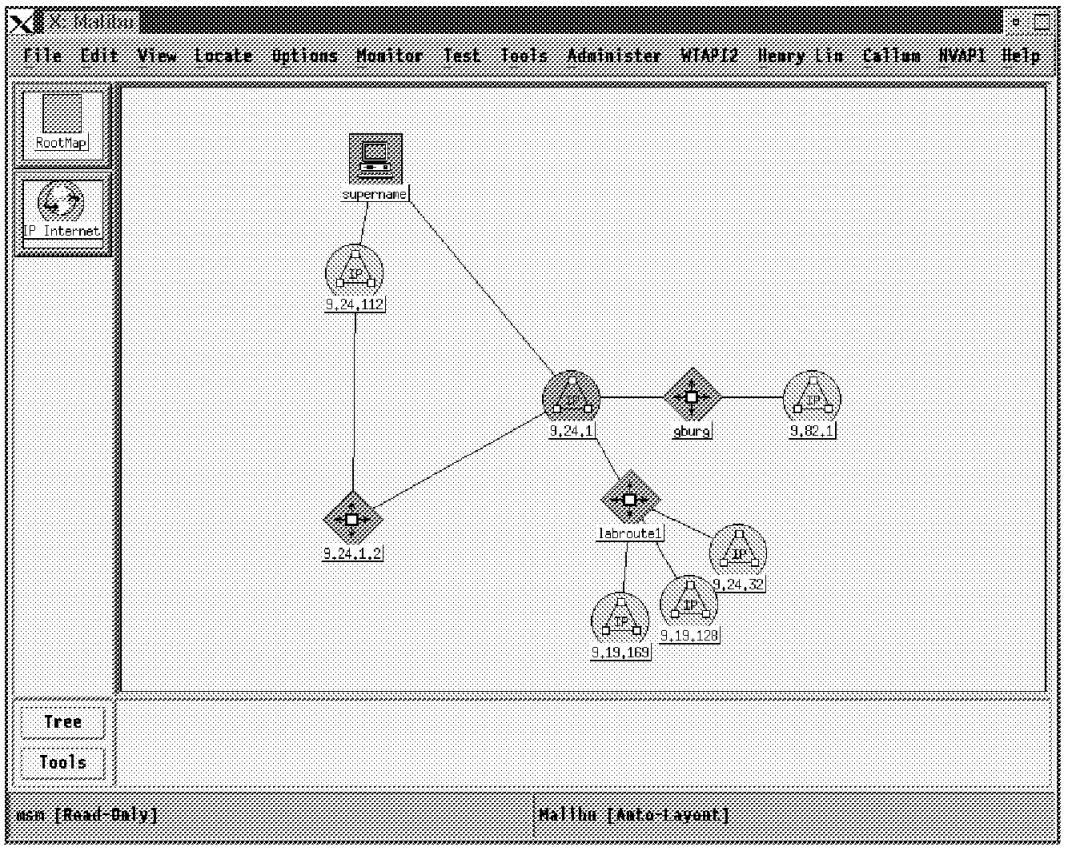


Figure 23. The Submap Malibu in NetView for AIX

In NGMF the icon of the location was connected to the 6611RAL as well as illustrated in Figure 24 on page 28.

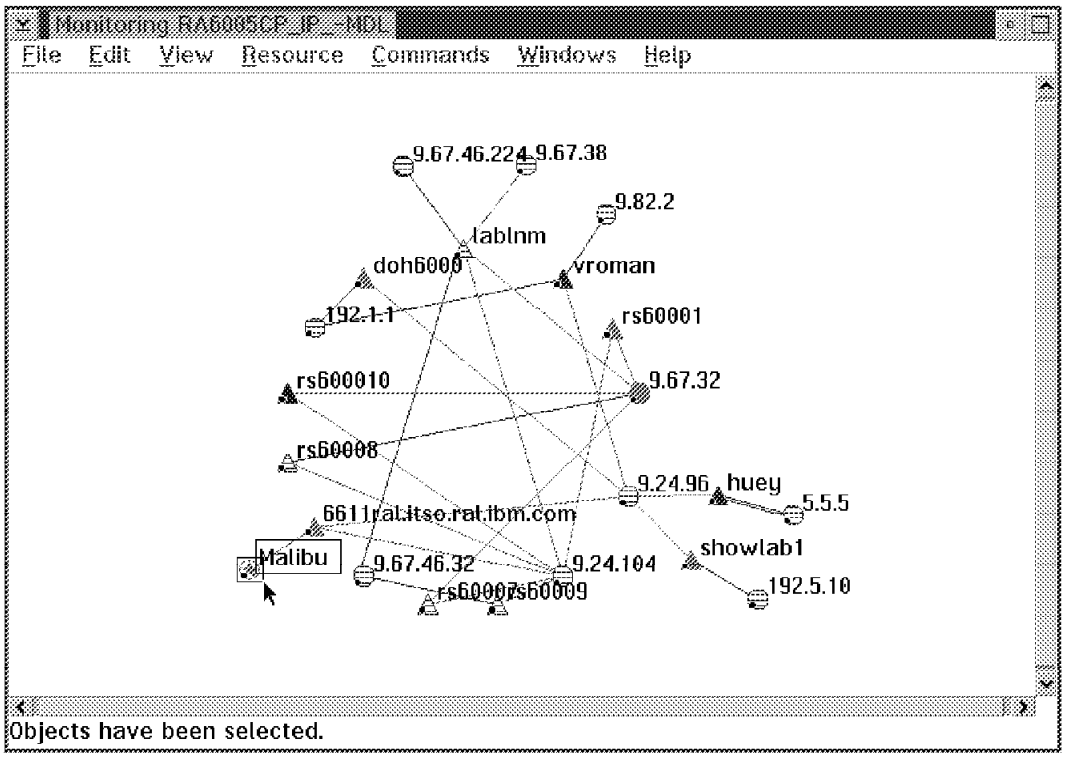


Figure 24. The RA6005CP_IP_MDL View Containing Malibu

Double clicking on the aggregate object Malibu in NGMF opens a view of the remote IP network (shown in Figure 25 on page 29) similar to that shown by NetView for AIX (Figure 23 on page 27).

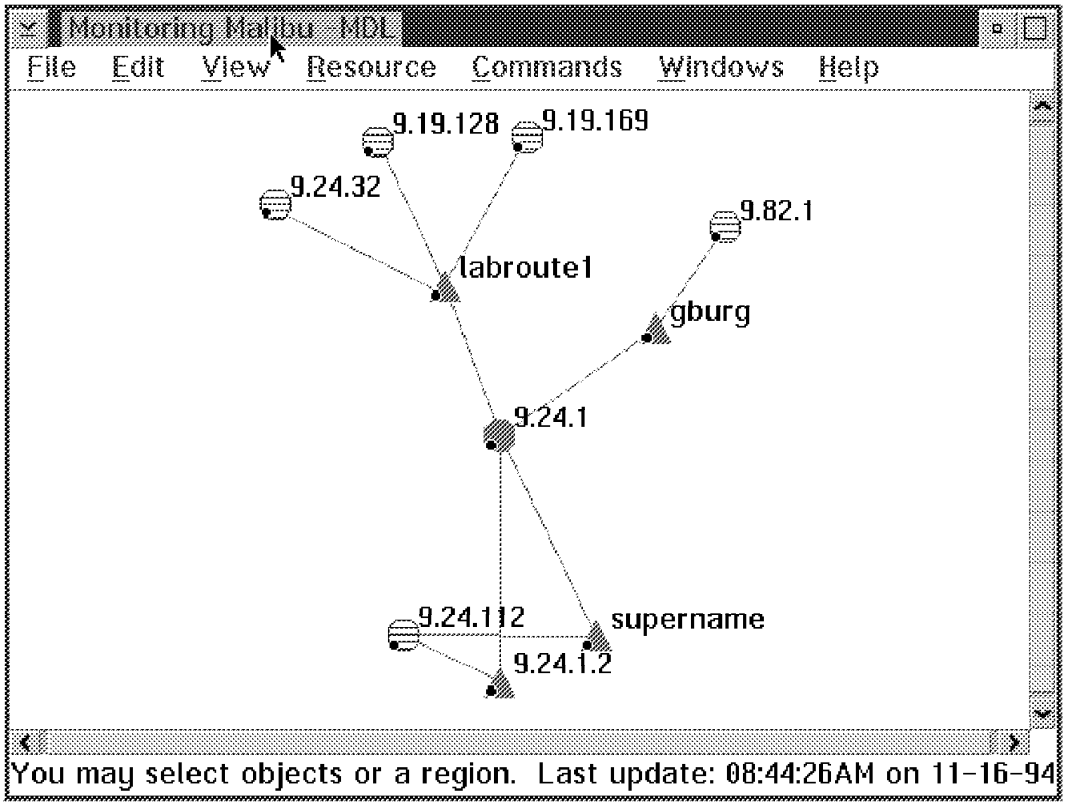


Figure 25. A More Detailed View of Map Malibu in NGMF

3.3 NetView for AIX to IBM NetView MultiSystem Manager Communication

MultiSystem Manager communicates with NetView for AIX using the following products on an AIX workstation:

- AIX SNA Server V2
- AIX NetView Service Point V1.2.1

or

- AIX SNA Services V1.2
- AIX NetView Service Point V1.2

SNA Server/Services only provides a connection; the Service Point is a transport vehicle, moving data. The following applications which use the Service Point are provided in NetView for AIX.

- Trap-to-Alert Daemon (TRALERTD)
- Service-Point-Application Daemon (SPAPPLD)

The flow of information between NetView for AIX and NetView for MVS is illustrated in Figure 26 on page 31.

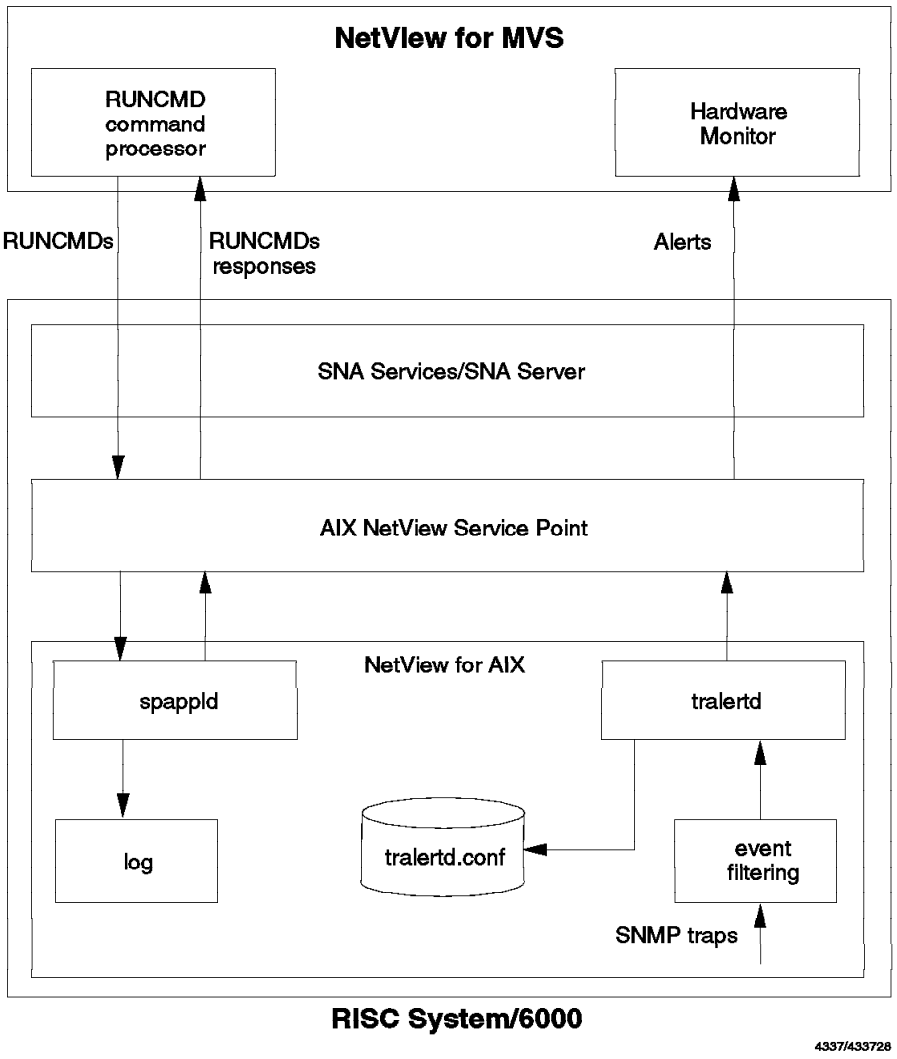


Figure 26. The Flow of Information between NetView for AIX and NetView for MVS

Note

NetView for AIX and Service Point have to run on the same physical machine in order to work with MSM.

The Trap-to-Alert Daemon TRALERTD receives SNMP traps and converts them into NetView for MVS Alerts (NMVTs). There is a special filter function, that allows you to customize which traps are forwarded to NetView for MVS. The TRALERTD provides default trap to alert conversion rules and default filter. The conversion rules are stored in the *tralertd.conf* file.

The Service-Point-application daemon SPAPPLD receives commands that are sent from NetView for MVS and sends RUNCMD responses. It also logs all activities in the NV390.log logfile.

3.3.1 NetView for MVS to Service Point Communication

NetView for MVS communicates with Service Point using one of the following SNA connections:

- An SSCP-PU session
- MDS Transport using LU 6.2 session

3.3.1.1 Communication over an SSCP-PU Session

This is not supported for NetView/6000-MSM communication. We tried it and found that it worked, but you should consider using LU 6.2 for support and performance reasons. If your AIX Service Point and your NetView focal point VTAM are in different SNA networks, you will have to use an LU 6.2 session since this provides the required cross domain support.

3.3.1.2 Communication over an MDS Transport LU 6.2 Session

An LU 6.2 connection is required when the Service Point node is not in the same SNA network or VTAM domain as NetView MSM. It is also required for APPN networks, where the role of the PU is taken over by the APPN control point.

When using SNA Server, the control point takes the place of the LU and is used to address the service point with the RUNCMD command. This facility has two advantages:

- Definition is much easier, because you don't have to define any LUs.
- It is possible to change the focal point NetView used by Service Point, which means you can share one Service Point machine between two NetView for MVS (not at the same time). All you have to do is to send a NetView *FOCALPT CHANGE* command to the service point and the host partner LU is changed.

Note

If an LU 6.2 session is used with SNA services, the connection is dependent on the status of the partner LU, which in this case is NetView for MVS. The connection is reestablished by the first RUNCMD sent by NetView for MVS after the LU-LU session has become inactive. It is necessary to define an LU 6.2 logmode for this.

If you are using SNA Server, there should be no problem if the host partner LU becomes inactive. SNA Server tries to reestablish the session continuously and so the session becomes active shortly after the VTAM major node is activated. SNA Server only has to be restarted when the connection has been down too long - SNA server stops trying to reconnect after a maximum of 500 attempts.

The retry frequency and number of retries is controlled by fields in the SNA DLC profile. The default is twenty retries at one minute intervals.

Note

When the VTAM switched major node is inactivated and activated, sometimes it may also be necessary to restart the SNA subsystem in addition to Service Point.

3.3.2 Service Point and Application Setup and Start

See Appendix A.1, “Service Point Installation and Configuration” on page 183 for details of Service Point setup.

When you have finished customizing the SNA Services and Service Point profiles you should do the following:

- Set up the applications (tralertd, spappld).
- Start up subsystems and processes.
- Control Status.
- Issue RUNCMD; send trap/alert to NetView for MVS.

3.3.2.1 Set up the Applications (Spappld, Tralertd)

There are two host connection daemons provided with NetView for AIX, the trap-to-alert daemon, called tralertd, and the Service-Point-application-daemon, called spappld. To configure them, call *SMIT nv6000* and select the following menu items from SMIT:

- Configure.
- Set options for AIX NetView/6000 daemons.
- Set options for host connection daemons.

You get a menu with two options:

- Set options for tralertd daemon.
- Set options for spappld daemon.

When you open these menus, a registration file for each of the daemons is created. These *lrf* files, which stands for local registration files, are necessary for the startup of the daemons. They are called /usr/OV/lrf/spappld.lrf and /usr/OV/lrf/tralertd.lrf. You may wish to consider changing the application names, which have generic defaults. They are used to address the spappld in the RUNCMD and as a qualifier in the alert sent to NetView/MVS by tralertd. Using meaningful names here may help you. As our machine is called rs60005 we named both applications rs60005s. For MultiSystem Manager, both applications must have identical names!

The following two figures show the options screens where the application names are defined for both daemons.

```
                        Set Options for tralertd daemon

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                    (Entry Fields)
  Tracing mask:                                    (0)
  Full path name of trace file:                    (/usr/OV/log/tralertd.t>
* Service point application name:                  (RS60005S)
  Service point host name:                         ()
* Are you using NETCENTER?                         no
       if yes:
     Domain name:                                  (SNMP)
     Standalone timeout:                           (90)
```

```
                        Set Options for spappld daemon

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                    (Entry Fields)
  Service point host name:                        ()
* Service point application name:                 (RS60005S)
  Execute shell state:                            bsh(Bourne)
  Execute shell path:                             (r/OV/bin:/usr/lpp/msmip)
  Log service point transactions?                 yes
  Full path name of log file:                     (/usr/OV/log/NV390.log)
  Tracing mask:                                   (0)
  Full path name of trace file:                   (/usr/OV/log/NV390.trac>
  Are you using NETCENTER:                        no
```

Note

In the above examples we did not fill out the Service Point host name. This is only required in case a distributed service point is being used. If the Service Point and NetView for AIX are running on the same machine, filling in this parameter makes the processes communicate via TCP sockets, which is superfluous.

You must add the PATH to MSM's executables to the execute shell path option. Shell scripts that are located in directories different from those specified here can only be executed if the path is specified with the command. Add `:/usr/lpp/msmip` to the PATH statement as shown above.

The execute shell state option requires no change. It specifies the shell used for the commands you send down with a RUNCMD command (bsh means bourne shell). As the RUNCMD command is considered to be a *root user* and therefore is authorized to issue any commands, this might be a way of reducing the

commands that are allowed by default. Nevertheless AIX-skilled operators have the possibility to by-pass this by specifying the full path name of the shell they want to use.

3.3.2.2 Startup

- Start Portmapper (or verify that it is already running).
- Start SNA (no attachment or connection needs to be started for SNA Services; for SNA Server the link has to be started).
- Start AIX NetView Service Point.

There is no message shown to display the Service Point status when you are using an LU 6.2 connection. The processes that must be active are:

- evp_nvixCrd, the command router process
- evp_nvixSrd, the send/receive process

For SNA Services you should check for the line saying:

```
MDS LU6.2 session is active using the profile NVIXLCMDS1
```

For SNA Server you should check for the line saying:

```
MDS session is active at the Service Point
```

These messages indicate that the connection has become active.

To see whether Service Point is active when using an LU 6.2 session you must start the NetView for AIX host connection daemons. This can be done every time you start NetView for AIX or by using NetView for AIX SMIT. You need to verify that both daemons are running.

Note

If one or both of the daemons are not running even though both SNA Services and Service Point look fine, try to stop and start them again with the *ovstop* and *ovstart* commands. Stop and start *tralertd* first. We found that this helps sometimes. If this still doesn't help, check the NV390.log (/usr/OV/log/) for hints.

Now you should be ready to send alerts from NetView/6000 to NetView/MVS and to receive RUNCMDs from NetView/MVS.

Note: It is not necessary to explicitly define the focal point to NetView for AIX. In NetView for AIX you define which Service Point to use and Service Point knows to which focal point it should connect.

3.4 Installation of the IP Agent Code

We installed the agent code and then made a check to see that it was working.

3.4.1 Installing the Agent Code on NetView for AIX

With the MultiSystem Manager IP feature you will get an AIX installation diskette providing the AIX topology agent code.

To install the code step through the SMIT menus to the panel shown below, select the diskette drive, and then enter `all` in the *SOFTWARE to install* option.

```
              Install Software Products at Latest Available Level

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                      (Entry Fields)
* INPUT device / directory for software               /dev/fd0
* SOFTWARE to install                                 (all)          +
  Automatically install PREREQUISITE software?       yes                      +
  COMMIT software?                                   no                       +
  SAVE replaced files?                               yes                      +
  VERIFY software?                                   no                       +
  EXTEND file systems if space needed?               yes                      +
  REMOVE input file after installation?              no                       +
  OVERWRITE existing version?                        no                       +
  ALTERNATE save directory                           ()
```

This creates a directory */usr/lpp/msmip* which contains the following files:

```
:/usr/lpp/msmip > ls -la
total 304
drwxr-xr-x   3 bin      bin          512 Oct 31 15:45 .
drwxr-xr-x  65 root     system      1536 Oct 31 15:27 ..
-rwxr-xr-x   1 bin      bin        12035 Sep  8 10:51 README
-rwxrwxrwx   1 root     system       307 Oct 31 15:27 copyright
drwxr-xr-x   2 root     system       512 Oct 31 15:27 deinstl
-r-xr-xr-x   1 bin      bin         2427 Sep  2 09:13 flc_alert_cust
-r-xr-xr-x   1 bin      bin         2105 Sep  2 09:15 flc_filter_cust
-r-xr-xr-x   1 bin      bin         2301 Sep  2 09:12 flc_trap_cust
-rw-r--r--   1 root     system       438 Oct 31 16:58 flcalerts.filter
-rw-rw-rw-   1 bin      bin         1366 Sep  2 09:17 flci.reg
-r-sr-sr-x   1 root     system     24823 Sep  2 09:19 flcidrv
-r-sr-sr-x   1 root     system     51059 Sep  2 09:18 flcitopo
-rwxr-xr-x   1 bin      bin         1536 Sep  2 09:11 flctraps.dat
-rw-r--r--   2 root     system       252 Oct 31 15:27 msmip.base.al
-rw-r--r--   2 root     system      2068 Oct 31 15:27 msmip.base.inventory
-rw-rw-rw-   1 root     system       283 Oct 31 15:27 msmip.base.prereq
-rw-r--r--   1 root     system        75 Oct 31 15:27 msmip.base.size
-rwxrwxrwx   1 root     system        15 Oct 31 15:27 productid
```

Following the installation guidance in the NetView MultiSystem Manager MVS/ESA for AIX Networks (SC31-8041) manual, you would then issue the command flc_trap_cust. This should result in the following output:

```
/usr/lpp/msmip > flc_trap_cust
Creating backup copy of /usr/OV/conf/trapd.conf
/usr/OV/conf/trapd.conf copied to /usr/OV/conf/trapd.conf.bak.msmip
Success adding trap id 565504401 for enterprise netviewMSM
Success adding trap id 565504402 for enterprise netviewMSM
Success adding trap id 565504403 for enterprise netviewMSM
Success adding trap id 58785794 for enterprise netView6000
Success adding trap id 58785795 for enterprise netView6000
Success adding trap id 58916866 for enterprise netView6000
Success adding trap id 58916867 for enterprise netView6000
Success adding trap id 50790441 for enterprise netView6000
Success adding trap id 50790442 for enterprise netView6000
Done
```

The enterprise for MultiSystem Manager is netviewMSM with the enterprise id of 1.3.6.1.4.1.2.6.67.

This process uses the NetView for AIX *addtrap* command. The addtrap command creates a trap and adds the new trap to the /usr/OV/conf/C/trapd.conf file. You may wish to manually back up this file before issuing the command. If there is no enterprise definition for the trap, the new enterprise definition is added. If a trap exists with identical enterprise-object-id, generic-trap, and specific-trap values, the addtrap command updates the existing trap with the new information. After updating the /usr/OV/conf/C/trapd.conf file, the addtrap command sends an event to the trapd daemon informing it of the update.

The traps added or updated for NetView for AIX enterprise ID are:

```
# event name   number       description

MI_EV        0050790441     Manage Interface     <=== new trap
UI_EV        0050790442     Unmanage Interface   <=== new trap
NADD_EV      0058785794     Node Added
NDEL_EV      0058785795     Node Deleted
IUP_EV       0058916866     Interface Up
IDWN_EV      0058916867     Interface Down
```

The traps added for the enterprise netviewMSM are:

```
# event name    number    description

MSMAGNT_START  565504401  MultiSystem Manager IP Agent Started/Waiting
MSMAGNT_UP     565504402  MultiSystem Manager IP Agent Up/Ready
MSMAGNT_STOP   565504403  MultiSystem Manager IP Agent Down
```

Note

These traps are only created by the map the topology agent is attached to, which means the IBM_MI_EV will be sent to the trapd daemon only if you start to manage a network on this map.

You should then run the flc_alert_cust shell script. This will add the SNA alert definitions to the tralertd configuration file */usr/OV/conf/tralertd.conf* using the NetView for AIX *addalert* command.

```
/usr/lpp/msmip > flc_alert_cust
Creating backup copy of /usr/OV/conf/tralertd.conf
/usr/OV/conf/tralertd.conf copied to /usr/OV/conf/tralertd.conf.bak.msmip
Success adding SNA alert definition for trap id 565504401 (MSMAGNT_START)
Success adding SNA alert definition for trap id 565504402 (MSMAGNT_UP)
Success adding SNA alert definition for trap id 565504403 (MSMAGNT_DOWN)
Success adding SNA alert definition for trap id 58785794 (IBM_NVNADD_EV)
Success adding SNA alert definition for trap id 58785795 (IBM_NVNDEL_EV)
Success adding SNA alert definition for trap id 58916866 (IBM_NVIUP_EV)
Success adding SNA alert definition for trap id 58916867 (IBM_NVIDWN_EV)
Success adding SNA alert definition for trap id 50790441 (IBM_NVMI_EV)
Success adding SNA alert definition for trap id 50790442 (IBM_NVUI_EV)
Done
```

The last step is to run the filter definition script flc_filter_cust. This script adds filters to your system and tries to activate them using the *selectfilter* command. The command output is shown below.

```
/usr/lpp/msmip > flc_filter_cust
Adding filter definition for trap id 565504401
Adding filter definition for trap id 565504402
Adding filter definition for trap id 565504403
Adding filter definition for trap id 58785794
Adding filter definition for trap id 58785795
Adding filter definition for trap id 58916866
Adding filter definition for trap id 58916867
Adding filter definition for trap id 50790441
Adding filter definition for trap id 50790442
Success creating alert filter definition file /usr/lpp/msmip/flcalerts.filter
Filter MultiSystem_Manager_Alert_Filter activated
```

If the *TRALERTD* daemon is not running, the filter cannot be activated. You have to activate it manually later. You will get a message saying

```
Selectfilter connect:: A remote host refused an attempted connect operation.
Failure activating filter
```

You can activate the filter either from the NetView for AIX EUI (by choosing Options from the menu bar and selecting event Customization and Trap to Alert Filter Control) or directly with the *selectfilter* command. When the filter has been activated once, it will automatically be started every time the *TRALERTD* daemon starts, until it is stopped manually. These filters are pass-filters, not block-filters. So the traps added are passed through to NetView for MVS.

The file flci.reg is also copied into the registration files directory /usr/OV/registration/C. You should remember this when changing this file!

Changes to the registration file are only effective when you do them in the /usr/OV/registration/C directory.

The two executable files *flcidrv* and *flcitopo* must have the proper access mode. The mode shown below allows anyone to execute and to read the files.

```
 /usr/lpp/msmip > ls -lisa flci*
180282  28 -r-sr-sr-x  1  root  system    24823 Sep  9 09:19 flcidvr
180281  52 -r-sr-sr-x  1  root  system    51059 Sep  2 09:18 flcitopo
```

During the initialization process, a temporary file is created in the /tmp directory. There has to be enough space left in the filesystem for this file. Verify that the agent has write access to this filesystem. The amount of disk space needed for the file depends on the number of resources monitored. The following examples show how much space is needed for our sample networks.

```
Mon May 16 11:37:22 1994 flcitopo 28153 IP Internet Totals:
   Networks  : 10
   Segments  : 10
   Locations : 0
   Routers   : 21
   Bridges   : 0
   Hubs      : 0
   Hosts     : 39
   Interfaces: 62
```

This retrieve process built a file called flci.out with a total of about 10KB storage needed:

```
/tmp > ls -l flci.out
-rw-r--r--  1 root    system    10163 May 16 13:13 flci.out
```

To show how the space requirement changes here is a second example:

```
Mon June 7 20:34:21 1994 flcitopo 14758 IP Internet Totals:
   Networks  : 15
   Segments  : 15
   Locations : 1
   Routers   : 180
   Bridges   : 0
   Hubs      : 3
   Hosts     : 553
   Interfaces: 616
```

This retrieve process built a file called flci.out with a total of about 130KB storage needed:

```
/tmp > ls -l flci.out
-rw-r--r--  1 root    system    128904 June 7 20:37 flci.out
```

As the executables are placed in the directory /usr/lpp/msmip you have to add this to the executable PATH statement for the RUNCMD. See Appendix A.1, “Service Point Installation and Configuration” on page 183, or the installation manual (SC31-8041) for further information.

3.4.2 Verify Agents Functions

To test if the topology agent is running, you can issue the flcidrv command simply by typing `flcidrv` from the AIX command line. The answer should be `topology agent available...` and look similar to this:

```
rs60005:/usr/lpp/msmip > flcidrv
FLCI018I Current topology agent configuration: Agent=available Port=6769
Host=rs60005 NvLevel=NetView for AIX V3R1 TopoLevel=1.2 DrvLevel=1.2
MapName=default
```

A NetView for AIX trap is sent whenever the topology agent is started or stopped. When you first start the agent a log called flcitopolog is created in the NetView for AIX log directory /usr/OV/log. So in flcitopolog you can also check when the agent is started, stopped or invoked.

3.5 IBM NetView MultiSystem Manager IP Code Functions

The agent code, running on NetView/6000, is used to perform a number of tasks under the control of NetView for MVS.

3.5.1 The Command Driver

Flcidrv is a command-line driver process, which triggers flcitopo functions. Those two processes communicate via socket communication. The default socket used is 6769 and is coded in the registration file. Verify that this socket address is not being used for any other process.

The registration file flci.reg invokes the MultiSystem Manager agent function in the NetView for AIX Tools Menu. As the flag -initial is set, the topology agent is started automatically with the end user interface (EUI). Each time the EUI on a machine is started (this may happen very often in a production environment), an attempt is made to start flcitopo. Only the first instance will be successful since each instance attempts to use the same socket.

You might consider changing the timer value. This value determines the time delay for the Agent Up/Ready alert to go to MSM. When the topology agent is started with the EUI it sends an Agent Started/Waiting trap to NetView for AIX. After waiting the designated time for NetView for AIX to synchronize its databases, the topology agent sends an Agent Up/Ready alert. This alert triggers the initial GETTOPO command. This will fail if NetView for AIX has not completed synchronization its topology database. The default is five minutes, as shown in the following command:

```
Command -Initial /usr/lpp/msmip/flcitopo 6769 5
```

To adjust this parameter for your environment, check for the time NetView for AIX needs until the message `Synchronizing` disappears from the lower-left corner, after you started the EUI.

If flcitopo is not running it can be started from the NetView for AIX menu bar by selecting **Tools** and **Start MultiSystem Manager IP Agent**.

3.5.2 The MAP Parameter

The topology agent can only be started when the EUI is running, as it is dependent on the process ovw. This is the only process that has access to the NetView for AIX Map database ovwdb. The reason for this is that flcitopo not only extracts topology information, but also gets user customization of NetView for AIX submaps out of the ovw database.

The NetView for AIX internal communication is illustrated in Figure 27.

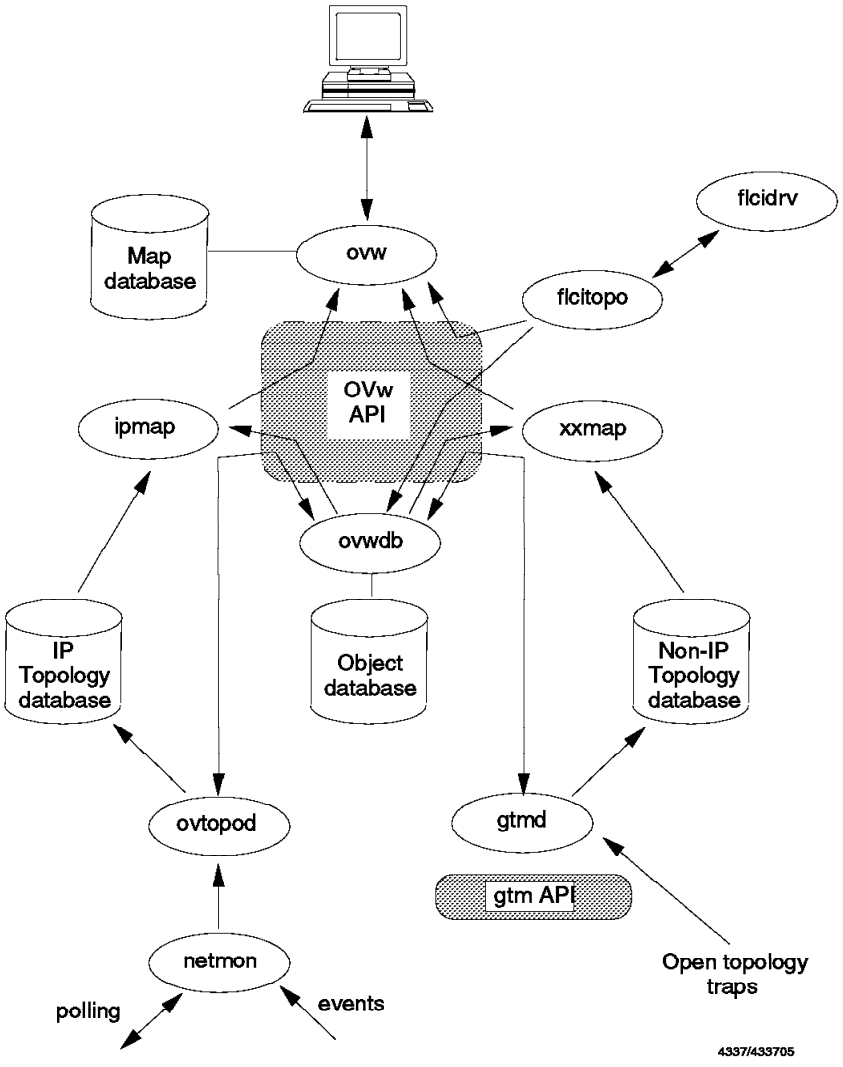


Figure 27. NetView for AIX Structure Diagram Including Flcitopo

Note

Because the topology agent is dependent on the EUI, it stops when the NetView for AIX EUI, from which the MSM topology agent was started, is stopped. It can then be restarted from any other NetView for AIX-screen by the menu. It is also stopped when a new map is opened in the same EUI that started the topology agent.

If you want the topology agent to get information from your map, you must ensure that flcitopo was started on your EUI. Otherwise stop it and restart it from your own EUI.

If you want only one map to run the topology agent, there are two ways to avoid the topology being retrieved from any other map:

- Specify the mapname in the registration file
- Specify the mapname in the GETTOPO command

If you specify the map name in the registration file *flci.reg*, only when this map is opened will the topology agent be automatically started. This means that the agent will become attached to this map only. The registration file */usr/OV/registration/C/flci.reg* should look like this:

```
Action "MSMIP_START"
{
     Command -Initial "usr/bin/flcitopo 6769 5 msmmap";
}
```

With this parameter the topology agent is started when the EUI with the specified map is started the first time. When any other map than the one specified in the registration file is opened, the following message will be issued:

```
FLCI015E Topology agent fatal condition: Map name and topology
registration map file name do not match: openmap msmmap
```

If you change the registration file, you must recycle the NetView for AIX EUI.

If you specify the parameter MAP= in the GETTOPO command, the topology is only retrieved if the agent is attached to this map. Otherwise MSM will return the following message:

```
FLCI011E Topology agent is managing map: nonmsmmap*
GETTOPO COMMAND ENDED IN MODULE FLCACCMD WITH RETURN CODE 8.
```

where nonmsmmap is the attached map. The service point icon will turn red on the NGMF workstation. In addition, the IP network will turn grey, which means unknown, as this message changes the status of the agent in RODM to unsatisfactory. Thus automation will stop, as the agent is considered to be down, and RODM is not updated with new resource information.

For more information on this topic refer to 3.7, “Monitoring IP Resources” on page 60.

Note

Since AIX is case sensitive, you must check whether upper or lowercase letters are used in NetView for AIX.

To control which map the topology agent is attached to, you can issue the *flcidrv* command either from the AIX command line or with a RUNCMD command from NetView for MVS.

If you don't want the topology agent to be started automatically, you can take the *-initial* parameter out of the registration file *flci.reg*. You will then need to start it manually from the NetView for AIX menu bar because it is not possible to start it with a line command.

3.5.3 Topology Agent Functions

3.5.3.1 Initial Topology Discovery

The categories of topology information being retrieved from the NetView for AIX map databases by the MSM IP agent are listed below:

- Network information
- Segment information
- Location information
- Router information
- Bridge information
- Hub information
- Host information
- Interface information

This topology information is retrieved from the MSM agents by executing a series of GETTOPO REXX command lists from NetView for MVS.

A sample call to the GETTOPO CLIST is shown below:

```
/* ************************************************** */
/* NetView MultiSystem Manager GETTOPO REXX Command List */
/* ************************************************** */
GETTOPO,
IPRES,
SP=RA6005CP,
NETWORK_AG_OBJECT=LAB_IP,
NETWORK_VIEW=MSM_Views/IP_Views,
APPL=RS60005S,
MAP=MSMMAP,
TRACE=YES
```

When the GETTOPO CLIST is executed, it:

- Tests the topology agent
- Creates a temporary file including the topology information
- Splits it into proper format
- Sends it to the MSM topology manager
- Removes the temporary files

You can see these RUNCMD commands by turning on the TRACE option in the initialization file. In the Service Point machine the RUNCMDs are logged in the /usr/OV/log/NV390.log, which is the logfile of the spappld. An extract of this logfile is shown below:

```
RUNCMD "FLCIDRV -t 86400" received from NetView.
RUNCMD "FLCIDRV -t 86400" executing.
RUNCMD response for "FLCIDRV -t 86400" sent to the host.
RUNCMD "FLCIDRV -f /TMP/USIBMRA.RABAN.AUTOMSM.FLC -n IP -d 5 -t 86400"
received from NetView.
RUNCMD "FLCIDRV -f /TMP/USIBMRA.RABAN.AUTOMSM.FLC -n IP -d 5 -t 86400"
executing.
RUNCMD response for "FLCIDRV -f /TMP/USIBMRA.RABAN.AUTOMSM.FLC
 -n IP -d 1 -t 86400" sent to the host.
RUNCMD "SPLIT -200 /TMP/USIBMRA.RABAN.AUTOMSM.FLC /TMP/USIBMRA.RABAN.AUTOMSM.FLC;
ECHO FLCI000I SPLIT" received from NetView.
RUNCMD "SPLIT -200 /TMP/USIBMRA.RABAN.AUTOMSM.FLC /TMP/USIBMRA.RABAN.AUTOMSM.FLC;
ECHO FLCI000I SPLIT" executing.
RUNCMD response for "SPLIT -200 /TMP/USIBMRA.RABAN.AUTOMSM.FLC
/TMP/USIBMRA.RABAN.AUTOMSM.FLC;ECHO FLCI000I SPLIT" sent to the host.
RUNCMD "CAT /TMP/USIBMRA.RABAN.AUTOMSM.FLCAA;ECHO FLCI000I CAT"
received from NetView.
RUNCMD "CAT /TMP/USIBMRA.RABAN.AUTOMSM.FLCAA;ECHO FLCI000I CAT"
executing.
RUNCMD response for "CAT /TMP/USIBMRA.RABAN.AUTOMSM.FLCAA;ECHO FLCI000I CAT"
sent to the host.
RUNCMD "RM /TMP/USIBMRA.RABAN.AUTOMSM.FLC*;ECHO FLCI000I RM" received
from NetView .
RUNCMD "RM /TMP/USIBMRA.RABAN.AUTOMSM.FLC*;ECHO FLCI000I RM" executing.
RUNCMD response for "RM /TMP/USIBMRA.RABANAUTOMSM.FLC*;ECHO FLCI000I RM"
sent to  the host.
```

You should back up and remove this logfile regularly. NetView for AIX logfiles generally expand continuously until the disk is full. The MSM heartbeat function for example, which checks if the Service Point and the MSM topology agent are still alive, results in three entries every time the heartbeat interval expires.

A procedure for doing log maintenance should be considered as described in Appendix B, “Customizing AIX for Topology Manager” on page 215.

The flcidrv command being used by GETTOPO to retrieve information from the topology agent can also be issued from AIX manually. These are the options that are available:

- -f file_name: creates temporary output file.
- -s start_entity: specifies the object where detailed unloading starts.
- -p socket_port: socket port for flcidrv-flcitopo communication.
- -t timeout: time to wait before timeout reply.
- -n network_type: only IP is valid.
- -d detail_level: specifies the level of detail to export which means whether hosts, hidden, or unmanaged objects will be included. The default is that hosts and unmanaged objects are retrieved and hidden objects are ignored (1 0 1, which makes a total of integer 5). For example to leave the unmanaged objects out the bit combination is 1 0 0, or integer 4.
- -k: used for stopping.

- -m: The map name to verify the agent is running against.
- -q: Is the query timeout the driver waits for an answer from flcitopo.

Note

Hidden objects in NetView for AIX means the objects that exist in the submap are not displayed by the NetView for AIX GUI.

The following diagram shows how the topology RUNCMDs work:

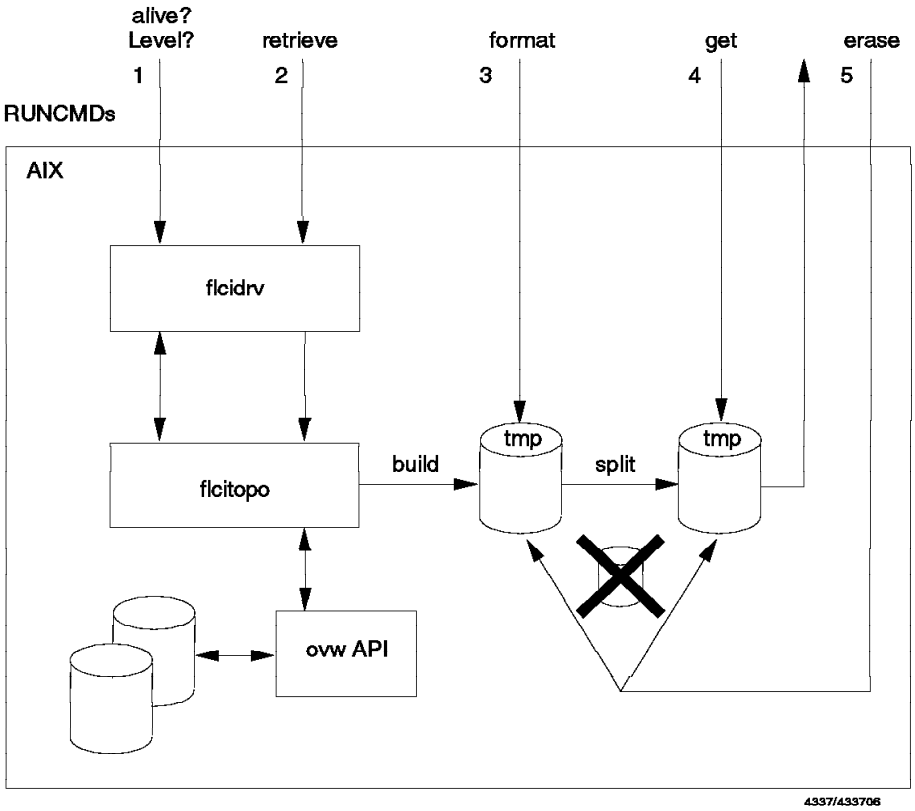


Figure 28. NetView/6000 Flowchart Showing GETTOPO RUNCMDs

The first step checks if the topology agent is up and retrieves some information; for example, the level of the agent installed. The second step causes the topology agent to build a file in the /tmp directory which in our environment was called /tmp/usibm.raban.automsm.flc.

Note

The topology agent extracts information from both the map database and the object database. As a result this command cannot be executed successfully when the NetView for AIX map is synchronizing, because the map database is being updated at this moment. If a failure occurs, you should try and issue the command again after synchronization. There is a timer parameter in the *flci.reg* file for the initial GETTOPO command.

The next step splits the temporary file into the proper format required by MSM. It is then retrieved by MSM. The last step in the process is the removal of the temporary files from the workstation.

3.5.4 Topology Initialization

Our sample IP network as it is displayed in NetView/6000′s IP Internet view is presented below. You can see one network, shown as a circle, two routers, shown as diamonds, and five workstations that act as routers. Six additional networks are unmanaged, which means they are ignored.

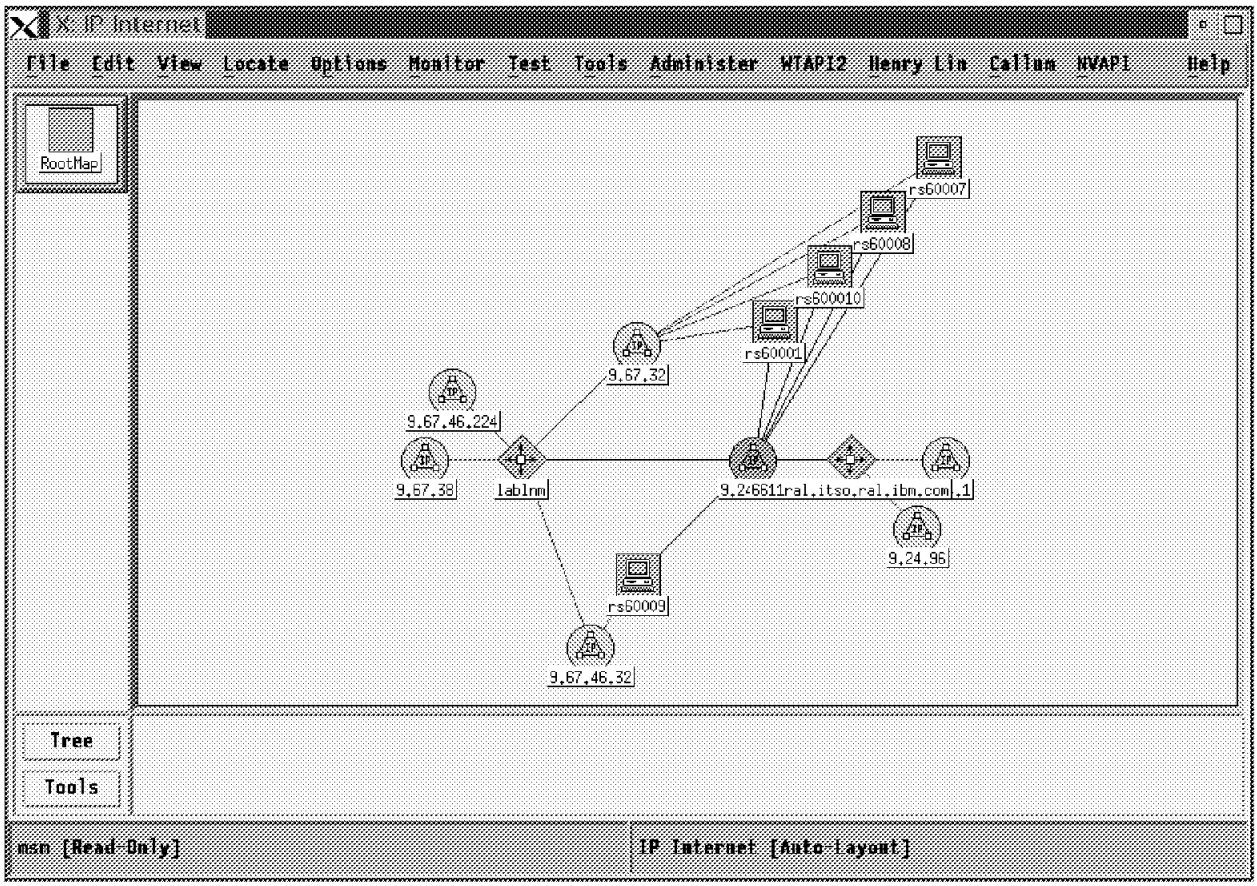


Figure 29. The IP Internet View in NetView for AIX

The topology agent extracts information from both the object and map databases and sends it to the MSM topology manager. The listing provided below shows the type of information that was sent from the topology agent to the topology manager.

```
************************************************************************
*        Topology information for MSM - Part 1    **********************
************************************************************************

 Network name=9.24.104 Plane=2
 Segment name=9.24.104.Segment1 Type=token Plane=2
  alias name=Segment1
 Router sysName=6611ral.itso.ral.ibm.com Plane=2
  sysContact=Hoyt Greeson T/352-2193 Carol Alexander T/352-3383
  sysLocation=Raleigh Bldg 657
  sysDesc=IBM 6611 Network Processor 170 Serial Number: 26-50224 Softwar: Multi
 Interface ipAddress=9.24.104.1 MACaddress=0x10005AC85005 Status=Satisfatory
 END OF ROUTER
 Router sysName=rs60001.itso.ral.ibm.com Plane=2
  alias name=rs60001
  sysContact=Rob Macgregor's V3.2.5  Rob is in: BB112   x1-2325
  sysDesc=IBM RISC System/6000 Machine Type: 0x0010 Processor id: 00014661000 T
 Interface ipAddress=9.24.104.26 MACaddress=0x10005A4F58CE Status=Satisfctory
 END OF ROUTER
 Router sysName=lablnm.itso.ral.ibm.com Plane=2
  alias name=lablnm
  sysContact=Mohammad Shabani X2339
  sysLocation=ITSO LAB, Raleigh
  sysDesc=IBM 6611 Network Processor 170 Serial Number: 26-50220 Softwar: Multi
 Interface ipAddress=9.24.104.81 MACaddress=0x10005AC89063 Status=Satisfctory
 END OF ROUTER
 Router sysName=rs600010.itso.ral.ibm.com Plane=2
  alias name=rs600010
  sysDesc=IBM RISC System/6000 Machine Type: 0x0101 Processor id: 00003317600 T
 Interface ipAddress=9.24.104.109 MACaddress=0x10005AB1AFE9 Status=Satisactory
 END OF ROUTER
 Router sysName=rs60008.itso.ral.ibm.com Plane=2
  alias name=rs60008
  sysDesc=IBM RISC System/6000 Machine Type: 0x0030 Processor id: 00000733000 T
 Interface ipAddress=9.24.104.30 MACaddress=0x10005AA8B5EA Status=Satisfctory
 END OF ROUTER
 Router sysName=rs60009.itso.ral.ibm.com Plane=2
  alias name=rs60009
  sysDesc=IBM RISC System/6000 Machine Type: 0x0034 Processor id: 00002013400 T
 Interface ipAddress=9.24.104.60 MACaddress=0x10005AC92CEB Status=Satisfctory
 END OF ROUTER
 Router sysName=rs60007.itso.ral.ibm.com Plane=2
  alias name=rs60007
  sysDesc=IBM RISC System/6000 Machine Type: 0x0034 Processor id: 00001903400 T
 Interface ipAddress=9.24.104.76 MACaddress=0x10005AC92031 Status=Satisfctory
 END OF ROUTER
 END OF SEGMENT
 Router sysName=6611ral.itso.ral.ibm.com Plane=2
  sysContact=Hoyt Greeson T/352-2193 Carol Alexander T/352-3383
  sysLocation=Raleigh Bldg 657
  sysDesc=IBM 6611 Network Processor 170 Serial Number: 26-50224 Softwar: Multi
 END OF ROUTER
 Router sysName=rs60001.itso.ral.ibm.com Plane=2
  alias name=rs60001
  sysContact=Rob Macgregor's V3.2.5  Rob is in: BB112   x1-2325
  sysDesc=IBM RISC System/6000 Machine Type: 0x0010 Processor id: 00014661000 T
 END OF ROUTER
 Router sysName=lablnm.itso.ral.ibm.com Plane=2
  alias name=lablnm
  sysContact=Mohammad Shabani X2339
  sysLocation=ITSO LAB, Raleigh
  sysDesc=IBM 6611 Network Processor 170 Serial Number: 26-50220 Softwar: Multi
 END OF ROUTER
```

```
**************************************************************************
*        Topology information for MSM - Part 2    **********************
**************************************************************************

 Router sysName=rs600010.itso.ral.ibm.com Plane=2
  alias name=rs600010
  sysDesc=IBM RISC System/6000 Machine Type: 0x0101 Processor id: 00003317600 T
 END OF ROUTER
 Router sysName=rs60008.itso.ral.ibm.com Plane=2
  alias name=rs60008
  sysDesc=IBM RISC System/6000 Machine Type: 0x0030 Processor id: 00000733000 T
 END OF ROUTER
 Router sysName=rs60009.itso.ral.ibm.com Plane=2
  alias name=rs60009
  sysDesc=IBM RISC System/6000 Machine Type: 0x0034 Processor id: 00002013400 T
 END OF ROUTER
 Router sysName=rs60007.itso.ral.ibm.com Plane=2
  alias name=rs60007
  sysDesc=IBM RISC System/6000 Machine Type: 0x0034 Processor id: 00001903400 T
 END OF ROUTER
 END OF NETWORK
 Router sysName=6611ral.itso.ral.ibm.com Plane=2
  sysContact=Hoyt Greeson T/352-2193 Carol Alexander T/352-3383
  sysLocation=Raleigh Bldg 657
  sysDesc=IBM 6611 Network Processor 170 Serial Number: 26-50224 Software: Multi
 END OF ROUTER
 Router sysName=rs60001.itso.ral.ibm.com Plane=2
  alias name=rs60001
  sysContact=Rob Macgregor's V3.2.5  Rob is in: BB112   x1-2325
  sysDesc=IBM RISC System/6000 Machine Type: 0x0010 Processor id: 00014661000 T
 END OF ROUTER
 Router sysName=lablnm.itso.ral.ibm.com Plane=2
  alias name=lablnm
  sysContact=Mohammad Shabani X2339
  sysLocation=ITSO LAB, Raleigh
  sysDesc=IBM 6611 Network Processor 170 Serial Number: 26-50220 Software: Multi
 END OF ROUTER
 Router sysName=rs600010.itso.ral.ibm.com Plane=2
  alias name=rs600010
  sysDesc=IBM RISC System/6000 Machine Type: 0x0101 Processor id: 00003317600 T
 END OF ROUTER
 Router sysName=rs60008.itso.ral.ibm.com Plane=2
  alias name=rs60008
  sysDesc=IBM RISC System/6000 Machine Type: 0x0030 Processor id: 00000733000 T
 END OF ROUTER
 Router sysName=rs60009.itso.ral.ibm.com Plane=2
  alias name=rs60009
  sysDesc=IBM RISC System/6000 Machine Type: 0x0034 Processor id: 00002013400 T
 END OF ROUTER
 Router sysName=rs60007.itso.ral.ibm.com Plane=2
  alias name=rs60007
  sysDesc=IBM RISC System/6000 Machine Type: 0x0034 Processor id: 00001903400 T
 END OF ROUTER
 END OF REPORT
```

Note

For simplicity, all hosts have been left out of the above extract, but they were in fact loaded. The file has also been cut at the right side to fit the page size and split into two parts, to fit the page length. The network and the seven routers in the file have been highlighted to improve readability. Information from adapters that belong to networks not being monitored is also retrieved. You can find this information behind the END OF NETWORK, as these interfaces do not belong to the one managed network. In the NGMF views you will see unmanaged networks similar to those you would see in NetView for AIX. This is the default and may be changed by defining *Unmanage=no* in the GETTOPO CLIST. Hidden resources, which means resources that are not displayed on the NetView for AIX EUI, are not retrieved unless you specify `Hidden=yes` as a parameter with the GETTOPO command.

Figure 30 shows the IP network view on the NGMF screen. Here you can see the display of the IP network created by MultiSystem Manager.

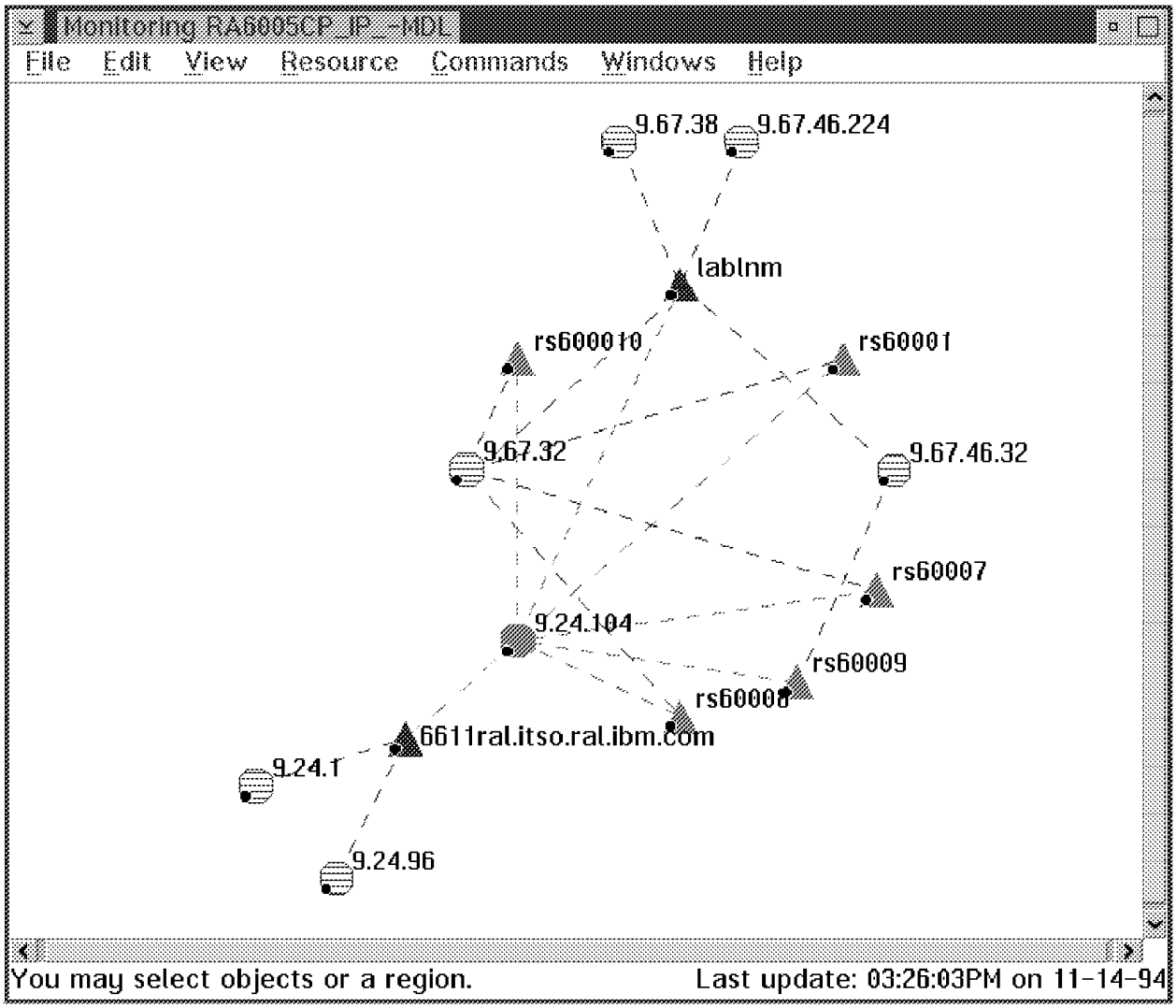


Figure 30. The IP Internet View RA6005CP_IP_-MDL in NGMF

This is the default arrangement that NGMF creates. To make comparison more convenient, we rearranged the icons in NGMF to make the view more similar to NetView for AIX.

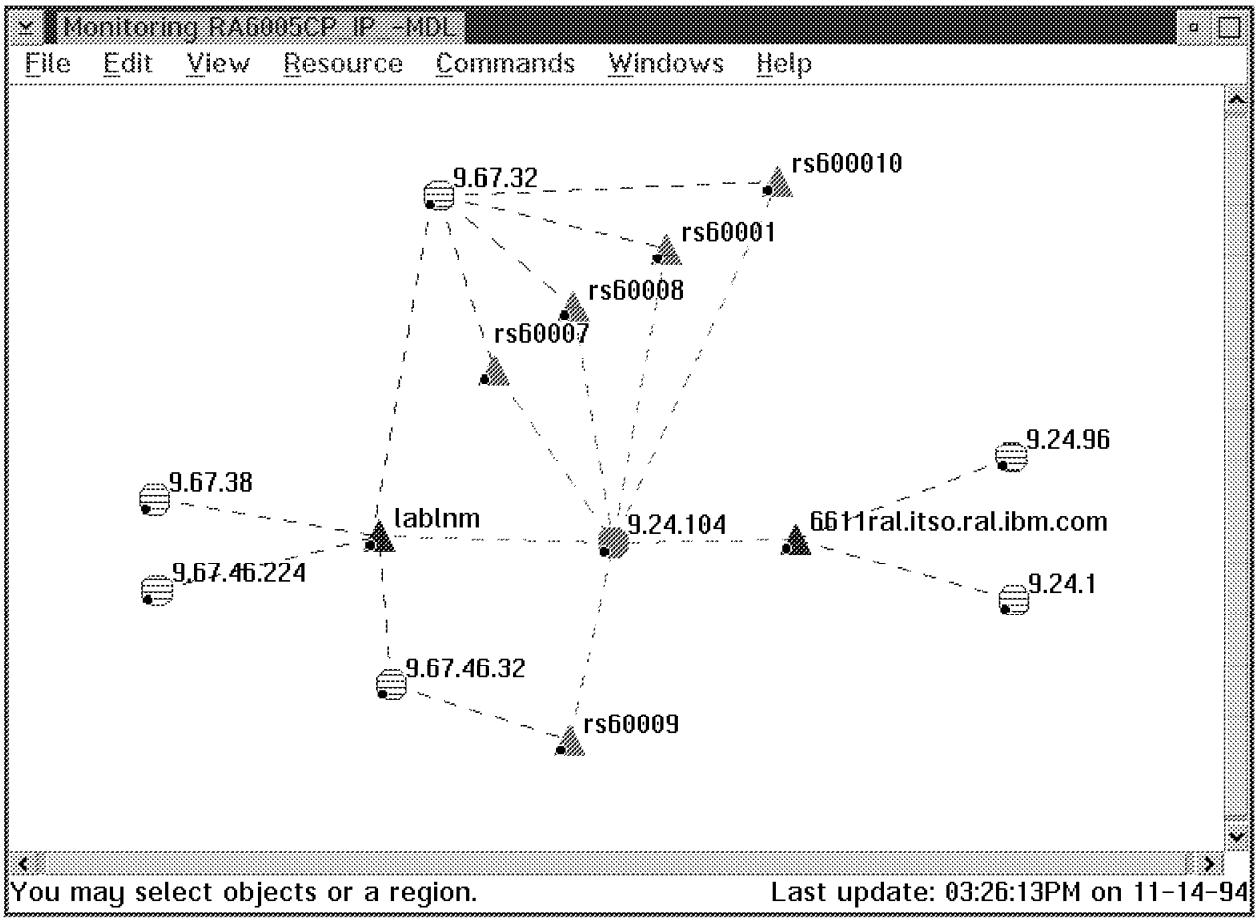


Figure 31. The IP Internet View RA6005CP_IP_-MDL in NGMF after Rearrangement

This customization was done by dragging the icons (pressing the right mouse button). This arrangement is lost when you close and open the view. How to customize the views permanently is described in the next chapter.

3.6 Customizing the IP Views

You may well want to change the style and layout of the views in NGMF to make them easier to use.

3.6.1 Changing the Lines

You might have wondered why the connecting lines between routers and networks are dotted. The reason for this is that they are not REAL but AGGREGATE links. By NGMF standards that means they have to be dotted and not solid. To make these lines solid you just have to change the TypeNumber value from 01006D to 01006C. This makes the lines much more visible:

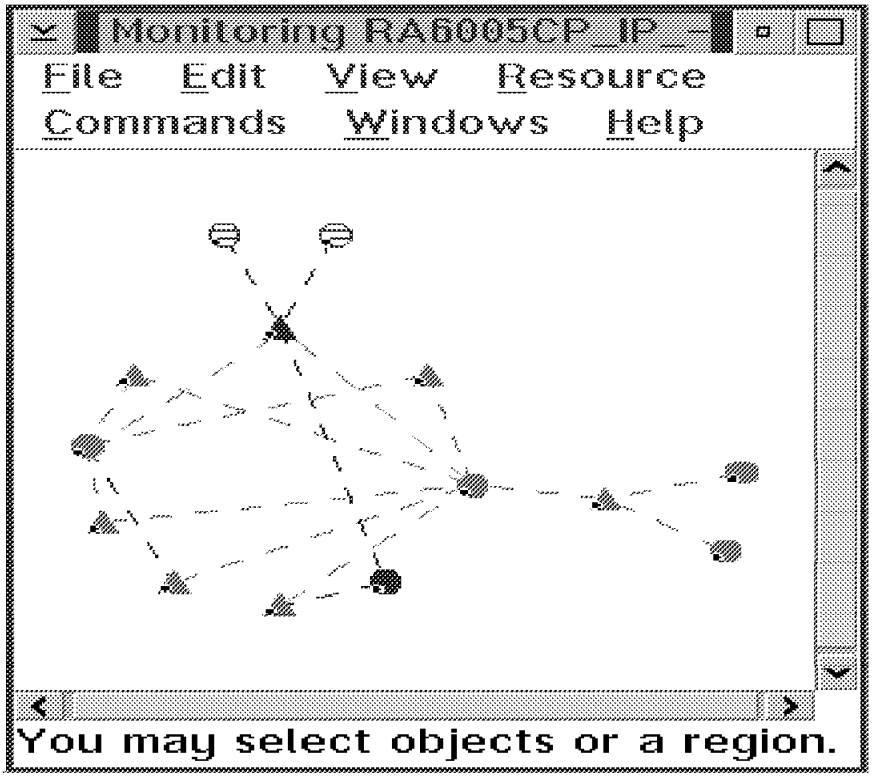


Figure 32. View with Original Links

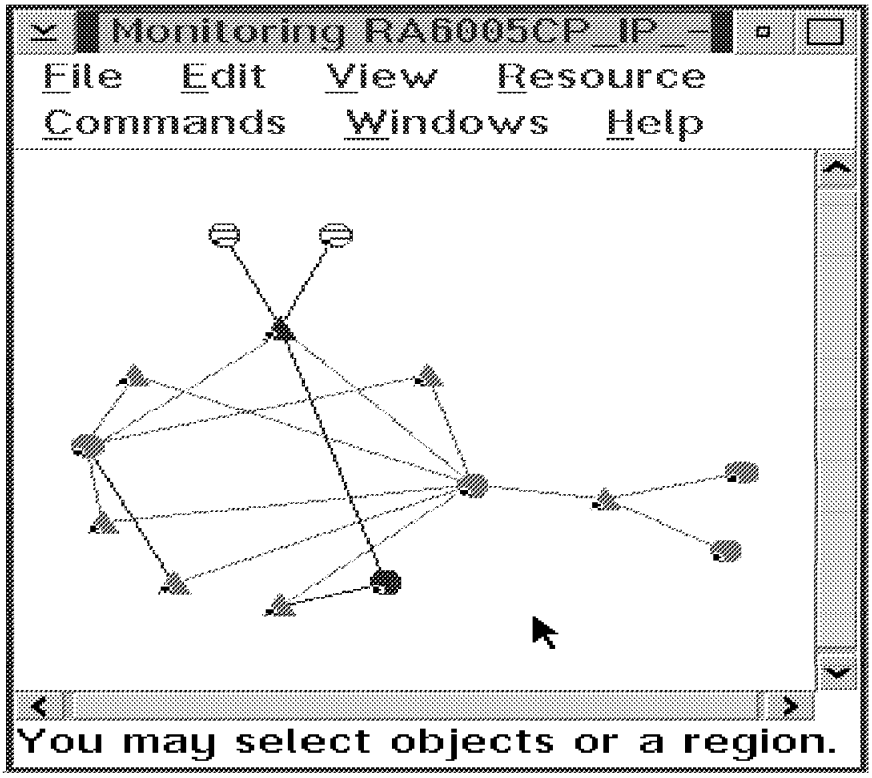


Figure 33. View with Modified Links

There are two ways to do this:

1. Temporary change in RODM

   If you have RODMVIEW installed (part of the RODM Toolkit), you can just change the field in RODM:

   - Class name=>Display_Resource_Type_Class
   - Object name=>DUIXC_LTN_LINK_AGG
   - Field name=>TypeNumber
   - Field data type=>ANON
   - Field data=>01006C

   To see the change, you will need to close the view and reopen it.

2. Permanent change in the GMFHS data model

   Copy the GMFHS data model load file NETVIEW.V2R4M0.CNMSAMP(DUIFSTRC) to another data set so that the original is safe. Search for the definition of the link:

```
-- DUIXC_LTN_IP_LINK_AGG
--  (Internet link aggregate)
CREATE
 INVOKER  ::= 0000001;
 OBJCLASS ::= Display_Resource_Type_Class;
 OBJINST  ::= MyName = (CHARVAR) 'DUIXC_LTN_IP_LINK_AGG';
 ATTRLIST
  DefaultThresholdDegraded         ::= (INTEGER) 1,
  DefaultThresholdSeverelyDegraded ::= (INTEGER) 1,
  DefaultThresholdUnsatisfactory   ::= (INTEGER) 1,
  TypeNumber                       ::= (ANONYMOUSVAR) X'01006D';
```

   Change the TypeNumber value to 01006C.

   Change the EKGIN1 DD statement in the GMFHS data model load job to locate the changed file. Submit the job to load the new data model.

   Please note that this requires a RODM cold start to take effect!

3.6.2 Customizing Views

NGMF has a facility called retained views that will allow you to create and save customized views.

If you want to save a customized view as a *retained* view, look for the MODEL View in the Graphic Monitor list as shown in Figure 34.

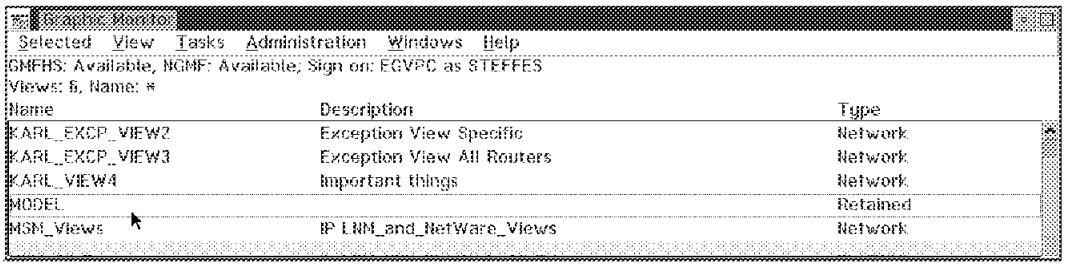


Figure 34. The MODEL View

Select the MODEL view and open it by selecting *Open as* and *Customize* from the menu bar:

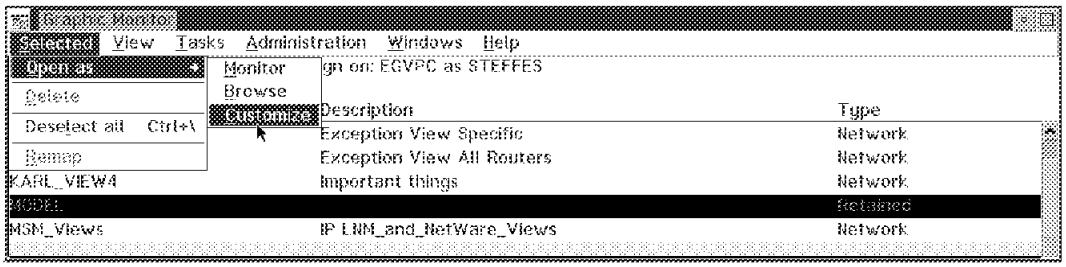


Figure 35. Opening the MODEL View

An empty window will appear.

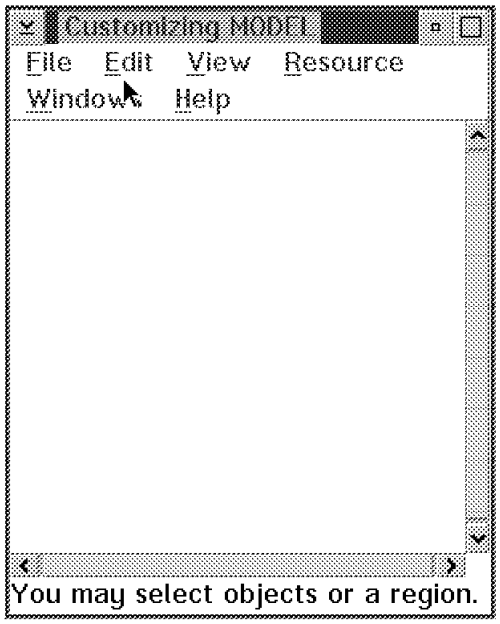


Figure 36. The Customizing Model Window

Open your IP network view and draw a frame around the network using the left mouse button.

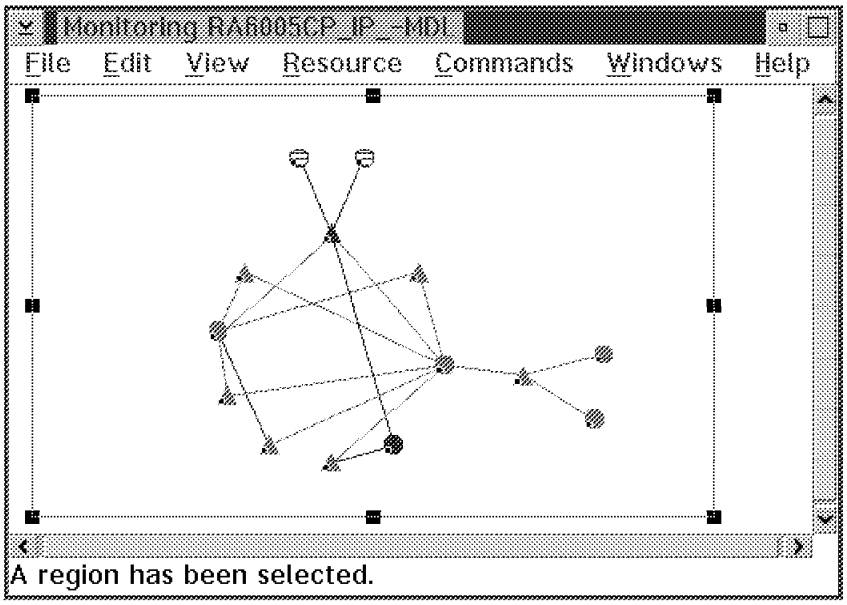


Figure 37. Selecting Your View

Then select **Edit** from the menu bar and click on **Copy** as shown in Figure 38.

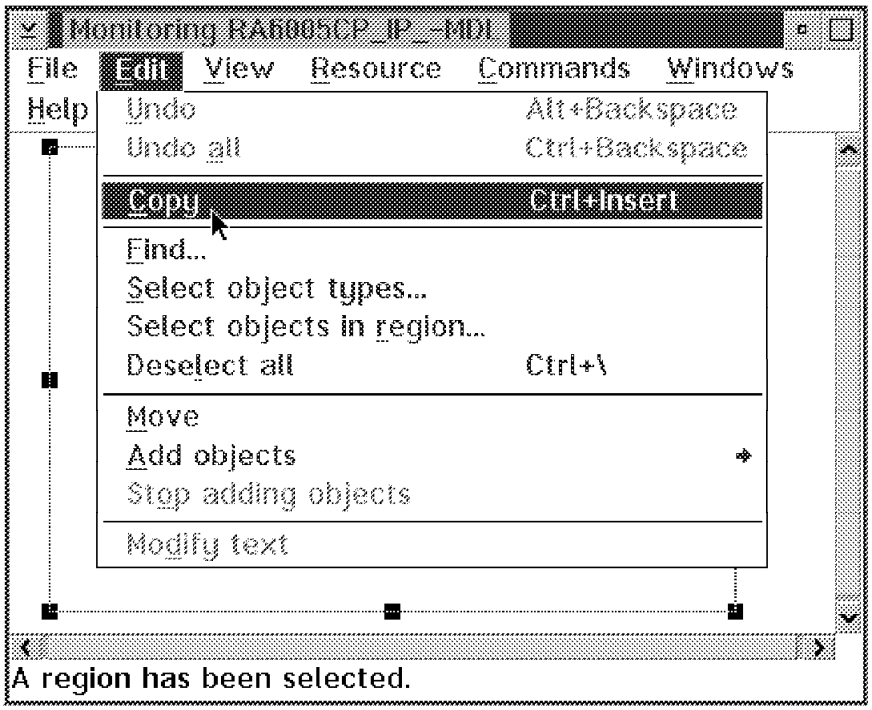


Figure 38. Copying Your View

In the pop-up window select all the options and **copy**.

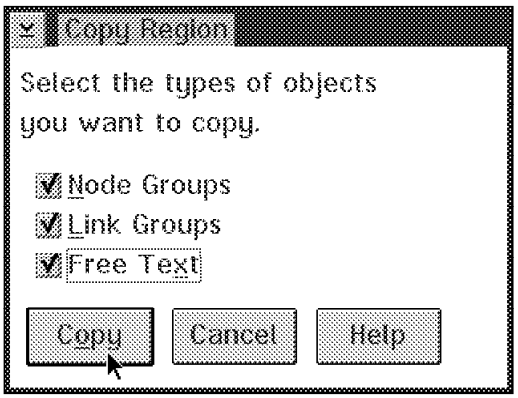


Figure 39. The Copy Region Selection Window

Then go to your empty Model view window and select **Edit** and **Paste**.

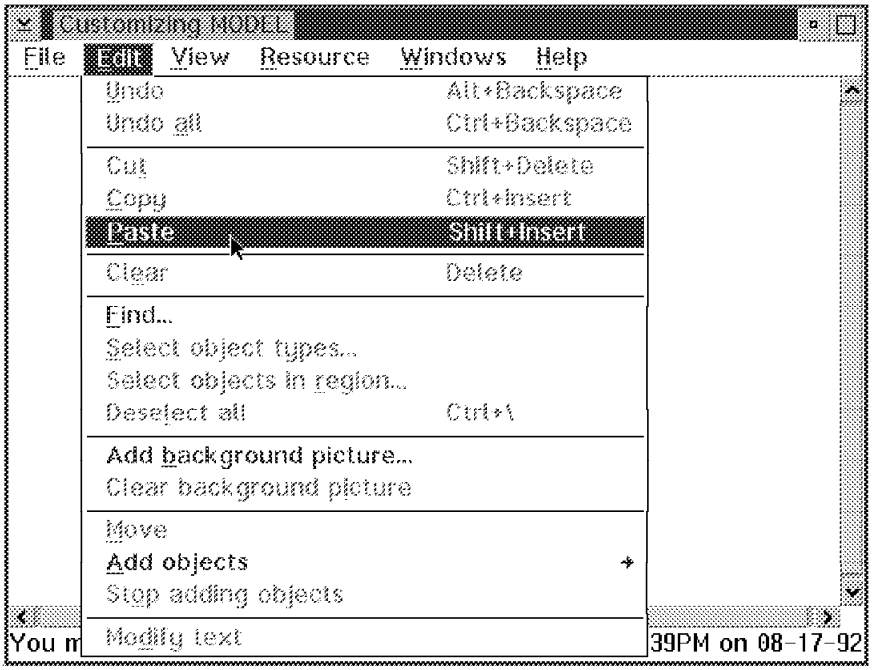


Figure 40. Pasting Your View - Step 1

When the empty frame appears, press the left mouse button.

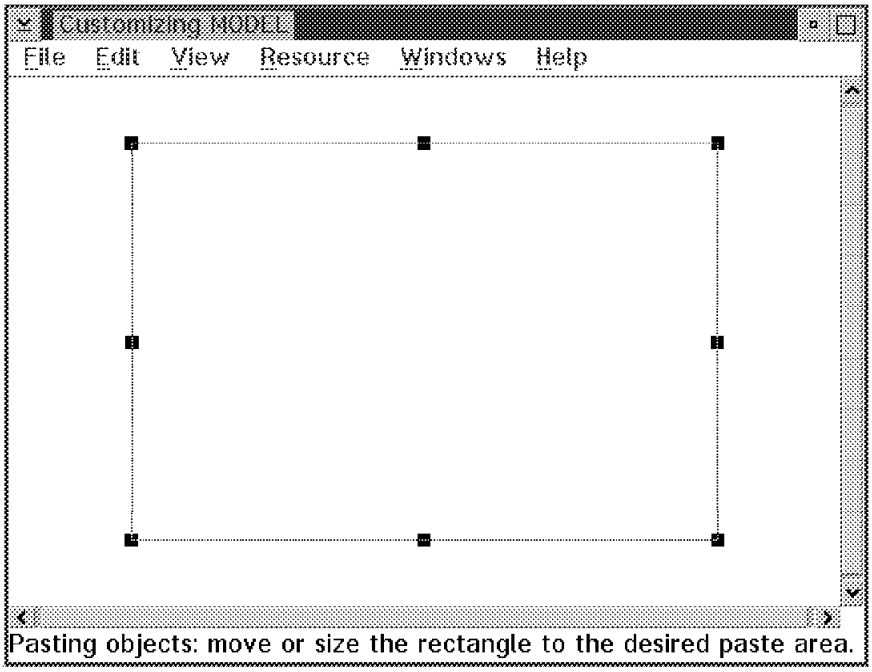


Figure 41. Pasting Your View - Step 2

The view will appear in a bright blue color. If it doesn't fit the window, select **View** and **Zoom to fit**.

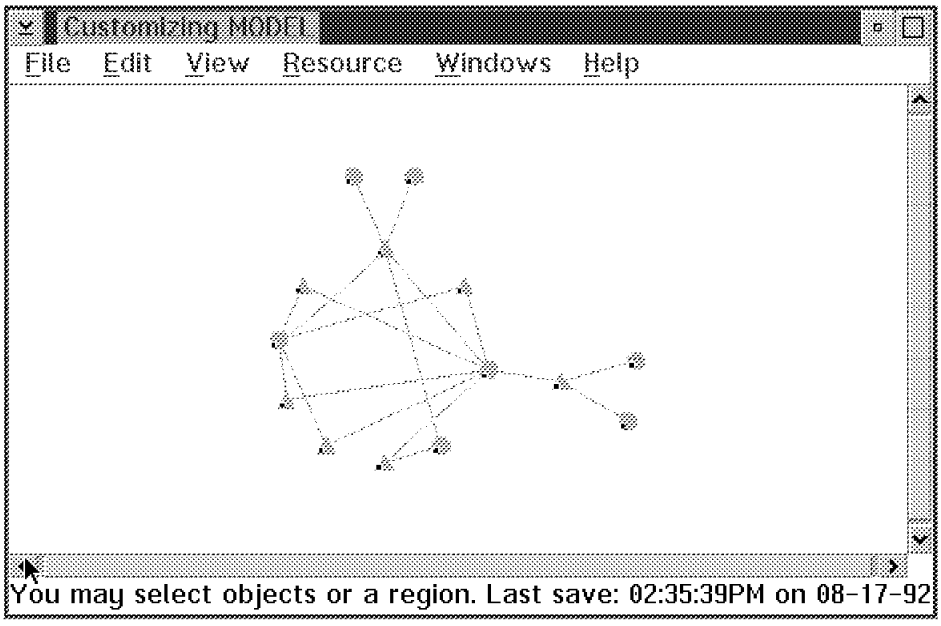


Figure 42. The Customized Model View

Draw the icons to the position you would like and save the view as shown in Figure 43 on page 57.

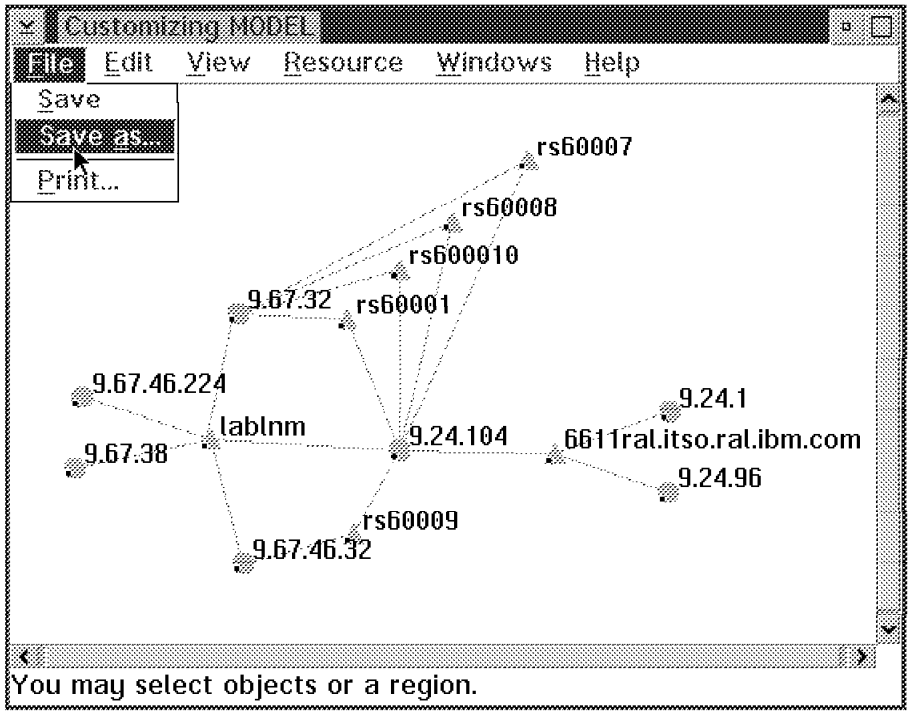


Figure 43. Saving the Customized View - Step 1

Enter the name of the view and a description as shown in Figure 44.

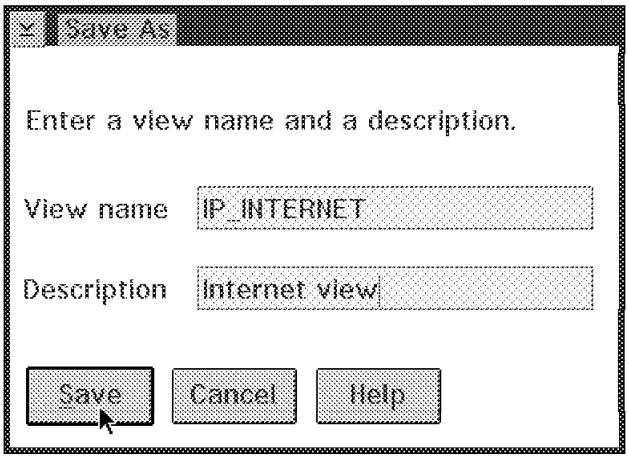


Figure 44. Saving the Customized View - Step 2

On returning to the main Graphic Monitor window, the new view will appear as a retained view in the list of views as shown in Figure 45.

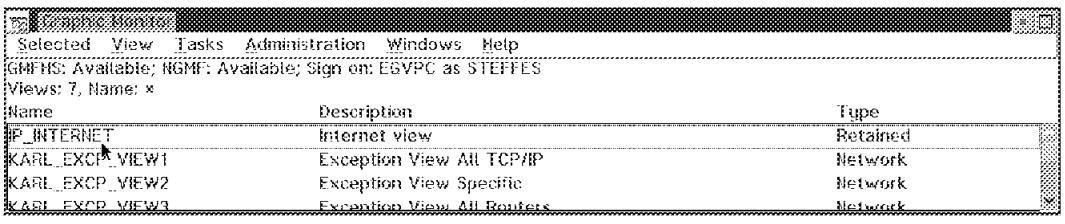


Figure 45. The New View

When you open the view with a double click, you will find your customized views with the proper status colors.

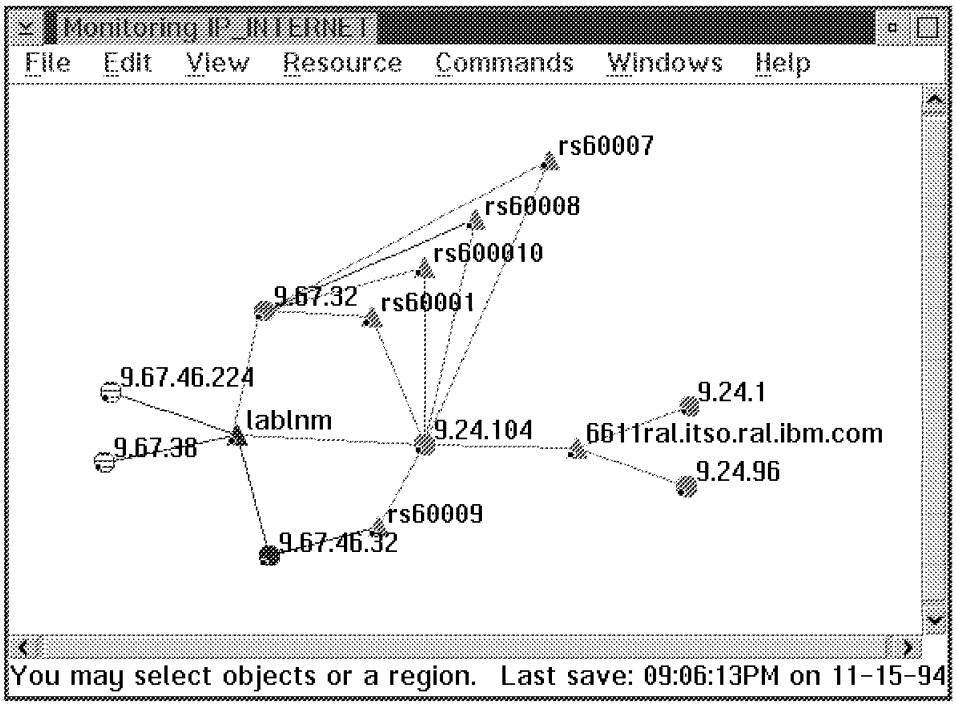


Figure 46. The Customized View

If you want to make further changes select the view, then open it and select the **customize** option as shown in Figure 47.

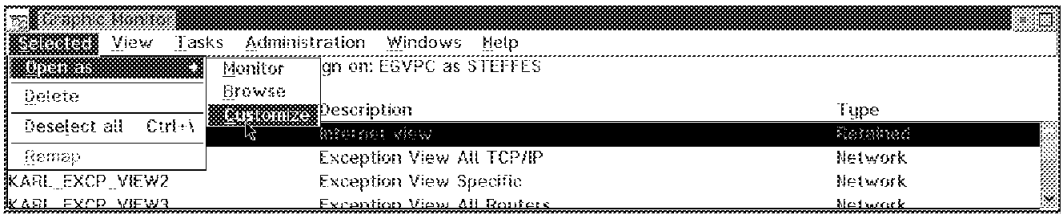


Figure 47. Opening the View for Further Customization

As an example we selected **Add background picture** from the Edit pull-down.

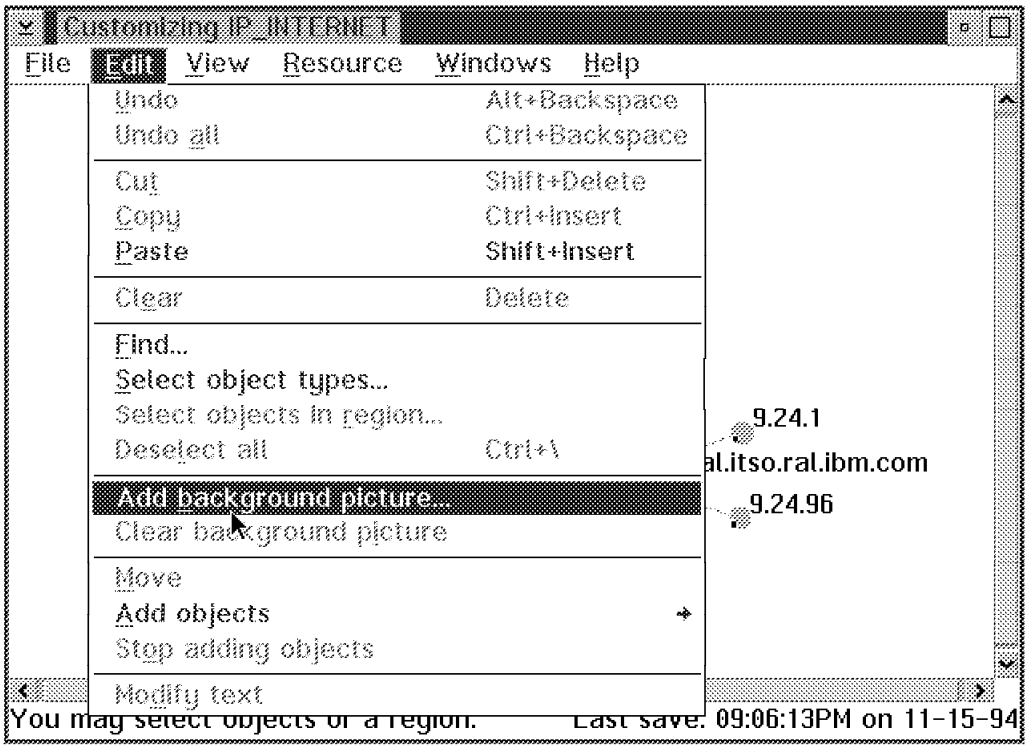


Figure 48. Adding a Background Picture

We chose the **Europe** map, which resulted in the final view as shown in Figure 49.

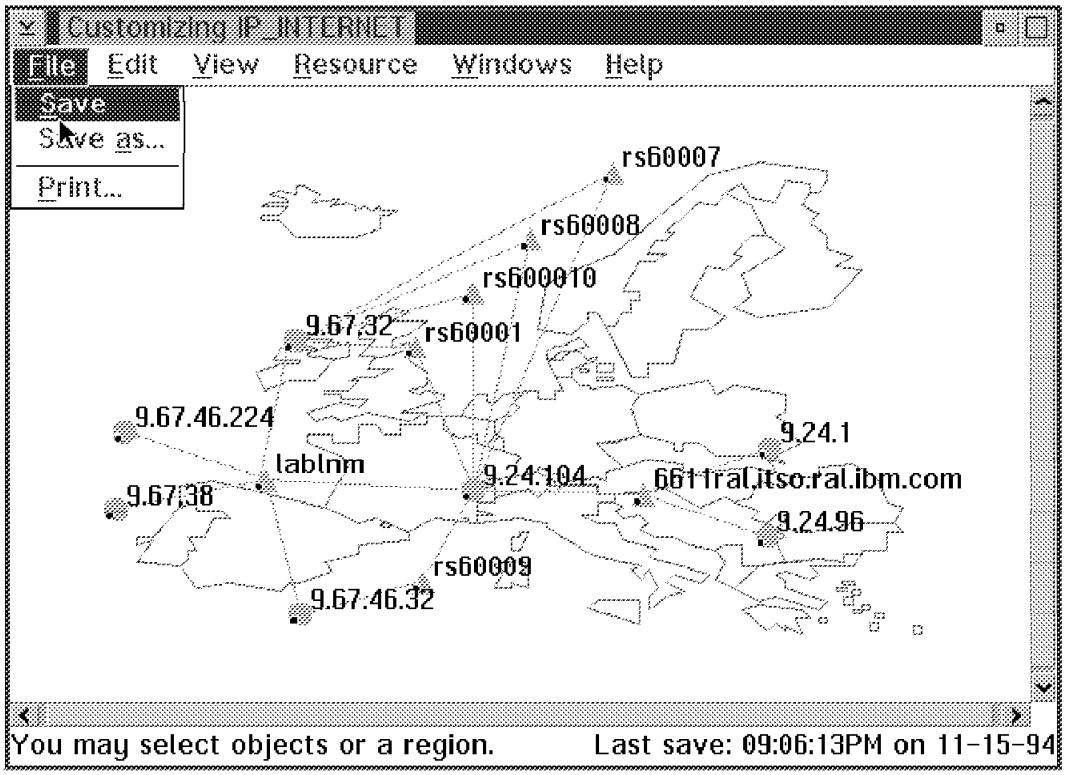


Figure 49. The Final View

If your topology changes, for example new objects are added, you will need to add them manually or even to re-do your picture.

3.7 Monitoring IP Resources

As the Service Point can't send out a node down alert if it is failing itself, you should enable the MSM heartbeat function. This function regularly checks if the connection to the Service Point is still active.

However, bear in mind that every heartbeat will issue a RUNCMD which could flood the Service Point application log on the AIX machine as mentioned in 3.5.3.1, "Initial Topology Discovery" on page 43.

Once MultiSystem Manager has collected topology information, it also needs to provide timely status information about the discovered resources.

MultiSystem Manager receives status change notifications via SNA/MS Major Vectors - Alerts(0000) and Resolutions(0002). NetView for AIX only uses alerts.

The following diagram shows how the topology RUNCMDs and the alerts flow through MultiSystem Manager.

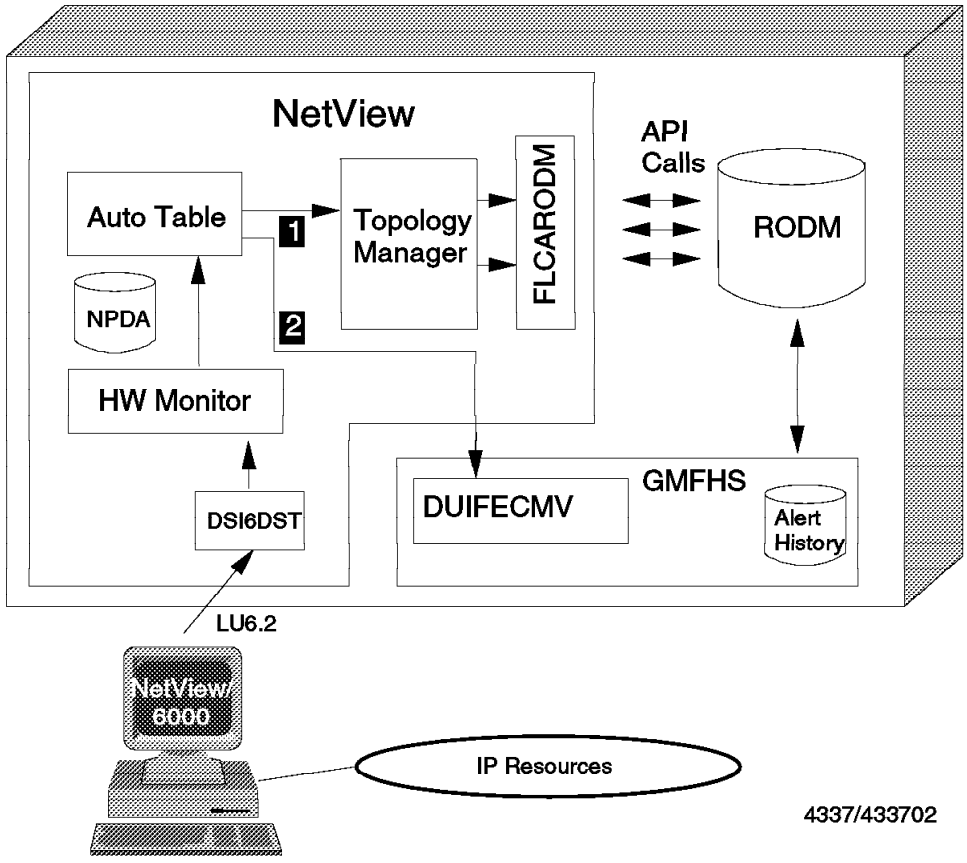


Figure 50. Alert Flow

Key Explanation:

1 The NetView Automation Table routes the alerts to the Topology Manager, which in turn queries RODM and creates the instance when necessary.

2 The NetView Automation Table also routes the alerts to the GMFHS Event Manager.

Note

Filtering is usually desirable to reduce the number of alerts that can be sent from NetView/6000 to NetView for MVS. To make sure you do not filter out any of the alerts that the MSM IP agent sends to MSM, use the sample filter provided by the topology agent. The default filter provided by MSM is automatically activated in the installation process. After it has been included once, it will become active every time the *TRALERTD* daemon starts. The MSM alert filter is shown in Figure 51.

```
RuleName=MultiSystem_Manager_Alert_Filter
RuleDescription=MultiSystem Manager trap-to-alert filter conversion
RuleContent=(
(CLASS=1.3.6.1.4.1.2.6.67 && (
SNMP_SPECIFIC=565504401
|| SNMP_SPECIFIC=565504402
|| SNMP_SPECIFIC=565504403
)) ||
(CLASS=1.3.6.1.4.1.2.6.3 && (
SNMP_SPECIFIC=58785794
|| SNMP_SPECIFIC=58785795
|| SNMP_SPECIFIC=58916866
|| SNMP_SPECIFIC=58916867
|| SNMP_SPECIFIC=50790441
|| SNMP_SPECIFIC=50790442
)))
```

Figure 51. Alert Filters

This filter describes the traps that pass through to NetView for MVS in addition to those specified in the default filter. If the default filter was not changed, the *IUP_EV* and the *IDWN_EV* pass through anyhow (those are the trap ids 58916866 and 58916867). In the filter shown in Figure 51, you find six NetView for AIX traps and the three MultiSystem Manager traps that have been added during the agent installation process.

When alerts arrive in the NetView Automation Table, they are analyzed by IBM NetView MultiSystem Manager's automation table entries. The IP entries as they ship in the file FLCSTBLI are shown in Figure 52.

```
/*********************************************************************/
/*       5655-044 (C) Copyright IBM Corp. 1994.                      */
/*       All Rights Reserved.                                        */
/*********************************************************************/
/*                                                                   */
/*                                                                   */
/*                                                                   */
/*********************************************************************/
/*  Act upon the alerts from NetView for AIX.                        */
/*********************************************************************/

IF (MSUSEG(0000.10.11(2) 3 5) = '0100') &
  (MSUSEG(0000.10.11(2).02 3) = '5696-3620' . |
   MSUSEG(0000.10.11(2).06 3)=HEX('C1C9E740D585A3E58985A661F6F0F0F0') |
   MSUSEG(0000.10.11(2).02 3) = '5696-7310' . |
   MSUSEG(0000.10.11(2).06 3)=HEX('D585A3E58985A64086969940C1C9E7')) &
 HIER ¬= ''
THEN
  EXEC(CMD('FLCAIAUT') ROUTE(ONE DUIFEAUT))
  CONTINUE(N);
```

Figure 52. Default IP Code in the NetView Automation Table

FLCSTBLI verifies that the alerts are originating from the MSM IP agent by checking the product ID. FLCSTBLI then calls the REXX Command List FLCAIAUT which parses the contents of the alert and then executes the appropriate commands.

Please Note!

If you modify FLCSTBLI, you must ensure that FLCAIAUT runs under the DUIFEAUT autotask. It is not possible to change this to another autotask.

FLCAIAUT is shipped as a compiled REXX clist but also as an uncompiled sample in SFLCSAMP member FLCSIAUT. To modify it copy FLCSIAUT into a data set before the MSM data sets in the DSICLD concatenation, rename it to FLCAIAUT, and run CLIST FLCBLODI to load it.

The following tables show what action MSM takes on the alerts.

Table 1. MSM Alerts

Trap ID number	Meaning	MSM Action
565504401	Agent started and waiting	Change the agent's status to intermediate.
565504402	Agent up and ready	Change the agent's status to satisfactory and issue a GETTOPO IPRES.
565504403	Agent down	Change the agent's status to unsatisfactory.

Table 2. NetView/6000 Alerts		
Trap ID number	**Meaning**	**MSM Action**
58785794	Node added	Issue a GETTOPO IPDETAIL.
58785795	Node deleted	Purge the node from RODM.
58916866	Interface up	Change the interface's status to satisfactory.
58916867	Interface down	Change the interface's status to unsatisfactory.
50790441	Interface managed	If the interface does not exist in RODM, issue a GETTOPO IPDETAIL
50790442	Interface unmanaged	Change the interface's status to unknown.

If many interface managed traps arrive, many GETTOPOs are sent in short intervals and some catch NetView/6000 doing database resync. This might cause the GETTOPO to fail and put the agent into unsatisfactory state and the network into unknown. Following traps are then ignored. The next heartbeat will put the agent into satisfactory but leave the net in unknown state.

This can happen if you do new discoveries on NetView/6000 while the connection to MSM is up.

If you run into this problem, just do a manual GETTOPO from the NetView command line, but if this happens a lot, remove the Node added and Interface managed traps from FLCAIAUT. To get the updated topology you might issue the GETTOPO manually or put it on a NetView timer. If you use a timer, you can set heartbeat on the GETTOPO command to zero.

3.8 Managing Resources

NetView uses RUNCMDs to forward commands to the Service Point application.

There are various ways of issuing commands to the NetView for AIX environment, for example using the NetView console, or the NGMF workstation with Command Tree/2.

Provided below are some comments regarding these two ways of sending commands to the Service Point applications.

3.8.1.1 RUNCMDs from the NetView Command Line

One way to send commands to a NetView for AIX workstation is to type in the RUNCMD directly at the NetView command line (NCCF). A brief description of the command syntax is provided below to illustrate the information required as input to the RUNCMD.

```
RUNCMD SP=service_point_name,
   APPL=application name,
   NETID=netid,
   command
```

Where:

SP

- Is either the PU name for an SSCP-PU session
- The LU name for an LU 6.2 session using SNA Services
- The CP name for an LU 6.2 session using SNA Server

APPL is the name of the Service Point application SPAPPLD as specified in the Set Options... menu for host connection daemons in NetView for AIX SMIT.

Note

See Appendix A.1, “Service Point Installation and Configuration” on page 183 for details. The transaction program name you specify in the RUNCMD should be the application name you specified for the spappld in NetView for AIX.

NETID is the network ID if the partner LU belongs to another SNA network.

command can be any AIX, SNMP or NetView for AIX command string, or an AIX shell script may also be invoked.

3.8.1.2 Command Tree/2 Commands

To simplify the process of sending commands to the service points, MSM ships Command Tree/2 command sets for IP. By using a combination of CT/2 and the DMCS REXX CLIST, the user can build the appropriate RUNCMD command in a “point and click” process. For CT/2 examples see Chapter 4, “Sample IBM NetView MultiSystem Manager Scenarios” on page 67.

When a resource is selected, required information about the resource will be filled in by the system. Some of this information is passed over to CT/2 from the NGMF command exit, and the rest of the information (like service point name) is retrieved from RODM using the DMCS CLIST as illustrated Figure 53 on page 65. When the required information has been retrieved, the appropriate RUNCMD is built and sent to the Service Point.

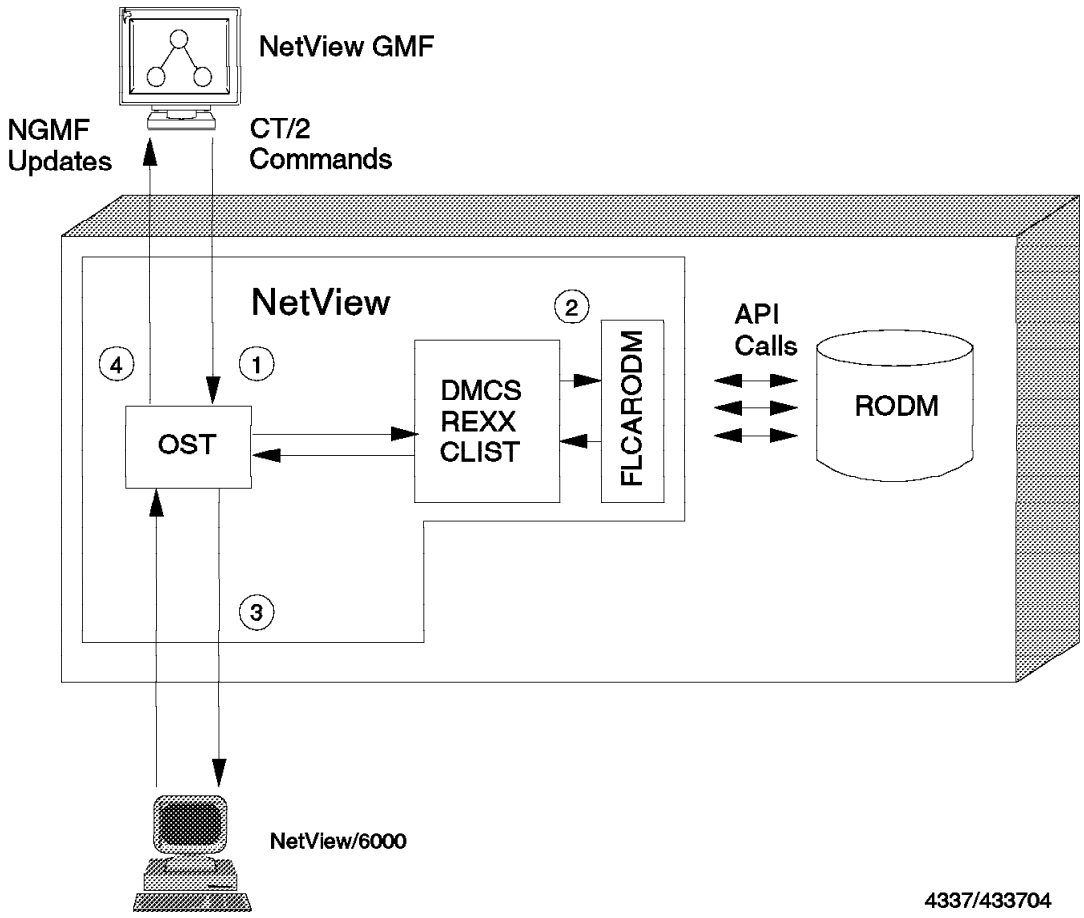


Figure 53. DMCS CLIST Sending RUNCMDs to NetView for AIX

Chapter 4. Sample IBM NetView MultiSystem Manager Scenarios

The following section describes some examples of how the IP topology agent can be used. We will illustrate some management scenarios that cover the following areas:

- Invoking IP commands from NGMF
- Working with the Management Information Base
- The Remote Console Function
- The Backup Manager Function of NetView for AIX

4.1 Invoking IP Commands from NGMF

This chapter describes two different ways to issue IP command from NGMF:

- Command Tree/2
- The Non-SNA command line

The CLIST NETVCMDX offers another way to issue IP commands. It is described in Chapter 7, “IBM NetView MultiSystem Manager Tools” on page 149.

4.1.1 Using Command Tree/2

MSM provides a easy-to-use command interface, based on Command Tree/2, to issue commands to the resources represented by the objects in your NGMF views. This command interface builds the command based on the object you select in the NGMF view. It asks you to complete only those parameters that it cannot complete for you. You are not required to enter the object′s name or address.

Before you start using the Command Tree/2 function, you should activate the Command responses window by selecting **Commands**, **Network** and **Command responses** from the menu bar in a view and the pull-down menus. Minimize the Command responses window and leave it in the background. It appears automatically and presents you with the command responses when you issue a command.

To start Command Tree/2 select **Build commands** from the Commands pull-down menu as shown below:

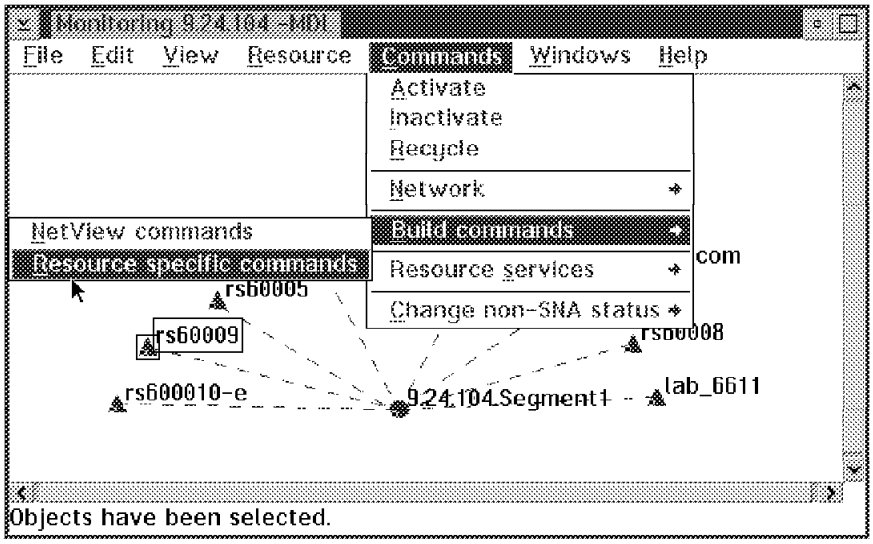


Figure 54. Selecting the Command Tree/2 Support in NGMF

Note

Verify that you have an IP object selected before attempting to open the Command Tree/2. Otherwise opening the Command Tree will fail without issuing an error message (the workstation just beeps!). Selecting **Resource specific commands** opens a window as shown below:

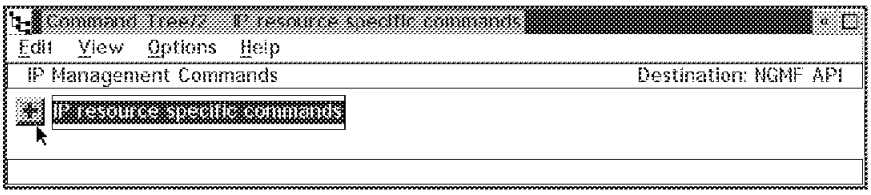


Figure 55. Selecting the Command Tree/2 for IP Commands

By clicking on the plus symbol you can open the different branches of the command tree. An example is shown below.

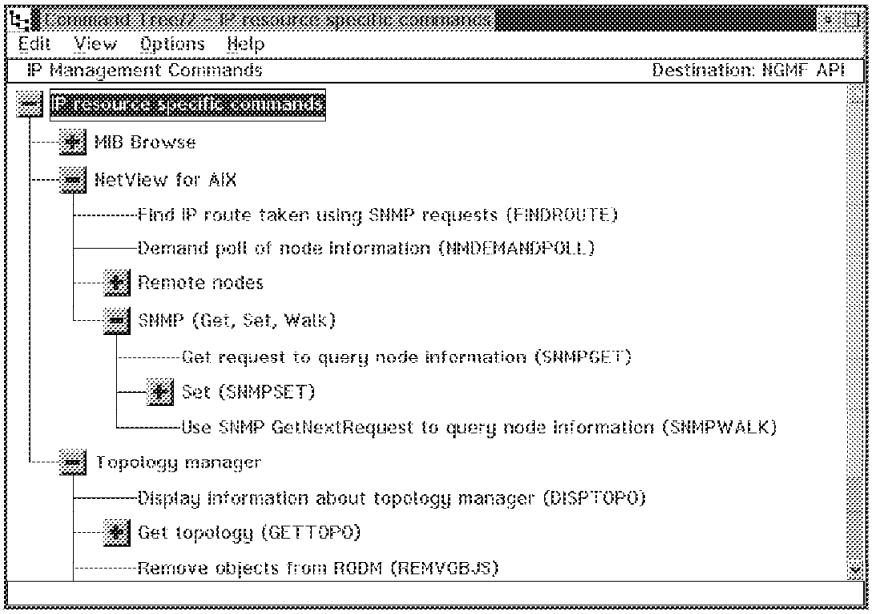


Figure 56. The Command Tree/2 for MSM IP

In the example below we chose **Demand poll** option from the branch NetView for AIX. The Demand poll is an operation that checks for network nodes. It is used when NetView/6000 collects information about new nodes. It provides information about the node's configuration and status and checks for exceeded thresholds and log events. To invoke a command you have to double-click on the **Command Tree/2** entry.

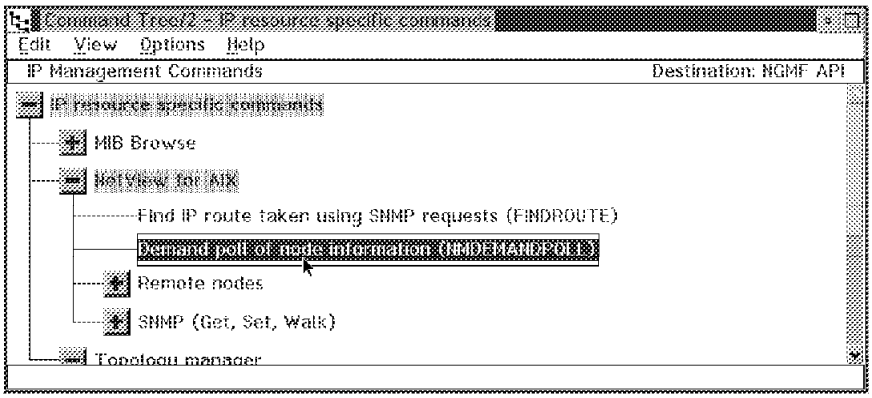


Figure 57. Selecting Demand Poll from the Command Tree/2

The Command window appears and displays the built command containing the object information and the RUNCMD command information which will be needed. The resource you chose is selected automatically. This window is shown in Figure 58 on page 70.

Figure 58. The Command Window

When you confirm the command by clicking on the **Send** push button, the Command Responses window appears. It presents the information NetView/6000 retrieved from rs60002, the RISC/6000 we had selected, by issuing a Demand poll. You can see this in Figure 59.

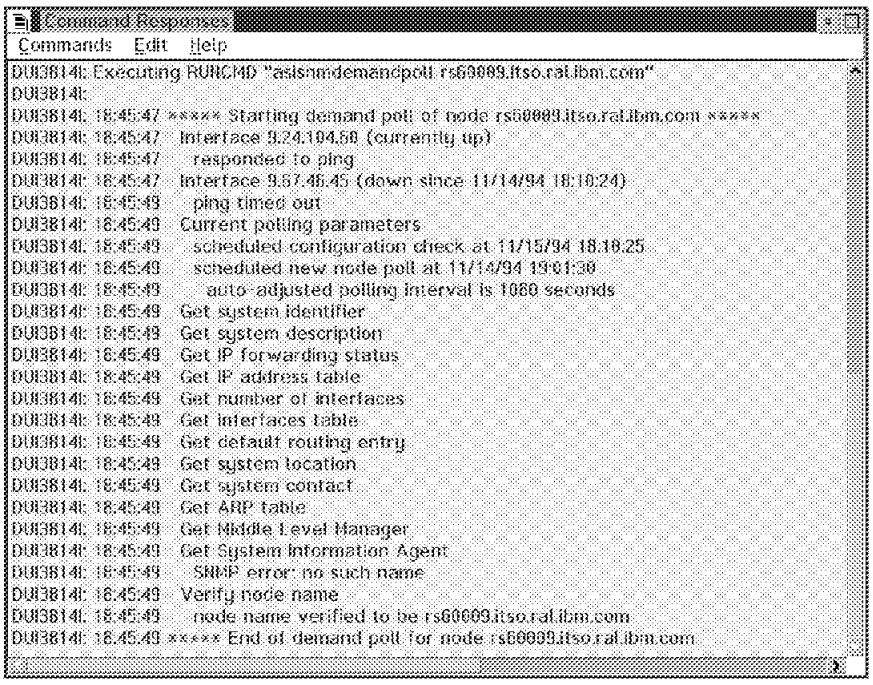


Figure 59. The Command Responses Window Containing Demand Poll Information

Figure 60 on page 71 shows all options available with the default Command Tree/2 support. Some of the commands are valid only with certain resource types.

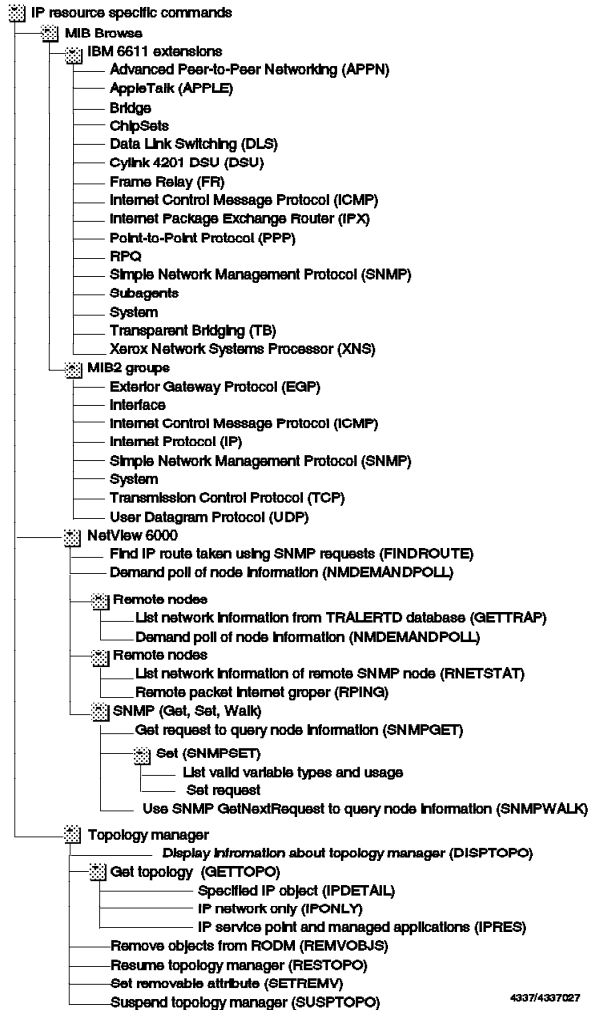


Figure 60. Available Commands with MSM IP Command Tree/2 Support

4.1.1.1 Using an Alternate Command Definition Profile

Included with each NetView MSM agent is a command definition file (.CDF file). This file defines the commands that can be issued to each agent using CommandTree/2 and MultiSystem Manager. The command definition file for each agent includes all of the commands for that agent sorted by special items. For the LNM agent, the CDF file contains commands named by resource, and for the NetWare agent, commands are named by action, for example, QUERY. For the IP agent, commands are structured by target as shown in Figure 60.

The name of the command definition file for the IP MSM agent (that means the one which is installed by default) is FLCI0001.CDF and is located in ibmfkb/flccmds.

It is possible to change the appearance of the Command Tree/2 for MSM IP. You might want to add a command or to rearrange the commands. This can be done by modifying the command definition file or by creating a new one.

Note

If you change the *.CDF file, you will have to stop and to restart NGMF including Graphic Data Server to make it active.

We added a branch called SP to the Command Tree/2. It contains some useful commands controlling the NetView for AIX machine. This is what we added to the FLCI0001.CDF file:

```
CommandNode "IP.SP"
 NLS_DisplayText "Testing the agents machine"
 HelpId 30712
SubSetID 0
SubSetID 1
SubSetID 2
SubSetID 3

CommandNode "IP.SP.TRALERTDTEST"
 NLS_DisplayText "Display Status of trap_to_alert daemon (OVSTATUS TRALERTD)"
 HelpId 32230
SubSetID 0
 CommandString "DMCS RODMOBJECTID=&RESOURCE.,SP=%spname%,APPL=%applname%,CMD=ovs
tatus tralertd"
 WhenToPreview Always
SubSetID 1
SubSetID 2

CommandNode "IP.SP.NV6000TEST"
 NLS_DisplayText "Display Status of NV/6000 daemons (OVSTATUS)"
 HelpId 32230
SubSetID 0
 CommandString "DMCS RODMOBJECTID=&RESOURCE.,SP=%spname%,APPL=%applname%,CMD=ovs
tatus"
 WhenToPreview Always
SubSetID 1
SubSetID 2

CommandNode "IP.SP.DISKCHECK"
 NLS_DisplayText "Check Disk Space (DF)"
 HelpId 30713
SubSetID 0
 CommandString "DMCS RODMOBJECTID=&RESOURCE.,SP=%spname%,APPL=%applname%,CMD=df"
 WhenToPreview Always
SubSetID 1
SubSetID 2
* /
```

So when we open the Command Tree/2 after selecting any resource, we get additional options as shown in Figure 61 on page 73.

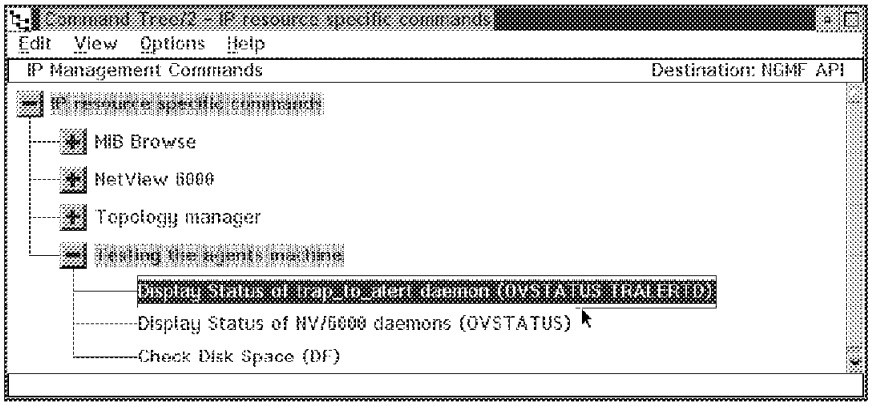


Figure 61. The Customized Command Tree/2

Double-clicking on the first branch (**Display Status of trap_to_alert daemon (OVSTATUS TRALERTD)**) leads to the following result in the command response window:

Figure 62. The Command Response Window Showing the Status of tralertd

You can see that the TRALERTD state is RUNNING.

Our new commands always apply to the Service Point machine itself, no matter which resource was selected! This is only for reasons of simplicity, it is also possible to use the selected resource as a variable, that is passed to the AIX service point machine as in the provided default commands.

4.1.2 Using the Non-SNA Command Line

NGMF provides a non-SNA command line as a fast and convenient way to issue RUNCMD commands against the Service Point machine. Select the service point and click open the **Non-SNA command line** as shown in Figure 63 on page 74

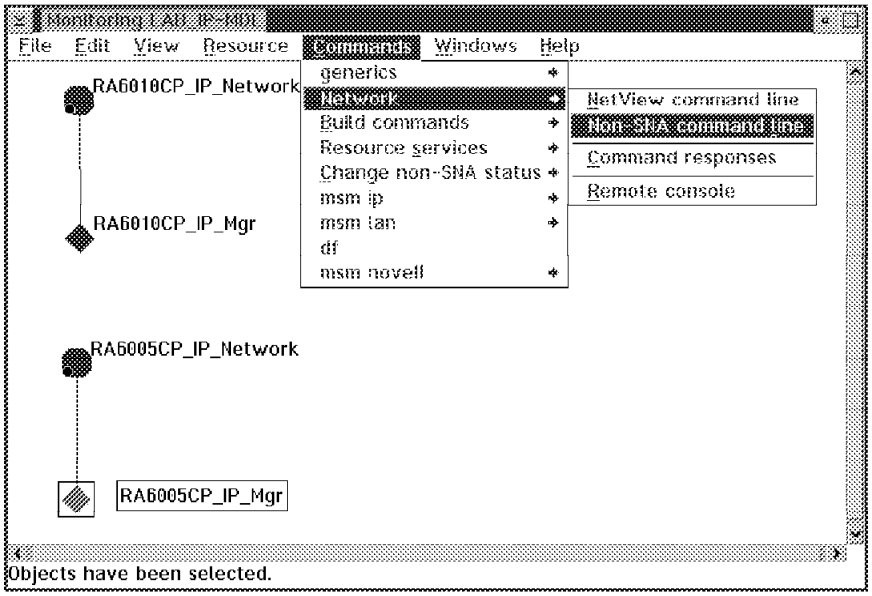


Figure 63. Accessing the Non-SNA Command Line

Type any non-SNA command and click on **Send**:

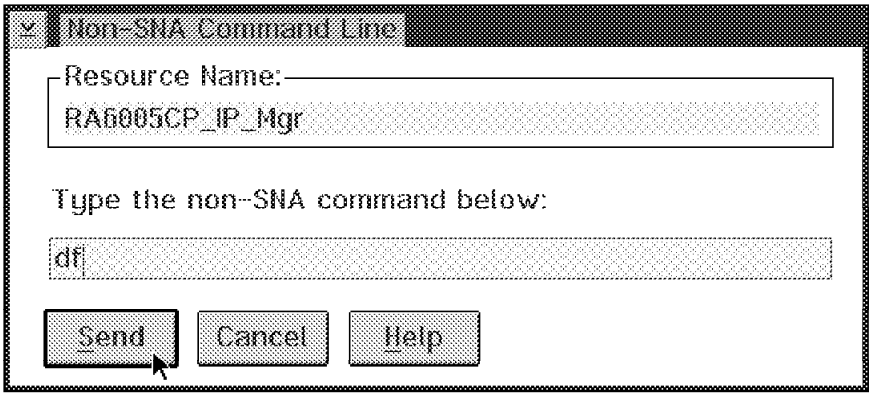


Figure 64. Invoke Non-SNA Command

The output is displayed in the command response window as shown in Figure 65.

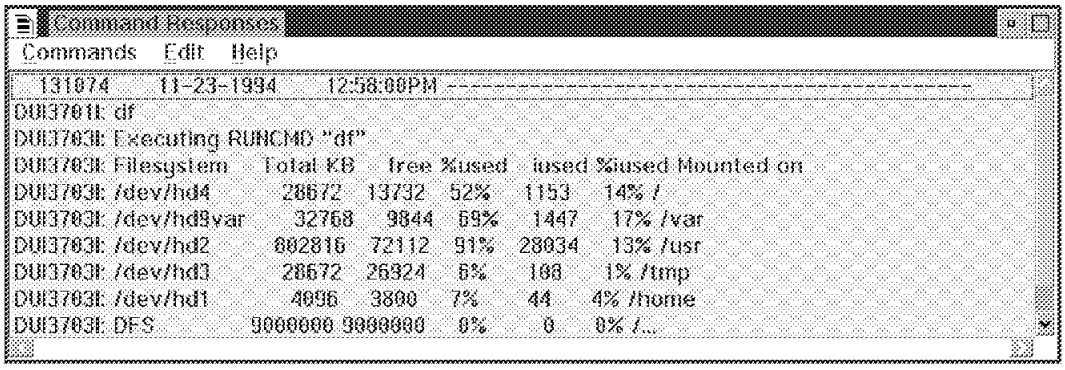


Figure 65. Command Response

Note

The pipe (|) is not accepted in the Non-SNA command line window.

4.2 Working with the Management Information Base

The MSM agent running on NetView/6000 makes MIB management functions available from NetView for MVS, using NGMF.

4.2.1 MIB Structure

The Management information base (MIB) is a collection of network objects. It is not actually a database residing somewhere on the network. The individual pieces of information, called MIB objects, reside on the agent system, where they can be accessed (GET request) and changed (SET request) by an SNMP manager.

Because the objects within an internet have many common characteristics across subnetworks, vendor products, and individual components, the Internet MIB provides a registration scheme wherein objects can be defined and categorized. This concept is founded on the ISO/CCITT agreement convention that the Internet standard uses to identify objects within a system. The Internet standard uses ASN.1 syntax in the MIB to describe the object types. An overview of the MIB tree is provided in Figure 66 on page 76.

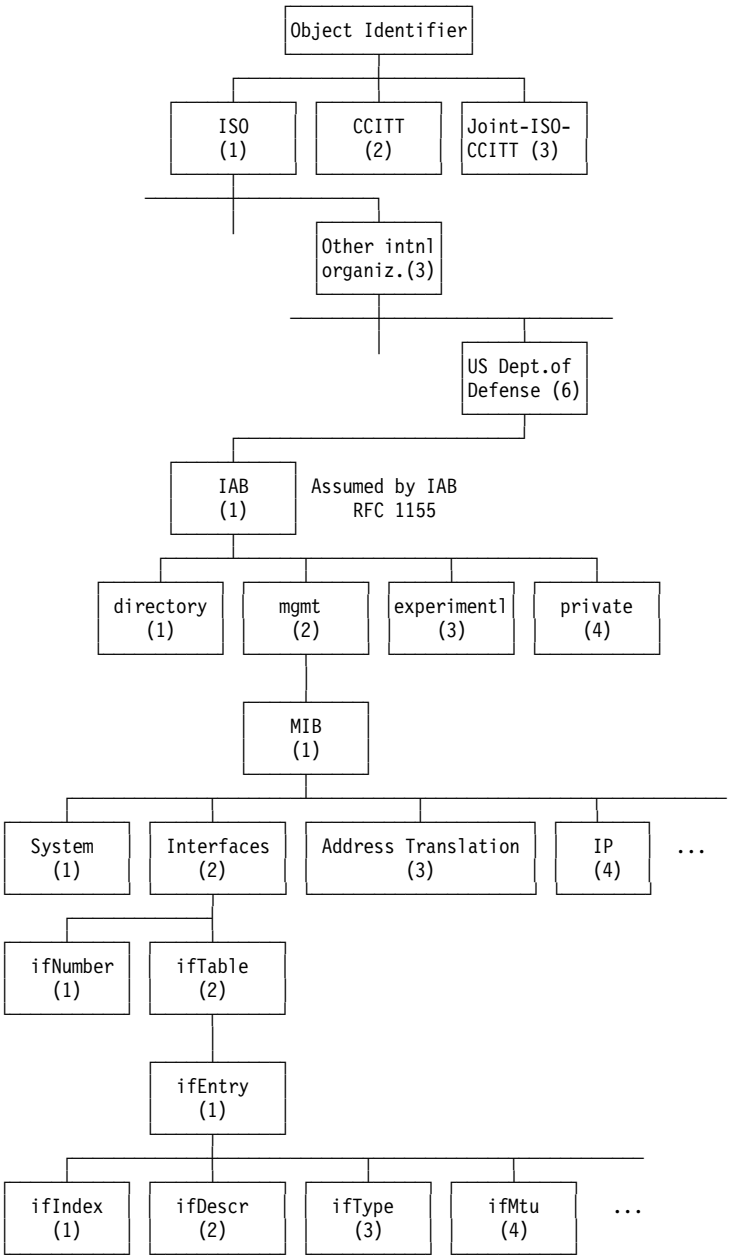


Figure 66. Object Identifier

The MIB variables can be addressed either by their object type number and their instance or by their object type names. A MIB object's name is derived from its location in the tree structure. This name, called an object ID, is created by tracing the path from the top of the tree structure, or the root, to the bottom, the object itself. Each place where the path branches is called a node. If a node has no children, it is called a leaf node. A leaf node is the actual MIB object. Only leaf nodes return MIB values from agents.

Note

Some of the terms used in this chapter are the same as in RODM, but they have different meanings (for example children, object, instance).

For example the MIB variable ifNumber can be identified by:

1.3.6.1.2.1.2.1

or by:

iso.org.dod.internet.mgmt.mib.interface.ifNumber.

Each MIB object name has an instance sub-identifier appended. For objects with only one instance such as ifNumber, this instance is 0. That is, 1.3.6.1.2.1.2.1.0 identifies the one and only instance of ifNumber.

The instance is important for MIB variables which are part of a table, for example, the variable:

iso.org.dod.internet.mgmt.mib.interface.iftable.ifEntry.ifType.

This variable exists for every interface of an agent. Each interface of an agent has a number. The instance specifies the number of the interface described. For example:

iso.org.dod.internet.mgmt.mib.interface.ifTable.ifEntry.ifType.4

or:

1.3.6.1.2.1.2.2.1.3.4

describes the type of the fourth interface of this agent. The number of interfaces is specified in:

iso.org.dod.internet.mgmt.mib.interface.ifNumber

and the number of a specific interface is the value of the MIB entry:

iso.org.dod.internet.mgmt.mib.interface.ifTable.ifEntry.ifIndex

To get a *"*feeling*"* for the MIB tree structure, MIB variables, and their contents you may use the MIB Browser, a tool provided with NetView for AIX. Select an object in NetView for AIX, then click on **Tools** at the menu bar. In the pull-down menu select **MIB Browser**. You can easily go *up* and *down* in the tree, query for variables or browse a description.

For further information on the MIB, refer to RFC 1157 and RFC 1213. RFCs are the documents describing the TCP/IP family of protocols. They are administered by the *Internet Activity Board (IAB).* See *TCP/IP Tutorial and Technical Overview, GG24-3376,* for detailed information on TCP/IP.

4.2.2 Getting MIB Information When the Agent Is Up

There are two different methods to get MIB information from an SNMP agent:

- SNMPGET, which retrieves from one MIB variable
- SMPWALK, which *"*walks*"* through the agent's MIB and can retrieve more than one MIB variable. It retrieves a group.

4.2.2.1 SNMPGET

You can issue the SNMPGET command with the help of the command tree against any SNMP resource you select in NGMF. To do so select **SNMPGET** from the command tree as shown in Figure 67.

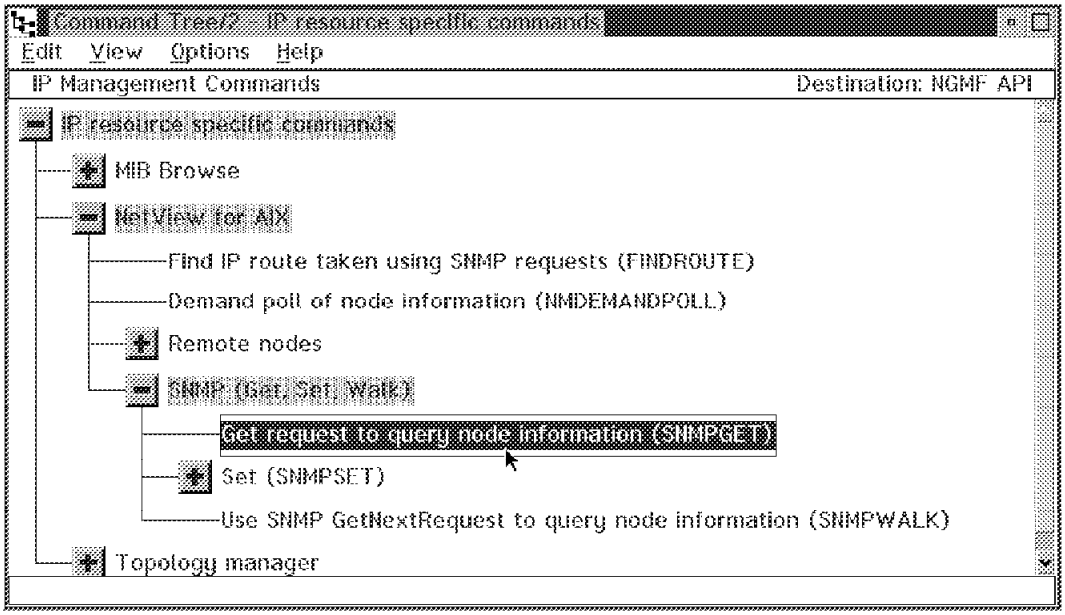


Figure 67. Selecting SNMPGET from the Command Tree

The following window appears:

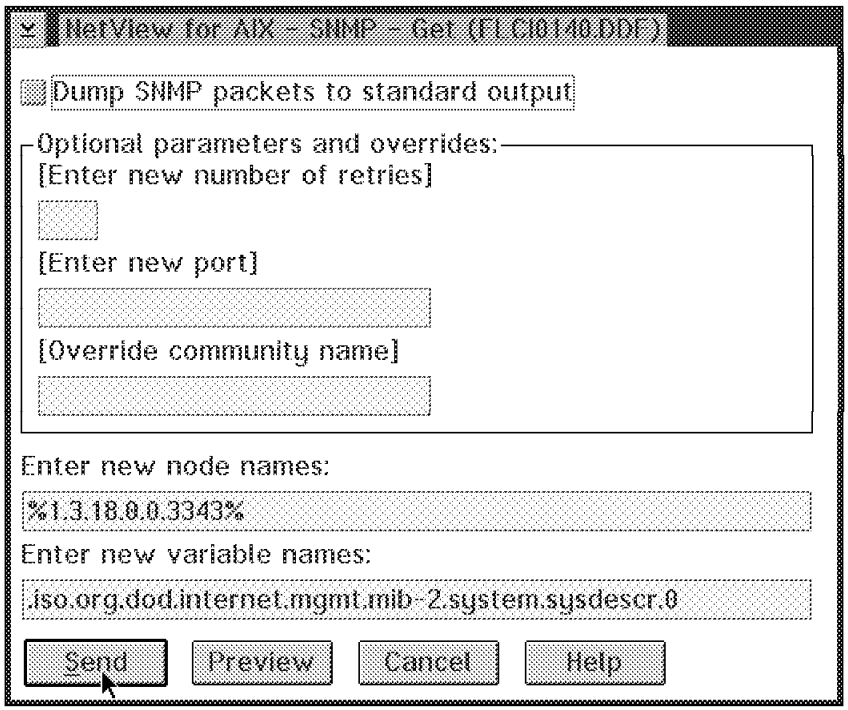


Figure 68. The SNMPGET Input Window

The node name is the RODM object ID of the resources you have selected. Sysdescr.0 is the default, so you can query a description of the system easily

just by clicking on **Send**. The result for our Hub module, which we had selected, is shown in Figure 69 on page 79.

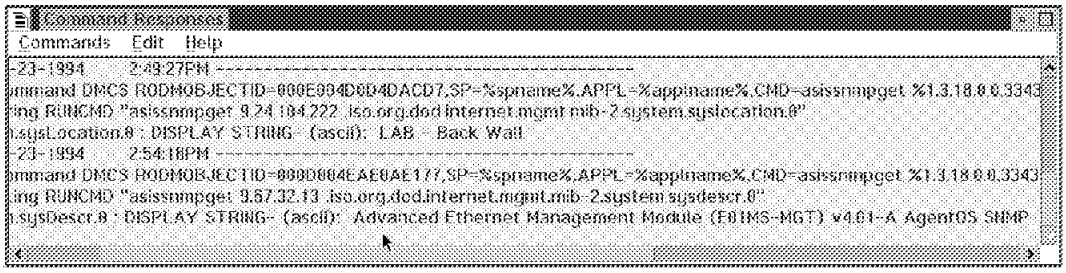


Figure 69. The Response to SNMPGET

The information you enter in the screen shown in Figure 68 on page 78 is used to build an SNMPGET command string. The command syntax of the SNMPGET command might help you to understand the input fields.

```
-------------------------------------------------------------------
snmpget
-------------------------------------------------------------------


Syntax

snmpget
   -d  -t timeout  -r retries  -p port  -c community  node  variable(s)



Description

The snmpget command uses the SNMP GetRequest to query a node for
information.

Each variable has the format of A.B.C.D..., where A, B, C, and D
are subidentifiers in decimal notation.  The default variable
prefix is .iso.org.dod.internet.mgmt.mib.

Options

The default values for the option are determined by the
configuration in /usr/OV/conf/ovsnmp.conf.

-d
    Dumps to standard output all SNMP packets in a hexadecimal
    and decoded ASN.1 format.

-r
    Overrides the default number of retries to retries.  An
    exponential backoff algorithm is used, so if timeout was 10
    (1 second) and retries was 3, the first timeout would occur
    at 1 second, the second (first retry) at 2 seconds, the third
    (second retry) at 4 seconds, and the last (third retry) at 8
    seconds.  It would take 15 seconds before the command gave
    up.
```

```
-p
    Overrides the default port for sending and receiving to port.

-c
    Overrides the SNMP community name (as configured in
    /usr/OV/conf/ovsnmp.conf) to community.
```

You can also query MIB variables from a private MIB tree. As an example we used the 6611 specific MIB and issued a snmpget command against our 6611 router 6611ral.itso.ral.ibm.com. The MIB variable we browsed is:

```
iso.org.dod.internet.private.enterprises.ibm.ibmProd.ibm6611.ibmsnmp.ibmTrapNum
```

This variable contains the number of IBM enterprise specific traps generated by this node. Figure 70 shows the input window.

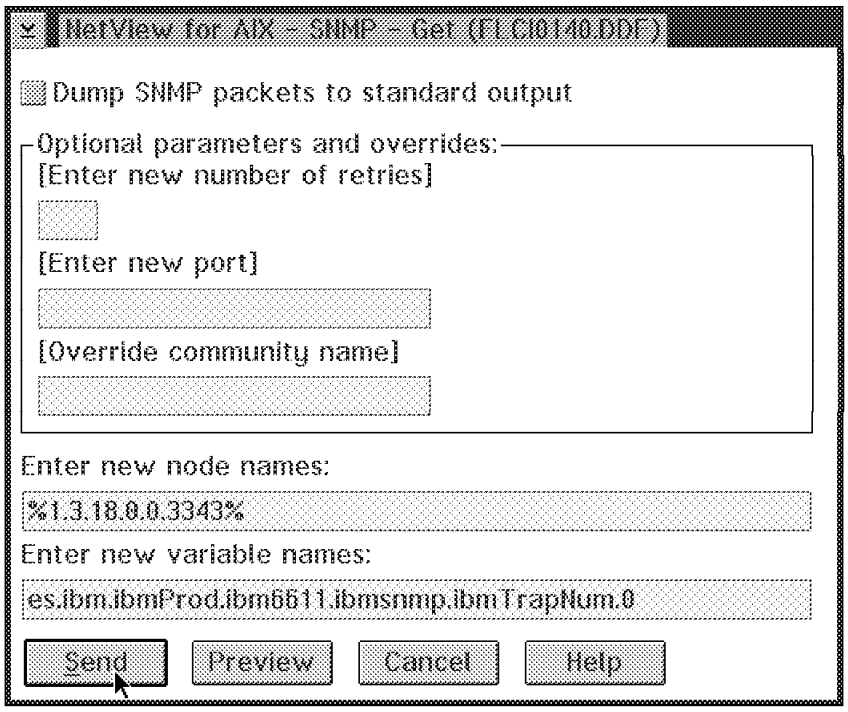


Figure 70. The SNMP Input Window

Figure 71 on page 81 shows the command output that was displayed in the command response window:

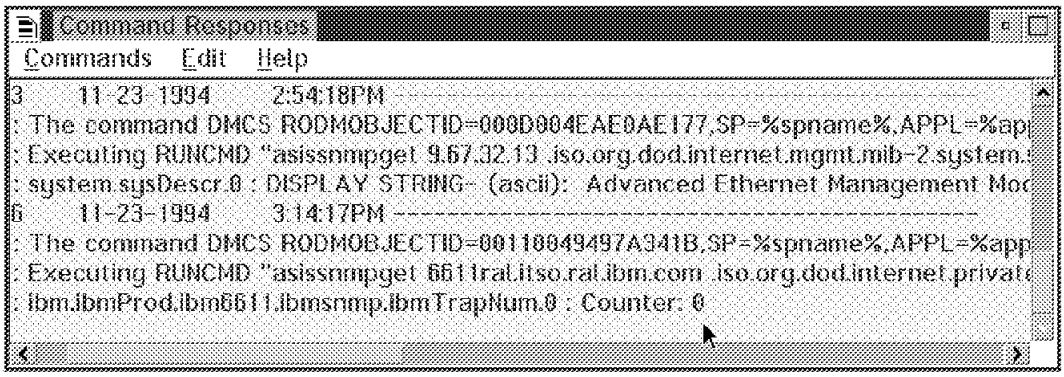


Figure 71. The Response to SNMPGET for 6611

The counter is zero; no enterprise-specific traps have been generated by this node.

4.2.2.2 SNMPWALK

The SNMPWALK command retrieves the MIB variable information of a MIB group. The groups contained in the Command Tree/2 support for the IP agent are eight of the MIB-2 object groups. Those are:

- System (1)
- Interfaces (2)
- Internet Protocol (4)
- Internet Control Message Protocol (5)
- Transmission Control Protocol (6)
- User Datagram Protocol (7)
- Exterior Gateway Protocol (8)
- Simple Network Management Protocol (11)

As NetView/6000 assumes the MIB-2 object group as a default, the command `snmpwalk resourcename 1` retrieves all information of the system group (1) for the resource specified in resourcename.

You can issue the SNMPWALK command with the help of the command tree against any SNMP resource you select in NGMF. To retrieve information from one of eight provided MIB-2 groups click on **MIB2** groups and select the group you want, which, in our example, is the **System group**.

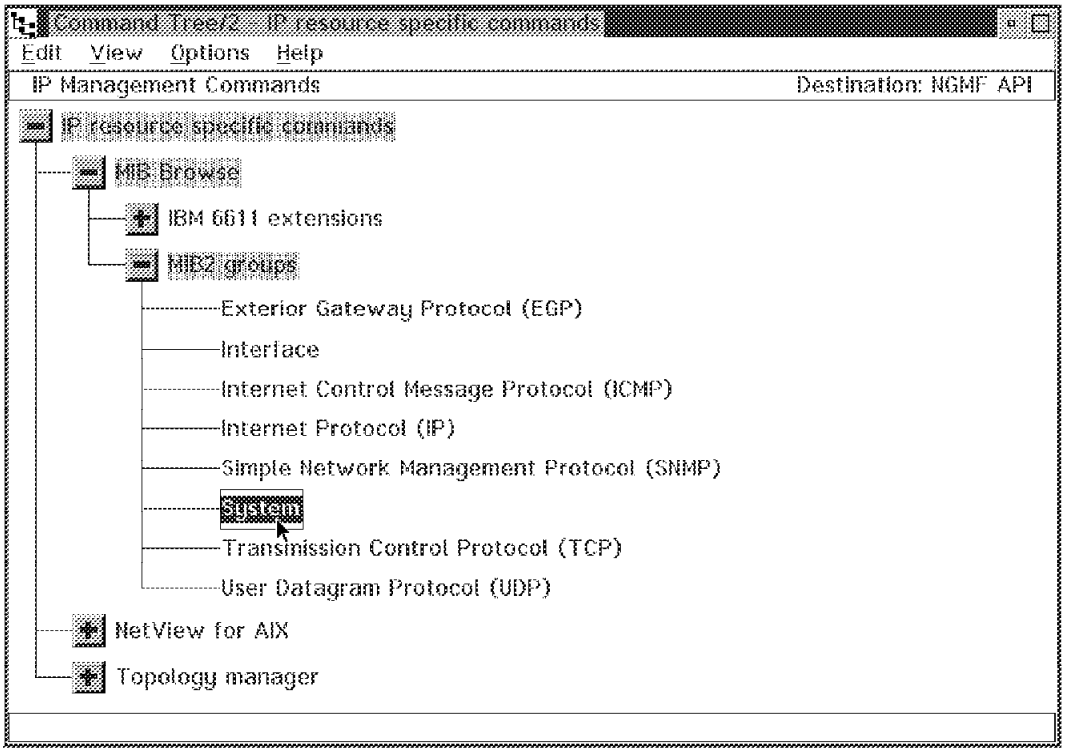


Figure 72. Selecting the System Group from the CT/2

The following window appears:

Figure 73. The SNMPWALK Pop-up Window

If you click on the **Send** button, the command is executed and the command response window appears on your screen showing the MIB group ″system″ for the selected resource:

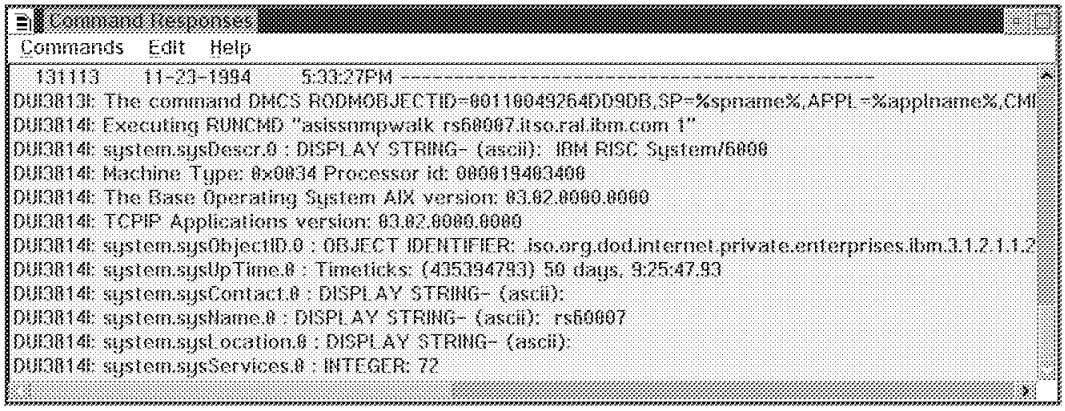


Figure 74. The Response to SNMPWALK

You can also query MIB groups from a private MIB tree. To do so you have to select SNMPWALK from the command tree as shown in Figure 75.

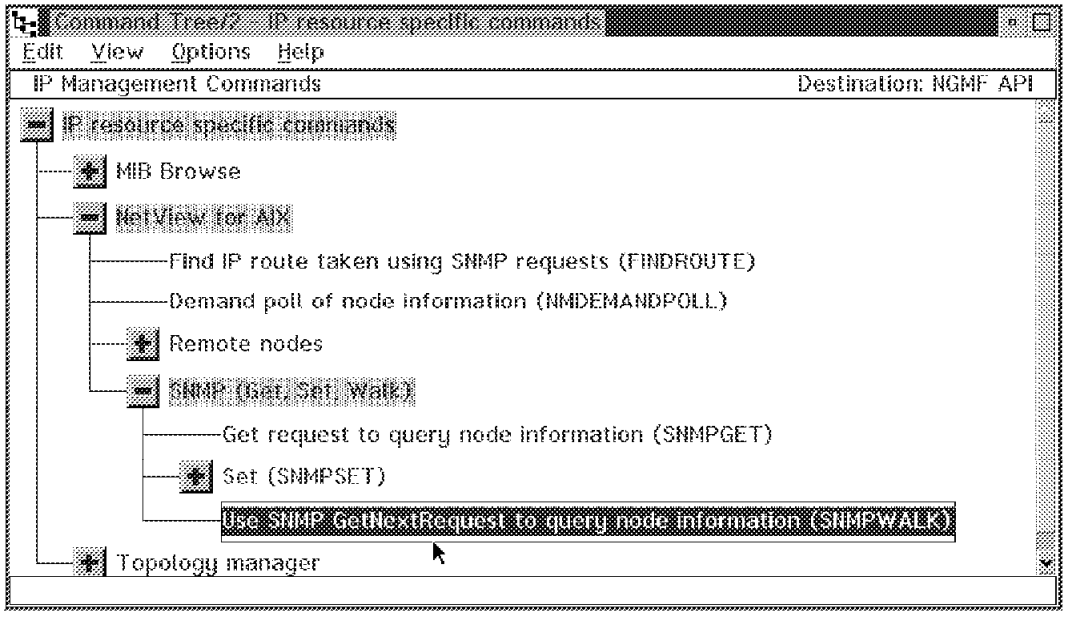


Figure 75. Selecting SNMPWALK from the Command Tree

The SNMPWALK command input window appears. The default group to display is the system group. You can change this to any MIB group. As an example we used the 6611 specific MIB again and issued an SNMPWALK command against our 6611 router 6611ral.itso.ral.ibm.com. The MIB group we browsed is:

`iso.org.dod.internet.private.enterprises.ibm.ibmProd.ibm6611.ibmsnmp.`

This group contains 4 MIB variables:

- ibmTrapNum
- ibmTrapThrottleCount
- ibmTrapThrottleId
- ibmTrapThrottleTime

Figure 76 on page 84 shows the completed input window.

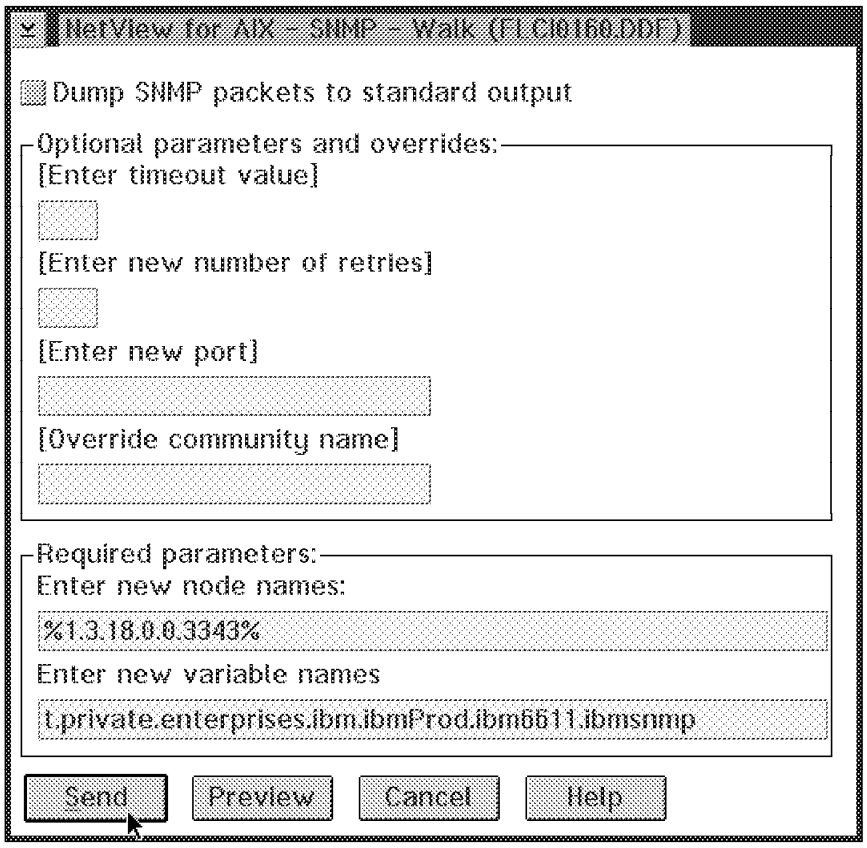


Figure 76. The SNMP Input Window

Figure 77 shows the command output that was displayed in the command response window:

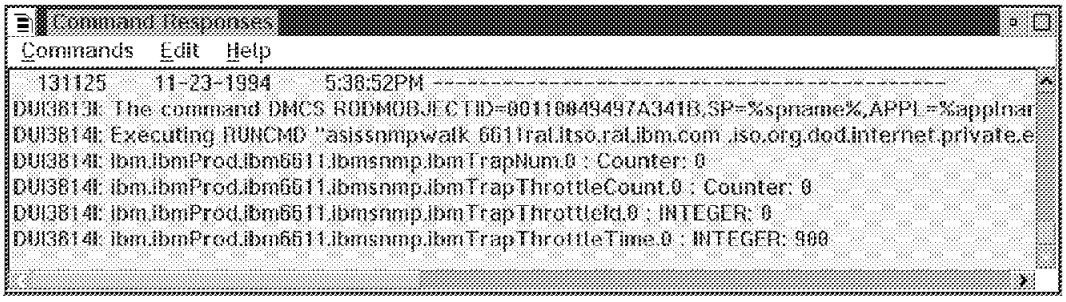


Figure 77. The Response to SNMPWALK for 6611

4.2.3 Getting MIB Information When the Agent Is Down

When a IP host goes down, it is not possible to reach it and to get helpful SNMP information from it. As some information is stored in RODM, you can then display important information about this resource by selecting it and opening the resource information window as shown in Figure 78 on page 85.

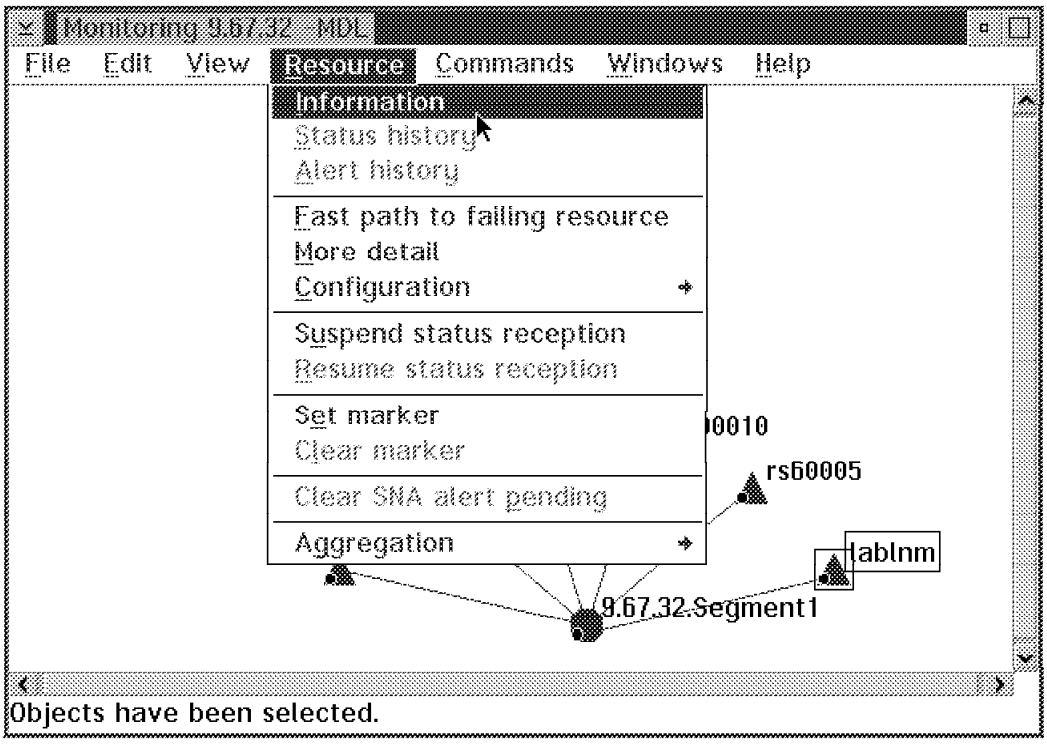


Figure 78. Selecting the Resource Information Window

The result is shown in Figure 79 on page 86.

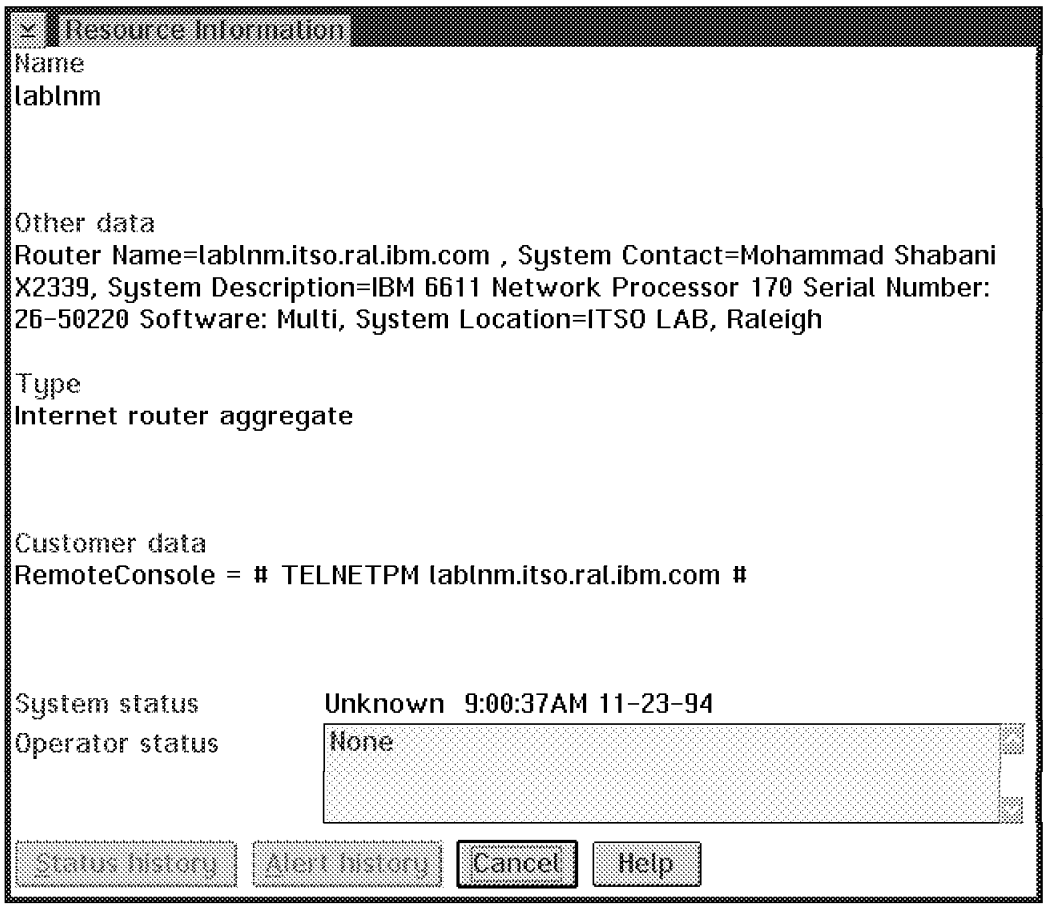


Figure 79. The Resource Information Window

4.2.4 The SNMPSET Command

This standard SNMP command can be issued from NetView for MVS.

4.2.4.1 SNMPSET

You can issue the SNMPSET command with the help of the command tree against any SNMP resource you select in NGMF. To do so, select **SNMPSET** from the command tree as shown in Figure 80 on page 87.

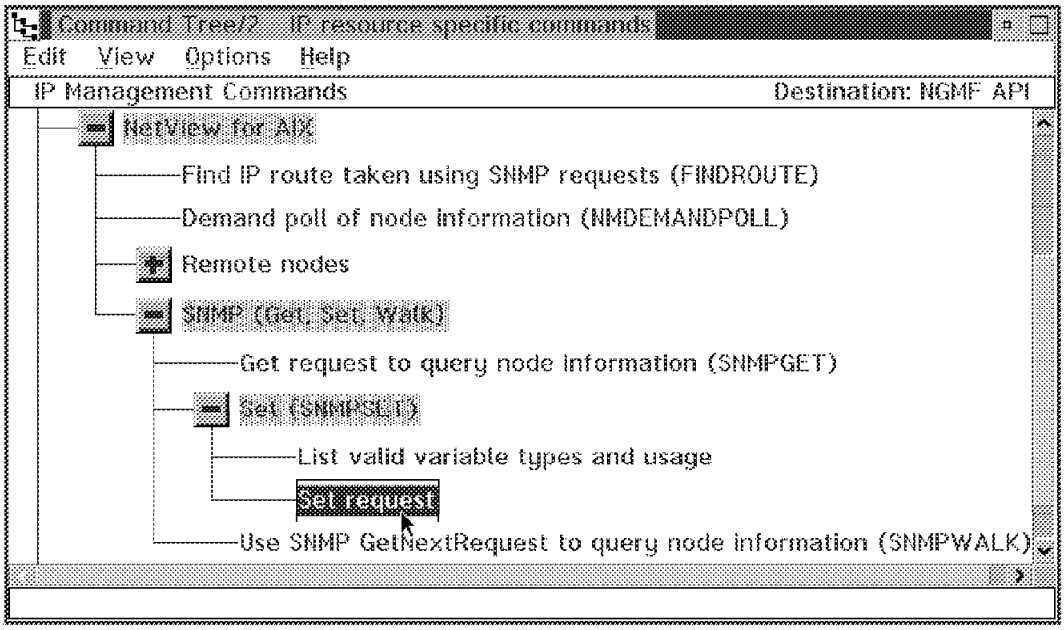


Figure 80. Selecting SNMPSET from the Command Tree

The following window appears:

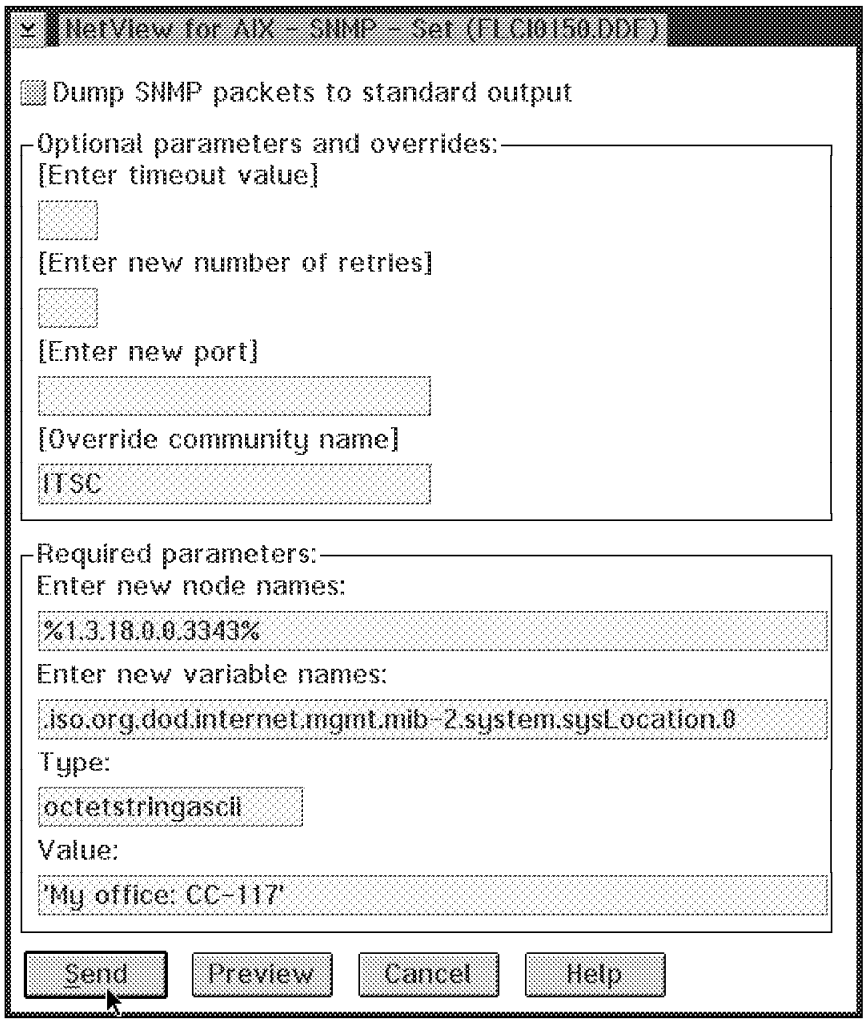


Figure 81. The SNMPSET Input Window

The node name is the RODM object ID of the resources you have selected. Sysdesc.0 is the default, but it is not a MIB variable with write access. You have to change it to the variable you want to set. In this example we selected the **8229** bridge resource, and we want to change the location. The default community that most SNMP devices use is ″public″. This is usually only valid for get requests. The community for write access in our bridge was set to ITSC. If you do not enter the proper community name, the bridge generates an authentication failure trap and sends it to NetView for AIX. The response you get in NGMF is misleading: it is `This variable does not exist` as shown in Figure 82.

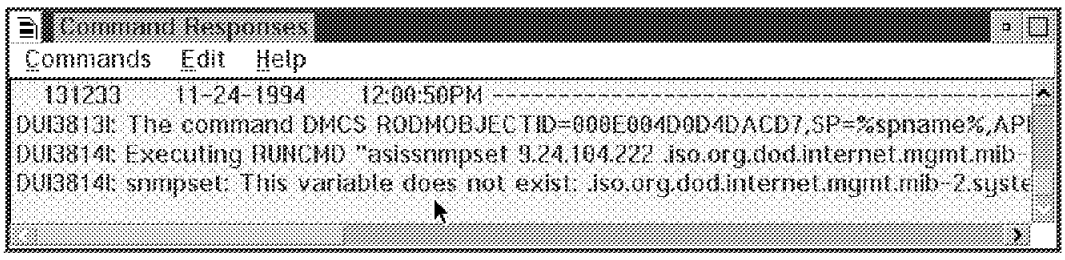


Figure 82. Failure Caused by Incorrect Community

The field type describes the type of the MIB object you want to change. It has to match the MIB specifications. You can query the valid data for the type field using the command tree as shown in Figure 83 on page 89.

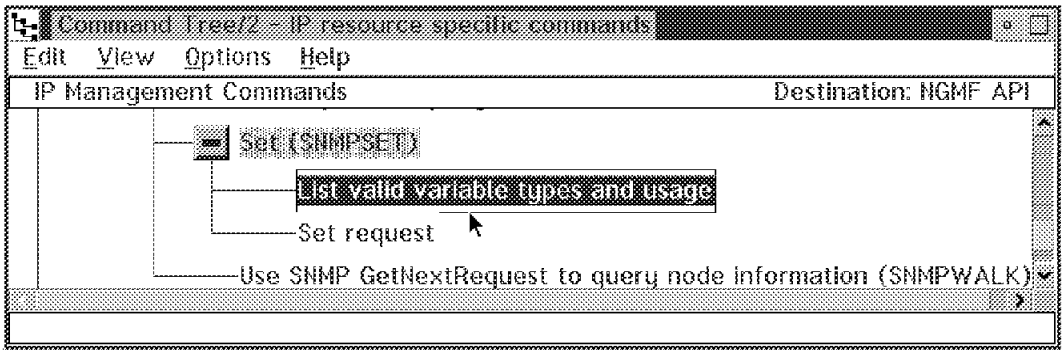


Figure 83. Querying the Valid Variable Types

The command sent is `snmpset -?`, preceded by asis so that the case sensitivity is maintained. It lists the valid types:

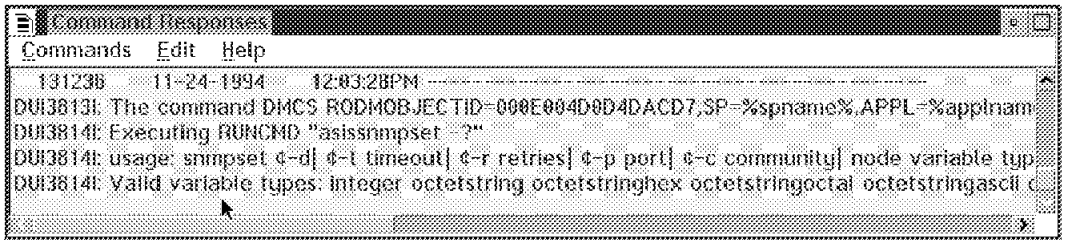


Figure 84. Command Output Listing the Valid Variable Types

These are the valid types listed:

- Integer
- Octetstring, octetstringhex, octetstringoctal, octetstringascii
- Objectidentifyer
- Null
- Ipaddress
- Counter
- Gauge
- Timeticks
- Opaque, opaquehex, opaqueoctal, opaqueascii

To find the correct type for a variable you want to set, you can use the SNMPGET command as shown before. Below you find the result of a query of the system group and behind each variable the type.

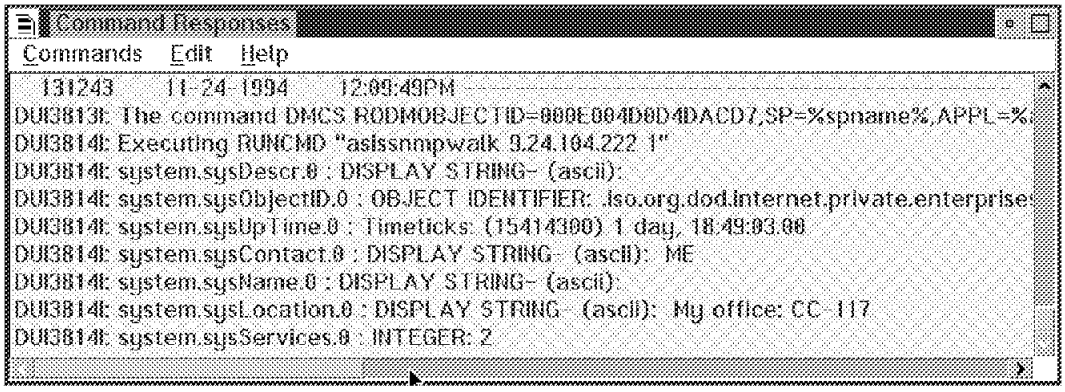


Figure 85. The MIB Group System Including Types

The type for the sysLocation is DISPLAY STRING (ascii). In Figure 81 on page 88 we have to fill in octetstringascii for the type.

When you have entered all the information needed, click on the **Send** button. The result for the bridge that we selected is shown in Figure 86.

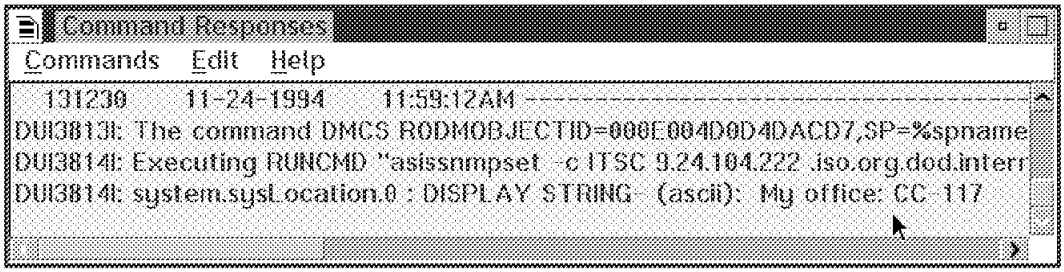


Figure 86. The Response to SNMPSET

The information you entered in the screen shown in Figure 68 on page 78 is used to build a SNMPSET command string. The command syntax of the SNMPSET command might help you to understand the input fields:

```
-------------------------------------------------------------
snmpset
-------------------------------------------------------------


Syntax

snmpset  -d -t timeout -r retries -p port -c community
    node variable type value



Description

The snmpset command issues an SNMP SetRequest to alter MIB
objects on the remote node and returns the result of the Set
Request.  The snmpset command accepts 1-to-20 sets of the
arguments "variable type value".

Each variable has the format A.B.C.D..., where A, B, C, and D are
subidentifiers in decimal notation and group.variable notation.
```

The default variable prefix is .iso.org.dod.internet.mgmt.mib.

Each type must be one of the following types: Integer, OctetStringHex, OctetStringOctal, OctetStringASCII (special cases of OctetString), ObjectIdentifier, Null, IpAddress, Counter, Gauge, TimeTicks, OpaqueHex, OpaqueOctal, or OpaqueASCII (special cases of Opaque). See RFC 1155 for a complete description of each type.

The value must be valid for the type specified. When using a type where a hexadecimal or octal value is needed (OctetStringHex, OctetStringOctal, OpaqueHex, OpaqueOctal), the value must have each byte fully defined. For example, fff (or 17377) is not allowed, whereas 0fff (or 017377) is allowed. For type Null, a value must be specified on the command line, but it is ignored when the request is created. A value must not occupy more than 256 bytes.

Options

The default values for the options is determined by the configuration in /usr/OV/conf/ovsnmp.conf.

-?
    Lists the valid variable types and the usage message.

-d
    Dumps to standard output all SNMP packets in a hexadecimal and decoded ASN.1 format.

-r
    Overrides the default number of retries to retries. An exponential backoff algorithm is used, so if timeout was 10 (1 second) and retries was 3, the first timeout would occur at 1 second, the second (first retry) at 2 seconds, the third (second retry) at 4 seconds, and the last (third retry) at 8 seconds. It would take 15 seconds before the command gave up.

-p
    Overrides the default port for sending or receiving to port.

-c
    Overrides the SNMP community name (as configured in /usr/OV/conf/ovsnmp.conf) to community.

    If all arguments are formatted correctly, a message appears indicating that the SNMP trap was sent to the remote node.

-t
    Timeout value.

The snmpset command supports single-byte character code sets.

4.2.4.2 SNMPSET in a Private MIB Tree

You can also set MIB variables in a private MIB tree. As an example, we used the 8229-specific MIB.

There are only a few variables that allow write access in the MIB-2. Private MIBs can provide remote operation facility via SNMP. With the SNMP set command, you can switch or disable ports, change filters or even reboot communication devices, whatever the vendor allows. We used the 8229 private MIB and changed the value for the srtbBridgeStatus from forwarding to restart. The complete name of the variable is:

```
iso.org.dod.internet.private.enterprises.ibm.ibmProd.ibm8229.srtbBridge.
                    srtbBridgeTable.srtbBridgeEntry.srtbBridgeStatus
```

This variable contains the current status of the bridge. Figure 70 on page 80 shows the description we displayed with the NetView for AIX MIB browser:

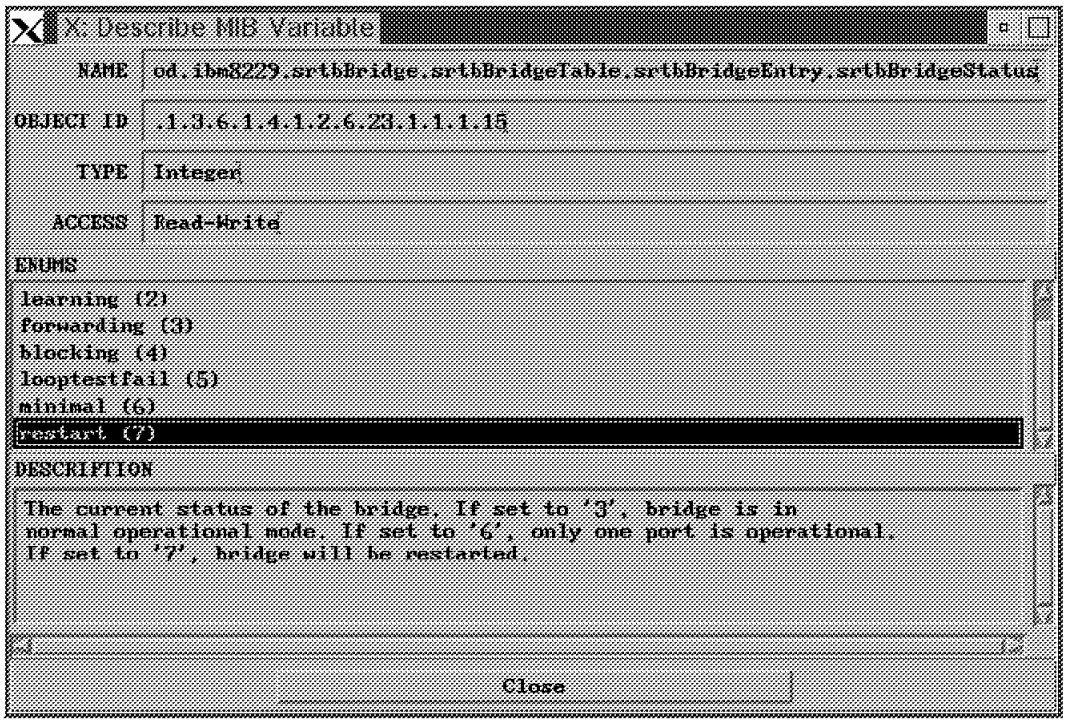


Figure 87. Describe MIB Variable Window

We opened the SNMPSET input window again and entered the MIB variable. Because the input field for the MIB variable is too short for the srtbBridgeStatus we used the numeric notation. The dot before the first number means that the default MIB tree path should not be used. NetView for AIX defaults to the MIB-2 object group. Figure 88 on page 93 shows the complete input window:

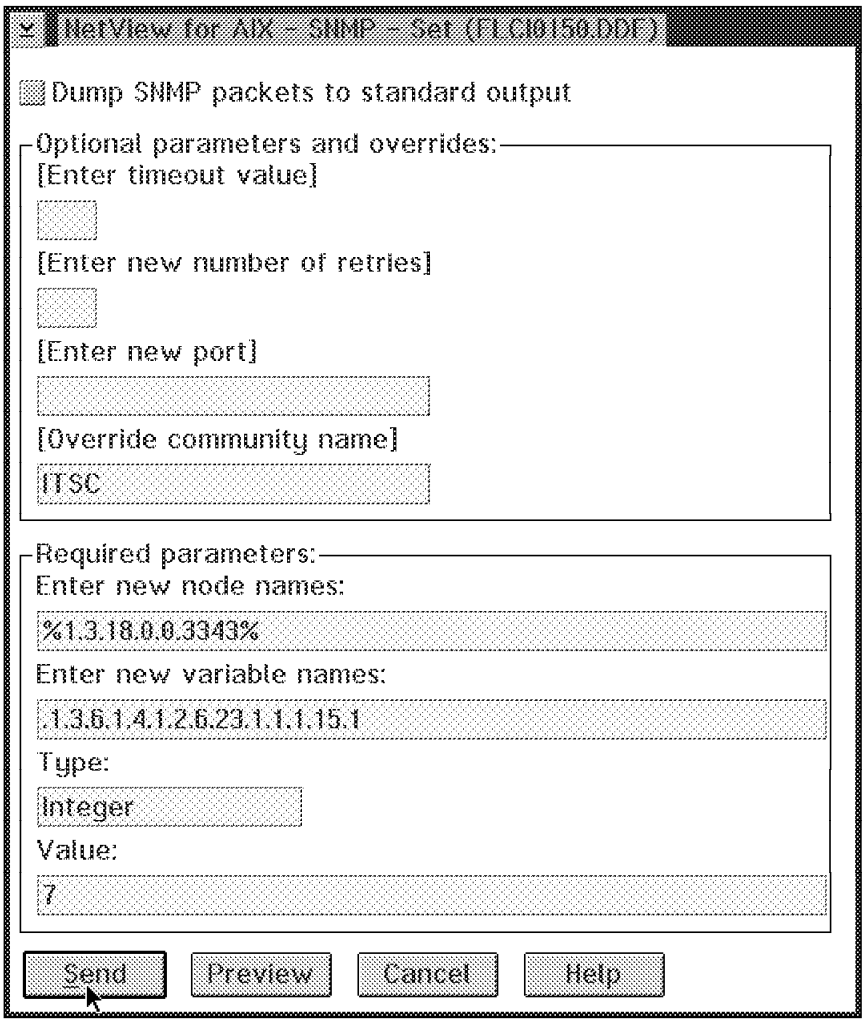


Figure 88. Sending SNMPSET

When we clicked on the **Send** button the bridge was restarted. This is the command output that was shown in the command response window:

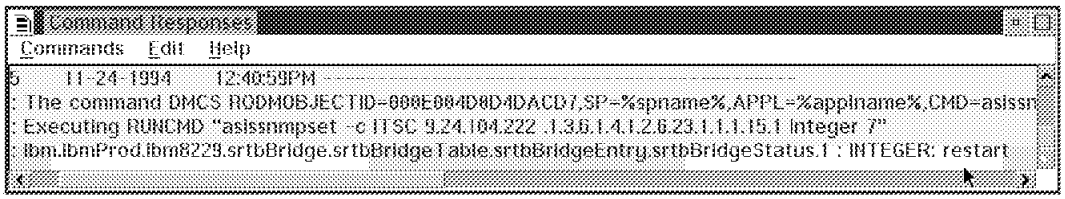


Figure 89. The Response to SNMPSET for 8229 Bridge

The status of the bridge is restart.

4.2.5 Using MIB Applications

MIB applications are very commonly used in a NetView for AIX environment. They make it easy to build collections of SNMPGET commands. NetView for AIX provides a tool to build those applications, the MIB application builder. The result may be presented as a list, a table or a graph. The MIB variables are selected with the help of the MIB browser, which is another NetView for AIX tool that helps you to query MIB information without knowing the MIB tree by heart.

For our example we built one application to query system information from any SNMP resource, one application to query 8229 private MIB information presented as a table and a third application querying bridge specific system information. The definitions for the third application as entered in NetView for AIX are shown in Figure 90.

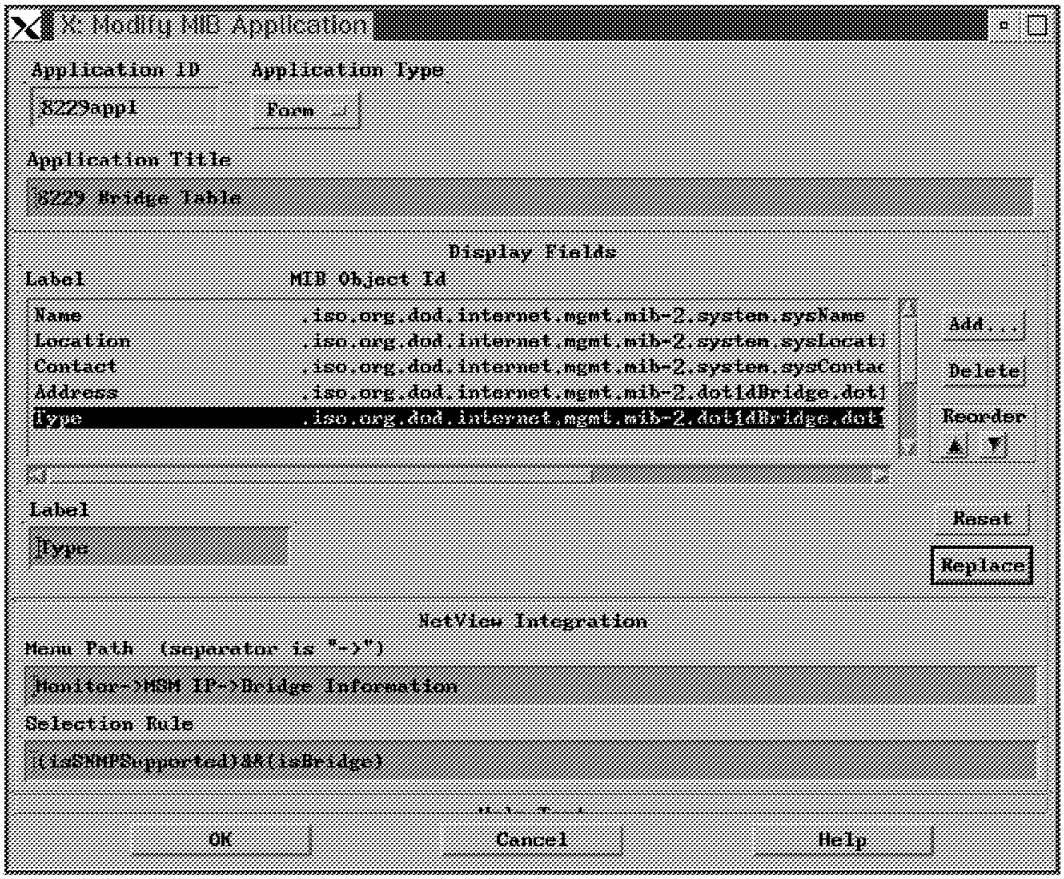


Figure 90. The MIB Application Builder

For usage with IBM NetView MultiSystem Manager we used only lowercase letters in the application ID to avoid the case-sensitive asis option in the RUNCMD command. We combined some parts of the MIB-2 system group with some variables of the MIB-2 dot1dBridge group. So you get system information and bridge specific information in one shot. The selection rule defines that this application is only valid for SNMP-supported bridges. This application will present the information as a list.

Our new applications are located under Monitor and MSM IP as shown in Figure 91 on page 95.

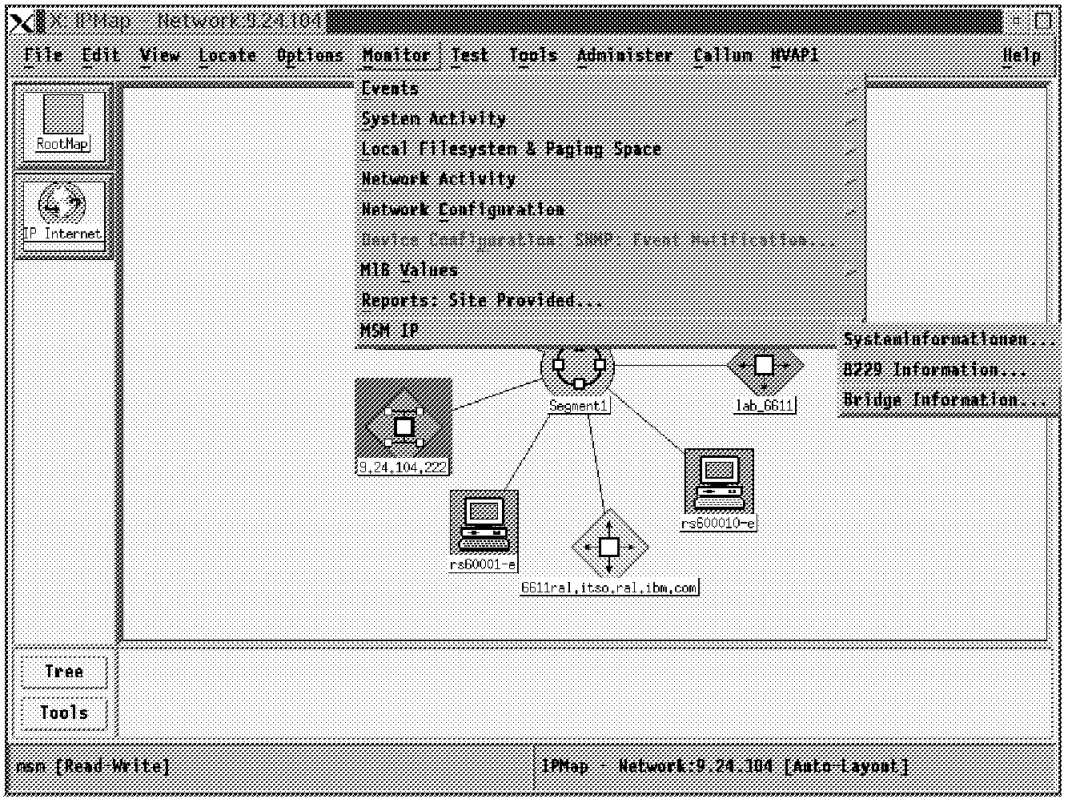


Figure 91. The MIB Applications

Selecting the **8229 bridge** and clicking on the **Bridge Information** application leads to the following result:

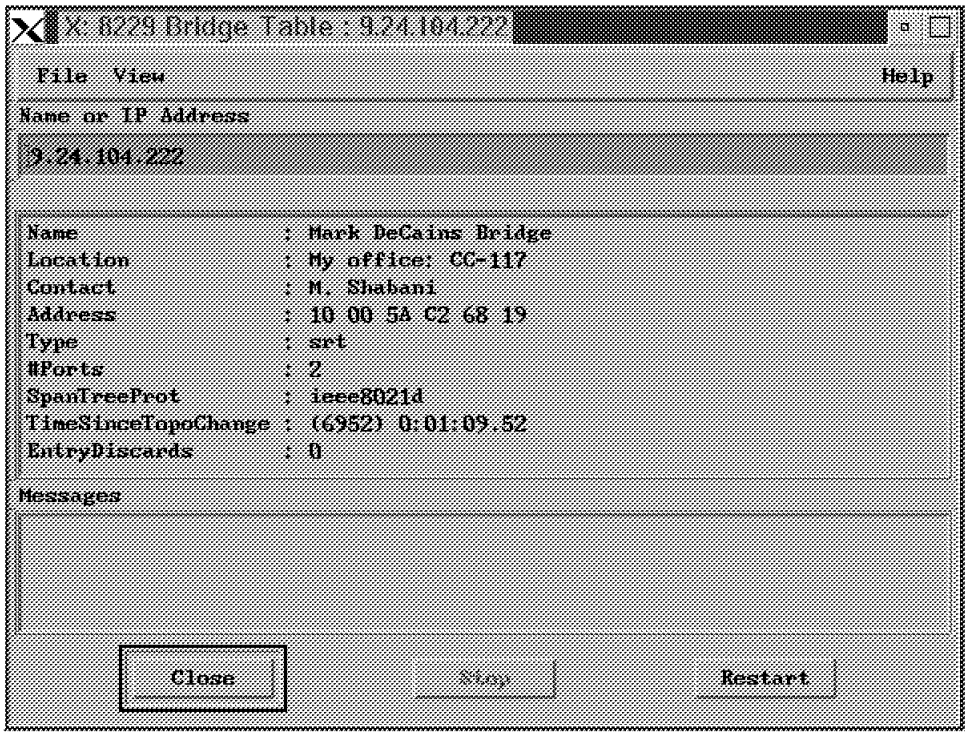


Figure 92. The Bridge Table

4.2.5.1 Using MIB Applications from the Non-SNA Command Line

To use the same MIB application from NGMF with a RUNCMD command, we used a shell script. The command text is provided in Appendix F, “Mibappl Shell Script” on page 265. This shell script examines the files that contain the MIB applications. They are located in the /usr/OV/registration/C/ovmib directory. The script extracts the function and runs it as a command using a specific resource. The README file explains the usage:

MIBAPPL.README (extract)

```
MIBAPPL is a AIX shell script that allows you to "execute"
MIB applications from host NetView via RUNCMD.  It "reads"
the specified MIB application, searches for the MIB variables
and then queries and displays them via SNMPWALKs.


To run from host NetView:

   RUNCMD APPL=xxxxxxxx SP=xxxxxxxx MIBAPPL appl host {community}


Where:

      appl is the MIB application
      host is the TCP/IP host
      community is the community name (optional)
```

To use our MIB applications, we opened the non-SNA command line and entered the following command:

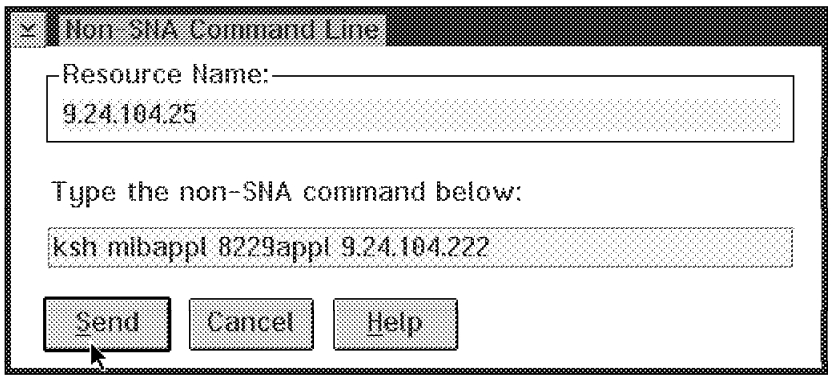


Figure 93. Non-SNA Command Line Calling a MIBAPPL

Because the shell script cannot run in a bourne shell environment, which is the default of the *SPAPPLD* daemon, you have to specify ksh before the command. If you have uppercase letters in your MIB application, name you also have to enter asis before the command. The name of our 8229 bridge is 9.24.104.222. The resource name is our Service Point machine. Clicking on **Send**, we got the following result in the command response window:

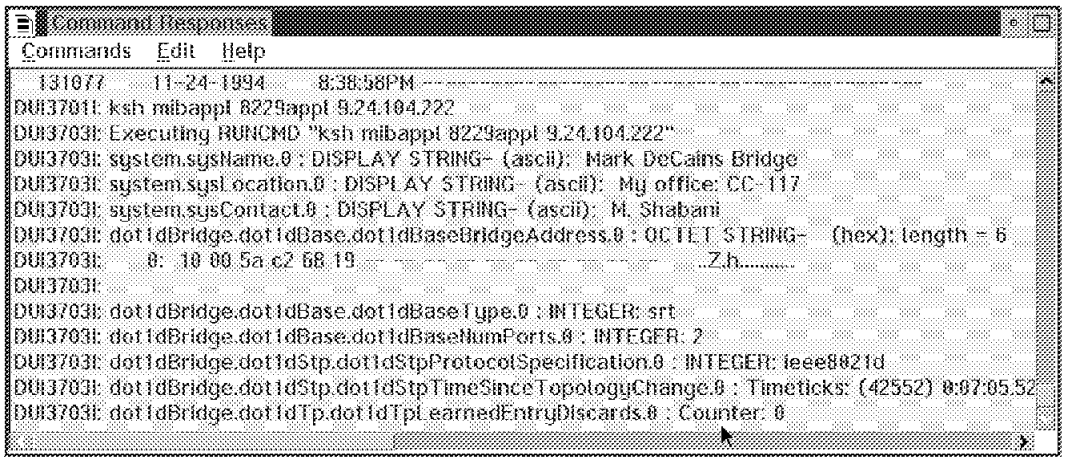


Figure 94. Command Response Window

You find the same information as in Figure 92 on page 95.

4.2.5.2 Integrating MIB Applications in the Command Tree

To make the use of the MIB applications more convenient, you might want to integrate the commands into the resource specific Command Tree/2. To do so we changed the command definition file FLCI0001 like this:

```
CommandNode "IP.MIBAPPLICATIONS"
 NLS_DisplayText "MIB Applications"
 HelpId 30712
SubSetID 0
SubSetID 1
SubSetID 2
SubSetID 3
SubSetID 4
SubSetID 5

CommandNode "IP.MIBAPPLICATIONS.FIRST"
 NLS_DisplayText "Display information about the System (msmappl)"
 HelpId 32230
SubSetID 0
 CommandString "DMCS RODMOBJECTID=&RESOURCE.,SP=%spname%,APPL=%applname%,CMD=ksh
 mibappl msmappl %1.3.18.0.0.3343% "
 WhenToPreview Always
SubSetID 1
SubSetID 2
SubSetID 3
SubSetID 4
SubSetID 5

CommandNode "IP.MIBAPPLICATIONS.SECOND"
 NLS_DisplayText "Display information about a Bridge (8229appl)"
 HelpId 32230
SubSetID 0
 CommandString "DMCS RODMOBJECTID=&RESOURCE.,SP=%spname%,APPL=%applname%,CMD=ksh
 mibappl 8229appl %1.3.18.0.0.3343% "
 WhenToPreview Always
SubSetID 1
SubSetID 2
SubSetID 3
SubSetID 4
SubSetID 5

CommandNode "IP.MIBAPPLICATIONS.THIRD"
 NLS_DisplayText "Display information about a 8229 Bridge (8229port)"
 HelpId 32230
SubSetID 0
 CommandString "DMCS RODMOBJECTID=&RESOURCE.,SP=%spname%,APPL=%applname%,CMD=ksh
 mibappl 8229port %1.3.18.0.0.3343% "
 WhenToPreview Always
SubSetID 1
SubSetID 2
SubSetID 3
SubSetID 4
SubSetID 5

* /
```

The resource name of the selected resource is filled in using the RODM object ID. The new part of the Command Tree/2 is shown in Figure 95 on page 99.

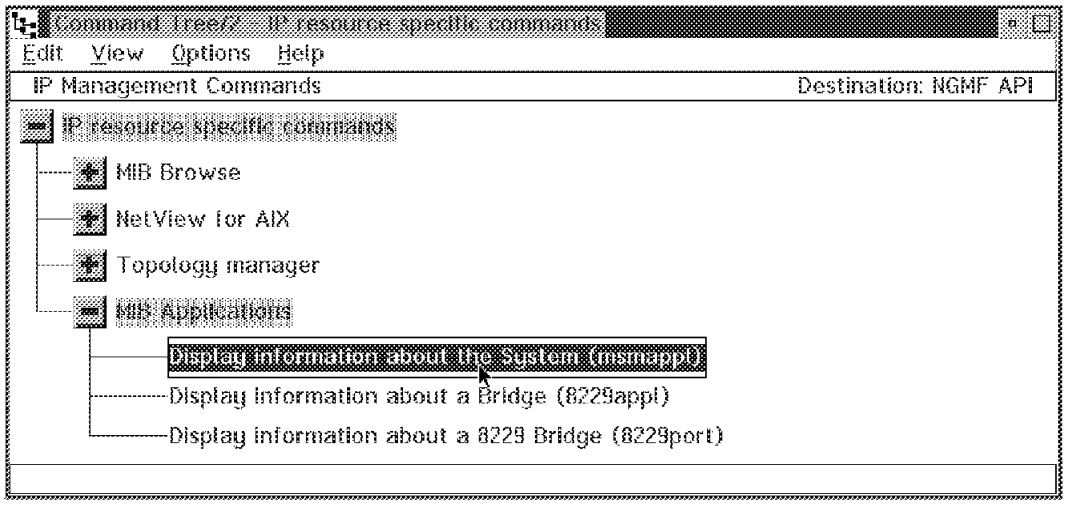


Figure 95. Selecting MSMAPPL in CT/2

We selected the host rs60001 prior to opening the command tree. Clicking on **msmappl**, we get the system information for the rs60001 that is retrieved by this MIB application:

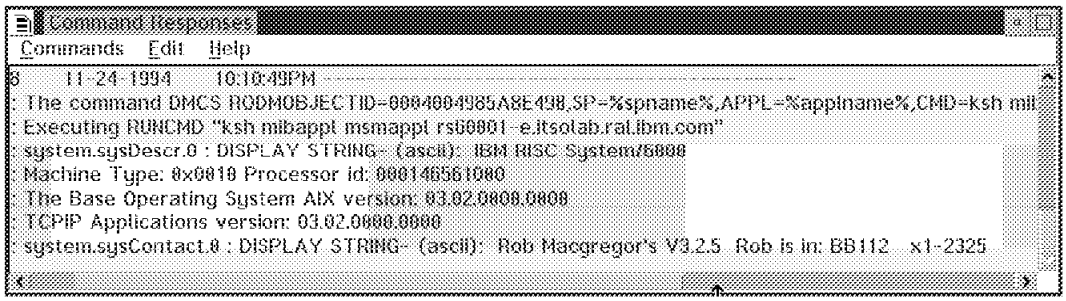


Figure 96. The Response to MSMAPPL

4.3 Remote Console Function

MSM for IP provides a remote console function. Select **Commands**, **Network** and **Remote Console** to invoke this function. It can be used to issue a TELNET command to the machine selected. To use this function, you have to install TCP/IP for OS/2 on your NGMF workstation.

4.3.1 Using Remote Console Function for IBM 6611

When one interface of a router goes down, it is still possible to reach the router with TCP/IP. When you realize a problem at the 6611, for example, because one interface went down, you can either retrieve MIB information as described before or you can use the Remote Console function.

Select the 6611 resource and invoke the Remote Console function as shown in Figure 97 on page 100.

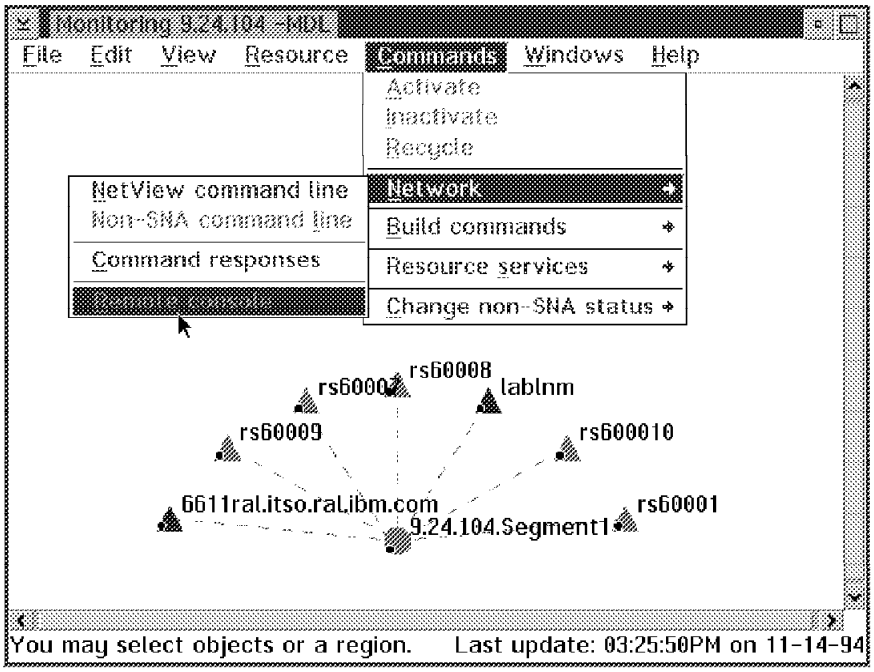


Figure 97. Invoke Remote Console Function for 6611RAL

You get the login screen from 6611 System Manager:

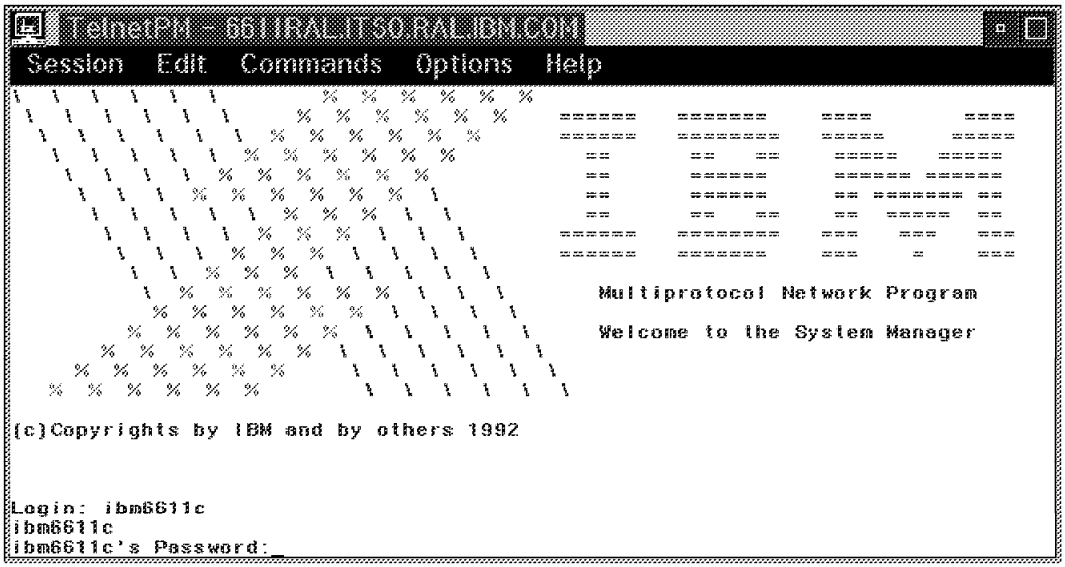


Figure 98. IBM 6611 System Manager Login Screen

When you enter user ID and password you get the 6611 System Manager main menu as shown in Figure 99 on page 101. Now you can use the console window for problem determination.

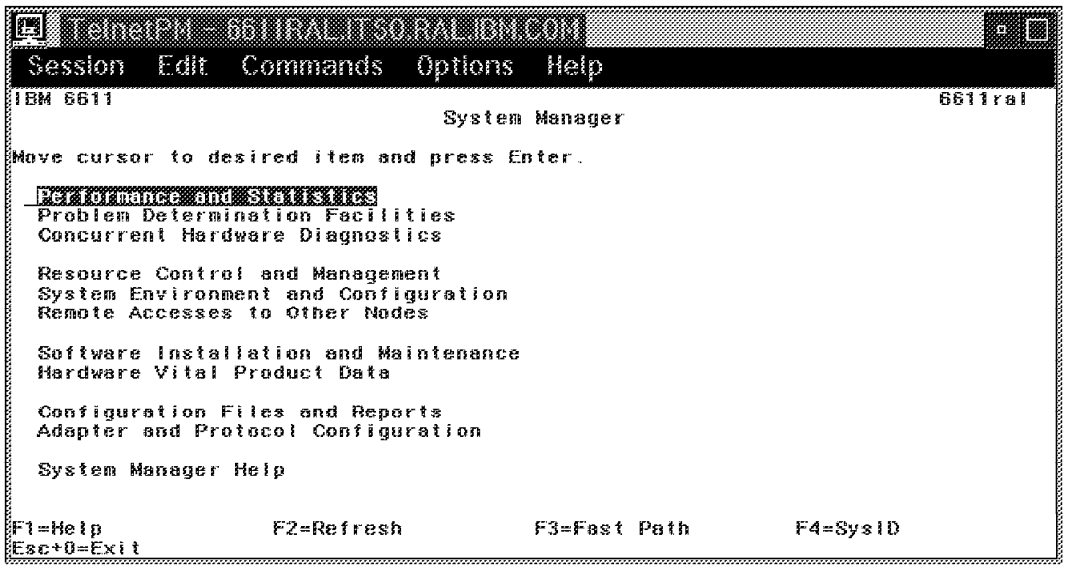


Figure 99. The 6611 System Manager Main Menu

4.3.2 Using Remote Console Function for IBM 8250

When problems occur at a hub, it is often still possible to reach the hub with TCP/IP. When you realize a problem at the 8250, you can either retrieve MIB information as described before or you can use the Remote Console function.

Select the 8250 resource and invoke the remote console function as shown in Figure 100.

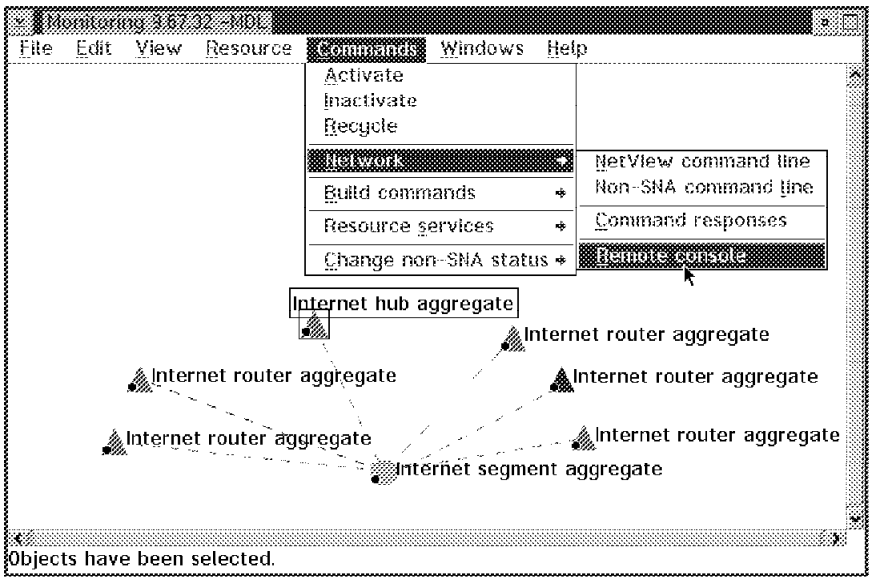


Figure 100. Invoke Remote Console Function for Hub

You get the log in screen from 8250 Management Module:

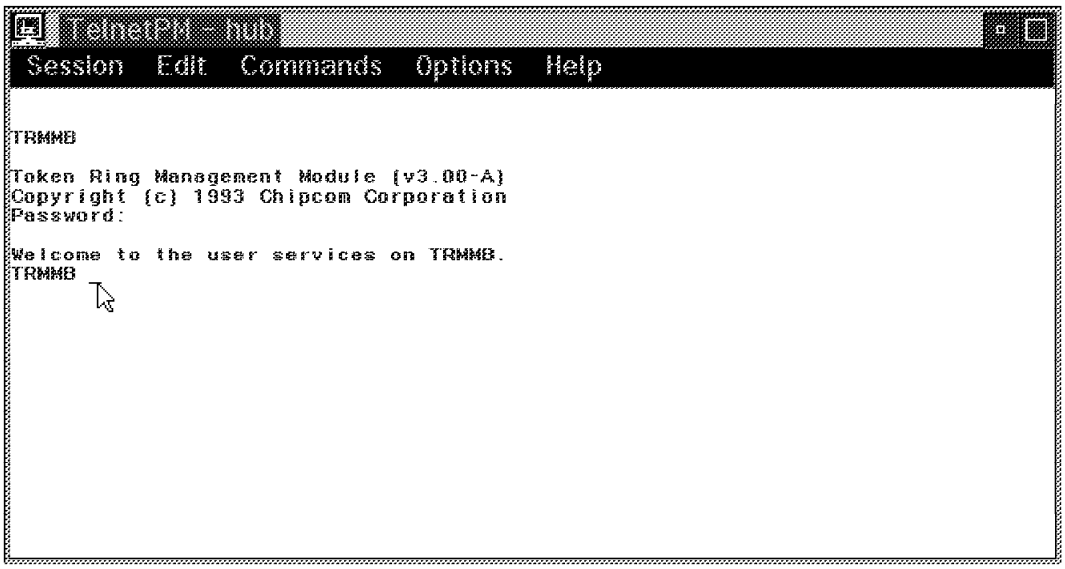


Figure 101. IBM 8250 Management Module Login Screen

You can issue any 8250 Management command now - for example, the `show module all` command as shown in Figure 102.

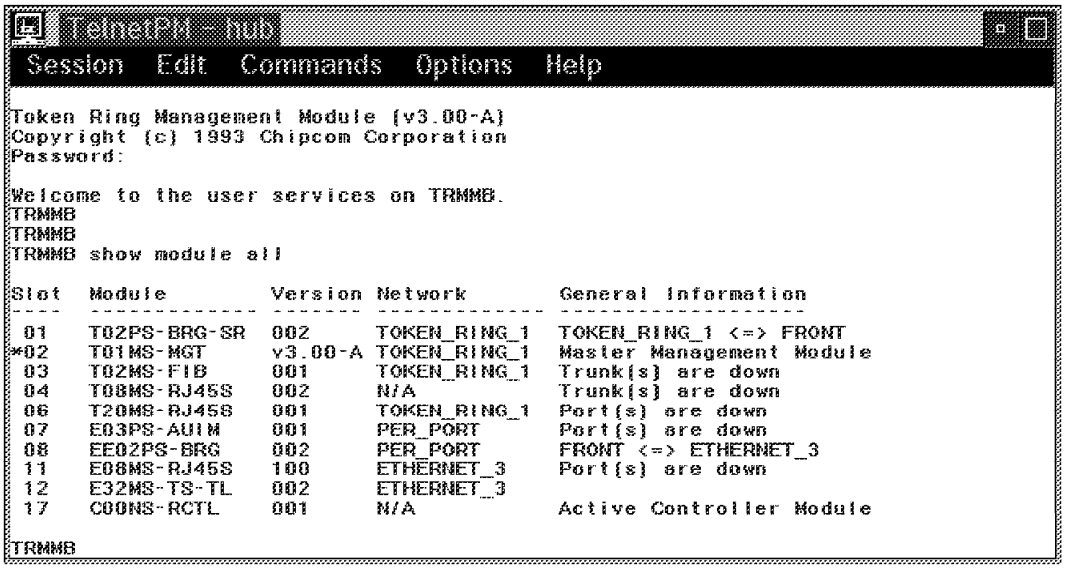


Figure 102. 8250 Modules

Now you can use the console window for problem determination.

4.4 Using PMX as NetView/6000 Remote Console

PMX, running under OS/2, allows you to use a native RS/6000 console.

4.4.1 Using NetView/6000 Remote Console Function

When problems occur in an IP network, it might be helpful to use NetView/6000 native console for problem determination or for configuration and maintenance purposes. There are some functions that cannot be triggered by line commands, so display the end user interface (EUI) on your NGMF workstation by running the *X Windows server* (PMX) as well as the TCP/IP for OS/2 base. The setup will be described later, in 4.4.2, "Setting Up the NetView/6000 Remote Console" on page 105.

Select the NetView/6000 resource and invoke the remote console function as shown in Figure 103.

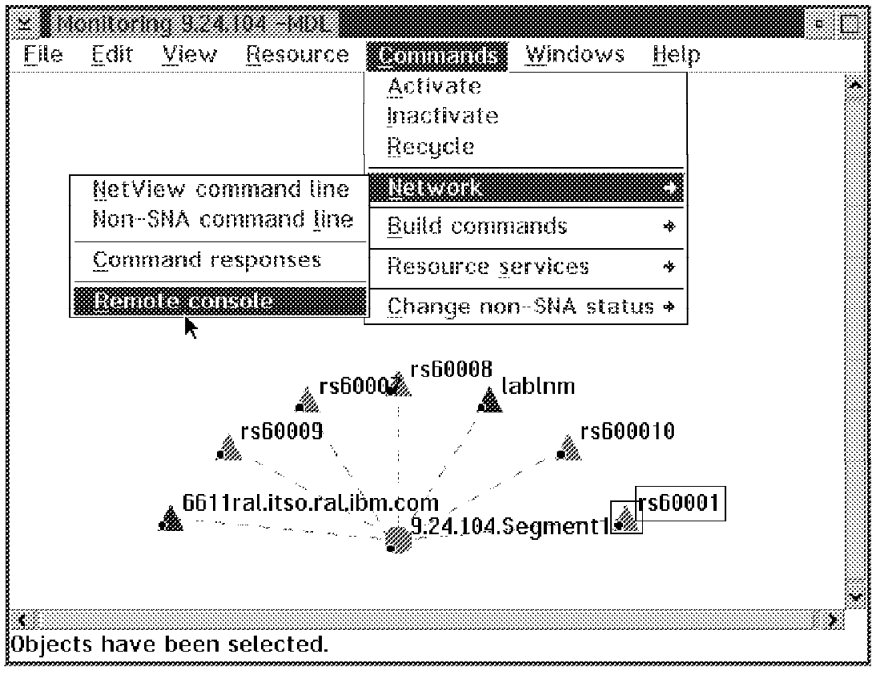


Figure 103. Invoke Remote Console Function for NetView/6000

You get the login screen from AIX. In our installation the network management application starts automatically as shown in Figure 104 on page 104.

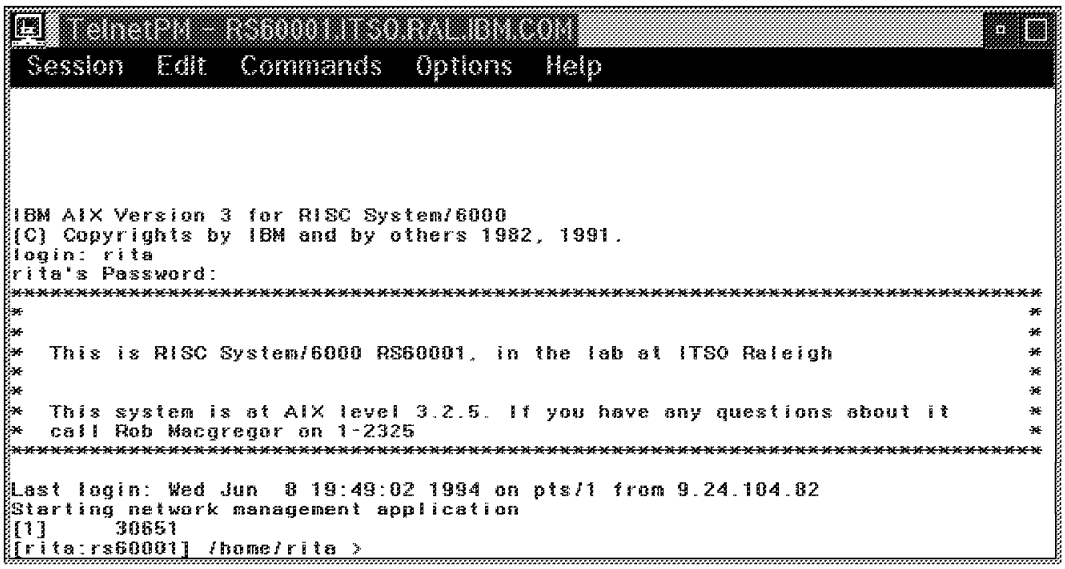


Figure 104. AIX Log In and Automatic Startup of NetView/6000

This may take some minutes, depending on your RISC/6000 and PS/2 configuration. You get the NetView/6000 EUI displayed as shown in Figure 105 on page 105.

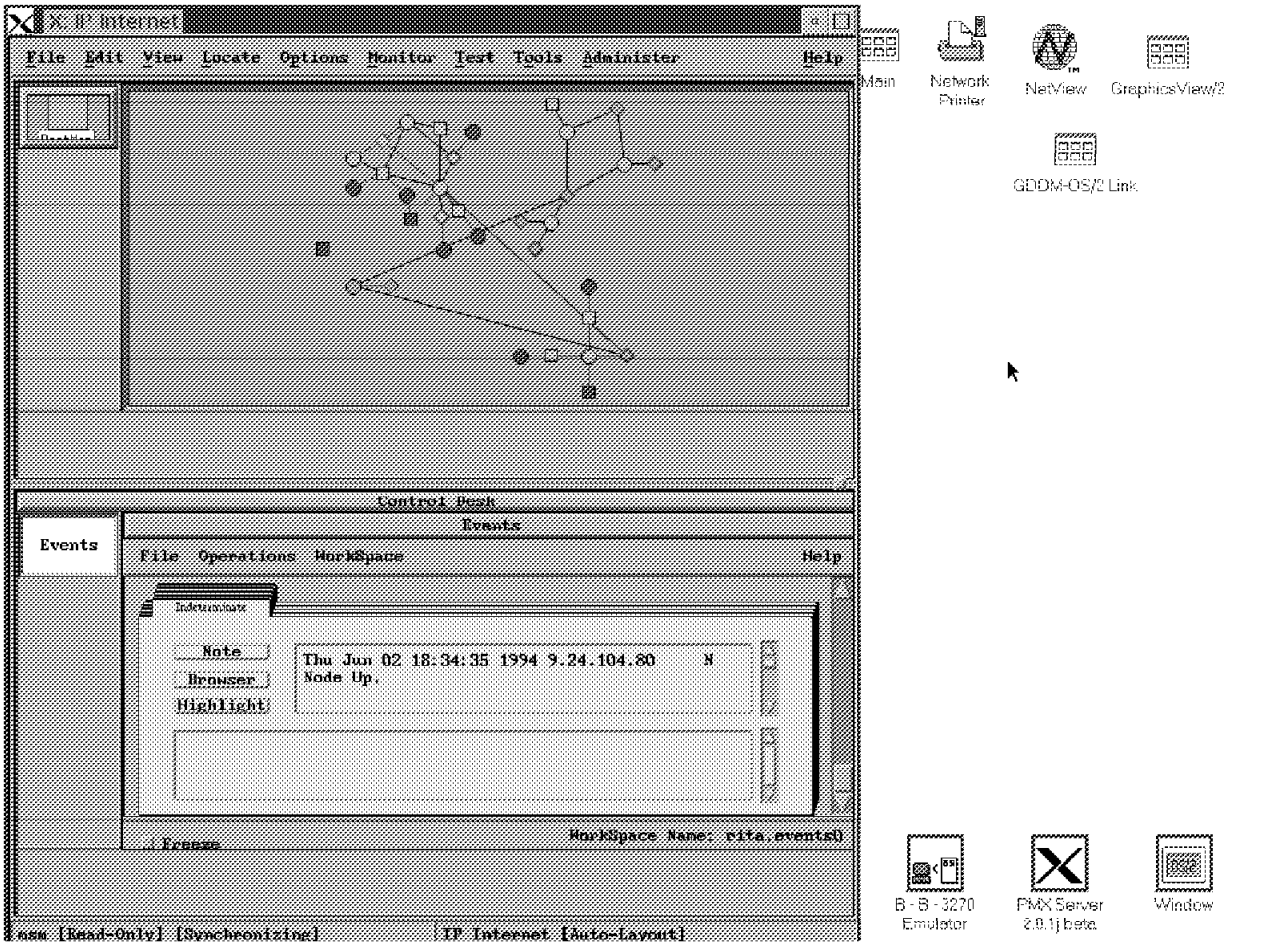


Figure 105. NetView/6000 on OS/2 Using PMX

Now you can use NetView/6000 as if you were at a RISC/6000 workstation. If you are using NGMF and NetView/6000 remote console simultaneously, you should watch your OS/2 SWAPPER.DAT carefully.

4.4.2 Setting Up the NetView/6000 Remote Console

With TCP/IP for OS/2 Version 2.0, you can use your NGMF workstation to display NetView/6000 windows. This is done with the X-Windows Server provided by TCP/IP for OS/2: PMX. To be able to run NGMF and PMX on the same workstation, you have to configure your token-ring adapter's buffers carefully. Open LAPS configuration and select **Edit** for the token-ring adapter as shown in Figure 106 on page 106.

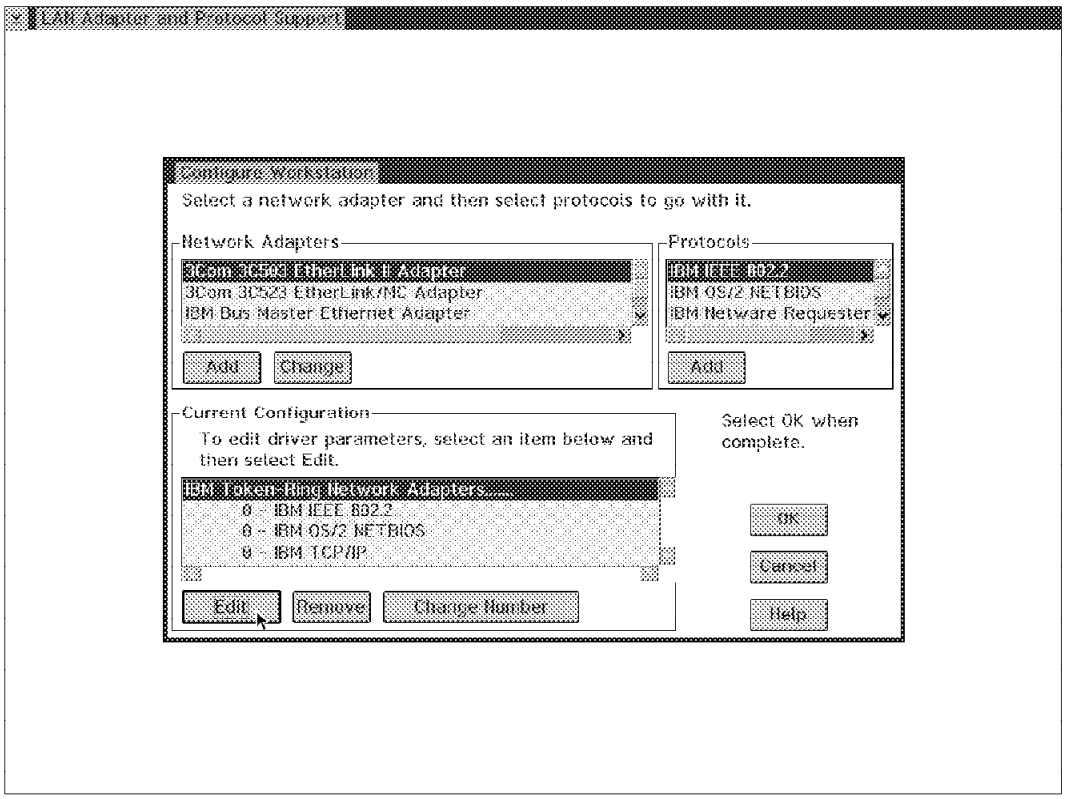


Figure 106. LAPS Configuration Menu

You get a screen that allows you to adjust parameters for your token ring adapter. You should minimize the number of buffers. Otherwise you might get errors or event system traps. Our configuration is shown in Figure 107 on page 107.

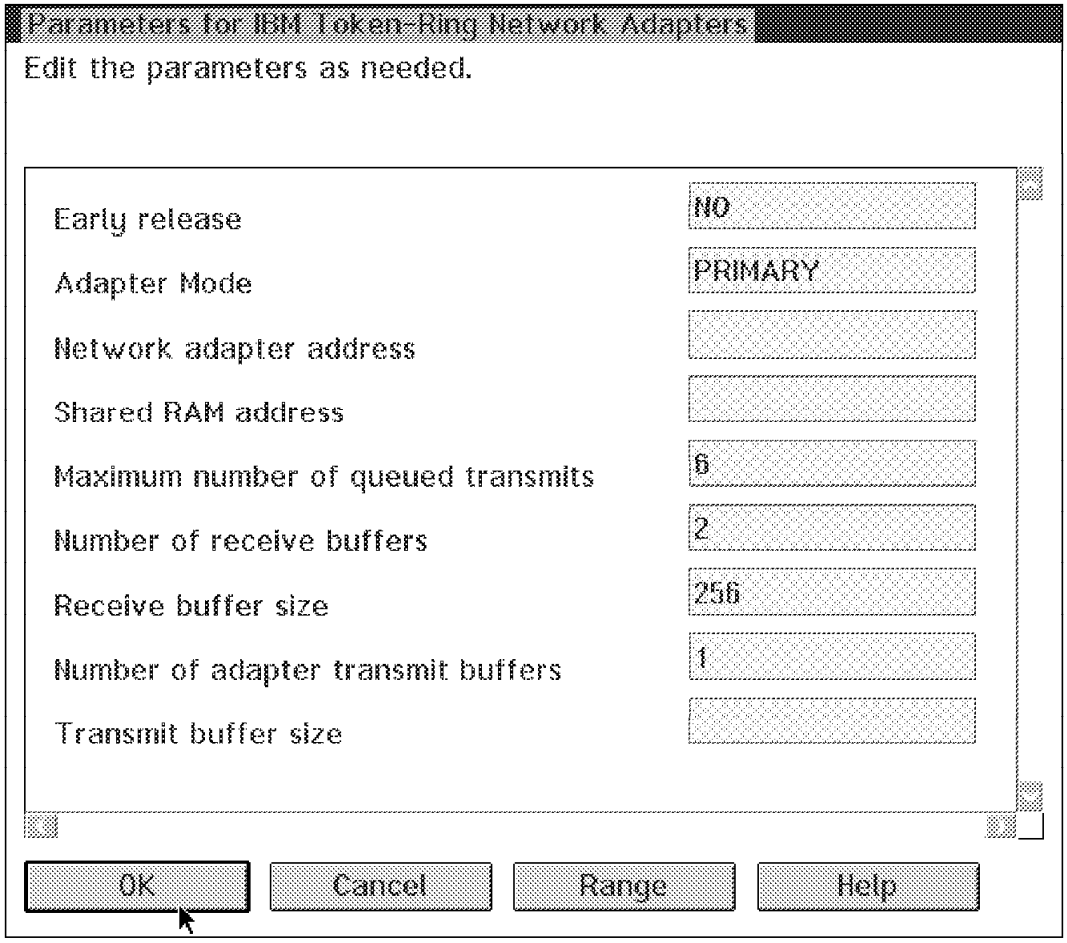


Figure 107. The Token-Ring Network Adapter Parameters

To run PMX on OS/2, you should follow these general rules:

- Use a fast machine; as a minimum a 486 processor is recommended.
- Get as much memory as you can; a minimum of 16MB is highly recommended.
- Apply the latest CSDs to TCP/IP and PMX.

To fit NetView/6000 windows onto the PS/2 screen, you may consider changing the window sizes for the user that usually uses PMX for NetView/6000. To do so, edit the .Xdefaults file in the user's home directory in AIX by adding the following:

```
OVw*shellHeight:                  390
OVw*shellWidth:                   640
OVw*mainWindowControlHeight:      350
OVw*mainWindowMessageHeight:      25
OVw*scrolledBoxBoxHeight:         50
OVw*scrolledBoxBoxLabelHeight:    100
OVw*viewAreaHasControl:           False
OVw*toolShellIconify:             True
OVw*navTreeShellIconify:          True
OVw*controlDeskBoxHeight:         15
OVw*toolPaletteBoxesFont:    -ibm--medium-r-medium--14-10-100-
100-c-80-ibm-850
OVw*applicationCacheAndParkFont: -ibm--medium-r-medium--14-10-
100-100-c-80-ibm-850
```

This reduces the overall height and increases the space for topology displays and event cards as much as possible.

We further decided to minimize the tools palette and the navigation tree as defaults on the smaller PS/2 screen. The font statements were added because the default fonts used for those two text types are not provided by PMX as defaults. These definitions are related to the user, so whenever this user ID logs into AIX and starts the NetView/6000 application, it shows up in the specified size.

Note

We used a 8514 screen on the PC.

4.4.3 Using PMX

You can start PMX in three different ways:

- Automatically with TCP/IP startup; you can specify the start options using `tcpipcfg`.
- Typing `xinit`.
- Typing `pmx`.

It is invoked whenever you start an X-Windows application on a remote IP host. To start NetView/6000 on your workstation, TELNET to the RISC/6000 system that is running NetView/6000, and set the display variable by typing:

```
export DISPLAY=youradress:0
```

then you can start the application by typing:

```
/usr/OV/bin/nv6000 &
```

For our scenario described before, we also customized the .profile for this user for our workstation. The .profile file contains startup parameter and is placed in the user's home directory. We added the following statement:

```
export DISPLAY=9.24.104.82:0
```

This means that this user will only be usable from the PS/2. If this user logs into AIX from any other workstation, it will be unable to display any X-Windows.

We also included the NetView/6000 startup into the user's $HOME/.profile by adding the statement:

```
nv6000 -map msm &
```

If we now select the **Remote Console** function for the NetView/6000 machine in NGMF, we can log in with our customized user ID, which opens NetView/6000 as shown before. To get only an AIX command line we have to log in with the root user or an other user. In this case a user is not really used for a person but for a specific machine.

Note

Remember that PMX has to be active at the time you log in with your customized user.

4.5 MSM and the NetView for AIX Backup Manager Function

One of the new features of NetView for AIX is the Manager Takeover function.

4.5.1 Manager Takeover

This feature allows the management of the IP network to be split up into parts, with multiple copies of NetView for AIX each managing their own defined resources. These separated parts are called spheres of control (SOC). Devices outside the SOC of a particular manager will be *unmanaged*: That is, no polling for status or configuration will be performed.

In Figure 108 on page 110 an area is defined as a group of containers that are in the sphere of control (SOC) of a manager.

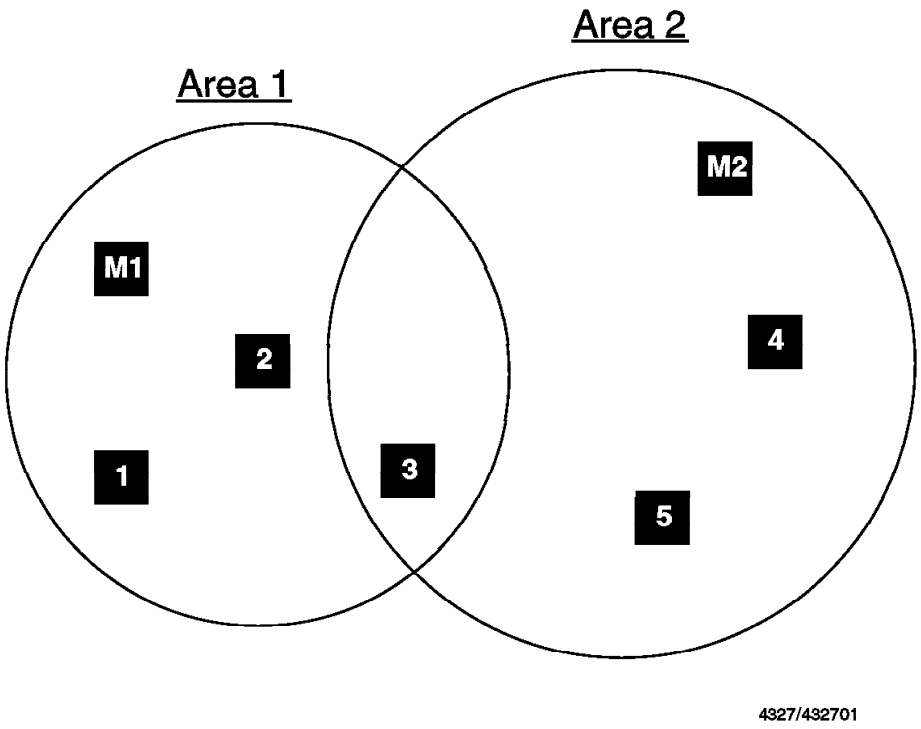


Figure 108. A Possible SOC Configuration

Each of the manager nodes will check the status of the other manager nodes on the network. When one of the manager nodes becomes inactive, a message box is displayed to notify the operator and to ask if management takeover is wanted. If it is, the resources that were defined to be managed in a backup situation are managed and displayed in a separate submap. This definition is customized in NetView for AIX in advance.

Manager takeover is currently not supported by MSM.

4.5.2 MSM and Manager Takeover

To test how MSM works with two NetView for AIX managers using the backup function we implemented a second Service Point. The second topology agent is added to the IP view as shown in Figure 109 on page 111.

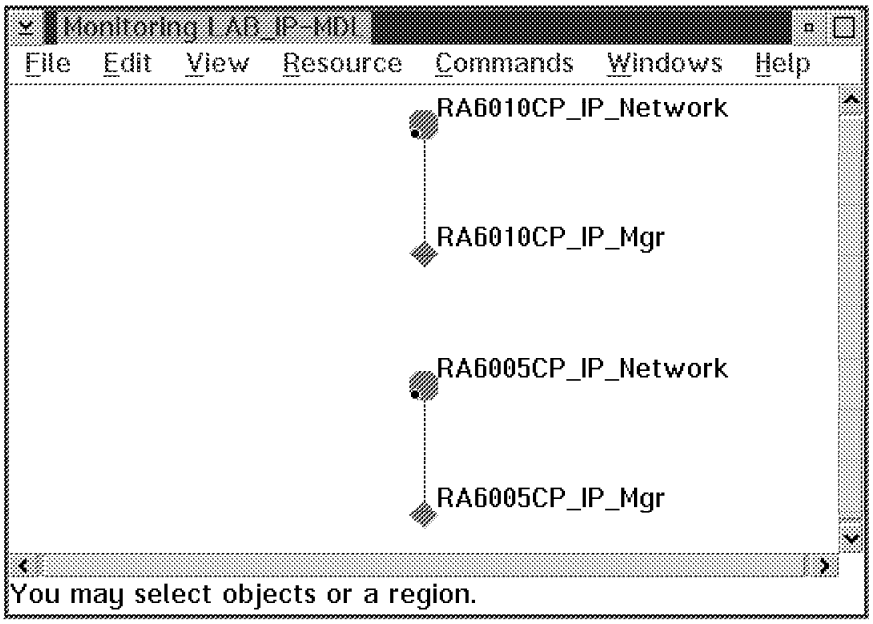


Figure 109. Two Service Points Managed by MSM

The additional RS/6000 is called rs600010; the name of the CP is RA6010CP. This manager manages the locations Atlanta and Malibu. The NetView for AIX on rs60005 running with the CP name RA6005CP manages the resources that are located in Raleigh. The NGMF view of this network is shown in Figure 110 on page 112.

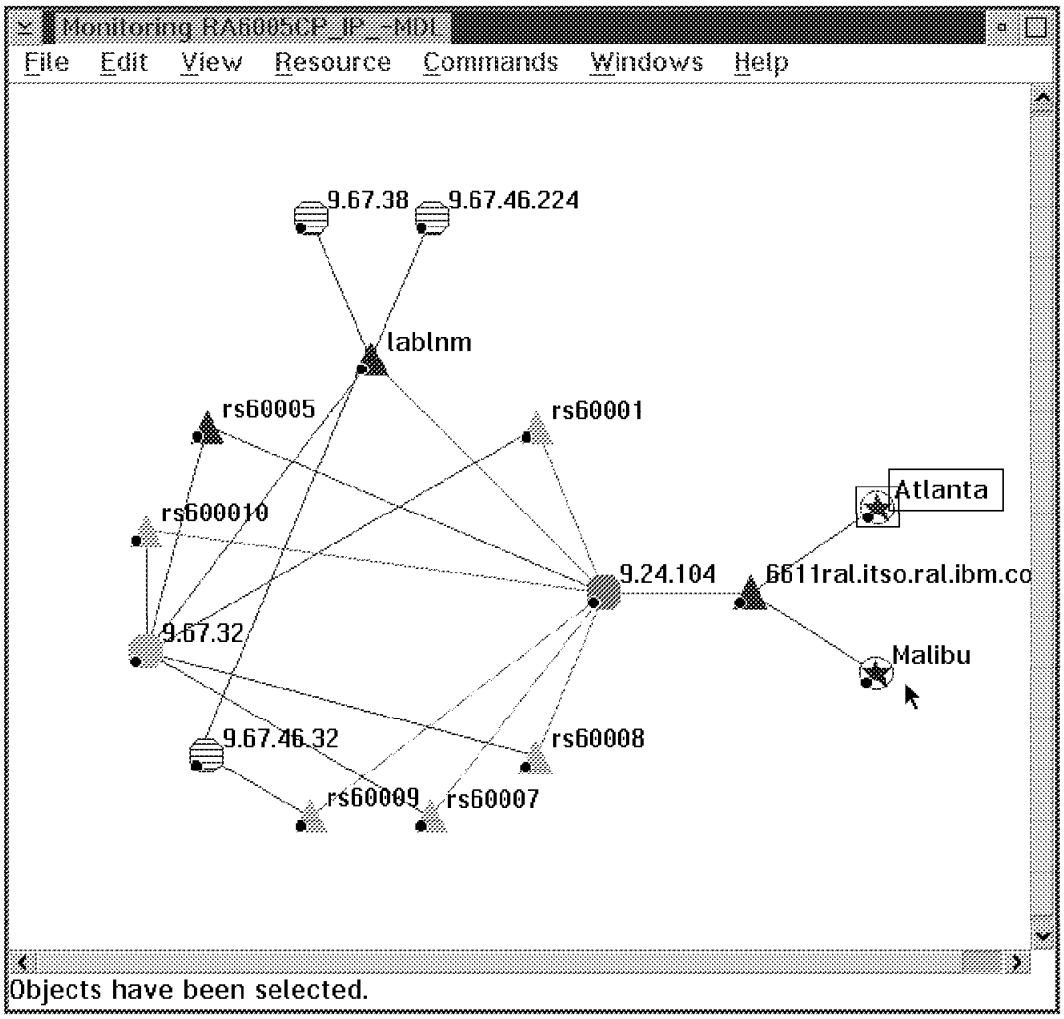


Figure 110. The Raleigh IP Network and Locations Malibu and Atlanta as Seen by RS60005

You can see the two locations Malibu and Atlanta that are both unmanaged. We selected these two containers in NetView for AIX on rs60005 and defined them to be managed only in the backup case, as shown in Figure 111 on page 113.

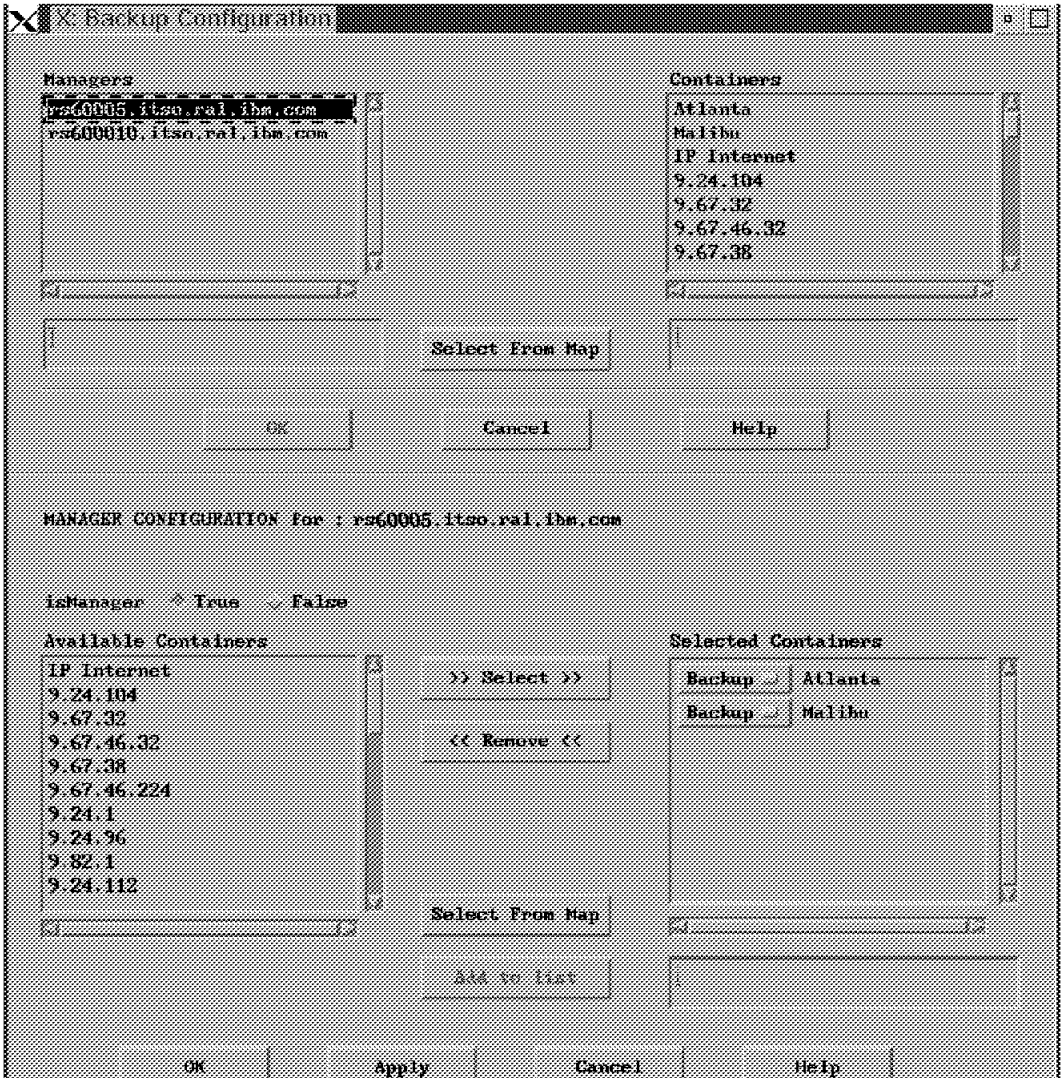


Figure 111. Defining the Backup Manager

NetView for AIX polls the manager it provides backup for, in our case rs600010; and if it goes down, a node down trap is generated. The following window appears on the NetView for AIX console, which is in our case the NGMF workstation running PMX:

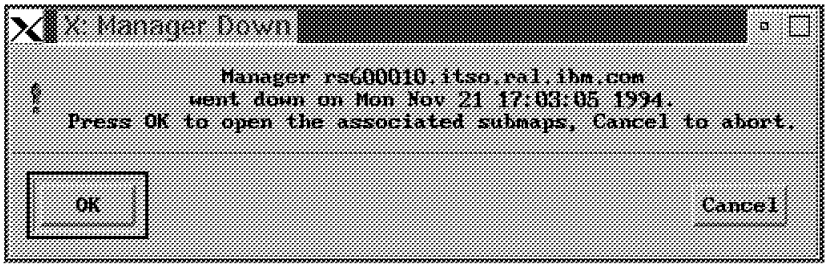


Figure 112. Manager Down Pop-up

The service point icon of the failing machine turns red, and its resources become unknown. The manager that takes over then opens the submaps Malibu and Atlanta and sets the resources contained in these submaps to managed. If the

topology agent is running on that map, it generates interface managed traps that are passed to MSM. Thus, GETTOPO commands are triggered for those resources that did not exist in RODM, and the resources will become known in NGMF as shown in Figure 113. Nothing happens for those resources that were already known.

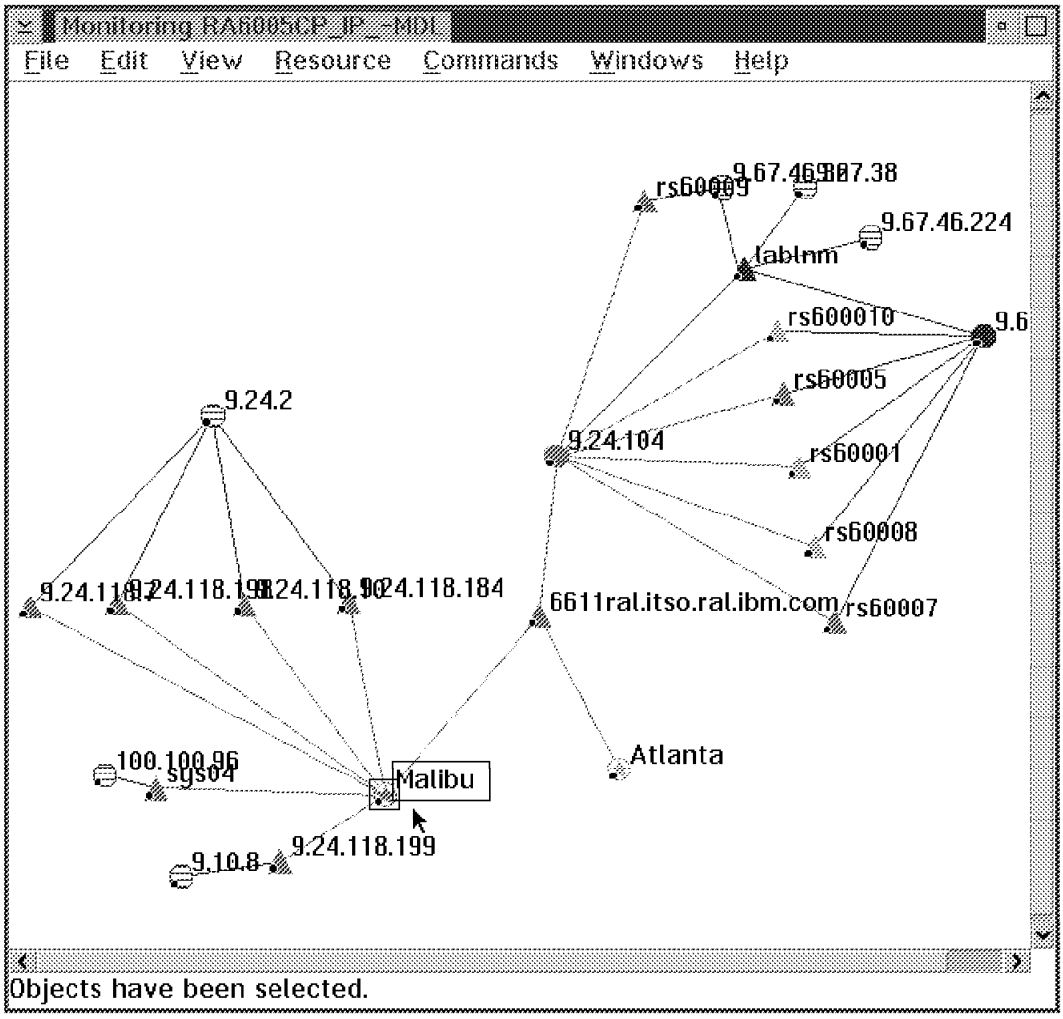


Figure 113. Management Takeover. We rearranged the icons in this screen for clarity.

Malibu and Atlanta are colored now, since they are known resources and some resources behind Malibu have been discovered. No additional resources were discovered behind Atlanta.

Note

If a lot of Interface managed or Node added traps are forwarded to NetView for MVS, many GETTOPO commands might be sent back to the Service Point. As NetView for AIX is usually synchronizing when it does discovery these commands will fail. This may lead to problems in the automation process. For further information refer to 3.7, “Monitoring IP Resources” on page 60. If the network stays unknown in NGMF you have to issue a GETTOPO manually after the takeover process.

When the second manager comes back (″Node up trap″) the following pop-up window appears on the NetView for AIX console:

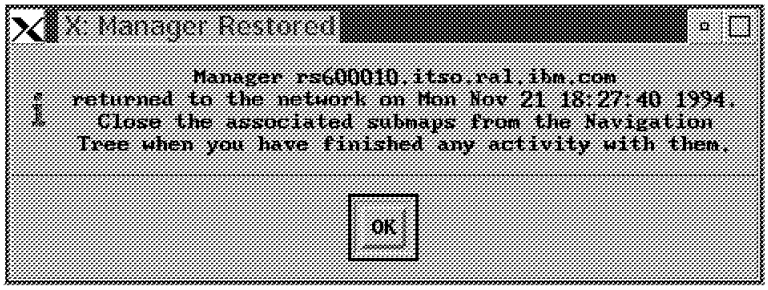


Figure 114. Manager Up Pop-up

If you close the submaps in NetView for AIX on rs60005 using the Navigation Tree the resources turn white - they are unmanaged again. The topology agent generates NetView/6000 specific traps ″Interface unmanaged″ and MSM sends a message to RODM to remove these resources.

When MSM get the ″MSM agent up and ready″ alert from the service point RA6010CP that has now come back to manage Malibu and Atlanta, a GETTOPO command runs against the agent automatically.

Chapter 5. Installation and Customization

The installation consists of the following steps:

- IBM NetView MultiSystem Manager MVS/ESA host installation
- IBM NetView MultiSystem Manager workstation installation
- IBM NetView MultiSystem Manager agent installation
- IBM NetView MultiSystem Manager informal documentation installation
- Installation of the NetView/6000 agent is described in Chapter 3, “The MSM IP Tower” on page 11.
- Installation of NetWare and LNM features is described in *Centralized Management of LNM and NetWare Networks Using NetView MultiSystem Manager MVS/ESA*.

5.1 Installing IBM NetView MultiSystem Manager at the Host Site

The product manuals explain the installation of the host component - our experiences are documented to show an example.

5.1.1 Software Prerequisites

- SMP/E 1.8 or SMP/E 1.7 with PTF number UR40251.
- NetView Version 2 Release 4 with PTFs:

  See the program directory and the PSP bucket - initially we did not apply all of these and hit problems until we did.
- IBM Library for SAA REXX/370 or the REXX/370 Alternate Library (shipped with MultiSystem Manager).

5.1.2 Installation of the Base Component

In our installation we used the following naming conventions:

- NETVIEW.V2R4M0 for NetView libraries
- NETVIEW.NV24.RABAN for NetView and IBM NetView MultiSystem Manager customized libraries and data sets
- MSM.V1R2M0 for IBM NetView MultiSystem Manager libraries
- RABAN as the NetView domain
- RODM11 as the RODM name

Use the instructions from the program directory to install the product files with SMP/E.

The following files are shipped with base MSM:

SFLCCLST	CLISTS
SFLCINST	installation jobs
SFLCLINK	MSM load modules
SFLCMSGU	messages
SFLCPNLU	panels

SFLCPS2U	NGMF workstation code
SFLCSAMP	samples

The following files are shipped with MSM optional material (JFLC299):

SFLCINS1	installation jobs
SFLCPS21	MSM tools documentation
SFLCREX1	additional CLISTS (tools)
SFLCSAM1	samples (tools)

5.1.3 Changes in the MVS Environment

The following changes must be made in your MVS environment:

- Make sure the MSM load library SFLCLINK is APF authorized.
- Add a RODM user ID to RACF or other security system. The user ID for MSM is your NetView domain ID concatenated with MSM (in our environment, RABANMSM). The RODM security name and class are defined in the RODM customization file EKGCUST (in our environment, DATAMGR and RODM). The RACF object, for which you need a permit, is the RODM security name concatenated with the security level. MSM needs a level of three; a user who loads, stops and starts RODM needs six. The MSM user ID doesn't need a password.

```
//'USER' JOB ......
//*
//STEP1    EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=A
//SYSTSIN  DD *
 AU 'RABANMSM' -
    PASSWORD(IBMUSER) -
    DFLTGRP(SYS1) OWNER(IBMUSER) UACC(ALTER)

 PERMIT RODM3 CLASS(DATAMGR) ID('RABANMSM')
```

In our environment we gave operators read access to the RODM6 profile in the Datamgr Class. We also gave each user a RACF security level of SECLVL6.

5.1.4 Changes in the NetView Environment

1. Add the IBM NetView MultiSystem Manager libraries to your NetView start procedure:

STEPLIB:	SFLCLINK
DSICLD:	SFLCCLST
	SFLCREX1
DSIPARM:	SFLCSAMP
	SFLCSAM1
DSIPRF:	SFLCSAMP
DSIMSG:	SFLCMSGU
CNMPNL:	SFLCPNLU

   See Figure 185 on page 257 for a listing of the NetView procedure we used.

2. Change or add the following IBM NetView MultiSystem Manager statements in your NetView data sets:

- Modify member DSICMDU (DSIPARM data set).

  Add MSM Commands

  ```
  %INCLUDE FLCSCMD
  ```

- Modify your NetView initial command list (CNME1034 in DSICLD).

  – The following CLIST and autotask statements should be added to the NetView initial CLIST.

  Add in NetView Initial CLIST CNM1034

  ```
  FLCBLODC              /* common     */
  FLCBLODL              /* for LNM    */
  FLCBLODN              /* for NetWare */
  FLCBLODI              /* for IP     */
  AUTOTASK OPID=AUTOMSM     /* common     */
  AUTOTASK OPID=AUTOIPA     /* for IP     */
  AUTOTASK OPID=AUTONWA     /* for NetWare */
  AUTOTASK OPID=AUTOLNMA    /* for LNM    */
  ```

  This will load each of the necessary MSM CLISTs into NetView memory using the LOADCL command, which should ensure optimum performance.

  The autotask statements will automatically start each of the required MSM autotasks.

- Add the operator profile to the DSIPRF data set.

```
*********************************************************************
*    5655-044 (C) COPYRIGHT IBM CORPORATION 1993                    *
*     ALL RIGHTS RESERVED.                                          *
*                                                                   *
*    DESCRIPTION: AUTOMATED OPERATOR PROFILE DEFINITION FOR         *
*                 MULTISYSTEM MANAGER.                              *
*                                                                   *
*********************************************************************
*-------------------------------------------------------------------*
* THIS IS A SAMPLE PROFILE FOR THE AUTOMATED OPERATOR USED BY       *
* MULTISYSTEM MANAGER DURING INITIALIZATION.                        *
*-------------------------------------------------------------------*
FLCSPRFA     PROFILE  IC=INITTOPO
             AUTH     MSGRECVR=NO,CTL=GLOBAL
             OPCLASS  1,2
             END
```

- Assign operator profiles to the different MSM tasks (member DSIOPFU of DSIPARM data set):

  ```
  %INCLUDE FLCSOPF
  ```

- Include MSM help panel IDs (member HELPMAPU of DSIPARM data set):

  ```
  %INCLUDE FLCS1048
  ```

- Modify the automation table (DSITBLxx of DSIPARM):

```
* LAN Network Manager
*
%INCLUDE FLCSTBLL
*
* NetWare Agent
*
%INCLUDE FLCSTBLN
*
* IP Networks
*
%INCLUDE FLCSTBLI
*
```

The automation table processes MSUs (topology data, alerts and resolutions) that are generated by the agent and calls the appropriate CLIST or command processor.

In a test environment it is helpful to route MSM messages to an OST task too. We defined our operators in an operator group +MSMOP.

```
************************************************************************
*  MSM messages                                                        *
************************************************************************
IF (MSGID='FLC'.|  MSGID='DSI' .) &
   (OPID='AUTOMSM' | OPID='AUTOIPA' | OPID='AUTONWA' |
    OPID='AUTOLNMA')
        THEN EXEC(ROUTE(ALL +MSMOP));
*
```

The automation table entries, provided in our sample, will route all MultiSystem Manager (FLC prefix) and NetView (DSI prefix) messages to NCCF operators defined in the +MSMOP group of NetView operators. (See the INITMSM CLIST listed in Figure 115.)

```
'assign group=+msmop,op=(georges,skibeli,karl,steffes)'
'assign msg=FLC*,pri=automsm,sec=+msmop'
exit
```

Figure 115. INITMSM CLIST

3. Start MSM.

   To start the MSM environment on the host you have to:

   - Initialize the NetView automation table which contains the definitions. This can be done during NetView startup or by using the AUTOTBL command.
   - Start the AUTOMSM task.
   - Start the additional autotasks that have been defined for processing GETTOPOs.
   - Issue an INITTOPO command.

   If you issue an INITTOPO or a GETTOPO command and the corresponding autotask is not yet running it will be started automatically, but if this takes too long (NetView very busy) MSM will use the default autotask, which is normally AUTOMSM. This can cause performance problems because the load is not spread over different autotasks anymore.

Note that there is no command to stop the MSM environment.

4. REXX Environment

   Since all MSM CLISTs are written in REXX, you should check and customize your REXX environment parameters. The NetView defaults for the REXX environments are for systems that have lots of storage available. If storage is a concern in your installation, we recommend that you reduce the REXXENV for all your tasks to 2 (the default is 10). Use the DEFAULTS command to change the default value.

   ```
   DEFAULTS REXXENV=2
   ```

   REXXENV is the number of REXX environments to be allocated per task. Keeping the REXX environments allocated will reduce your CPU utilization but will increase your storage usage.

   The REXXSLMT is another parameter which has an impact on the size of storage your NetView task has to allocate. It defines when and how much storage has to be freed after a REXX CLIST finishes its execution. The default is no limit and the storage will never be freed. We recommend that you set the REXXSLMT to 800KB. In this case, NetView will free the REXX environment when it is no longer needed, that is, after the REXX CLIST using it ends, if the environment grew beyond 800KB. Use the DEFAULTS command to set the value.

   ```
   DEFAULTS REXXSLMT=800
   ```

   Refer to the *NetView Tuning Guide* for more information regarding the REXX environments.

5. RUNCMD Timeout Value

   MSM uses RUNCMDs to gather initial topology and status information from its agents. To prevent the RUNCMDs from prematurely timing out, you have to adjust the time-out value defined in DSICTMOD. You can do this permanently by changing the value in DSICTMOD or temporarily by using the COSTIME parameter in the DEFAULTS command.

   Some RUNCMDs need a long time to execute. We set it to 180 seconds.

   This parameter has additional importance because it is taken by MSM and sent down to the service point with the flcidrv command as the -t parameter. It is then taken by flcidrv as a timeout value for flcitopo operations.

6. MSM Initialization File

   Tailor the MSM initialization file FLCAINP for your environment. The INITTOPO command defaults to use member FLCAINP in DSIPARM, but you can use any other member if you specify it on the INITTOPO command. We used FLCAINP for the MSM defaults (see our sample in Figure 191 on page 263) and included separate members for each agent (see our sample member FLCSIIP in Figure 192 on page 264).

5.1.5 RODM Parameters

- To shorten paths on RODM API calls, the PLI_ISA value should be set to 24KB or greater.
- The values for CONCURRENT_USERS and ASYNC_TASKS should be adjusted as follows:
  - One asynchronous task for alert processing

- One asynchronous task for each topology feature
- One asynchronous task for each additional defined autotask that uses the GETTOPO command
- The number of concurrent users must be at least the number of MSM autotasks plus one

• The values for the following parameters should be be set to:

- EXTEND_HEAP_SIZE 32KB
- PRIMARY_HEAP_SIZE 64KB
- LOCK_LOOPLIMIT (128, 1024, 1024)
- LOCK_SLEEPTIME (1, 1, 1)

If you have defined a region size in your RODM startup procedure, you might have to adjust the region size, too.

5.1.6 Update GMFHS

If you had MSM Release 1 installed on your system, remove the SFLCLINK data set from your STEPLIB concatenation.

See Figure 188 on page 260 for the GMFHS procedure we used.

5.1.7 MSM Data Model and RODM

RODM must be loaded with the class definitions for MSM to be operational. Each class contains field descriptions of the characteristics of an object. Classes also contain presentation fields that describe how an instance of an object appears in NGMF views. These classes are defined in the SystemView data model, GMFHS data model and MSM data model. The models have been broken into separate samples, so you can omit reloading classes that are already loaded.

The class definitions are done using the RODM loader syntax. For the SystemView data model the class and field names are in dotted decimal format, but for your convenience there is also a corresponding text format provided for these classes and fields. The text format is defined as comment statements and will not be loaded.

5.1.7.1 Data Model Installation

To load RODM you can use the load procedure provided in the RODM sample library SEKGSMP1, members EKGLLOAD and EKGLOADP.

The order of loading your data models is important. You have to load the GMFHS data model first, followed by the SystemView and MSM data models.

A sample load job for the GMFHS data model is provided in CNMSAMP(CNMSJH12). Delete the step INSTLOAD. This step is not needed.

For the MSM data model the sample job is provided in library SFLCSAMP(FLCSJDM).

See Figure 189 on page 261 and Figure 190 on page 262 for the jobs we used.

Note

After successfully loading the data models, you should checkpoint RODM.

5.1.8 MSM Data Model Files

FLCSDM1 This file defines SystemView classes that are common to MSM and the APPNTAM feature. If you have already installed the APPNTAM feature, you don′t need to load this file again, so comment the DD statement out of the loader job.

FLCSDM2 This file defines the SystemView classes for the LNM and Novell features.

FLCSDM3 The statements in this file define private MSM classes for the LNM and Novell features.

FLCSDM4 This file defines the default threshold values set by MSM for real and aggregate resources for the LNM and Novell features.

FLCSDM5 These are the field definitions that are used for view navigation for the LNM and Novell features. This is done by linking objects under the GMFHS presentation classes with objects under the SystemView and MSM classes.

FLCSDM64 This file defines the special MSM display resource types.

FLCSDM7 This file defines SystemView MSM classes for IP.

FLCSDM8 This file defines private MSM classes for IP.

FLCSDM9 These are the field definitions which are used for view navigation.

FLCSDM10 This file defines some default values for IP resources.

Even if you install only the IP tower, you have to load all the files.

5.2 Installing IBM NetView MultiSystem Manager on the Workstation

The IBM NetView MultiSystem Manager workstation installation assumes you have installed NGMF in Appendix C, “Installing NetView Graphic Monitor Facility on the PC Workstation” on page 231 of this book. MSM uses the standard NGMF workstation code. The MSM workstation code is only some CT/2 command sets that enable the NGMF operator to send commands from CT/2 to the supported service point applications (for example, the SNMP get command).

We had some problems with code pages. We got the best results by defining a CM/2 emulator session for PC code page 037 and host code page 437 and using this session to download the code.

With NetView V2R4 the Software Installer for OS/2 should be used to install the MultiSystem Manager CT/2 extensions on the workstation as described below:

- Shut down NGMF and CT/2

  Note

  If NGMF is currently in session with NetView, you should use the NETCONV command to discontinue the LU 6.2 pipe between NGMF and NetView as shown below.

```
NETCONV ACTION=STOP LU=xxxxxx
```

This task should be performed before attempting to close the Graphics Communication task on the NGMF workstation.

- Make sure you are logged on to the MVS system (and currently at the TSO READY prompt).
- Go to an OS/2 window command line prompt and change to the IBMDUI directory as shown below:

  ```
  CD\IBMDUI
  ```

- Enter the following command to start the Software Installer for OS/2 process. The last character in the member name (FLC001C_) determines whether the Software Installer for OS/2 should download the LNM commands (B), the NetWare commands (D) or the IP commands (E).

  ```
  DUIINSTS /S:MSM.V1R2M0. /C:MSM.V1R2M0.SFLCPS2U(FLC001CE) /O:MVS
  ```

Note

In our ITSO lab the MSM downloadable code was located in a data set prefixed MSM.V1R2M0; you may need to change this to reflect your environment.

As a result of the previously discussed DUIINSTS command, Software Installer for OS/2 should present a window like the one shown in Figure 116.

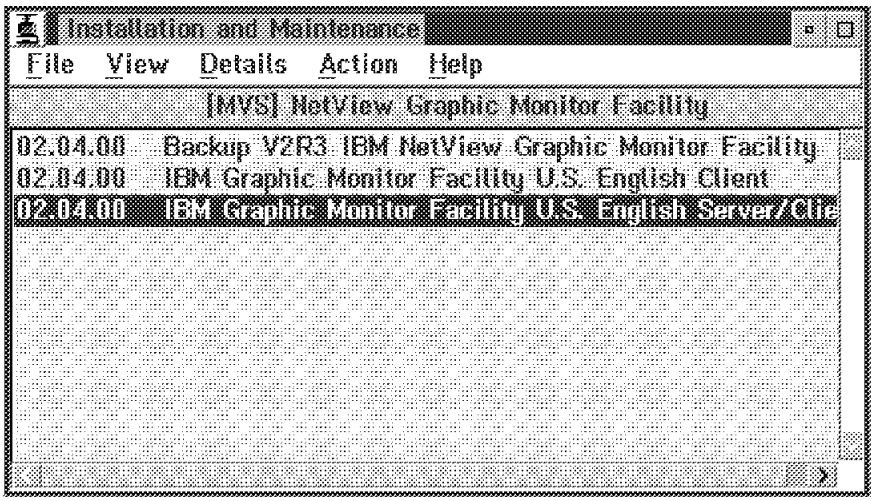


Figure 116. Installation and Maintenance Window

Do the following:

- Select **File**, then **Open Catalog**, then **Host** from the menu bar as shown in Figure 117 on page 125

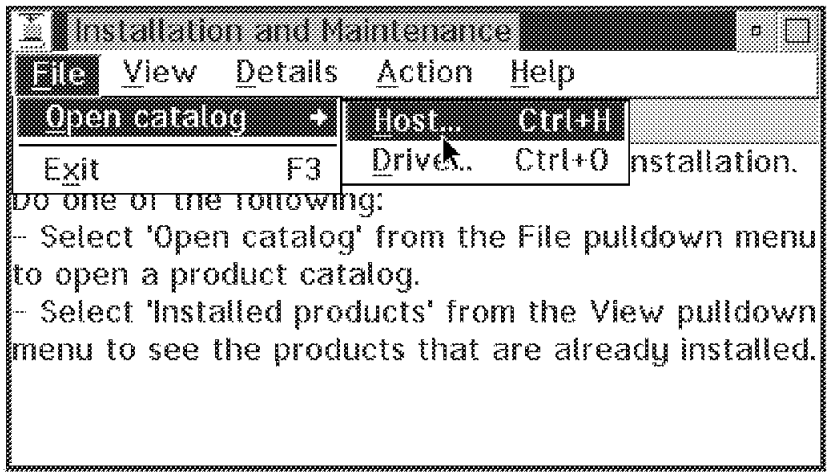


Figure 117. Selecting Host Catalog

Sometimes you get automatically the window as shown in Figure 118 (overlaying the first one). This window should be used to verify that the download will be performed from the correct data set, on the correct host session, and that MVS is specified as the host operating system.

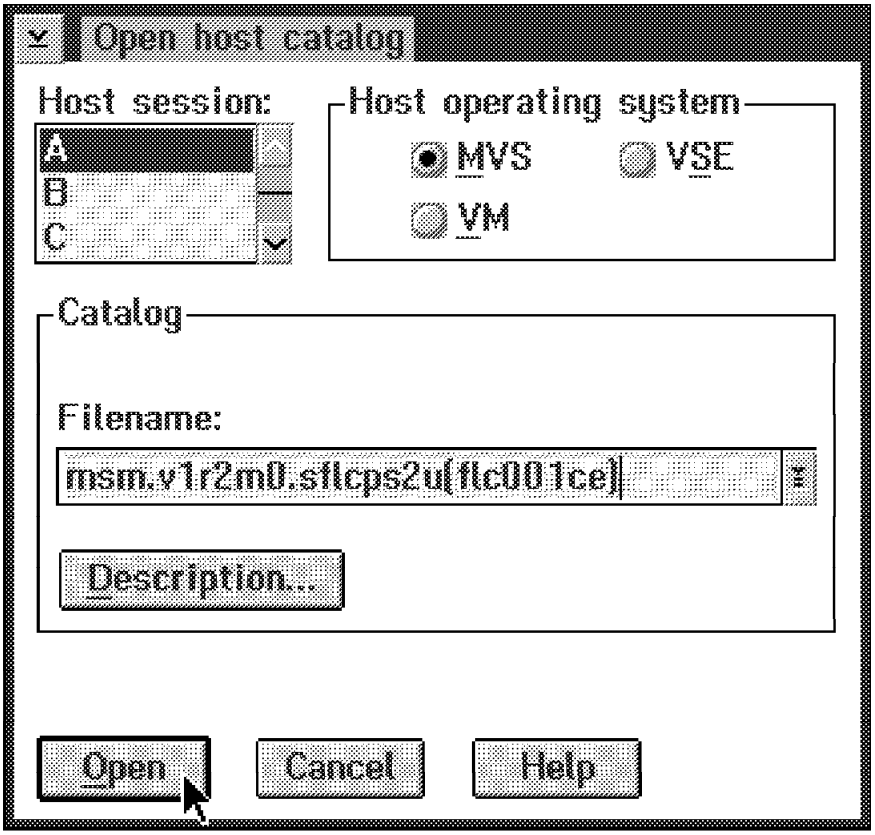


Figure 118. Open Host Catalog Window

- In the Open host catalog window, enter the following in the filename field if it isn't already there:

  `MSM.V1R2M0.SFLCPS2U(FLC001CE)`

Note: In our ITSO lab the MSM downloadable code was located in a data set prefixed MSM.V1R2M0; you may need to change this to reflect your environment.

- Select your host session.
- Click on the **Open** push button in the Open host catalog window to download the IBM NetView MultiSystem Manager catalog file. In the Installation and Maintenance window, (see Figure 119) the *NetView MultiSystem Manager US English Package* should now be highlighted.

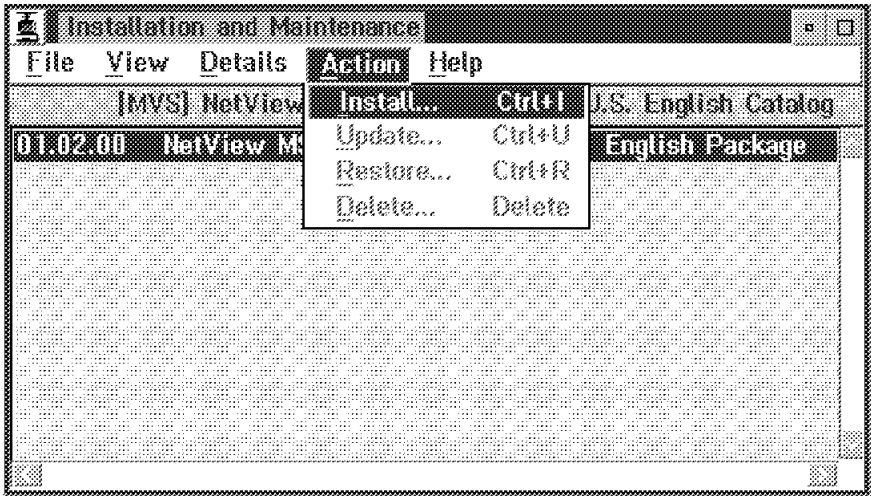


Figure 119. Selecting Install

- Select **Action** then **Install...** from the menu bar. As a result Software Installer for OS/2 should present a window like the one shown in Figure 120.

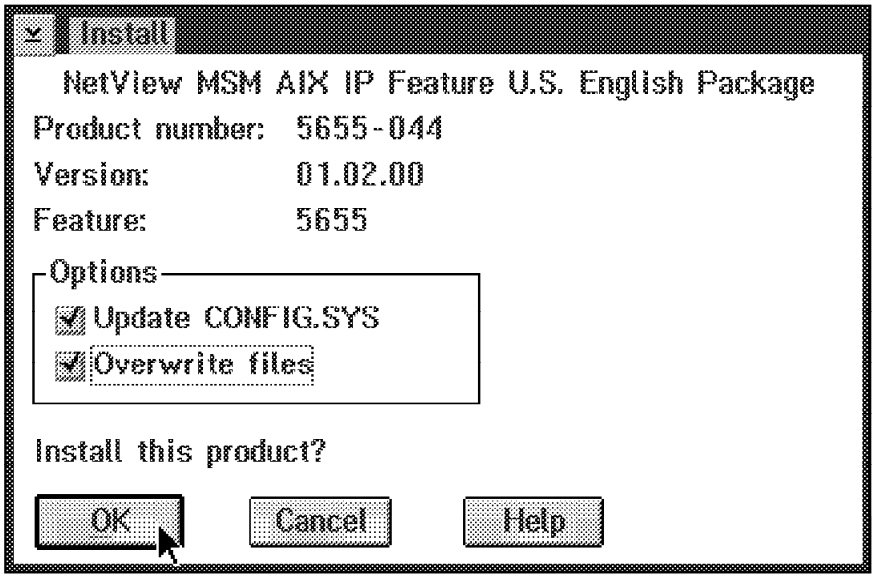


Figure 120. Install Window

- Select **Update CONFIG.SYS** and **Overwrite files** and then click on the **OK** push button. Software Installer for OS/2 should now present a window like the one shown in Figure 121 on page 127.

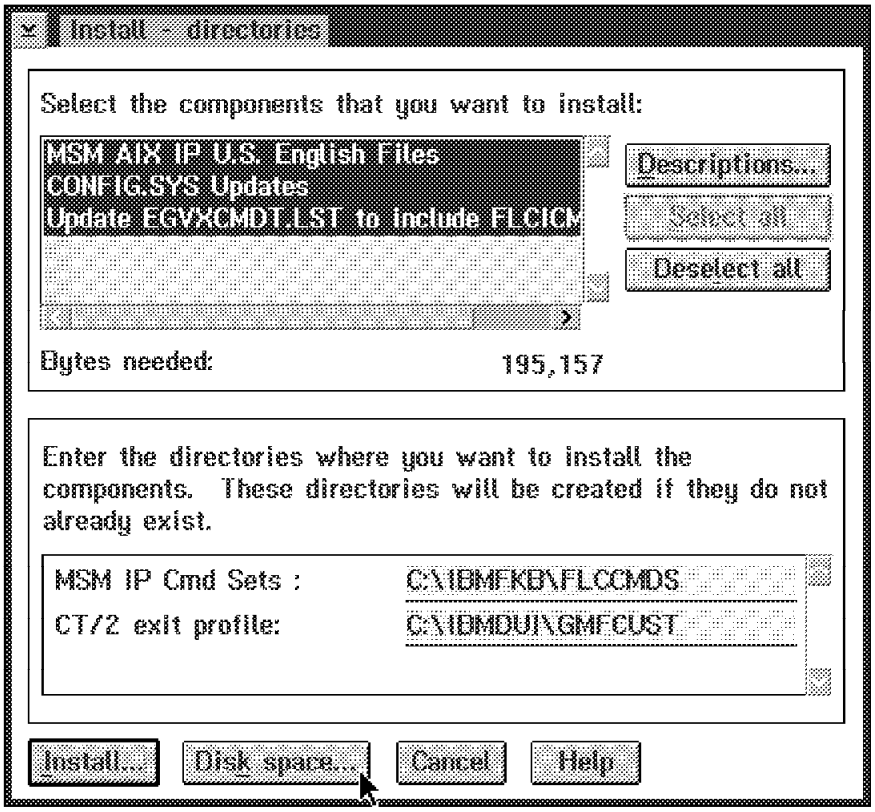


Figure 121. Install - Directories Window

- In this window, perform the following tasks:
  - Select all the components.
  - Leave default directory options; you may however want to change the drives from C: to D:. The recommended way to change the target drive and check available disk space is to click on the **Disk space** push button. You get a window like the one shown in Figure 122 on page 128.

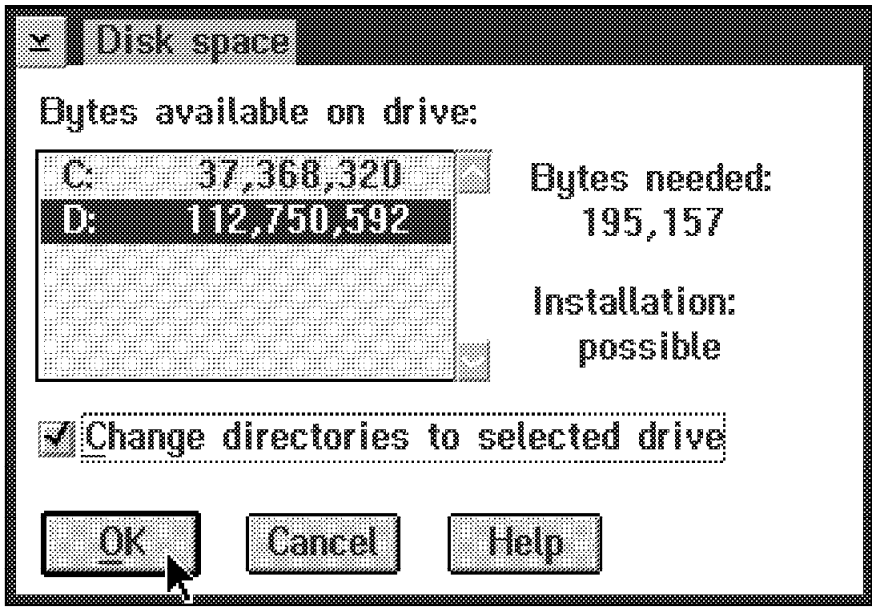


Figure 122. Install - Disk Space Window

– Select your drive, click **Change directories to selected drive** and select **OK**. You will return to the window shown in Figure 121 on page 127.

– Click on the **Install** push button.
The download process should start and a status window like the one shown in Figure 123 will be presented by Software Installer for OS/2.

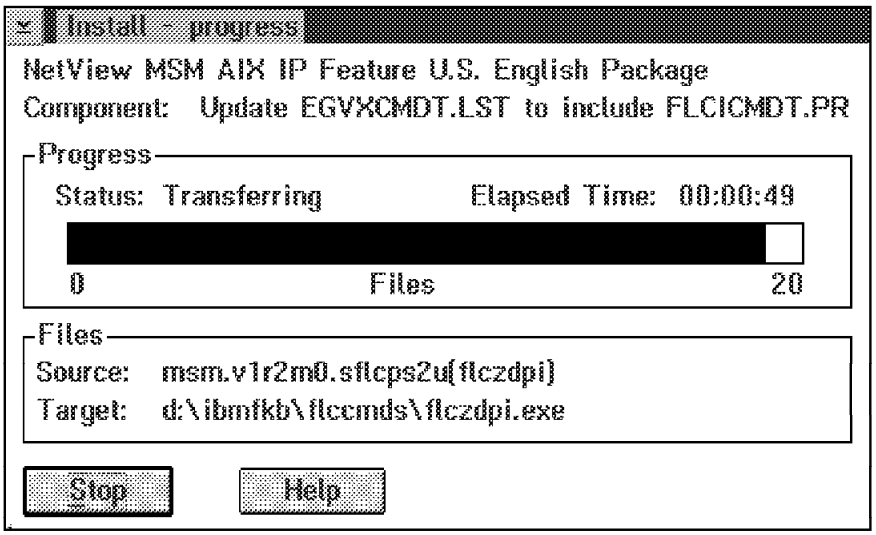


Figure 123. Install - Progress Window

- When the installation has finished, you get the window shown in Figure 124 on page 129.

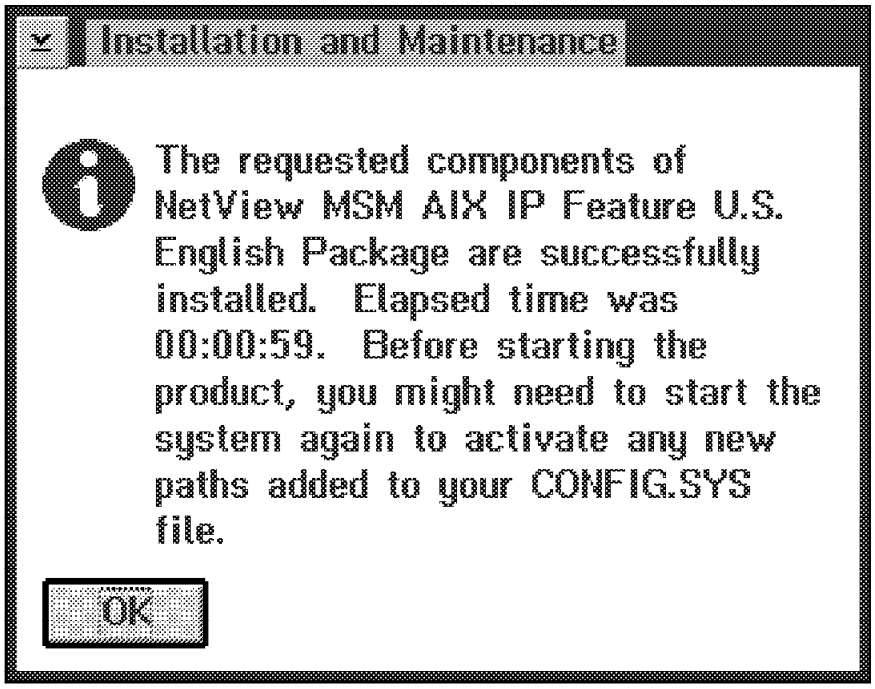


Figure 124. Completing Installation

- Select **OK** to return to Figure 116 on page 124. You can now repeat the sequence to install the other MSM towers (same host data set, member flc001cb for LNM, flc001cd for NetWare) or exit.

5.3 Installing MSM Informal Documentation

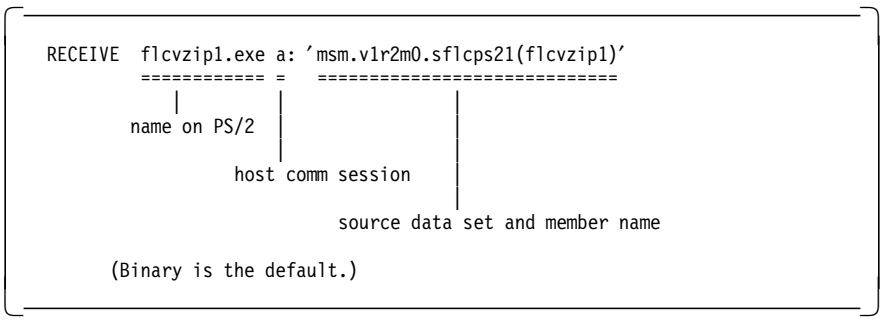
The informal documentation (in BOOK format and READIBM2) is supplied to enable you to read the documents on a PS/2 running OS/2. The following books are supplied:

- MultiSystem Manager Data Model
- User Guide for RODM Access Tool
- User Guide for Build Views Tool
- User Guide for Correlate Utility
- User Guide for Resource Monitor
- Hints and Tips

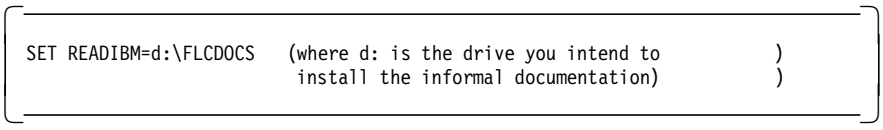
If you already have READIBM2 or IBM′s Book Manager product installed on your PS/2, you will have to install only the bookshelf, so skip to 5.3.2, “Installing the MSM Informal Documentation Bookshelf” on page 130.

5.3.1 Installing READIBM2

1. Create a subdirectory on your PS/2 named READIBM2.
2. Make READIBM2 your current subdirectory. Download MSM.V1R2M0.SFLCPS21(FLCVZIP1) from the host into your READIBM2 subdirectory. Use binary download. The syntax for CM/2 (if you named the MSM data sets MSM.V1R2M0....., as we did) would be:



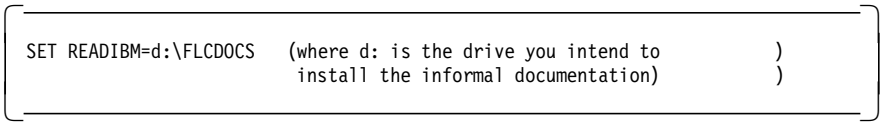
3. Type FLCVZIP1. The self extracting ZIP file will unload the READIBM2 parts.
4. In your CONFIG.SYS, add the READIBM2 subdirectory to your:
   - PATH statement
   - LIBPATH statement
   - DPATH statement
   - HELP statement
5. Add the following line to your CONFIG.SYS:



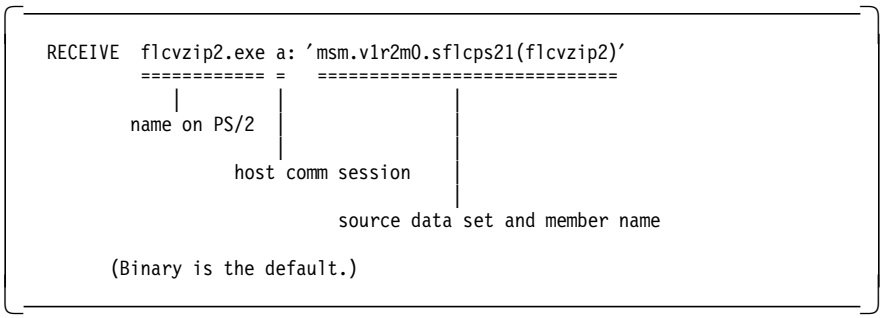
6. Boot your system to make the new CONFIG.SYS values take effect.

5.3.2 Installing the MSM Informal Documentation Bookshelf

1. Create a subdirectory on your PS/2 named FLCDOCS.
2. If you haven't already done so, add the following line to your CONFIG.SYS:



   and boot your system to make the new CONFIG.SYS values take effect.
3. Make FLCDOCS your current subdirectory. Download FLC.V1R2M0.SFLCPS21(FLCVZIP2) from the host into your FLCDOCS subdirectory. Use binary download. The syntax for CM/2 (if you named the MSM data sets MSM.V1R2M0....., as we did) would be:



4. Type FLCVZIP2. The self extracting ZIP file will unload the bookshelf and books.
5. Type FLCVDOCS. The .CMD file will invoke READIBM and open the bookshelf.

5.3.3 Temporary Install into a Single Subdirectory

This is a quick way if you just want to see what is in these books.

1. Create a subdirectory on your PS/2.
2. Make the subdirectory you just created your current directory and download the two parts FLCVZIP1.EXE and FLCVZIP2.EXE as shown before.
3. Type FLCVZIP1 and after the file expands type FLCVZIP2.
4. Type FLCVDOCS. The .CMD file will invoke READIBM and open the bookshelf.

Chapter 6. MSM Data Models and Usage for IP

MSM stores the topology of its managed networks in the RODM data cache using object-oriented technology and the GMFHS, SystemView and MSM data models. You can take advantage of this and use it in your own tailored management and automation processes.

To hide the complexity of this process, MSM provides applications and tools you can use:

- MSMAccess

  This is a high-speed REXX interface for RODM API calls. It is actually the application which the MSM topology manager uses to update RODM.

- BLDVIEWS

  This is a sample REXX CLIST, based on MSM Access, also known as FLCARODM, which is shipped with the MSM base code. BLDVIEWS can be used to tailor your presentation views of all defined objects in RODM. You can use it to build customized views and exception views.

- CORRELATE

  This is a sample REXX CLIST, also based on FLCARODM. CORRELATE can use the MAC addresses in each of the agent's (IP, LNM and NetWare) views of the same LAN adapter to present one coordinated view of the adapter.

Before you can take advantage of these tools, you need to have an understanding of object-oriented concepts such as:

- Class
- Instance
- Objects
- Linking objects

You will find a quick introduction to these concepts in *Overview of IBM NetView RODM and Data Models, GG24-3956*.

You can use the *Applied Use of IBM NetView RODM and Automation, GG24-4018*, to understand how RODM uses the data models and the definitions of:

- Fields
- Subfields
- RODM API
- RODM MAPI
- Methods

A detailed description of the data models can be found in the

- *NetView RODM Programming Guide* for the GMFHS data model
- *NetView IBM NetView MultiSystem Manager MVS/ESA Topology Data Model Reference* for the MSM data model

In this chapter we will discuss only the classes, fields and logic of the data model that are most important in understanding how MSM manages its networks.

6.1 Overview

MSM is designed as a NetView application using RODM and GMFHS to manage and show in a graphical way multiprotocol networks. It will do this through a manager-agent relationship. This is defined by:

- Management Resources. These are the agents or, in SNA terms, service points. The service point is an application that handles the communication to its manager and managed resources. It will report status and topology changes to its manager and works as the focal point for commands from the manager to its managed resources.
- Managed Resources. These are the resources managed by the agent. The communication with the manager is through the agent, using the RUNCMD command.
- Graphical presentation. The graphical layout and configuration are defined in the different data models. MultiSystem Manager uses part of the GMFHS data model for presentation, service point definition and services and the SystemView data model for for the managed resource definition.

6.2 GMFHS Data Model

The GMFHS data model is organized around four major classes. All four classes are children of the UniversalClass in RODM.

- Agent_Parent_Class

  Under this class you will find the definition of how the agents communicate with their manager.

- Name_Space_Parent_Class

  This class contains the resource types for all objects, so GMFHS can translate them into view icons.

  The objects defined under the DisplayResourceType class are the different icons and their presentation attributes. MSM links its resources to these objects for presentation purposes.

- GMFHS_Displayable_Objects_Parent_Class

  This class contains:

  – All object definitions for real resources managed by GMFHS. MSM creates its real resource objects under SystemView data model and private classes.

  – Domain definitions for non-SNA and SNA domains:

    - SNA domain defines the NetView domain which will receive alerts from the agents.

    - Non_SNA domain defines an element manager that is running under the control of an agent.

MultiSystem Manager uses the field definitions and design of the domain definitions (using GMFHS methods) to manage its agents through commands and MSUs.

  - Aggregate resources and their rules of aggregation.

    MSM uses these rules and design (using GMFHS methods) for aggregation.

  - Shadow objects. Since GMFHS does not manage or show SNA resources, you can define them here to build a complete view of the SNA and non-SNA parts of your network.

    MultiSystem Manager does not use any of the shadow definitions, but they can be used to link, for example, an SNALINK IP connection to the SNA LUs.

- The Presentation_Service_Class defines how the views should be presented to the end user interface.

  This part of the GMFHS data model can be called a presentation, platform which is available to any other data model.

6.3 SystemView Data Model

The SystemView data model provides detailed definition of enterprise-wide systems management data that can be used by SystemView products across operating system platforms. The roles defined by the SystemView structure ensure the ability to share data among application programs.

SystemView:

- Defines the information that passes between the managing applications and the end user through the service of the *End-Use Dimension*.
- Defines the data that managing applications are sharing using the *Data Dimension* structure.
- Defines the information that flows between the *managing applications*.
- Defines the way information is passed between the managing applications and managed resources using *common management protocols*.

MSM has implemented a part of the SystemView data model using object-oriented technology provided by the resource object data manager (RODM). To manage its resources, it uses the classes conforming to the SystemView data model and creates the instances under these classes dynamically.

6.4 MSM Data Model

MSM has implemented an object-oriented approach, which means the network is defined through abstract object definitions. These definitions are referred to as the MultiSystem Manager data model.

There are two definition sets for a data model:

- **The data model structure**. This is the definition of the data model classes and their fields with initial values including the methods used by the data model. MSM uses the GMFHS data model and the SystemView data model

plus some private classes which are defined on top of the SystemView data model.

Refer to 5.1.7.1, “Data Model Installation” on page 122 to see how to load the data model structure.

- **The data model instances**. The instances are the objects and the associate values defined under the classes. MultiSystem Manager creates the objects dynamically, based on the topology information received from its agents.

In this way MSM can take advantage of the GMFHS design for view presentation, navigation, aggregation, alert history and command support provided by GMFHS.

6.4.1 MSM Data Model Files

FLCSDM1 This file defines SystemView classes that are common to MSM and the APPNTAM feature. If you have already installed the APPNTAM feature, you don’t need to load this file again, so comment the DD statement out of the loader job.

FLCSDM2 This file defines the SystemView classes for the LNM and Novell features.

FLCSDM3 The statements in this file define private MSM classes for the LNM and Novell features.

FLCSDM4 This file defines the default threshold values set by MSM for real and aggregate resources for the LNM and Novell features.

FLCSDM5 These are the field definitions that are used for view navigation for the LNM and Novell features. This is done by linking objects under the GMFHS presentation classes with objects under the SystemView and MSM classes.

FLCSDM64 This file defines the special MSM display resource types.

FLCSDM7 This file defines SystemView MSM classes for IP.

FLCSDM8 This file defines private MSM classes for IP.

FLCSDM9 These are the field definitions which are used for view navigation.

FLCSDM10 This file defines some default values for IP resources.

Even if you install only the IP tower, you have to load all the files.

6.4.2 MSM Classes

To use the GMFHS presentation platform MultiSystem Manager has defined five SystemView classes in its data model for IP:

- 1.3.18.0.0.3321 collectionOfSpots
- 1.3.18.0.0.3327 autonomousSystem
- 1.3.18.0.0.3328 internet
- 1.3.18.0.0.3329 internetHost
- 1.3.18.0.0.3330 internetRouter

In addition to the SystemView classes, MSM also defined six private classes:

- autonomousSystems
- interface
- internetGraphSegment
- internetHub
- internetBridge
- interfaceLink

MSM also defines some additional private attributes to the SystemView data model classes. These attributes are used to link (to create relationships) MSM objects with GMFHS data model objects for use of the presentation service of the GMFHS data model.

These attributes are defined with the same names as those found in the GMFHS data model and with the same behavior characteristics. In this way MSM can use the same GMFHS methods.

The following table is an example how MSM uses the presentation field display for its objects. A complete list can be found in the *IBM NetView MultiSystem Manager MVS/ESA Topology Data Model Reference SV40-0093*.

Table 3. Resource Information Fields and Values

NGMF Name	RODM Field	MSM Usage
Name	*DisplayResourceName*	In general this is the OSI name of the resource and is also used as last RDN in the OSI DN stored in MyName.
Other Data	*DisplayResourceOtherData*	For every resource, this is built with topology information stored in RODM (max 254 char.).
Type	*DisplayResourceType*	For every resource, this is built with values supported by GMFHS.
Customer data	*DisplayResourceUserData*	MSM uses this field for remote console. It can be used for customer data, but then the remote console function wouldn′t be available

To make the deletion of objects easier, MSM has defined a private field Purge, to SystemView and MSM private classes. MSM will store information here that it will use for the delete process.

One of the following values is set by MSM:

0 The real object and its link may be removed.

1 The real object cannot be removed. The object links to other objects, where Purge=0, may be removed.

2 The object and its links cannot be removed.

6.5 Managing Resource

When a NetView/6000 agent is added to the network, MSM has to create the objects in RODM to represent it. Table 4 shows the objects and some of the fields filled by MSM.

Table 4. Objects Created and Some of the Fields Filled

Class	MyId(object name)	Field	Contents
SNA_Domain	RABAN	Netid	USIBMRA
NMG_Class	RA62221A	TransportProtocolName	COS
	AgentStatusEffect	60	
Non_SNA_Domain_Class	RA62221A.RS60001S	EMDomain	RA62221A
	PresentationProtocolName	DOMP020	
	SessionProtocolName	PASSTHRU	
	TransactionProgram	rs60001s	
Agent agentName=RS60001S	systemId=RA62221A, ipHostName	NetworkAddress rs60001	USIBMRA.RA62221A
	TimerId(for heartbeat)	SYS0003	
	heartbeatRate	1800	

Note: To make this more meaningful, the following ASN.1 notations were replaced with their values:

1.3.18.0.0.3315.0.3.1	agent
2.9.3.2.7.4	systemId
1.3.18.0.0.3519	agentName
1.3.18.0.0.3315.0.7.3	heartbeatRate

For the agent the systemId is the LU name and the agentName is the transaction program name of spappId and tralertd which must be the same.

MSM creates links between these objects and the objects defined in the MSM classes. Figure 125 on page 139 shows these links.

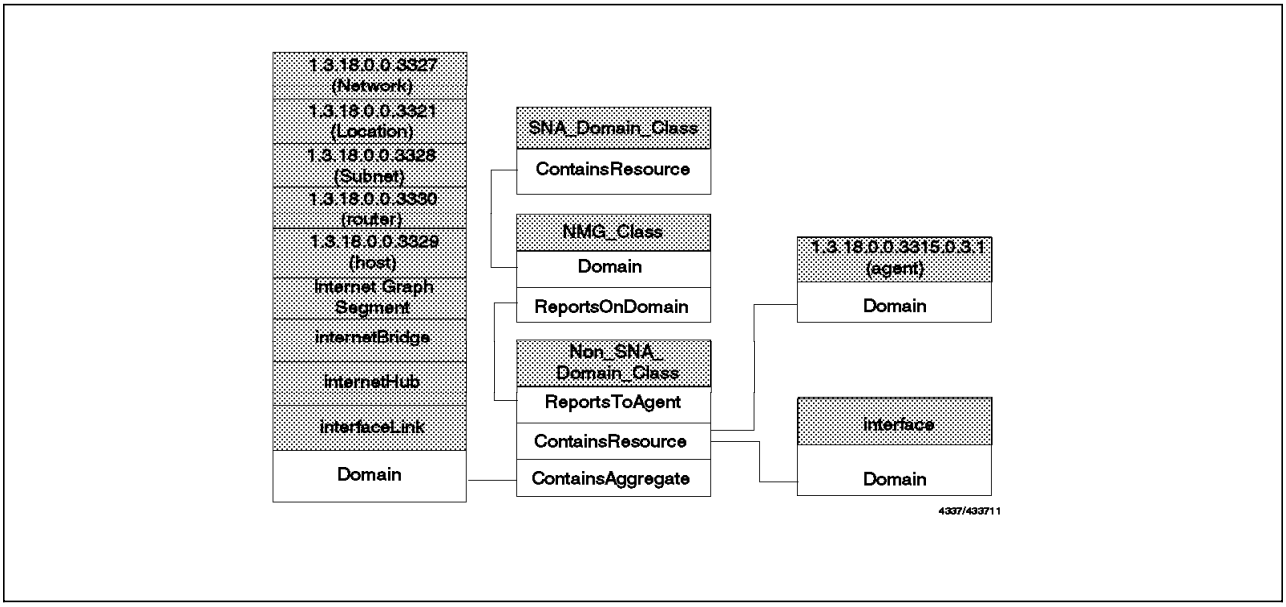


Figure 125. Links Between Managing Resources and MSM Resources

6.6 Managed Resources

When topology information is sent from the NetView/6000 agent to the topology manager, MSM will create objects in RODM. The following list shows one object of each class created by MSM on our network and the contents of some fields:

- Network, class: 1.3.18.0.0.3327

Field	Value
MyName	2.9.3.2.7.4=RA62221A,1.3.18.0.0.3325=RS60001S
DisplayResourceType	DUIXC_RTN_IP_NETWORK_AGG
DisplayResourceName	RA60001A_IP_Network
AggregateContents	IPRES HIDDEN=NO HOSTS=YES UNMANAGED=YES MAP=msm
DisplayStatus	129

- Subnet, class: 1.3.18.0.0.3328

Field	Value
MyName	2.9.3.2.7.4=RA62221A,1.3.18.0.0.3325=9.24.1
DisplayResourceType	DUIXC_RTN_IP_SUBNET_AGG
DisplayResourceName	9.24.1
DisplayStatus	129

- Location, class: 1.3.18.0.0.3321

Field	Value
MyName	2.9.3.2.7.4=RA62221A,1.3.18.0.0.3325=Malibu
DisplayResourceType	DUIXC_RTN_IP_LOCATION

Field	Value
DisplayResourceName	Malibu
DisplayResourceOtherData	Location Name=Malibu
DisplayStatus	129

- Segment, class: internetGraphSegment

Field	Value
MyName	2.9.3.2.7.4=RA62221A,1.3.18.0.0.3555=9.24.1.Seg
DisplayResourceType	DUIXC_RTN_IP_SEGMENT_AGG
DisplayResourceName	9.24.1.Segment1
DisplayResourceOtherData	Segment Name=9.24.1.Segment1, Segment Type=token
DisplayStatus	129

- Router, class: 1.3.18.0.0.3330

Field	Value
MyName	2.9.3.2.7.4=RA62221A,1.3.18.0.0.3343=6611slk
DisplayResourceType	DUIXC_RTN_IP_ROUTER_AGG′
DisplayResourceName	6611slk
1.3.18.0.0.3340	Duane Reeves or Karen Mazzei at T/L 421-7511 or 7186
1.3.18.0.0.3341	IBM 6611 Network Processor 32H Serial Number: 26-DUMMY Software: Multi
1.3.18.0.0.3342	E4-408 Computer Room at Southlake in Roanoke, TX.
DisplayResourceOtherData	Router Name=6611slk, System Contact=Duane Reeves or Karen Mazzei at T/L 421-7511 or 7186., System Description=IBM 6611 Network Processor 32H Serial Number: 26-DUMMY Software: Multi, System Location=E4-408 Computer Room at Southlake in Roanoke, TX.
DisplayStatus	129

- Host, class: 1.3.18.0.0.3329

Field	Value
MyID	2.9.3.2.7.4=RA6010CP,1.3.18.0.0.3343= rs60005.itso.ral.ibm.com
MyName	2.9.3.2.7.4=RA62221A,1.3.18.0.0.3343=9.19.129.14
1.3.18.0.0.3341	IBM RISC System/6000 Machine Type: 0x0201 Processor ID: 00003930 4100 T
1.3.18.0.0.5273	9.24.104.Segment1
DisplayResourceType	DUIXC_RTN_INTERNET_HOST_AGG
DisplayResourceName	rs6004

Field	Value
DisplayResourceOtherData	Host Name=rs60004.itso.ral.ibm.com, System Description=IBM RISC System/6000 Machine Type: 0x0201 Processor ID: 000039304100 T
DisplayStatus	129

- Hub, class: internetHub

Field	Value
MyName	2.9.3.2.7.4=RA62221A,1.3.18.0.0.3343=9.24.32.42
1.3.18.0.0.3341	T01MS Token Ring Management Module (Basic-MGT) v2.10-B pSOS+ SNMP
DisplayResourceType	DUIXC_RTN_IP_HUB_AGG′
DisplayResourceName	9.24.32.42
DisplayResourceOtherData	Hub Name=9.24.32.42, System Contact=Leonard Hand T/L 421.5035, System Description=T01MS Token Ring Management Module (Basic-MGT) v2.10-B pSOS+ SNMP, System Location=Unknown
DisplayStatus	129

- Bridge, class: internetBridge

Field	Value
MyName	2.9.3.2.7.4=RA62221A,1.3.18.0.0.3343=8229BR
1.3.18.0.0.3341	T01MS Token Ring Management Module (Basic-MGT) v2.10-B pSOS+ SNMP
DisplayResourceType	DUIXC_RTN_IP_BRIDGE_AGG′
DisplayResourceName	9.24.32.42
DisplayResourceOtherData	Bridge Name=8229BR , System Contact=Mark DeCain x2330, System Location=LAB - Back Wall′
DisplayStatus	129

- Adapter, class: interface

Field	Value
MyID	2.9.3.2.7.4=RA62221A,1.3.18.0.0.3343=9.24.1.1
DisplayResourceType	DUIXC_RTN_IP_INTERFACE
DisplayResourceName	9.24.1.1
1.3.18.0.0.5273	9.24.1.Segment1
DisplayResourceOtherData	IP Address=9.24.1.1, MAC Address=02608C2C8561
1.3.18.0.0.5263	02608C2C8561

- Link, class: interfaceLink

Field	Value
MyID (OBJECTID)	2.9.3.2.7.4=RA62221A,interfaceLinkName=9.24.1.1
DisplayResourceType	DUIXC_LTN_IP_LINK_AGG

Field	Value
DisplayResourceName	9.24.1.1
MyName	2.9.3.2.7.4=RA62221A,interfaceLinkName=9.24.1.1
DisplayResourceOtherData	IP Address=9.24.1.1, MAC Address=10005AC81099

Figure 125 on page 139 shows the links between the objects and the domain.

6.7 Locations

In NetView/6000 you can define locations and put subnets and routers into them. These location objects (class 1.3.18.0.0.3321) are linked in RODM logically between networks (class 1.3.18.0.0.3327) and subnets (class 1.3.18.0.0.3328) as well as on the same level as subnets and routers (class 1.3.18.0.0.3330). The links that result depend very much on how the location is defined in NetView/6000.

6.8 Presentation Data Model

View objects and relationships are part of the presentation data model for RODM. The presentation data model for RODM consists of common classes and relationships, made available on both the GMFHS data model and SystemView data model. NGMF supports the presentation data model for RODM by automatically providing graphic views, view navigation, status aggregation and alert history for topology managers, such as MSM, which store data and relationships in RODM conforming format with the presentation data model.

The following figure gives you an overview of how the classes and related fields are used and linked together to present a logical view of the managed network.

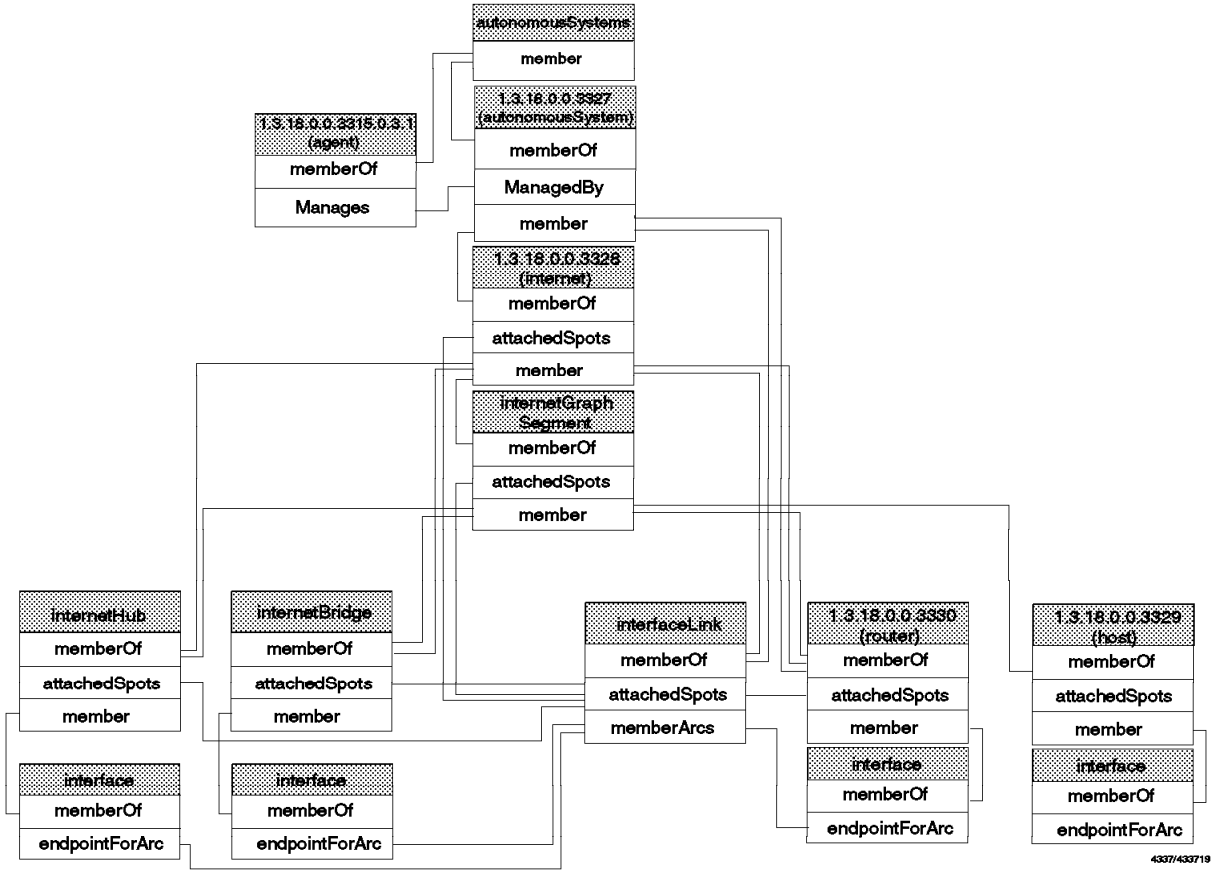


Figure 126. MSM Presentation Links

Figure 127 on page 144 shows how an aggregation parent - aggregation child link between a router and a location is stored in RODM as an example.

```
Fields in RODM for Router object rs60009:

 AggregationParent (OBJECTLINKLIST)
       (OBJECTID) 00010045E420EC06
                  '2.9.3.2.7.4=RA62221A,1.3.18.0.0.'
                  '3325=Malibu'
       (CLASSID)  69
                  '1.3.18.0.0.3321'
       (FIELDID)  121
                  'AggregationChild'

Fields in RODM for Location object Malibu:

 AggregationChild (OBJECTLINKLIST)
       (OBJECTID) 0001004919E6332E
                  '2.9.3.2.7.4=RA62221A,1.3.18.0.0.'
                  '3343=rs60009'
       (CLASSID)  73
                  '1.3.18.0.0.3330'
       (FIELDID)  87
                  'AggregationParent'
```

Figure 127. Link Between Two Objects

6.8.1 Aggregation

Aggregation consists of propagating status changes from child resources to parent resources. Real resources that contribute status to an aggregate will also contribute to the parent of that aggregate (depending on the setting of field AggregationPriorityValue in RODM).

To define the aggregation links MSM uses the following fields:

- AggregationParent
- AggregationChild

Figure 128 on page 145 shows the connection from the class interface up to the aggregate class autonomousSystems

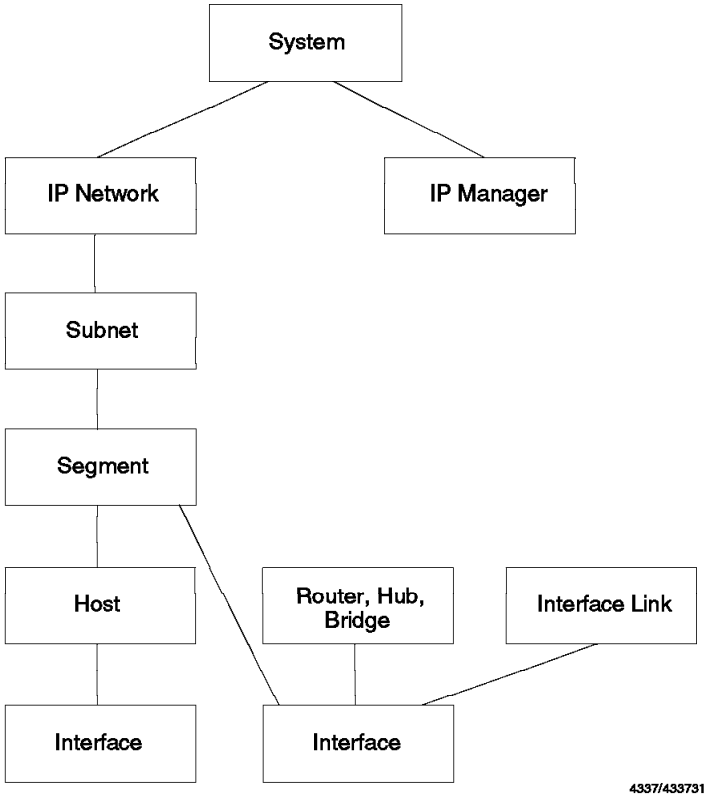


Figure 128. Aggregation Structure

Only objects of the classes interface and agent are used by MSM for aggregation.

6.8.2 NGMF Views

MultiSystem Manager creates a set of graphic views showing your IP networks at various levels of detail. These views are based on topology information and on the information specified in the initialization file or GETTOPO command keywords.

6.8.2.1 Static Views

MultiSystem Manager lets you create and name network views and name the objects appearing in these network views, which represent each of your networks.

Network Views: By default the MultiSystem Manager creates a single network view named MultiSysView.

You can create your own name using:

- DEF_NETWORK_VIEW

in the initialization file or with your GETTOPO command. These view objects are instances under the Network_View_Class of the GMFHS data model.

By using the field ContainsObjects/ContainedInView in the Network_View_Class, nwNetworks, physicalLANNetworks, and/or IPNetworks(Systems) classes, instances of these classes are linked to all the objects of your network under one high level view.

To split your network into more high level views, use the GETTOPO command with the NETWORK_VIEW keyword and MSM will create network views linked only to the resources against which the GETTOPO command was used.

View Objects: MSM creates two aggregate objects that you can tailor to your environment:

- **System Object**

  This represents a group of IP systems.

- **Domain Object**

  This represents a single IP network (a NetView/6000 service point and its monitored resources).

  – If you would like to use your own name for your network views use the NETWORK_VIEW parameter on the GETTOPO command to do so.

  – If you would like to rename your network aggregate objects use the NETWORK_AG_OBJECT parameter on the GETTOPO command.

  – You can allow your IP domain to appear alone on a network view by not aggregating it with other IP systems, specify on the GETTOPO command:

    ```
    NETWORK_AG_OBJECT=NONE
    ```

6.8.2.2 Dynamic Views

More Detail Views: These views are built with the relationship member/memberOf through aggregate resources. Figure 129 on page 147 shows the connection from the aggregate class autonomousSystems to the class interface.

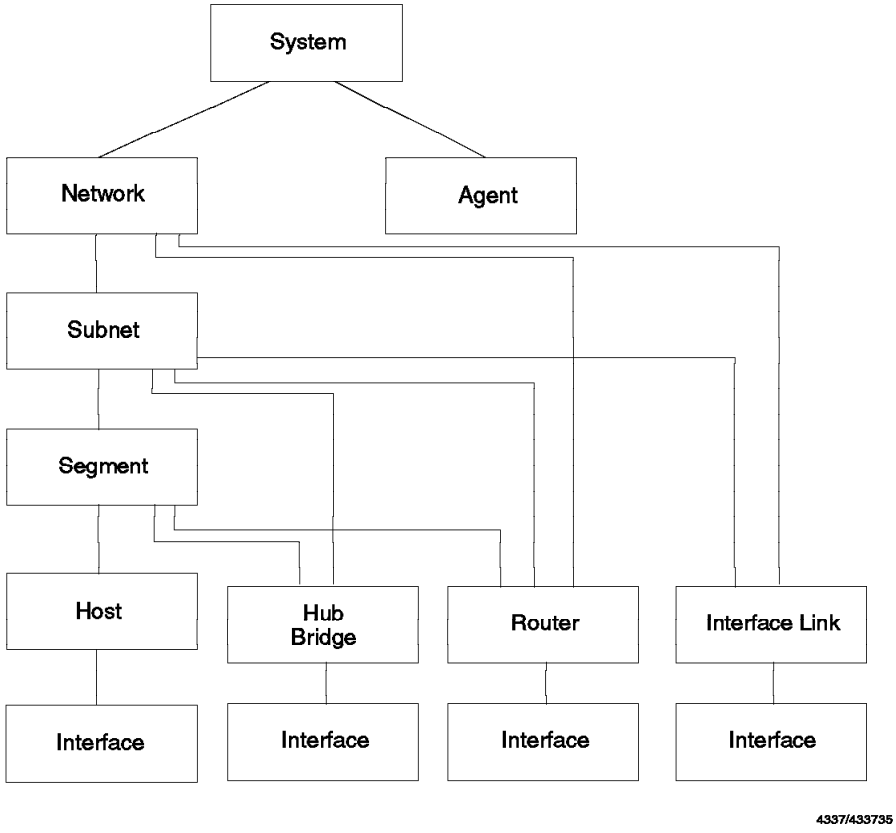


Figure 129. More Detail View Links

Fast Path to Failing Resource: These views are built with the relationship AggregationParent/AggregationChild through aggregate resources.

Configuration Parent and Child Views: These views are built with the relationship ParentAccess/-ChildAccess through aggregate resources. Figure 130 on page 148 shows the connection from the aggregate class autonomousSystems to the object class interface.

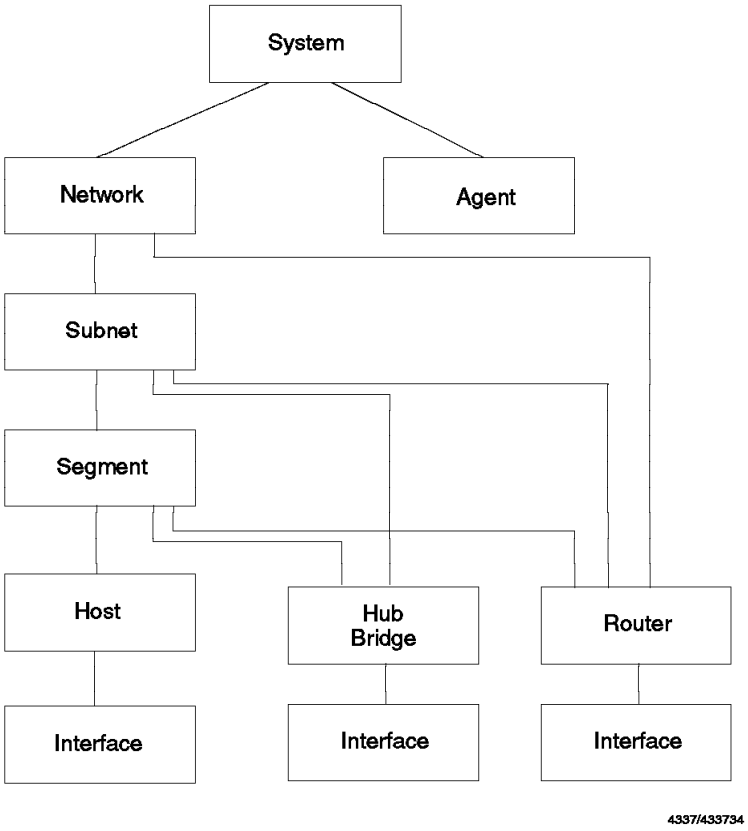


Figure 130. Parent/Child Links

Configuration child views will contain many resources and might not be very useful. Configuration parent views will show the path from the selected resource up to the system aggregate.

Chapter 7. IBM NetView MultiSystem Manager Tools

This chapter describes some tools:

- BLDVIEWS
- Correlate Utility
- NETVCMDX
- RODMTool/2
- NetView Resource Monitor

BLDVIEWS, Correlate Utility and NetView Resource Monitor are shipped as MSM optional material. NETVCMDX and RODMTool/2 are available to IBM employees from MKTTOOLS, please see your IBM representative for details.

7.1 BLDVIEWS

BLDVIEWS is a REXX CLIST that uses FLCARODM to build customized views and aggregate objects. You can specify the aggregate resources and views you want to create along with the resources that you want them to contain. You can link these new aggregates to existing objects in your views. You can also change the aggregation settings from the MSM defaults to the values you prefer.

To get a complete description of BLDVIEWS, see the user guide in the MSM Informal Documentation - refer to 5.3, “Installing MSM Informal Documentation” on page 129.

The input parameters can be taken from different sources:

- Sequential data set
- Member of a partitioned data set
- NetView Pipe

For example we created a member VIEW1 in our DSICLD data set:

```
BLDVIEWS NETVIEW.NV24.RABAN.DSICLD(VIEW1)
```

BLDVIEWS defaults to the ddname DSIPARM. If your input parameter member is in dsiparm you just specify the member name. For this example our member VIEW2 was in our DSIPARM data set:

```
BLDVIEWS VIEW2
```

7.1.1 Required CMDMDL Statements for BLDVIEWS

Add the following statements to DSICMD:

```
FLCVBLDV CMDMDL    MOD=DSICCP
         CMDSYN  BLDVIEWS
FLCVDELV CMDMDL    MOD=DSICCP
         CMDSYN  DELVIEWS
```

7.1.2 Aggregation Thresholds

MSM uses default values for aggregation thresholds that may not suit your installation.

With BLDVIEWS you have the ability to change the aggregation thresholds for any aggregate resources, including the aggregates you create with BLDVIEWS. The aggregation thresholds are:

- ThresholdDegraded
- ThresholdSeverlyDegraded
- ThresholdUnsatisfactory

They are specified in real resources and are the minimum number of real resources underneath the aggregate, in unsatisfactory states, required for the aggregate to change status.

7.1.2.1 Setting Thresholds by Number of Resources

MSM defaults the threshold values for IP-HOSTS, IP-ROUTERS, IP-HUBS and IP-BRIDGES as follows:

- ThresholdDegraded=1
- ThresholdSeverlyDegraded=2
- ThresholdUnsatisfactory=3

This is absolutely incorrect for IP-Hosts, IP-Hubs and IP-Bridges because they report only one interface. It is only partly correct for IP-ROUTERS. Therefore we set the aggregation values for Hosts, Hubs and Bridges to:

- ThresholdDegraded=1
- ThresholdSeverlyDegraded=1
- ThresholdUnsatisfactory=1

The BLDVIEWS input statement to do this is:

```
IPSPNAME=RA60O5CP.RS60OO5S
IPHOST=ALL,AGGTHRESH=(#1,#1,#1)
IPHUB=ALL,AGGTHRESH=(#1,#1,#1)
IPBRIDGE=ALL,AGGTHRESH=(#1,#1,#1)
```

A good starting value for IP-ROUTERS would be:

- ThresholdDegraded=1
- ThresholdSeverlyDegraded=1
- ThresholdUnsatisfactory=2

The BLDVIEWS input statement to do this is:

```
IPSPNAME=RA6005CP.RS60005S
IPROUTER=ALL,AGGTHRESH=(#1,#1,#2)
```

The above example is good for routers with 2 or 3 interfaces. If a router has more interfaces, you can change the values for this router only. Our router TRIDNX2 has seven interfaces so we set the threshold values:

- ThresholdDegraded=1
- ThresholdSeverlyDegraded=4
- ThresholdUnsatisfactory=6

The BLDVIEWS input statement to do this is:

```
IPROUTER=tridnx2,AGGTHRESH=(#1,#4,#6)
```

If the threshold value you specify is greater than the number of resources, BLDVIEWS will set the threshold to the number of resources.

7.1.2.2 Setting Thresholds by Percentage of Resources

For segments, locations, subnets and internets, the MSM defaults are absolute numbers. BLDVIEWS allows you to specify the thresholds as percentages of the number of resources.

In the following example, if more than 20% of the resources are unsatisfactory, we will put the aggregate resource into degraded, if more than 50% into severely degraded and if more than 90% into unsatisfactory.

```
*-------------------------------------------------------------
*  Input parameters for BLDVIEWS
*-------------------------------------------------------------
* first define the service point. this is a must for IP
*-------------------------------------------------------------
IPSPNAME=RA6005CP.RS60005S
*-------------------------------------------------------------
* Set value threshold for all IP system clusters
*-------------------------------------------------------------
CLUSTER=ALL,AGGTHRESH=(%20,%50,%90),TYPE=IP
*-------------------------------------------------------------
* Set value threshold for all IP networks
*-------------------------------------------------------------
NETWORK=ALL,AGGTHRESH=(%20,%50,%90),TYPE=IP
*-------------------------------------------------------------
* Set value threshold for all IP networks
*-------------------------------------------------------------
NETWORK=ALL,AGGTHRESH=(%20,%50,%90),TYPE=IP
*-------------------------------------------------------------
* Set value threshold for all subnets
*-------------------------------------------------------------
IP_SUBNET=ALL,AGGTHRESH=(%20,%50,%90)
*-------------------------------------------------------------
* Set value threshold for all segments
*-------------------------------------------------------------
IP_SEGMENT=ALL,AGGTHRESH=(%20,%50,%90)
*-------------------------------------------------------------
```

BLDVIEWS queries the aggregate's TotalRealResourceCount field and then multiplies it by the specified percentages to calculate the new values for the thresholds.

If resources are later added or deleted from an aggregate, it may be necessary to rerun BLDVIEWS to readjust the thresholds.

This could be part of your automation. Trap the alert when the topology has changed and readjust your thresholds. Another way would be to trigger a change method when the TotalRealResourceCount changes.

Only real resources of the classes interface and agent are used for aggregation.

7.1.3 Generic Commands and Console Commands

You can also set the values for the generic commands and for remote console. We set the remote console to TELNETPM and the display to rping:

```
IPSPNAME=RA62221A
IP_HOST=ALL,
CONSOLE='TELNETPM %NAME%',
DISPLAY='asis rping -n 2 %NAME%'
IP_ROUTER=ALL,
CONSOLE='TELNETPM %NAME%',
DISPLAY='asis rping -n 2 %NAME%'
IP_ADAPTER=ALL,
CONSOLE='TELNETPM %NAME%',
DISPLAY='asis rping -n 2 %NAME%'
```

Note: If you use the NETVCMDX exit you might want to use the default display commands provided there.

7.1.4 Build Your Own Views

If you would like to group your monitored resources presented by NGMF, you can use BLDVIEWS to do so. You can choose any grouping you want. For example by:

- System and network
- Type of network
- Geographical
  - Locations
  - Regions
  - Buildings
  - Floors
- Individual operator responsibilities

BLDVIEWS supports two types of views:

- Network views
- Exception views (network views). Exception network views are views that will contain the resources you specify only when they go into a not satisfactory state.

7.1.4.1 Network View

BLDVIEWS is a static process. This means that the views built by the BLDVIEWS CLIST are up-to-date the moment you run the CLIST. Any topology change (delete/add) of real resources is not reflected in your personal views. You have to build your own automation process using messages, alerts or methods to keep your views accurate.

This is an example of a custom built view:

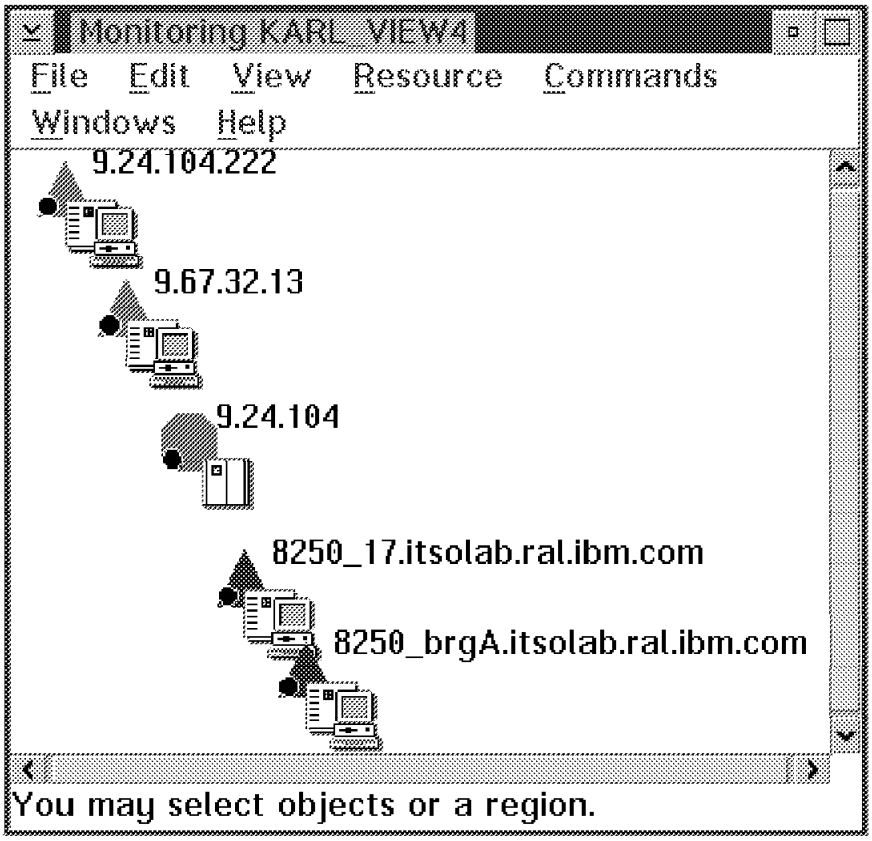


Figure 131. Customized View

The control statements for this view are as follows:

```
*-------------------------------------------------------------
*  Input parameters for BLDVIEWS
*-------------------------------------------------------------
VIEW=KARL_VIEW4,annotation='Important things'
IPSPNAME=RA6005CP.RS60005S
IP_BRIDGE=ALL
IP_HUB=ALL
IP_SUBNET=9.24.104
```

Instead of specifying ALL or a specific name you can also use wildcards. For example, you can specify IP_ROUTER=RS6*, which will put all routers with names starting with rs6 into the view.

7.1.4.2 Exception View

To simplify the monitoring of your resources, you can build exception views to monitor critical resources. Resources not in satisfactory state will be shown in an exception view. With the EVIEW control card you define the exception view and all resources which should be under this view when they turn into a not satisfactory state. IP resources that can be put into an exception view are:

- Adapters
- Hosts
- Routers
- Hubs
- Bridges

To create a view with all IP resources that are not in satisfactory state the control statement would be:

```
EVIEW=KARL_EXCP_VIEW1,ANNOTATION='Exception View All TCP/IP'
IPSPNAME=RA6005CP.RS6005S
IP_HOST=ALL
IP_ROUTER=ALL
IP_HUB=ALL
IP_BRIDGE=ALL
INTERFACE=ALL
```

More useful would be to show bridges, hubs and routers that are not in satisfactory state. The control statement would be:

```
EVIEW=KARL_EXCP_VIEW2,ANNOTATION='Exception View All Routers'
IPSPNAME=RA6005CP.RS6005S
IP_ROUTER=ALL
IP_BRIDGE=ALL
IP_HUB=ALL
```

You may want to put some specific resources into an exception view. The control statement would be:

```
EVIEW=KARL_EXCP_VIEW3,ANNOTATION='Exception View Specific'
IPSPNAME=RA6005CP.RS6005S
IP_HOST=9.24.104.82
IP_HOST=9.24.104.83
```

When you run BLDVIEWS, it will search RODM for the specified resources and put them in the views if they are not in satisfactory state. To update the views you have to provide an automation table entry for:

- LNM alerts and resolution alerts
- NetWare alerts and resolution alerts
- IP alerts

These alerts have to trigger the FLCVXVU CLIST, which links or unlinks these resources to the exception view. The automation table entry for IP resources is:

```
IF MSUSEG(0000.10(*).11(*).02 3)='5696-3620'.
THEN
  EXEC(CMD('FLCVXVU') ROUTE(ONE AUTOIPA))
  CONTINUE(Y);
IF MSUSEG(0000.10(*).11(*).02 3)='5696-7310'.
THEN
  EXEC(CMD('FLCVXVU') ROUTE(ONE AUTOIPA))
  CONTINUE(Y);
```

7.1.4.3 Deletion of Views

You may not want any of the customized views anymore. So there is a way to delete them.

For example, if you want to delete the view KARL_EXCP_VIEW3, you enter from the NetView command line:

```
DELVIEWS KARL_EXCP_VIEW3
```

7.1.4.4 Deletion of Objects from Exception Views

There might be some resources in an exception view that you don't want to see any more but you want to keep them in the standard views and in RODM. You can do this with the DELETE_FROM_EXCEPTION_VIEW command provided by the NETVCMDX exit. See 7.3, "NETVCMDX - NetView Host REXX CLIST and NGMF Cmd Exit" on page 161

7.1.5 BLDVIEWS After GETTOPO

You can call BLDVIEWS (as you can any other CLIST) from your NCCF screen, or from another CLIST or trigger it through your automation table.

Since all the views built with BLDVIEWS are static, you have to find a way to keep them current. One way to do this is to update your views every time a GETTOPO or INITTOPO command is issued. The GETTOPO process will issue a FLC049I message when the topology update for the specific service point has been successfully completed:

```
C RABAN FLC049I GETTOPO COMMAND FOR SERVICE POINT RA62221A HAS COMPLETED
        SUCCESSFULLY.
```

Since the GETTOPO process retrieved all available topology information from this service point and updated RODM, we can now:

- Change values for aggregation threshold
- Update the customized views
- Update the exception views

In the automation table we will filter out the service point name and call BLDGET CLIST to call BLDVIEWS:

Automation Table

```
************************************************************
*  BLDVIEWS after GETTOPO                                  *
*                                                          *
************************************************************

IF (MSGID='FLCO49I' & TEXT=. 'SERVICE POINT ' SPNAME .)
  THEN EXEC(CMD('BLDGET ' SPNAME) ROUTE(ONE AUTOIPA)
  CONTINUE(Y);
************************************************************
```

BLDGET CLIST

```
/************************************************************
/*                                                          *
/*   BLDGET  : Create a procedure to issue a BLDVIEWS after a  *
/*             GETTOPO run.                                 *
/*                                                          *
/*   Syntax: BLDGET input SPname                            *
/*             BLDVIEWS parameters are stored in DSIPARM    *
/*             membername=Bspname (first 7 char)            *
/************************************************************
arg spname
say '*********************************************************'
say 'BLDVIEWS starts for SERVICE POINT = ' spname
say '*********************************************************'
bldpar= 'B' || substr(spname,1,7)
'BLDVIEWS' bldpar
exit
```

We used a CLIST instead of calling BLDVIEWS directly from the automation table because you could do more from the CLIST like calling the correlate utility.

Because we have to store all the input parameters for BLDVIEWS as a member in a PDS data set, we created a member for each service point in the DSIPARM data set (the default data set for BLDVIEWS) and used B concatenated to the service point name as the PDS member name.

If the IP network you are managing is dynamic (many resources added and removed, and new discoveries) you have to consider that each time a new resource is added a GETTOPO is issued and will then trigger BLDVIEWS.

7.1.6 Sample Input for BLDVIEWS

BRA6005c - Sample Input Parameters

```
IPSPNAME=RA6005CP.RS60005S
NETWORK=ALL,AGGTHRESH=(5%,6%,90%),TYPE=IP
CLUSTER=ALL,AGGTHRESH=(5%,6%,90%),TYPE=IP
IP_LOCATION=ALL,AGGTHRESH=(50%,60%,90%)
IP_SEGMENT=ALL,AGGTHRESH=(50%,60%,90%)
IP_SUBNET=ALL,AGGTHRESH=(5%,6%,90%)
NETWORK=ALL,AGGTHRESH=(5%,6%,90%),TYPE=IP
IP_HOST=ALL,AGGTHRESH=(#1,#1,#1),
CONSOLE='TELNETPM %NAME%'
IP_HUB=ALL,AGGTHRESH=(#1,#1,#1),
CONSOLE='TELNETPM %NAME%'
IP_BRIDGE=ALL,AGGTHRESH=(#1,#1,#1),
CONSOLE='TELNETPM %NAME%'
IP_ROUTER=ALL,AGGTHRESH=(#1,#1,#2),
CONSOLE='TELNETPM %NAME%'
INTERFACE=ALL,
CONSOLE='TELNETPM %NAME%'

EVIEW=KARL_EXCP_VIEW1,ANNOTATION='Exception View All TCP/IP'
IPSPNAME=RA6005CP.RS60005S
IP_HOST=ALL
IPROUTER=ALL
IP_HUB=ALL
IP_BRIDGE=ALL

EVIEW=KARL_EXCP_VIEW2,ANNOTATION='Exception View Specific'
IPSPNAME=RA6005CP.RS60005S
IP_HOST=9.24.104.82
IP_HOST=9.24.104.83
IP_HOST=6611ral
IP_ROUTER=6611ral
IP_ROUTER=lablnm

EVIEW=KARL_EXCP_VIEW3,annotation='Exception View All Routers'
IPSPNAME=RA6005CP.RS60005S
IP_ROUTER=ALL
IP_HUB=ALL
IP_BRIDGE=ALL

VIEW=KARL_VIEW4,annotation='Important things'
IPSPNAME=RA6005CP.RS60005S
IP_BRIDGE=ALL
IP_HUB=ALL
IP_SUBNET=9.24.104
IP_ROUTER=lab_6611
IP_HOST=9.24.104.82
IP_HOST=9.24.104.83
IPSPNAME=RA6010CP.RS60010S
IP_BRIDGE=9.24.104.222
```

7.2 CORRELATE

FLCVCORR uses FLCARODM to query RODM fields which identify (for example) the LAN adapter MAC address of different objects. When two or more resources are discovered which have the same MAC address, a GMFHS Peer View can be created and RODM links created to define those objects as members of that Peer View. The names of the views are COR_xxx where xxx is the value of the field which is common to to the correlated objects, in our example the MAC address of the adapter.

To get a complete description of FLCVCORR see the User Guide in the MSM Informal Documentation - refer to 5.3, “Installing MSM Informal Documentation” on page 129.

7.2.1 Invoking FLCVCORR

Issue FLCVCORR from the NetView command line:

Command Syntax

```
FLCVCORR input_spec_file (FUNCTION=xxx) (TRACE=yyy)
```

- input_spec_file

  This is a member in DSIPARM which contains the input to the correlate utility. If not specified the default FLCVCORS is used. A sample FLCVCORS is supplied in SFLCSMP1. This sample will provide input data to correlate MAC addresses of objects created by MSM. The statement to correlate APPNTAM generated objects is commented out. The syntax is as follows:

  CLASS=RODM class, ATTR=RODM field that you want to compare.

  The following samples from FLCVCORS are for MSM generated objects:

  - CLASS=tokenRingAdapter ATTR=1.3.18.0.0.5263 LNM
  - CLASS=1.3.18.0.0.3315.8.3.4 ATTR=1.3.18.0.0.3518 NetWare servers
  - CLASS=1.3.18.0.0.3482 ATTR=1.3.18.0.0.5263 NetWare requesters
  - CLASS=interface ATTR=1.3.18.0.0.5263 IP

  The following sample from FLCVCORS is for APPNTAM generated objects:

  - CLASS=1.3.18.0.0.2089 ATTR=1.3.18.0.0.2117

- FUNCTION

  Valid values for the FUNCTION keyword are:

  - CORRELATE

    This is the default. Correlate based on the input file.

  - DELETE_EMPTY_peer_views

    This will delete any Configuration Peer Views created by FLCVCORR that contain no objects anymore.

  - DELETE_ALL_peer_views

    This will delete all Configuration Peer Views created by FLCVCORR.

- TRACE

  Valid values for the TRACE keyword are:

NONE No tracing

LOW The default - displays messages indicating the actions taken on objects.

HIGH Display messages indicating all objects being checked

You can use the trace messages to create additional links in RODM, like linking a LAN adapter to an IP host.

The views generated by FLCVCORR are static and will not be accurate anymore if the network has changed. You have to provide for automation to run FLCVCORR, similar to that shown for BLDVIEWS in 7.1.5, “BLDVIEWS After GETTOPO” on page 155.

7.2.2 Select a Correlation View

To see a correlation view, select an object (here a LAN adapter) in a view, then select **Resource**, **Configuration** and **Peers**:

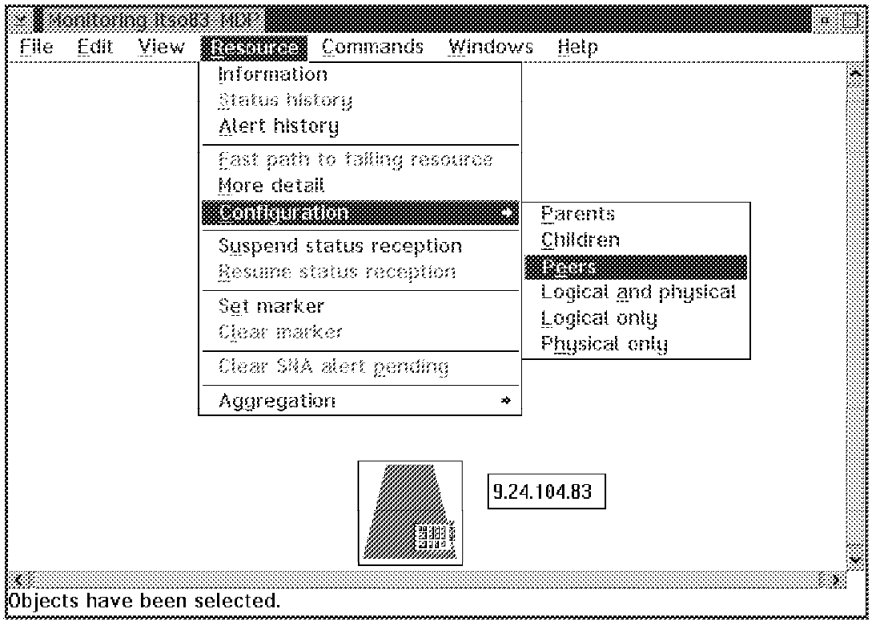


Figure 132. Select a Correlation View

7.2.3 Correlation View

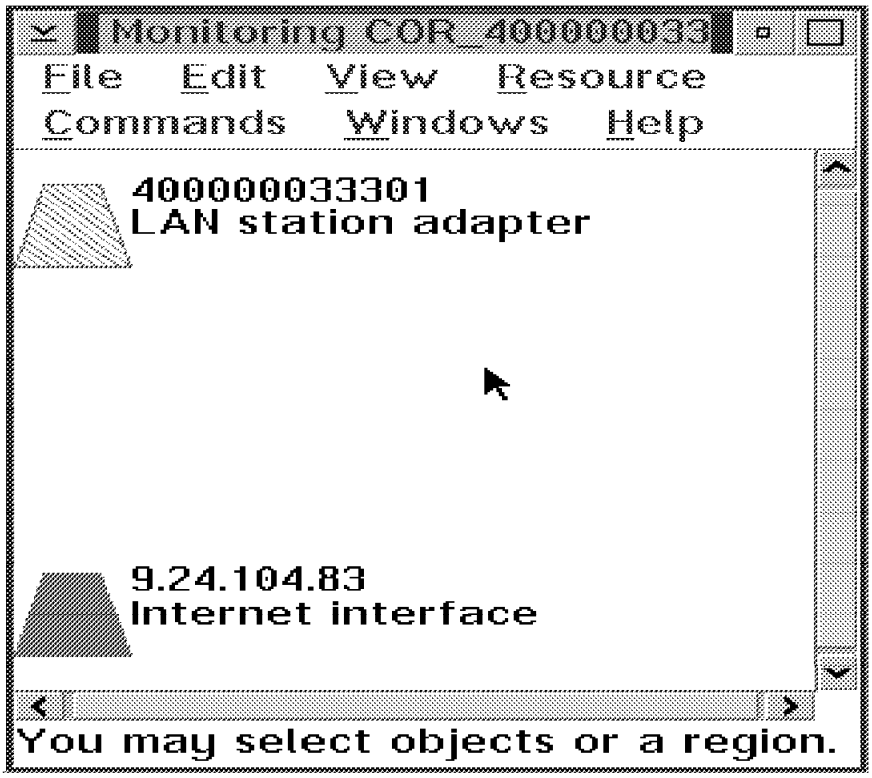


Figure 133. Correlation View

This view shows one adapter managed by an IP agent and an LNM agent. In our case the adapter has unsatisfactory status to IP and satisfactory to LNM. For problem determination this means the adapter is responding to LAN requests, but TCP/IP is not active.

7.2.4 Presentation Links

CORRELATE creates the following links in RODM:

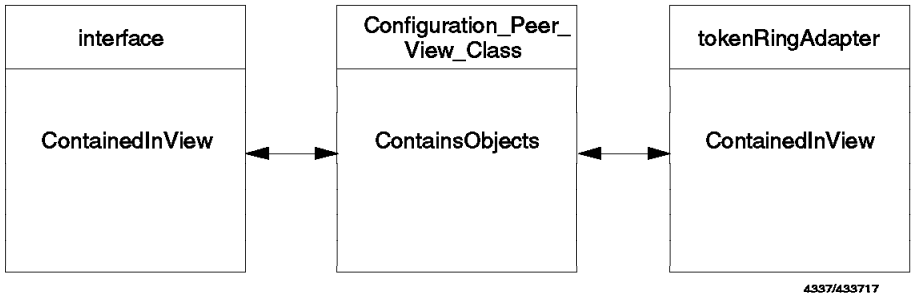


Figure 134. Presentation Links

7.3 NETVCMDX - NetView Host REXX CLIST and NGMF Cmd Exit

This is a two-part application that allows the NGMF user to issue customized commands from the NGMF command pull-down window.

NETVCMDX is available to IBM employees from MKTTOOLS - see your IBM representative for details.

This application only supports non-SNA resources in RODM. It does not support SNA resources managed by Statmon.

The parts of this application are:

- NETVCMDX CLIST running in host NetView
- NETVCMDX NGMF command exit
- NETVSPAN CLIST for span of control checking
- DMCS CLIST for span of control checking

When an operator selects a resource from a view on the NGMF workstation and selects the appropriate command, the NGMF REXX command exit NETVCMDX.CMD gets control. The RODM object ID of the resource selected is passed to NETVCMDX along with a sub_command, and an optional sub_command parameter. NETVCMDX.CMD then returns with `NETVCMDX object_id sub_command sub_command_parm`. That value is then sent up to host NetView by NGMF and is passed to the NETVCMDX Host REXX clist.

This NetView Host REXX clist queries RODM information on the resource and then issues the intended command. The resulting output of the command is displayed in the NGMF Command Response window.

7.3.1 Installation

- Host NetView
  - Copy the NETVCMDX REXX, the NETVSPAN and the DMCS CLIST into a library that is concatenated to DSICLD.
- NGMF
  - Copy the NETVCMDX.CMD and the NETVCMDX.EXE file to a directory that is reachable via the path statement in the CONFIG.SYS file.
  - Add the commands to your NGMF command profile. We used separate command sets for generic, LAN, Novell and TCP/IP commands.

7.3.2 NETVCMDX - Simple and Quick to Use

Figure 135 on page 162 shows how to use NETVCMDX and Figure 136 on page 162 shows part of the result.

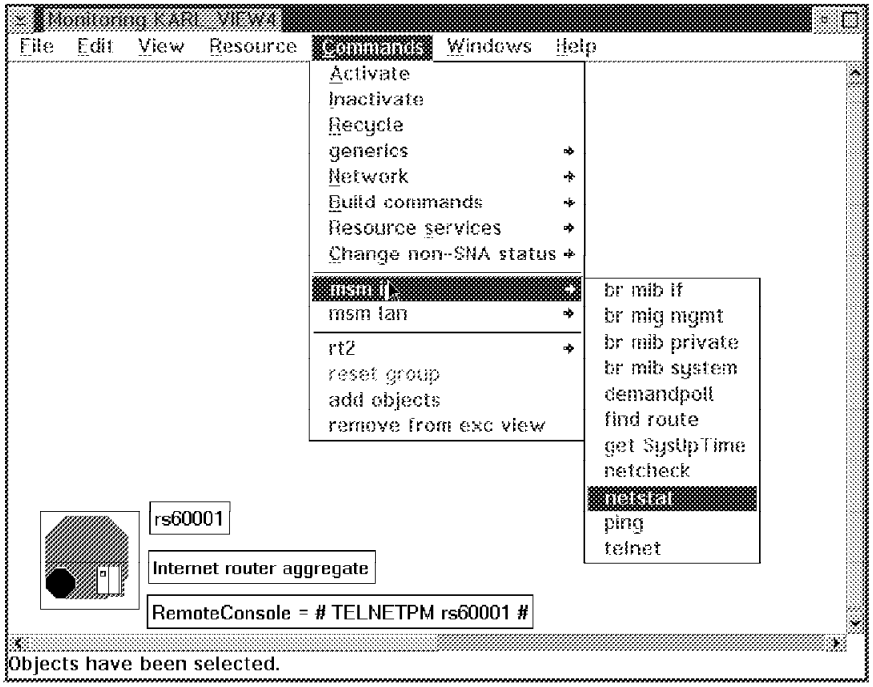


Figure 135. How to Use NETVCMDX

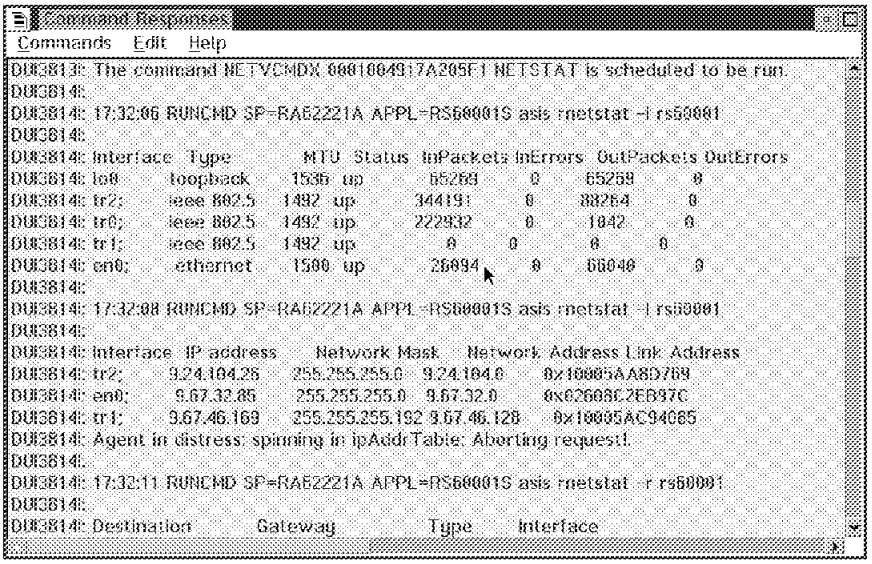


Figure 136. Result of the Netstat Command

7.3.3 NETVCMDX Features

NETVCMDX provides more function than the default NGMF non-SNA command exit (DUICNATV) and is easily customized. Additional function includes:

- NETVCMDX does not use CT/2 (Command Tree/2), so commands are easier to find and to use (less pointing and clicking).
- NETVCMDX allows commands to be issued against aggregate resources as well as real resources.

- NETVCMDX does not send commands to GMFHS to be issued. The commands are issued on the NetView operator that the NGMF operator is signed on to. The commands can be scope checked, and they are also logged in the NetView log.
- Span of control checking can be done for resources in RODM.
- NETVCMDX supports service points which are connected by LU 6.2 or SSCP-PU. If the service point is running SSCP-PU and the owning VTAM is not on the same host where NetView is running, the command will be routed to the appropriate NetView using RMTCMD.

- NETVCMDX supports the GMFHS substitution variables: %RESOURCE%, %SPNAME%, %APPL%, and %DOMAIN%. In addition, NETVCMDX has three of its own substitution variables:
  - %NAME% - Name of the resource known by the element manager.
  - %OPID% - NetView operator ID that the NGMF operator is signed on to.
  - %SEGMENT% - Segment where the resource resides. Only supported for MSM LAN adapters, LAN CAUs and IP interfaces.
  - %USERDATA% - Set to the RODM object's DisplayResourceUserData field.
  - %OTHERDATA% - Set to the RODM object's DisplayResourceOtherData field.
  - %RANDOM% - One to four digit random number.
  - You can define any RODM attribute field (defined on the object) as a variable by enveloping it with "%"s.

    For example, to define DisplayResourceUserData as a variable to be substituted in a command, specify %DisplayResourceUserData% in the command. NETVCMDX will query the field and substitute its value.
- NETVCMDX supports generic commands. It will query the appropriate RODM attribute fields, perform substitution of any variables and then issue the commands:
  - DisplayStatusCommandText
  - ActivateCommandText
  - DeactivateCommandText
  - RecycleCommandText

  If these commands are defined on an aggregate, you can issue them against an aggregate.
- NETVCMDX also has its own short form commands intended for MultiSystem Manager resources that it recognizes and will expand to the actual command text. The short form commands are easy to specify. You don't need to know or specify the command syntax. NETVCMDX will build the appropriate command for you and issue it.
- For any command that NETVCMDX doesn't recognize, it will perform substitution and then issue the command asis. This provides support for any resource in RODM and any command that the resource supports.
- By prefixing the command with NCCF you can execute any NetView command or clist and pass the substituted variables.

7.3.4 MSM TCP/IP, LAN and Novell Commands

7.3.4.1 TCP/IP Commands

Table 5. MSM TCP/IP Commands

Command in NGMF Command Profile	Command Issued by NETVCMDX
BROWSEMIB parm	asis snmpwalk -t 10 %NAME% parm
SNMPGET parm	asis snmpget -t 10 %NAME% parm
DEMANDPOLL	asis nmdemandpoll %NAME%
FINDROUTE	asis findroute -n %NAME%
NETCHECK	asis netcheck %NAME%
NETSTAT	asis rnetstat -i %NAME% asis rnetstat -I %NAME% asis rnetstat -r %NAME% asis rnetstat -e %NAME% asis rnetstat -S %NAME%
PING parm	asis rping -n parm %NAME%

7.3.4.2 Sample PARM Values

Here are the parm values that we used with the TCP/IP commands:

- BROWSEMIB:
  - .1.3.6.1.2.1.interfaces
  - .1.3.6.1.2
  - .1.3.6.1.4
  - 1
- SNMPGET:
  - system.SysUpTime.0
- PING:
  - 2

7.3.4.3 LAN Commands

Table 6. MSM LAN Commands

Command in NGMF Command Profile	Resource Type	Command Issued by NETVCMDX
QUERY	Bridge	BRG QUERY NAME=%NAME%
QUERY	CAU	CAU QUERY UNIT=%NAME%
QUERY	Adapter	ADP QUERY ADP=%NAME% SEG=%SEGMENT%
LINK_BRIDGE	Bridge	BRG LINK NAME=%NAME%
UNLINK_BRIDGE	Bridge	BRG UNLINK NAME=%NAME%
REMOVE_ADAPTER	Adapter	ADP REMOVE ADP=%NAME% SEG=%SEGMENT%
RESTART_CAU	CAU	CAU RESTART UNIT=%NAME% CONFIRM=N
TEST_SEGMENT	Segment	SEGMENT TEST SEG=%NAME% CONFIRM=N
TEST_UTIL	Segment	SEGMENT UTIL SEG=%NAME% CONFIRM=N

7.3.4.4 Novell Commands

Table 7. MSM Novell Commands	
Command in NGMF Command Profile	**Command Issued by NETVCMDX**
QUERY_STATUS	QUERY STATUS
ENABLE_LOGIN	ENABLE SERVER LOGIN
DISABLE_LOGIN	DISABLE SERVER LOGIN

7.3.5 Exception View Command

NETVCMDX will remove the selected resource from all BLDVIEWS exception views.

Table 8. Exception View Command	
Command in NGMF Command Profile	**Action by NETVCMDX**
REMOVE_FROM_EXCPVIEWS	The links from the object to the exception view will be deleted.

7.3.6 Status Change Commands

NETVCMDX will change the *DisplayStatus* field in RODM.

Table 9. Status Change Command	
Command in NGMF Command Profile	**Action by NETVCMDX**
STATUS=129	The status will be set to satisfactory.
STATUS=130	The status will be set to unsatisfactory.
STATUS=131	The status will be set to intermediate.
STATUS=132	The status will be set to unknown.

7.3.7 Generic Commands

For the *generic* commands, NETVCMDX queries RODM for the command to issue. If the field in RODM is empty, NETVCMDX has some hard coded default generic commands that will be used. You can modify NETVCMDX and change the hard coded defaults.

Table 10. Generic Commands and RODM Fields	
Command in NGMF Command Profile	**RODM Field**
GEN_ACTIVATE	ActivateCommandText
GEN_INACTIVATE	DeactivateCommandText
GEN_INACTIVATE	DeactivateCommandText
GEN_DISPLAY	DisplayStatusCommandText
GEN_RECYCLE	RecycleCommandText

Table 11. Generic Commands Defaults		
Command in NGMF Command Profile	**Resource Type**	**Default Command**
GEN_ACTIVATE	Bridge	BRG LINK NAME=%NAME%
GEN_INACTIVATE	Adapter	ADP REMOVE ADP=%NAME% SEG=%SEGMENT%
GEN_INACTIVATE	Bridge	BRG UNLINK NAME=%NAME%
GEN_DISPLAY	Novell	SNAME=%NAME% QUERY STATUS
GEN_DISPLAY	LAN Segment	SEG QUERY NAME=%NAME%
GEN_DISPLAY	Bridge	BRG QUERY NAME=%NAME%
GEN_DISPLAY	CAU	CAU QUERY UNIT=%NAME%
GEN_DISPLAY	LAN Adapter	ADP QUERY ADP=%NAME% SEG=%SEGMENT%
GEN_DISPLAY	IP Adapter	asis rping -n 2
GEN_DISPLAY	IP Host	asis nmdemandpoll
GEN_DISPLAY	IP Router	asis nmdemandpoll

The generic display command will always display some information from RODM before executing the actual display command.

7.3.8 Sample Command Sets

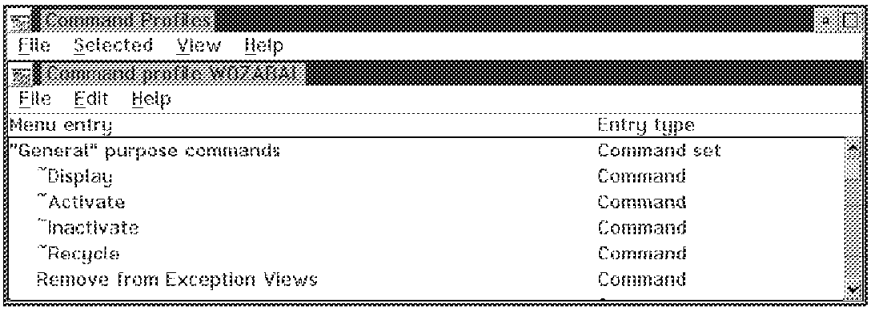


Figure 137. Command Set 1

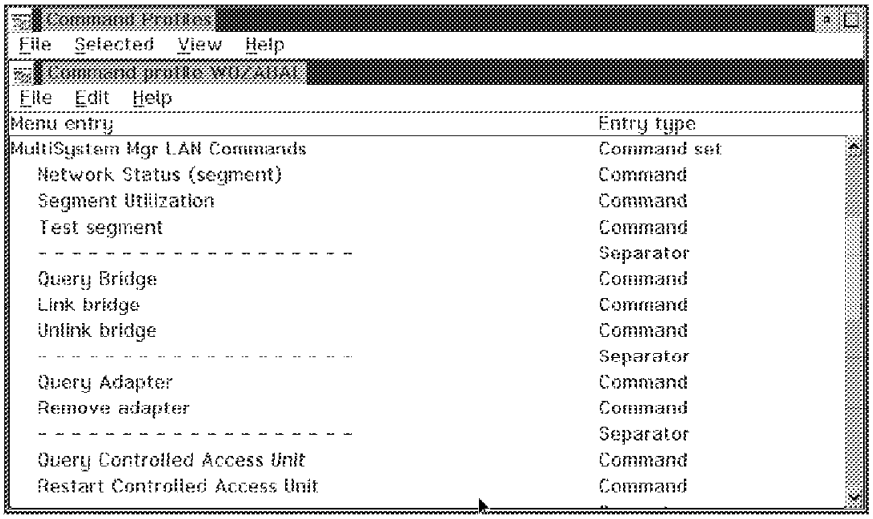


Figure 138. Command Set 2

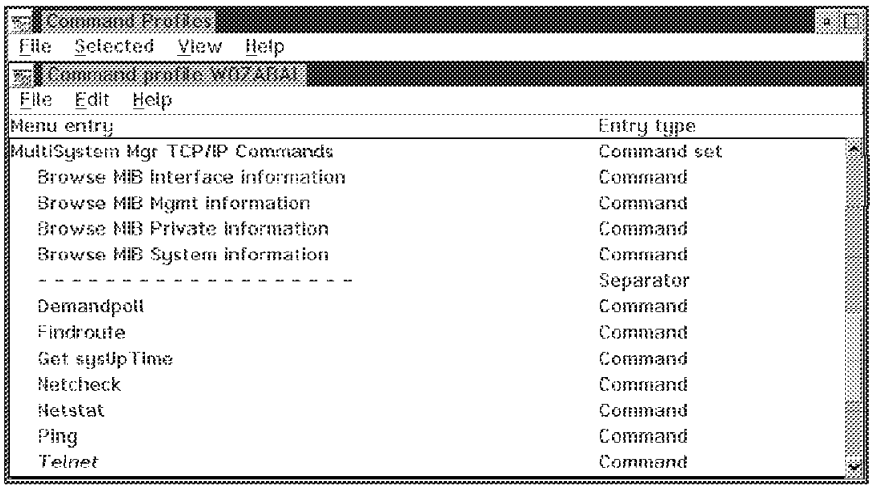


Figure 139. Command Set 3

7.3.9 Sample Commands

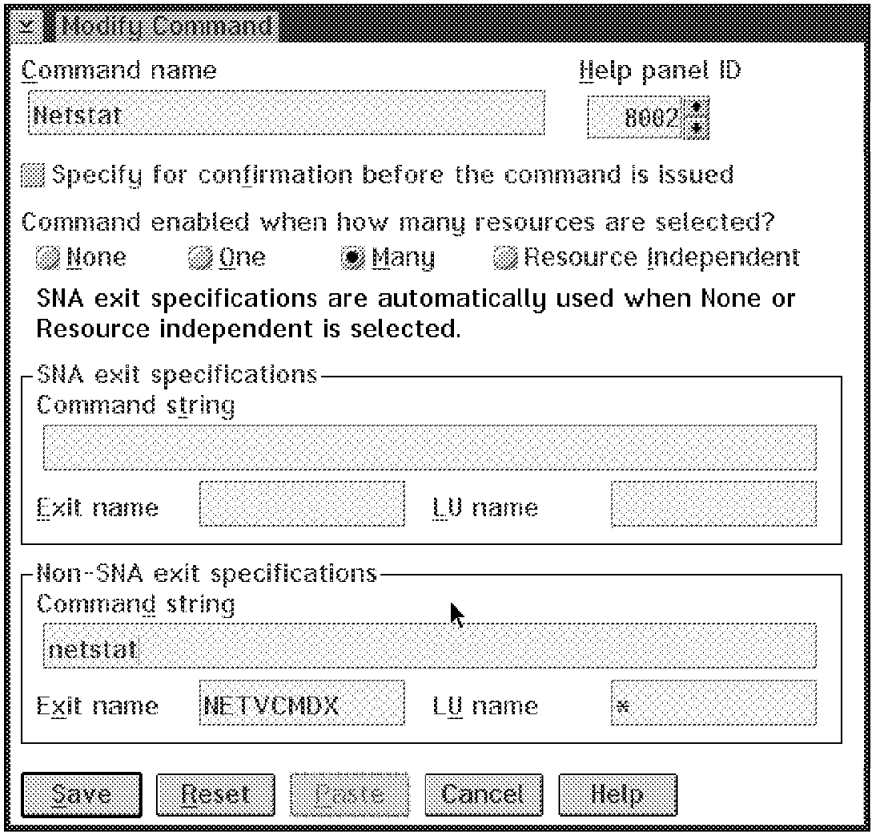


Figure 140. Netstat Example

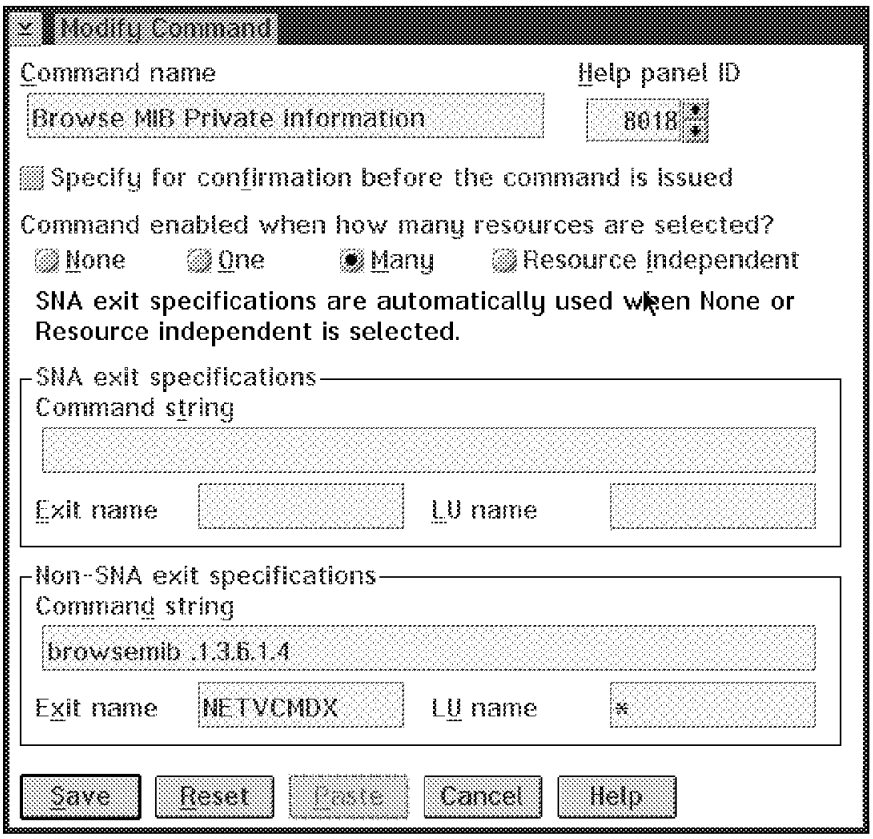


Figure 141. Browse MIB Example

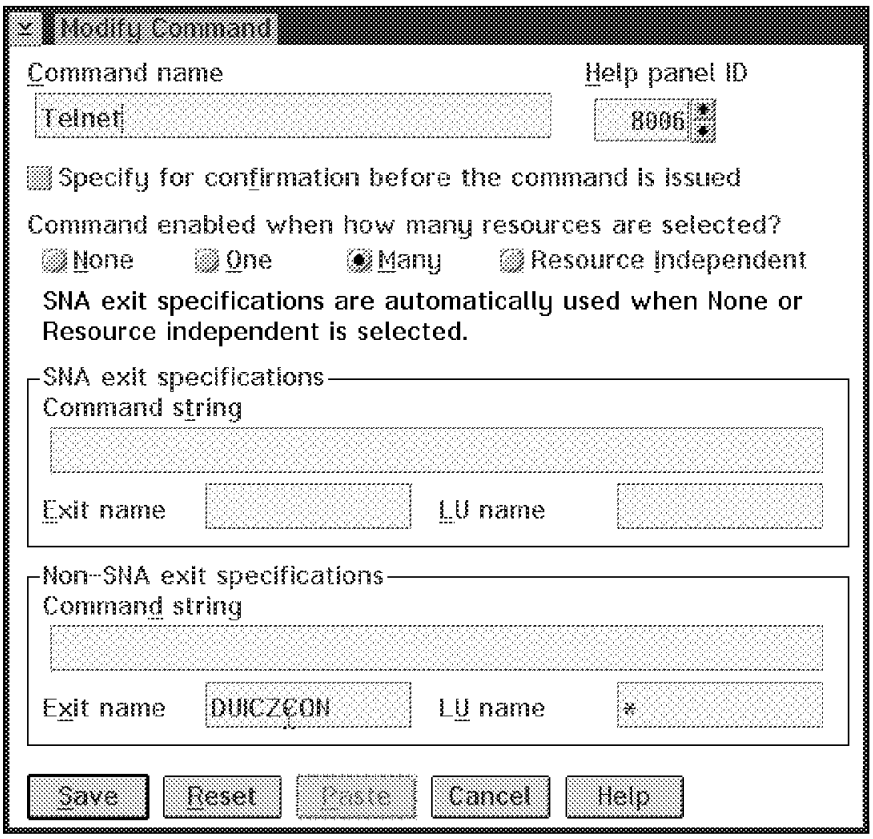


Figure 142. TELNET Command

For TELNET we used the remote console command.

7.3.10 Span of Control

- Installation
  - Add the field CommandSpanName to RODM

    Create a new RODM loader member with the following statement and concatenate it at the end of the RODM loader file EKGIN1 (after the MSM data model members):

    ```
    OP '2.9.3.2.3.14' HAS_FIELD(CHARVAR) 'CommandSpanName';
    ```

  - Comment out the CMDSYN DMCS statement in DSICMD:

    ```
    FLCADMCS CMDMDL MOD=DSICCP
    *        CMDSYN DMCS
             CMDCLASS 1,2
    ```

    Now the DMCS CLIST will do the span checking and check whether it can pass control to the ″real″ FLCADMCS clist.
- Customization
  - Define the span in the operator profiles.

```
PROFGARY PROFILE IC=GARY
         AUTH   MSGRECVR=NO,CTL=GENERAL
         ISPAN  SPAN1,SPAN2
         END
```

– Load the field in RODM. The easiest way to do this is with BLDVIEWS.

```
IP_BRIDGE=ALL,SPANNAME=(SPAN1,SPAN2)
```

7.3.11 If You DON′T Want Span Checking

The NETVCMDX package includes a dummy NETVSPAN CLIST which runs with return code zero. If you do not install a CLIST, you *must* use the dummy to get NETVCMDX working.

7.4 RODMTool/2

The RODMTool/2 (RT/2) package, which is available to IBM employees from MKTTOOLS (see you IBM representative for details) has now been extended to run with either RODMVIEW or MultiSystem Manager. The new MultiSystem Manager support means that if you do not have RODM Toolkit′s RODMVIEW (but have MultiSystem Manager installed) you can still enjoy most of the user-friendly functions provided by RT/2. A short description of the RT/2 package is provided below.

RT/2 enables a user without expert skills in RODM data models and ASN.1 syntax to perform RODM operations, such as adding customized views and aggregate resources, linking objects and even implementing exception-only views. One scenario: a user selects three IP routers in an NGMF view and then clicks on the command - Link as physical peers on NGMFs Commands pull-down menu customized for RT/2. This results in NGMF refreshing the view seconds later - showing the new link.

You can build your own RODM applications by enabling the recording function and then performing some RT/2 operations (the RT/2 commands are stored in an executable REXX CLIST).

RT/2 consists of some NetView host code and workstation (CT/2) code. It requires NetView V2R4 and RODM Tool Support/MVS V2 (5799-FFJ) or NetView MultiSystem Manager installed on MVS and the NGMF workstation code installed on your workstation.

Included in the RT/2 package is the RODMTool/2 code and presentation material. The redbook GG24-4292 provides the complete RT/2 documentation.

7.5 NetView Resource Monitor

The resource monitor for NetView provides an easy-to-use facility allowing you to monitor and manage the NetView product and many system and network management applications running in its environment.

In using the Resource Monitor for NetView, you can monitor the NetView main task, AUTO tasks, distributed tasks (DISTs), data services tasks (DSTs), optional

tasks (OPTs), operator station tasks (OSTs), NetView-to-NetView tasks (NNTs), and the primary POI task (PPT). Information (such as member name, date and time started) about the NetView automation table will also be monitored.

The Resource Monitor for NetView facility dynamically discovers the NetView main task and other subtask application resources running in NetView. It can continuously monitor the application resources to detect any application being terminated or new ones becoming active.

All the resource configuration and status information are stored in RODM to enable GMFHS and NGMF to display graphic views for monitoring and for use in automation.

For a complete description of NRM see the User's Guide in MSM Informal Documentation - refer to 5.3, "Installing MSM Informal Documentation" on page 129.

7.5.1 Views and Navigation

This section provides information on the views and navigation flows provided by the Resource Monitor for NetView.

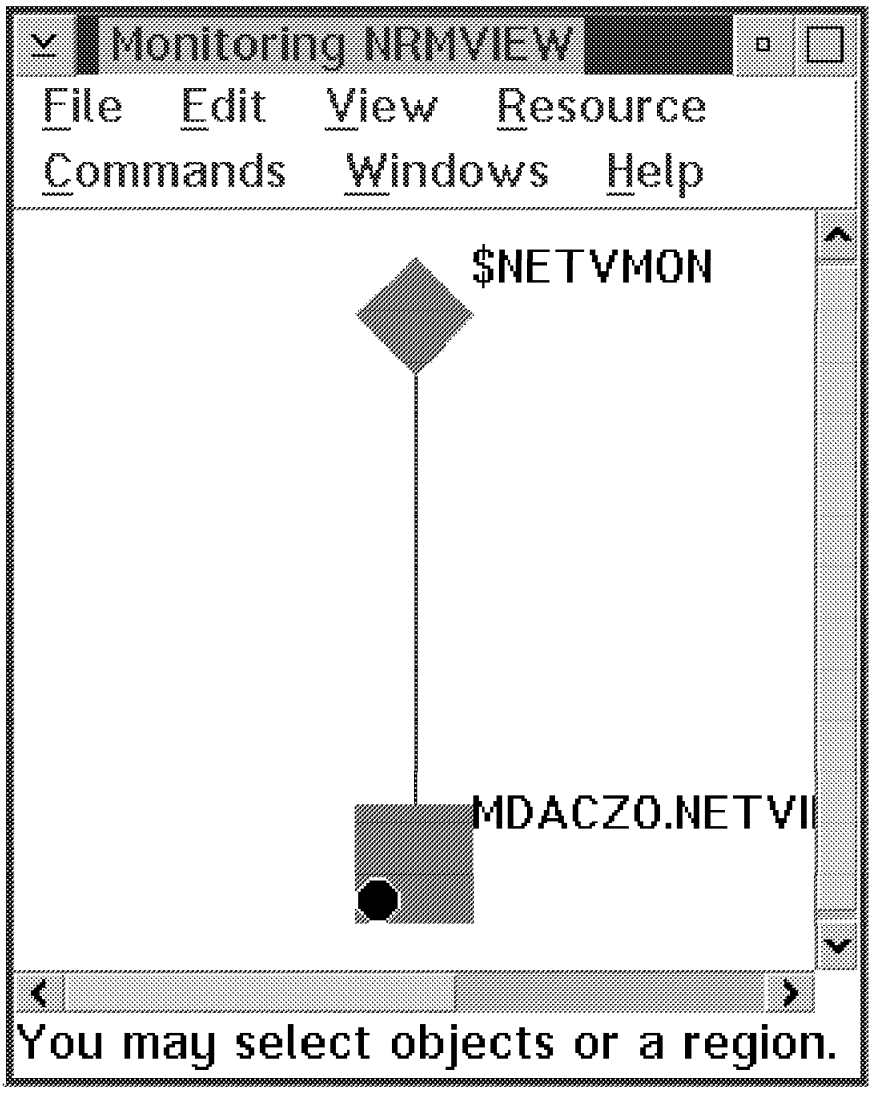


Figure 143. NRM Network View

Figure 143 shows the first-level view, which contains a system aggregate object for the NetView subsystem being monitored. In this example, one NetView (with DOMAIN ID = DACZO) is being monitored.

The $NETVMON real resource object is being displayed in this view to show the status of the Resource Monitor for NetView facility. If you select the $NETVMON resource object in Figure 143 and ask for resource information, the panel shown in Figure 144 on page 173 will be displayed.

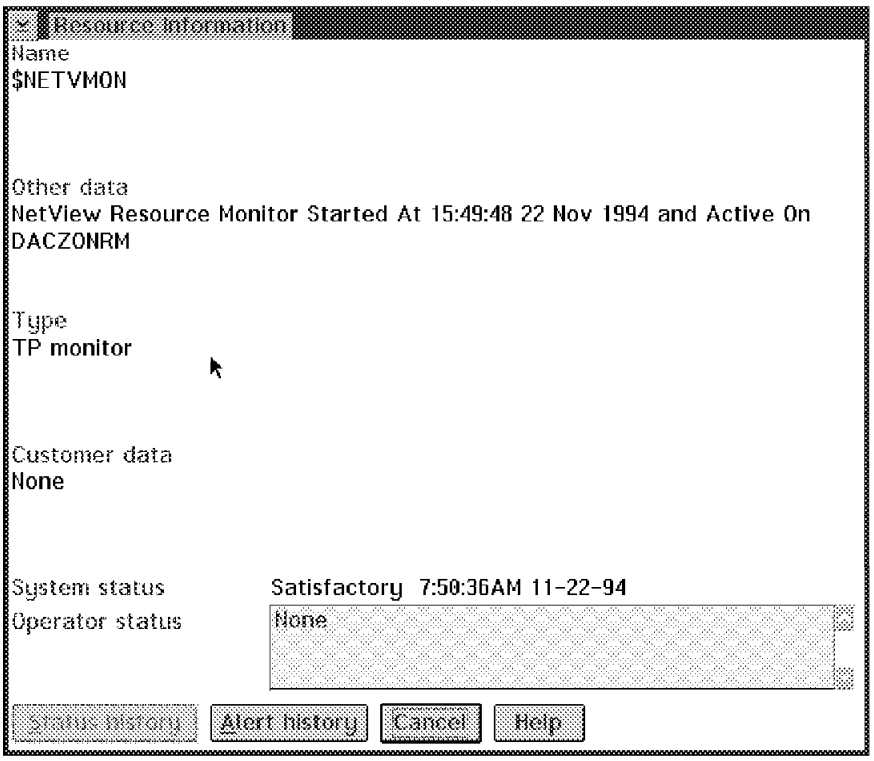


Figure 144. $NETVMON Resource Information Panel

The Other Data field for the $NETVMON resource object provides information such as the time and date the Resource Monitor for NetView facility was started, and the task which it is being executed on. If Resource Monitor for NetView becomes inactive, the status of this $NETVMON resource object will be UNKNOWN and the Other Data field will contain 'The Resource Monitor for NetView Facility is Terminated date time'.

If the MDACZO.NETVIEW.SUBSYSTEM resource object in Figure 143 on page 172 is selected and you ask for resource information, the resource information panel shown in Figure 145 on page 174 will be displayed.

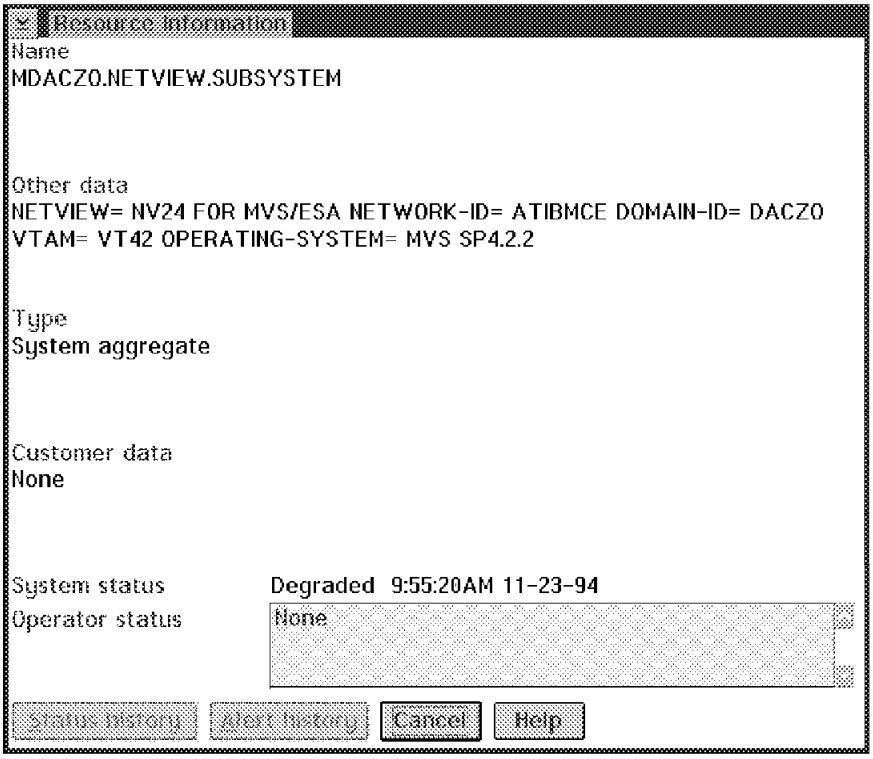


Figure 145. NETVIEW.SUBSYSTEM Resource Information Panel

The Other Data field details the NetView, VTAM and MVS versions, network ID and domain.

If the NetView subsystem aggregate object in Figure 143 on page 172 is selected and more detail view is requested, the view shown in Figure 146 will be displayed.

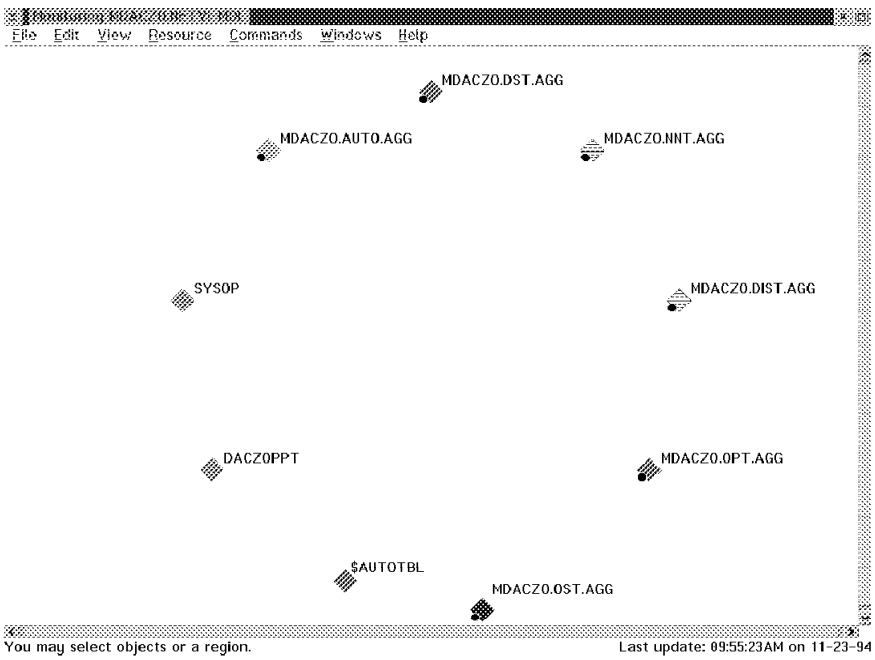


Figure 146. NRM NetView Aggregate View

Figure 146 contains the real resource objects for the NetView automation table ($AUTOTBL), the NetView main task (SYSOP), and the NetView PPT task (DACZOPPT). This view also contains the aggregate objects for the following NetView application task types: AUTO task (AUTO), distributed task (DIST), data services task (DST), NetView-to-NetView task (NNT), optional task (OPT), and operator station task (OST).

If the $AUTOTBL resource object is selected and asked for resource information, the resource information panel shown in Figure 147 will be displayed.

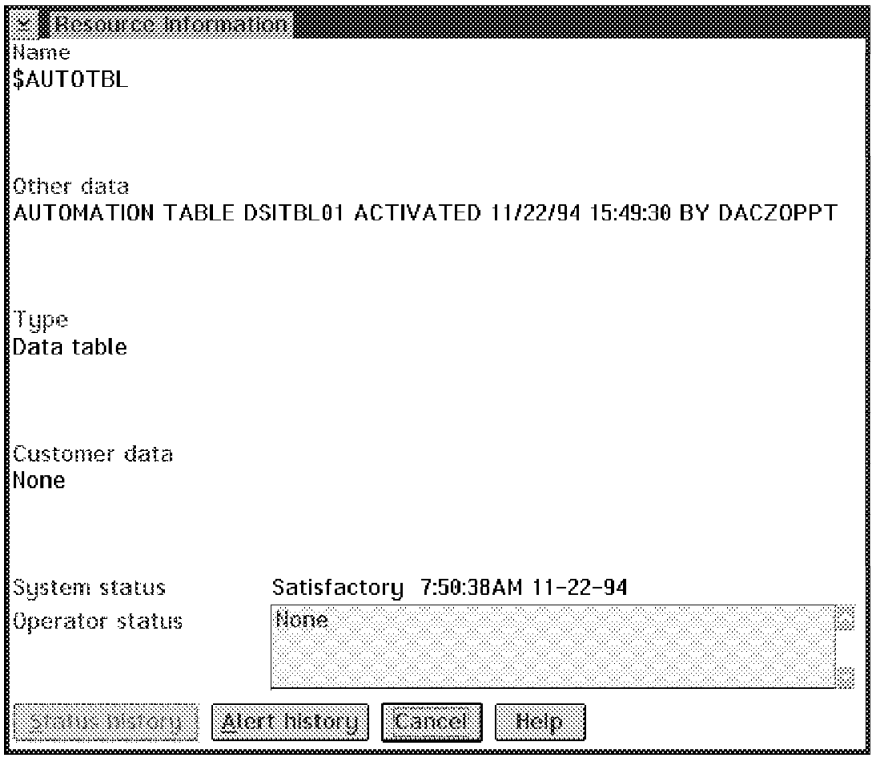


Figure 147. NRM $AUTOTBL Resource Information Panel

For a more-detail view of one of the task types, you need to select and obtain a more-detail view on one of the aggregate objects for the task types on the view shown in Figure 146 on page 174. For example, when the AUTO.AGG aggregate object (in Figure 148 on page 176) is selected and more-detail view is requested, the view shown in Figure 148 on page 176 will be displayed. This view contains the real resource objects for the AUTO tasks discovered by the Resource Monitor for NetView.

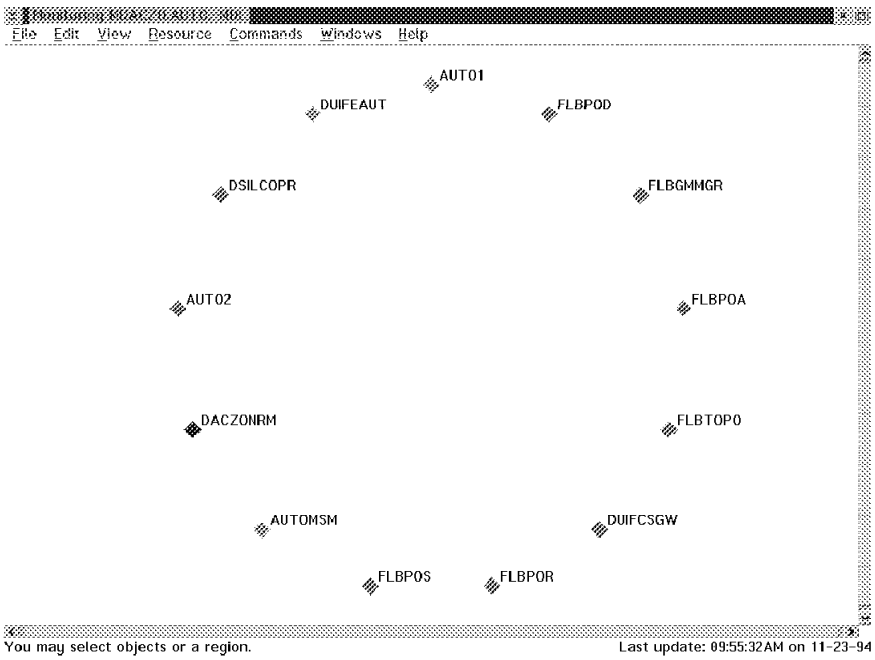


Figure 148. NRM AUTO Resource View

If the DUIFEAUT resource object is selected and you ask for resource information, the resource information panel shown in Figure 149 will be displayed.

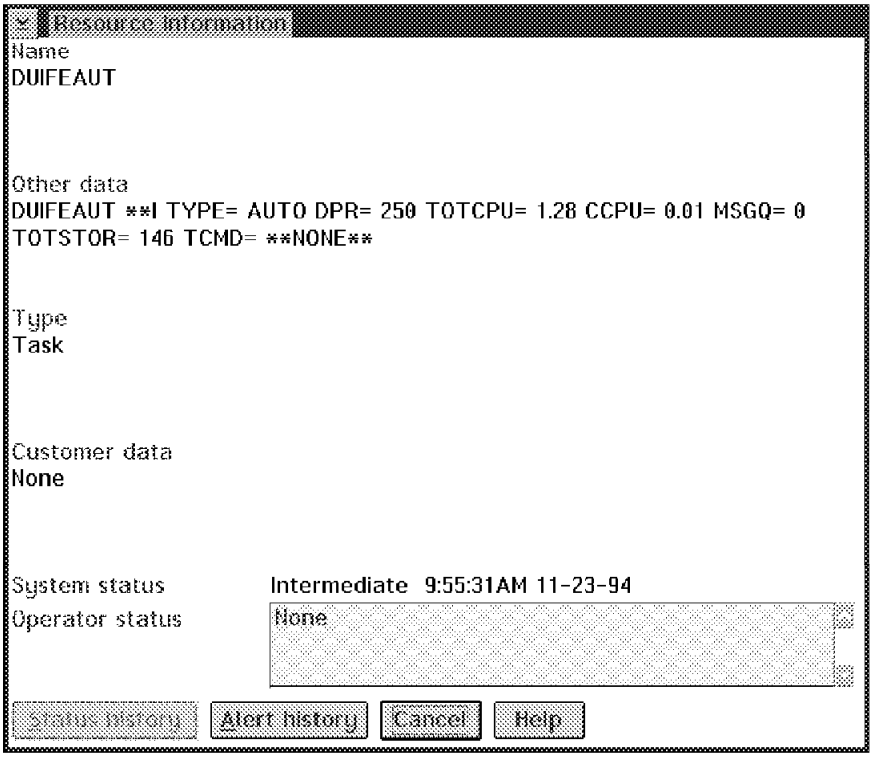


Figure 149. NRM DUIFEAUT Resource Information Panel

Note

The Other Data field provides pertinent information such as the three-character threshold indicator, task type (TYPE), dispatching priority number (DPR), total CPU usage (TOTCPU), current CPU usage (CCPU), the number of data buffers in the message queue (MSGQ), total storage usage (TOTSTOR), and the name of command currently being executed on this application task (TCMD). The first character is used for the CPU usage threshold, the second character is used for the message queue threshold, and the third character is used for the storage threshold. In Figure 148, the threshold indicator (**I) indicates that the threshold for the CPU and message queue have not been exceeded, and the intermediate threshold for storage usage has been exceeded. The information in this Other Data field will be updated at each monitor interval to provide the updated data at that time. The NRM operator should refresh the view to obtain the latest data for this Other Data field.

If the OST.AGG aggregate object (in Figure 148 on page 176) is selected and a more-detail view requested, the view shown in Figure 150 on page 178 will be displayed. This view contains the real resource objects for the operators discovered by the Resource Monitor for NetView. Operators that are not logged on are shown with unknown status. If an operator object is selected and you ask for resource information, a resource information panel similar as shown in Figure 149 on page 176 will be displayed.

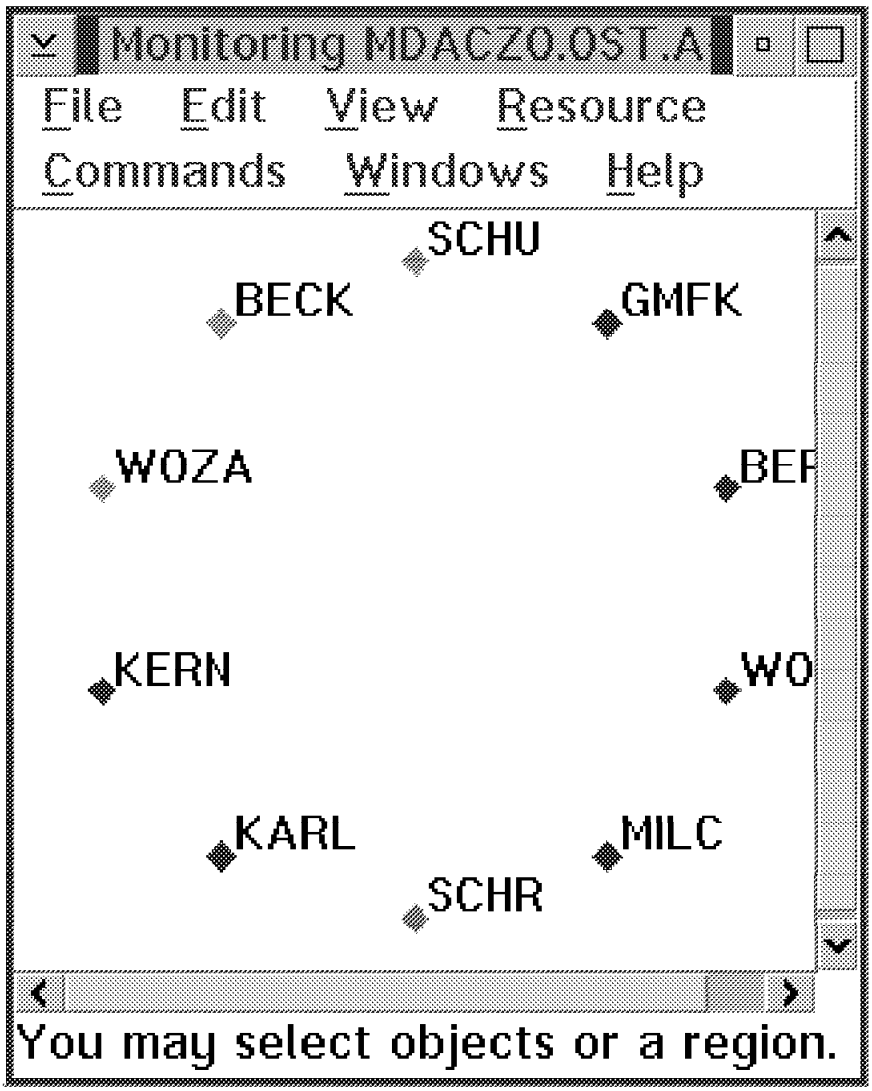


Figure 150. NRM OST Resource View

7.5.2 Installation

The NRM REXX Clists are in the SFLCREX1 data set. Make sure that this is in the DSICLD concatenation.

7.5.3 RODM Authorization

The NRM autotask (or if you run NRM from an operator task this user ID) needs a RODM authorization level of three.

7.5.4 Required Initialization Input File

The Resource Monitor for NetView requires an initialization file when it is started. You can refer to the FLCVSTRT command for more details on how to start up the Resource Monitor for NetView.

Initialization input file keywords:

RODMNAME=rodm-name

Specifies the name of the RODM to be used. Refer to the RODM programming guide for more details on this name. This statement is required.

NETWORK_VIEW_NAME= view-name

Specifies the name of the network view to be created by the Resource Monitor for NetView. Refer to the RODM programming guide for more details on this name. If this is not specified, the default view name is NRMVIEW.

NETWORK_VIEW_DESC= view-desc

Specifies the description of the network view to be created by the Resource Monitor for NetView. Refer to the RODM programming guide for more details on the view description. If this is not specified, the default view description is NV Res Monitor View For <domain-id> where <domain-id> is the NetView domain ID.

MONITOR=tasktype

Specifies for what type of task this statement applies.

- AUTO Specifies AUTOTASK type.
- DIST Specifies distributed task type.
- DST Specifies data services task type.
- MNT Specifies NetView main task type.
- NNT Specifies NetView-to-NetView task type.
- OPT Specifies optional task type.
- OST Specifies operator station task type.
- PPT Specifies NetView primary POI task type.
- START Specifies start monitoring of the specified task type.
- STOP Specifies stop monitoring of the specified task type.

CPUI = seconds

Specifies the intermediate CPU usage threshold, and seconds is a 1- to 7-digit number for seconds of CPU time.

CPUU = seconds

Specifies the Unsatisfactory CPU usage threshold, and seconds is a 1 to 7-digit number for seconds of CPU time.

MQI = buffers

Specifies the intermediate message queue buffer threshold, and value is a 1- to 7-digit number of data buffers in the message queue.

MQU = buffers

Specifies the unsatisfactory message queue buffer threshold, and value is a 1- to 7-digit number of data buffers in the message queue.

STORI = KB

Specifies the intermediate storage usage threshold, and KB is a 1- to 7-digit number of KB of storage.

STORU = KB

Specifies the unsatisfactory storage usage threshold, and KB is a 1- to 7-digit number of KB of storage.

INTERVAL= time

Specifies the monitoring interval. Time is hh:mm:ss where hh is 0-23 hours, mm is 0-59 minutes, and ss is 0-59 seconds.

Note

The value of an intermediate threshold must be less than the value of the corresponding unsatisfactory threshold. For example, the value o the STORI threshold must be less than the value of the STORU threshold. Also the intermediate keyword must precede the unsatisfactory keyword.

If a MONITOR statement is longer than than 71 characters, it must be split into multiple statements of 71 characters or less. And each statement must start with the the ″MONITOR″ keyword.

```
RODMNAME = RODMA
NETWORK_VIEW_NAME = NETV-VU
NETWORK_VIEW_DESC = This Is My NetView Resource Monitor View
MONITOR = OST START INTERVAL = 00:03:00 CPUI = 5 CPUU = 10
MONITOR = OST START MQI = 10 MQU = 20 STORI = 100 STORU = 2000
MONITOR = MNT START INTERVAL = 00:05:00 CPUI = 10 CPUU = 30
MONITOR = MNT START MQI = 10 MQU = 20 STORI = 1000 STORU = 5000
MONITOR = NNT STOP
MONITOR = DIST STOP
```

Figure 151. Sample Initialization File

The default is to start monitoring. Default values for various parameters are show in Figure 152.

```
AUTO INTERVAL=00:02:00 CPUI=5 CPUU=10 MQI=5 MQU=10 STORI=100 STORU=100
DIST INTERVAL=00:02:00 CPUI=5 CPUU=10 MQI=5 MQU=10 STORI=100 STORU=100
DST INTERVAL=00:02:00 CPUI=5 CPUU=10 MQI=5 MQU=10 STORI=200 STORU=2000
MNT INTERVAL=00:02:00 CPUI=5 CPUU=10 MQI=5 MQU=10 STORI=3000 STORU=600
NNT INTERVAL=00:02:00 CPUI=5 CPUU=10 MQI=5 MQU=10 STORI=100  STORU=100
OPT INTERVAL=00:02:00 CPUI=5 CPUU=10 MQI=5 MQU=10 STORI=100  STORU=100
OST INTERVAL=00:02:00 CPUI=5 CPUU=10 MQI=5 MQU=10 STORI=100  STORU=100
PPT INTERVAL=00:02:00 CPUI=5 CPUU=10 MQI=5 MQU=10 STORI=100  STORU=100
```

Figure 152. Defaults

7.5.5 NetView Command Scope Checking

The following sample NetView command model statements can be used to provide NetView command scope checking for the Resource Monitor for NetView. Although this is not required, it is recommended that the command scope checking be done for the FLCVSTRT, FLVVCHG and FLCVSTOP commands.

```
FLCVSTRT CMDMDL MOD=DSICCP
         CMDCLASS   1,2
*
FLCVSTOP CMDMDL MOD=DSICCP
         CMDCLASS   1,2
*
FLCVDISP CMDMDL MOD=DSICCP
         CMDCLASS   1,2
*
FLCVCHG  CMDMDL MOD=DSICCP
         CMDCLASS   1,2
```

Figure 153. Sample Command Models

7.5.6 Commands

- FLCVSTRT member

  Start Resource Monitor for NetView processing.

  The *member* keyword specifies the name of the initialization member for the Resource Monitor for NetView. If not specified, the default member name is NETVMON. This member must exist in one of the data sets for NetView DSIPARM.

  The Resource Monitor for NetView must be started and executed on an operation station task (OST) or an automation task (AUTO). When the FLCVSTRT command is used to start up Resource Monitor for NetView on an OST or AUTO task, this task will be used solely for the Resource Monitor for NetView until it is terminated. No other command should be entered on this task while the Resource Monitor for NetView is active.

- FLCVSTOP

  Stop Resource Monitor for NetView.

- FLCVCHG

  Change Resource Monitor for NetView processing options.

  The change command has the same format as the MONITOR keyword in the initialization file.

- FLCVDISP DISPLAY tasktype

  Display Resource Monitor for NetView processing options.

  The FLCVDISP command can be used to display the processing options for Resource Monitor for NetView. The FLCVDISP command can be issued at any time after NetView program initialization is completed.

  tasktype is any of the tasktypes you can specify on the initialization file. The default is ALL

```
FLC121I NV RESOURCE MONITOR INFORMATION
FLC120I NV RESOURCE MONITOR IS ACTIVE
FLC122I INPUT FILE NAME = NETVMON
FLC122I RODM NAME = RODMA
FLC122I NETWORK VIEW NAME = NRM-VU
FLC122I NETWORK VIEW DESC = NETVIEW RES MONITOR VIEW
FLC122I TASK ID = OPER1
FLC122I CONFIG_VIEW_CMD = YES
TYPE MON INTERVAL  CPU-I   CPU-U   MSGQ-I  MSGQ-U  STOR-I  STOR-U
---- --- -------- ------- ------- ------- ------- ------- -------
MNT  YES 00:02:00       5      10       5      10    2000    5000
PPT  YES 00:02:00       5      10       5      10     100    1000
NNT  NO  00:02:00       5      10       5      10     100    1000
AUTO YES 00:02:00       5      10       5      10     100    1000
DIST YES 00:02:00       5      10       5      10     100    1000
OST  YES 00:02:00       5      10       5      10     100    1000
DST  YES 00:02:00       5      10       5      10     100    1000
OPT  NO  00:02:00       5      10       5      10     100    1000
End of display
```

Figure 154. Sample Display Results

7.5.7 NGMF Generic Command Support

NGMF generic command support (activate, inactivate, display) is provided by Resource Monitor for NetView.

Note: The generic command support is only provided on the real resource objects because NGMF only allows this support on the real resource objects and not on the aggregate resource objects at this time. But you can use NETVCMDX to do this - see 7.3, “NETVCMDX - NetView Host REXX CLIST and NGMF Cmd Exit” on page 161.

7.5.7.1 $NETVMON Object

If you select the Resource Monitor for NetView object ($NETVMON), and issue the activate, inactivate or display commands, these will have the effect of executing FLCVSTRT, FLCVSTOP, and FLCVDISP, respectively.

7.5.7.2 NetView Application Task Objects

If you select the OPT or DST real objects, and issue the activate, inactivate or display commands, these will have the effect of executing START, STOP and LIST, respectively.

On the AUTO, DIST, NNT, and OST task real objects, only the generic display command is supported. This display command support is to execute the LIST command (for example, LIST OPER1).

Appendix A. AIX NetView Service Point Installation and Configuration

A.1 Service Point Installation and Configuration

This section provides a short description of how to install and implement Service Point on an IBM RISC/6000 system. Refer to *AIX Installation, Operation and Programming Guide, SC31-6120*, and to *Examples of Using NetView for AIX, GG24-4327*.

A.1.1 Hardware and Software

The following platform was used in our lab and generally represents the minimum configuration required to run NetView/6000 and AIX NetView Service Point.

A.1.1.1 Hardware Used

- RISC/6000 POWERstation 7013-530 (64 MB storage)
- Token-Ring Card or Ethernet Adapter

Note: A minimum of 64MB is highly recommended and this is the absolute minimum for NetView for AIX Version 3.

A.1.1.2 Software Used

Operating System: AIX V3.2.5

Group A:

- AIX SystemView NetView/6000 V2.1
- AIX SNA Services V1.2
- AIX NetView Service Point V1.2

Group B:

- AIX NetView for AIX Version 3 with PTF U434185
- AIX SNA Server V.2 with PTF U433040 and U433041
- AIX NetView Service Point V1.2.1 with PTF U434054

A.1.1.3 Configuration

The connection between MVS and AIX is provided by SNA Server. Its predecessor, SNA Services, might still be in use in some installations so it will also be described in this book.

Two different configurations are available with Service Point:

- SSCP-PU Session
- MDS transport using LU 6.2 Session

For performance reasons, SSCP-PU connection is not supported for the connection to the IBM NetView MultiSystem Manager. It may work, as it did in our test environment, but because it is not supported and performance is not as good as LU6.2, it should not be used and will not be described in this book.

We always had Service Point running on the same machine as NetView/6000 in our test environment, but this is actually not a requirement. The same configuration as explained here for token-ring should also work with the multiprotocol adapter and Ethernet. A short description of how to set up Ethernet connection is provided for both SNA Services and SNA Server.

Service Point Using New SNA Server Functions: This is not a full description of SNA Server functions, but is intended to give you a short overview about what you have to know to use Service Point.

SNA Server adds APPN functions to AIX. It supports the following types of network functions:

- APPN network nodes and end nodes.
- LEN nodes either connected to an APPN network or in a network using independent LU 6.2 for peer communication.
- Dependent communication using dependent LU types in a subarea network.
- SNA gateway connectivity using SNA Gateway/6000.

The APPN control point supports both PU and LU functions. Thus definitions are much less complex then using SNA Services. You do not have to define any LU 6.2 profiles in the RS/6000. The control point name is used to address the Service Point in the RUNCMD command.

There have been some changes in terminology:

- Attachments are now called link stations.
- Physical and logical link profiles were combined into the SNA DLC profile.
- Connections are replaced by sessions.

When using SNA Server, you have to verify changes of the profiles. The verification writes configuration data to the committed database - unverified profile changes are stored in the working database, which is not used for production. Profiles that do not pass the verification are not written to the committed database. Another thing you might consider useful is the facility to connect to different hosts using multiple links on one adapter. This means that if you are already using your adapter to connect to one host, you can add a second link to the IBM NetView MultiSystem Manager host, on that same adapter.

A.1.2 Summary of Installation Procedure

The installation procedure described below is a summary of the scenario we used in the lab:

- Install AIX (not discussed here).
- Install SNA and Service Point Software using SMIT (not discussed here).
- Configure SNA and Service Point.
- Customize VTAM.

A.1.3 Implementing a NetView Service Point Connection Using SNA Server

For use with SNA Server you have to use Service Point 1.2.1 with PTF U434054.

A.1.3.1 Miscellaneous

Including Service Point: After the installation you have to issue the AIX command `nvix_customize_sp`. This includes the Service Point into the SMIT menus. There are no default panels provided for the SNA configuration.

Activating Data Link Control: If SNA is being installed on your machine for the first time, you will need to activate Data Link Control for the adapter used. For use with token-ring for example do the following:

- Select option **Devices from SMIT**.
- Select option **Communication**.
- Select option **Token Ring**.
- Select option **Services**.
- Add (or you may first display) **Data Link Controls**.

Update TCP/IP Definitions: You may have to update two TCP/IP definition files in AIX:

- /etc/hosts
- /etc/services

Verify that there is a loopback entry in your hosts file as in this example:

```
#9.67.32.242   rs60002b rs60002
127.0.0.1      loopback localhost #needed for SMUX
#9.67.32.85    rs60001e rs60001
#9.67.32.25    robmac
```

The figure above shows a part of the /etc/hosts file being used in the ITSO RISC/6000.

Next you have to insert the following entries into the etc/services file:

```
nvixacm          7111/tcp
nvixclb          7112/tcp
nvixcr           7113/tcp
nvixfts          7114/tcp
nvixsp           7115/tcp
nvixspc          7116/tcp
```

Make sure the ports are not in use yet (usually ports 7111-7116 are not).

A.1.3.2 Customizing the Profiles Using Token-Ring Adapter

Customize Service Point Profile Summary: Go to *NetView Service Point Profile Summary* using SMIT (Communication, Service Point, Configure...). The only panel provided is shown in Figure 155.

```
                    NetView Service Point Profile Summary

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                    (Entry Fields)
* Use MDS transport?                                 yes           +
     If no, enter SSCP ID                           (05000000ffff)
     If no, enter Polling Period (msec)             (3000)                    #
     If no, enter PUNAME                            ()
     If yes, enter the COS FP NETID                 (USIBMRA)
     If yes, enter the COS FP NAU                   (RABAN)
     If yes, enter the ALERT FP NETID               (USIBMRA)
     If yes, enter the ALERT FP NAU                 (RABAN)
  Service Point Codepage                            ( )
```

Figure 155. NetView Service Point Profile Summary for SNA Services

In order to use LU6.2 MDS transport you have to answer the first question in this panel with yes. Then you have to fill in your Focal Point host. Fill in NETID, which is the network ID, defined in VTAM on the target NetView host. Specify the VTAM acbname of the target NetView in the NAU field. You can connect to different Focal Point NetViews for the RUNCMD command function (COS FP) and alert forwarding (ALERT FP). However, according to the SNA network management architecture RUNCMD commands can be sent from any NetView for MVS. The information you enter here is used to build up the LU 6.2 session, as no session will be defined in SNA Server, and you need this information because the session is initiated by AIX. You can change the Service Point's partner LU by issuing a FOCALPT CHANGE command from NetView; this command overwrites the definition you enter in this panel.

We entered the following command from the host NetView *RAKAN*:

```
* RAKAN    FOCAL POINT CHANGE TARGET=RA6005CP FPCAT=ALERT

- RAKAN    DSI258I CHANGE FOCAL POINT COMMAND HAS BEEN SENT TO RA6005CP FOR
           ALERT DATA
- RAKAN    DSI293I FOCAL POINT AUTHORIZATION FOR ALERT DATA HAS BEEN ACCEPTED
           BY RA6005CP
```

The *NetView Service Point Profile Summary* was changed like this:

```
                    NetView Service Point Profile Summary

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                   (Entry Fields)
* Use MDS transport?                              yes                      +
     If no, enter SSCP ID                         (050000000ffff)
     If no, enter Polling Period (msec)           (3000)                    #
     If no, enter PUNAME                          ()
     If yes, enter the COS FP NETID               (USIBMRA)
     If yes, enter the COS FP NAU                 (RABAN)
     If yes, enter the ALERT FP NETID             (USIBMRA)
     If yes, enter the ALERT FP NAU               (RAKAN)
  Service Point Codepage                          ( )
```

Alerts from NetView/6000 are sent to RAKAN, and RUNCMD commands are accepted from both RABAN and RAKAN. In the Service Point status summary panel, you will also find the appropriate information:

```
*** Focal Point Status Information : ***
COS FP: USIBMRA.RABAN
ALERT FP: USIBMRA.RAKAN
```

The command to change the COS focal point is shown below:

```
* RAKAN    FOCALPT CHANGE TARGET=RA6005CP FPCAT=SPCS

- RAKAN    DSI258I CHANGE FOCAL POINT COMMAND HAS BEEN SENT TO RA6005CP
           SPCS DATA
- RAKAN    DSI293I FOCAL POINT AUTHORIZATION FOR SPCS DATA HAS BEEN ACCE
           BY RA6005CP
```

In fact this doesn't affect anything. RUNCMD command still works with both RAKAN and RABAN. A display of the CP shows the following sessions, where *ACTIV/CP* indicates VTAM V4 (*DIS RA6005CP*):

```
ST206I  SESSIONS:
ST1081I  ADJACENT LINK STATION = RA60005
ST634I  NAME     STATUS         SID          SEND RECV VR TP NETID
ST635I  RABAN    ACTIV-S    E09B58133C5770B6            0  0 USIBMRA
ST635I  RAKAN    ACTIV-S    E09B58133C5770B5 0015 0000  0  0 USIBMRA
ST635I  RAK      ACTIV/CP-S E09B58133C5770B4 0007 0001  0  0 USIBMRA
ST635I  RABAN    ACTIV-P    F7EFD164B3F691A9            0  0 USIBMRA
ST635I  RAKAN    ACTIV-P    F8D3D1647961A20D 0002 0010  0  0 USIBMRA
ST635I  RAK      ACTIV/CP-P F8D3D1647961A203 0001 0007  0  0 USIBMRA
ST924I  ------------------------------------------------------------
```

There are two sessions to the control point RAK, which is the VTAM as a network node, and two sessions with each NetView, one primary and one secondary.

When you configure SNA Server and start to test it, watch your /var directory carefully - SNA Services creates logfiles in the directory /var/sna.

```
rs60005: /var/sna > ls -la
total 9984
drwxr-xr-x   2 root     system       512 Nov 10 10:37 .
drwxr-xr-x  13 bin      bin          512 Jun 16 09:30 ..
-rw-r--r--   1 root     system        25 Nov 10 13:44 .sna.status
-rw-rw-rw-   1 root     system    403372 Nov 10 22:02 @tok0.4
-rw-rw-rw-   1 root     system   1321256 Nov 10 21:54 RA60005
-rw-r--r--   1 root     system   1048580 Nov 10 10:37 SNA_ABEND.dmp
-rwxr-x---   1 root     system     92161 Nov 10 13:50 kernel_ras.log
-rw-rw-rw-   1 root     system     12392 Nov  9 11:55 snaservice.1
-rw-rw-rw-   1 root     system     12176 Nov  9 11:53 snaservice.10
-rw-rw-rw-   1 root     system   1451924 Nov 10 09:47 snaservice.2
-rw-rw-rw-   1 root     system     16436 Nov 10 10:37 snaservice.3
-rw-rw-rw-   1 root     system     34580 Nov 10 11:22 snaservice.4
-rw-rw-rw-   1 root     system    136036 Nov 10 13:50 snaservice.5
-rw-rw-rw-   1 root     system    402780 Nov 10 21:50 snaservice.6
-rw-rw-rw-   1 root     system     91900 Nov  9 11:31 snaservice.7
-rw-rw-rw-   1 root     system     24988 Nov  9 11:48 snaservice.8
-rw-rw-rw-   1 root     system     14108 Nov  9 11:51 snaservice.9
```

If your /var directory is full, AIX may get into trouble.

Now go to the SNA Server Advanced Configuration screen:

```
                              Advanced Configuration

Move cursor to desired item and press Enter.

  Links   ====>  SNA DLC and Link Station Profile
  Sessions
  SNA System Defaults
  Control Point
  Security
  Verify Configuration Profiles
  Export Configuration Profiles
  Import Configuration Profiles
  Migrate Configuration Profiles
```

Remember that you have to verify the configuration profiles every time you change anything. The four profiles you will have to change are:

- SNA Node Profile
- Control Point Profile
- Token-Ring SNA DLC Profile
- Link Station Profile

It is not necessary to configure any session profiles.

There is only one SNA Node Profile and Control Point Profile on each machine. The SNA Node Profile describes general parameters for SNA operations:

```
                           Change/Show SNA Node Profile

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                    (Entry Fields)
  Profile name                                      sna
  Maximum number of sessions (1-5000)              (200)                    #
  Maximum number of conversations (1-5000)         (200)                    #
  Restart action                                    once                   +
  Recovery resource manager (RRM) enabled?          no                     +
  Dynamic inbound partner LU definitions allowed?   yes                    +
  NMVT action when no NMVT process                  reject                 +
  Standard output file/device                      (/dev/console)
  Standard error file/device                       (/dev/console)

  Comments                                         ()
```

No change is required here.

The Control Point Profile provides identifying information such as the CP name, the XID and the network name. It also indicates the role of the local node in the network. It must be modified to fit your environment.

```
                    Change/Show Control Point Profile

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                        (Entry Fields)
* Profile name                                        node_cp
  XID node ID                                        (*)
  Network name                                       (USIBMRA)
  Control Point (CP) name                            (RA6005CP)
  Control Point alias                                (RA6005CP)
  Control Point type                                 appn_end_node          +
  Maximum number of cached routing trees             (500)                    #
  Maximum number of nodes in the TRS database        (500)                    #
  Route addition resistance                          (128)                    #

  Comments                                           ()
```

The node is identified either by the XID (that is IDBLK and IDNUM in VTAM) or by the CPNAME as defined in the VTAM switched major node. We used CPNAME. You have to enter the NETID of your domain. It is defined in the startlist of VTAM. The RS/6000 will act as an APPN end node in our network. You could instead define it as a network node. Both definitions work fine with VTAM V3 and VTAM V4.

The control point functions as a local LU for user transaction programs. This means you don't have to define a local LU on the workstation. When you are using VTAM V4 and its APPN functions, the CP of the VTAM network node will establish a CP-CP session. If you are using subarea SNA the CP acts as an LU 6.2.

The next screen shows the Change/Show Token-Ring SNA DLC Profile. You can have one DLC profile per adapter.

```
                    Change/Show Token Ring SNA DLC Profile

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

(TOP)                                                 (Entry Fields)
  Current profile name                               RS05ATT1
  New profile name                                   ()
  Data link device name                              (tok0)                  +
  Force disconnect time-out (1-600 seconds)          (120)                    #
  User-defined maximum I-Field size?                  no                     +
     If yes, Max. I-Field size (265-30729)           (30729)                  #
  Max. num of active link stationss (1-255)          (32)                     #
     Number reserved for inbound activation          (0)                      #
     Number reserved for outbound activation         (0)                      #
  Transmit window count (1-127)                      (16)                     #
  Dynamic window increment (1-127)                   (1)                      #
  Retransmit count (1-30)                            (8)                      #
  Receive window count (1-127)                       (8)                      #
  Ring access priority                                0                     +
  Inactivity time-out (1-120 seconds)                (120)                    #
  Response time-out (1-40, 500 msec intervals)       (4)                      #
  Acknowledge time-out (1-40, 500 msec intervals)    (1)                      #
  Local link name                                    (RS03TOK0)
  Local SAP address (02-fa)                          (04)                     X
  Trace base listening link station?                  yes                    +
     If yes, Trace format                             long                   +
  Dynamic link stations supported?                    yes                    +

  Link Recovery Parameters
     Retry interval (1-10000 seconds)                (60)                     #
     Retry limit (0 or 1-500 attempts)               (20)                     #
     Solicit SSCP sessions?                           yes                    +
     CP-CP sessions supported?                       yes
     Partner required to support CP-CP sessions?      no                    +

  Dynamic Link TG COS Characteristics
     Effective capacity                              (4300800)                #
     Cost per connect time                           (0)                      #
     Cost per byte                                   (0)                      #
     Security                                         nonsecure              +
     Propagation delay                                lan                    +
     User-defined 1                                  (128)                    #
     User-defined 2                                  (128)                    #
     User-defined 3                                  (128)                    #

  Comments                                           ()
```

We defined the support for CP-CP session here.

The last profile you should look at is the Token-Ring Link Station Profile. You can have more than one link per adapter, which means you can connect to different hosts using one adapter. Here you have to specify your destination token-ring address, which is in our case the 3745 Token-Ring adapter.

```
                Change/Show Token Ring Link Station Profile

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

(TOP)                                                 (Entry Fields)
  Current profile name                              RA60005
  New profile name                                 ()
  Use Control Point's XID node ID?                  yes                    +
     If no, XID node ID                            (*)
* SNA DLC Profile name                             (RS05ATT1)             +
  Stop link station on inactivity?                  no                     +
     If yes, Inactivity time-out (0-10 minutes)    (0)                     #
  LU address registration?                          yes                    +
     If yes, LU Address Registration Profile name  (RA60005)              +
  Trace link?                                       yes                    +
     If yes, Trace size                             long                   +

  Adjacent Node Address Parameters
     Access routing                                 link_address          +
     If link_name, Remote link name                ()
     If link_address,
        Remote link address                        (400001240000)
        Remote SAP address (02-fa)                 (04)

  Adjacent Node Identification Parameters
     Verify adjacent node?                          no                     +
     Network ID of adjacent node                   (USIBMRA)
     CP name of adjacent node                      (JUNK)
     XID node ID of adjacent node (LEN node only)  (*)
     Node type of adjacent node                     learn                  +
  Link Activation Parameters
     Solicit SSCP sessions?                         yes                    +
     Initiate call when link station is activated? yes                     +
     Activate link station at SNA start up?         yes                    +
     Activate on demand?                            no                     +
     CP-CP sessions supported?                      yes                    +
     If yes,
        Adjacent network node preferred server?     no                     +
     Partner required to support CP-CP sessions?    no                     +
     Initial TG number (0-20)                      (0)                     #

  Restart Parameters
     Restart on activation?                            no                  +
     Restart on normal deactivation?                   yes                 +
     Restart on abnormal deactivation?                 no                  +

  Transmission Group COS Characteristics
     Effective capacity                               (4300800)            #
     Cost per connect time                            (0)                  #
     Cost per byte                                    (0)                  #
     Security                                          nonsecure           +
     Propagation delay                                 lan                 +
     User-defined 1                                   (128)                #
     User-defined 2                                   (128)                #
     User-defined 3                                   (128)                #
```

Also in this panel we defined the support for CP-CP session. If you specify *Restart on normal deactivation* as yes, SNA Server will try to reconnect when the session is lost, for example, when the major node is inactivated.

A.1.3.3 Implementing a NetView Service Point Connection Using SNA Server

We used a 3172 as a gateway for Ethernet connectivity.

Activating Data Link Control: If SNA is being installed for the Ethernet adapter the first time, you will have to activate Data Link Control. To complete this, do the following:

- Select option **Devices from SMIT**
- Select option **Communication**
- Select option **Ethernet**
- Select option **Services**
- Add (or you may first display) **Data Link Controls**
- Select **IEEE Ethernet (802.3)**
- Press Enter

For the SNA connection, you have to use IEEE 802.3 Ethernet - standard Ethernet will not work.

Customizing the Profiles There are only two profiles you have to add to your SNA definitions:

- SNA DLC Profile
- Ethernet Link Station Profile

The first is used to add the ethernet interface as an SNA DLC; the second defines the link using this adapter. The definitions look similar to those used for token-ring:

```
                    Change/Show Ethernet SNA DLC Profile

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

(TOP)                                                 (Entry Fields)
  Current profile name                              RS05ATT2
  New profile name                                  ()
  Data link device name                             (ent0)                  +
  DLC protocol type                                 802.3           +
  Force disconnect time-out (1-600 seconds)         (120)                    #
  User-defined maximum I-Field size?                no                      +
     If yes, Max. I-Field size (265-30729)          (30729)                  #
  Max. num of active link stations (1-255)          (100)                    #
     Number reserved for inbound activation         (0)                      #
     Number reserved for outbound activation        (0)                      #
  Transmit window count (1-127)                     (16)                     #
  Retransmit count (1-30)                           (8)                      #
  Receive window count (1-127)                      (16)                     #
  Inactivity time-out (1-120 seconds)               (120)                    #
  Response time-out (1-40, 500 msec intervals)      (4)                      #
  Acknowledge time-out (1-40, 500 msec intervals)   (1)                      #
  Local link name                                   (RS03ENT0)
  Local SAP address (02-fa)                         (04)                     X
  Trace base listening link station?                yes                     +
     If yes, Trace format                           long                    +
  Dynamic link stations supported?                  no                      +

  Link Recovery Parameters
     Retry interval (1-10000 seconds)               (60)                     #
     Retry limit (0-500 attempts)                   (20)                     #

  Dynamic Link Activation Parameters
     Solicit SSCP sessions?                         yes                     +
     CP-CP sessions supported?                      yes             +
     Partner required to support CP-CP session?     no                      +

  Dynamic Link TG COS Characteristics
     Effective capacity                             (4300800)                #
     Cost per connect time                          (0)                      #
     Cost per byte                                  (0)                      #
     Security                                       nonsecure               +
     Propagation delay                              lan                     +
     User-defined 1                                 (128)                    #
     User-defined 2                                 (128)                    #
     User-defined 3                                 (128)                    #

  Comments                                          ()
(BOTTOM)
```

```
                    Change/Show Ethernet Link Station Profile

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

(TOP)                                              (Entry Fields)
  Current profile name                             RA60005E
  New profile name                                 ()
  Use Control Point's XID node ID?                  yes                          +
     If no, XID node ID                            (*)
* SNA DLC Profile name                             (RS05ATT2)                   +
  Stop link station on inactivity?                  no                           +
     If yes, Inactivity time-out (0-10 minutes)    (0)                           #
  LU address registration?                          yes                          +
     If yes, LU Address Registration Profile name  (RA60005)                    +
  Trace link?                                       yes                          +
     If yes, Trace size                             long                         +

  Adjacent Node Address Parameters
     Access routing                                 link_address                 +
     If link_name, Remote link name                ()
     If link_address,
        Remote link address                        (400060023172)     X
        Remote SAP address (02-fa)                 (04)                          X

  Adjacent Node Identification Parameters
     Verify adjacent node?                          no                           +
     Network ID of adjacent node                   (USIBMRA)
     CP name of adjacent node                      (JUNK)
     XID node ID of adjacent node (LEN node only)  (*)
     Node type of adjacent node                     learn                        +

  Link Activation Parameters
     Solicit SSCP sessions?                         yes                          +
     Initiate call when link station is activated? yes                           +
     Activate link station at SNA start up?         no                           +
     Activate on demand?                            no                           +
     CP-CP sessions supported?                      yes                          +
     If yes,
        Adjacent network node preferred server?     no                           +
     Partner required to support CP-CP sessions?    no                           +
     Initial TG number (0-20)                      (0)                           #

  Restart Parameters
     Restart on activation?                         no                           +
     Restart on normal deactivation?                no                           +
     Restart on abnormal deactivation?              no                           +

  Transmission Group COS Characteristics
     Effective capacity                            (4300800)                     #
     Cost per connect time                         (0)                           #
     Cost per byte                                 (0)                           #
     Security                                       nonsecure                    +
     Propagation delay                              lan                          +
     User-defined 1                                (128)                         #
     User-defined 2                                (128)                         #
     User-defined 3                                (128)                         #

  Comments                                           ()
```

We deactivated SNA, started it and activated the Ethernet link. This is the display active link window we got:

```
                                COMMAND STATUS

Command: OK            stdout: yes           stderr: no

Before command completion, additional instructions may appear below.

    Link           Adjacent      Node    Device             # of local  In
   station         CP name       type     name      State    sessions   use
-------------- ----------------- ----- --------- ---------- ---------- -----
@ent0.4                                 ent0      Starting            0 No
RA60005E       USIBMRA.RAB       NN    ent0      Active              2 Yes
@tok0.4                                 tok0      Starting            0 No
```

We tested some topology agent functions after this and everything worked fine.

A.1.4 Implementing a NetView Service Point Connection Using SNA Services

A.1.4.1 Miscellaneous

Including Service Point: After the installation, you have to issue the AIX command `nvix_customize_sp`. This includes Service Point into the SMIT menus and creates sample SNA profiles for both SSCP-PU session and LU 6.2 sessions. This command only works if your current directory is /usr/lpp/nvix/scripts or if you have defined this directory as a PATH either by command or in your .profile.

Activating Data Link Control: If SNA is being installed on your machine for the first time, you will have to activate Data Link Control for the adapter used. For use with token-ring for example, do the following:

- Select option **Devices from SMIT**
- Select option **Communication**
- Select option **Token Ring**
- Select option **Services**
- Add (or you may first display) **Data Link Controls**

The same has to be done for the multiprotocol adapter or the Ethernet adapter if used.

Update TCP/IP Definitions: You may have to update two TCP/IP definition files in AIX:

- /etc/hosts
- /etc/services

Verify that there is a loopback entry in your hosts file as in this example:

```
#9.67.32.242   rs60002b rs60002
127.0.0.1      loopback localhost #needed for SMUX
#9.67.32.85    rs60001e rs60001
#9.67.32.25    robmac
```

The figure above shows a part of the /etc/hosts file being used in the ITSO RISC/6000.

Next you have to insert the following entries into the etc/services file:

```
nvixacm          7111/tcp
nvixclb          7112/tcp
nvixcr           7113/tcp
nvixfts          7114/tcp
nvixsp           7115/tcp
nvixspc          7116/tcp
```

Make sure the ports are not in use yet (usually ports 7111-7116 are not).

Updating SNA

Note: This step has only to be done if you want to use an SSCP-PU session.*:* To avoid VTAM errors when trying to start the Trap to Alert Daemon tralertd, you should export the SNA profiles to a file by stepping through the following SMIT menus:

- Communications
- SNA Services
- Configure
- Advanced Configuration
- Export SNA profiles

This will write out the definitions to a file. Go to the file and find the *sna* SNA Profile. Change the parameter nmvt_action_when_no_nmvt_process=reject to =queue as shown below.

```
#SNA  01.02.0101.0315   ***DO NOT MODIFY OR REMOVE***

sna_SNA:
    type = SNA
    profile_name = sna
    total_active_open_connections = 200
    total_sessions = 200
    total_conversations = 200
    server_synonym_name = sna
    nmvt_action_when_no_nmvt_process = queue
    restart_action = once
    stdin = /dev/console
    stdout = /dev/console
    stderr = /dev/console
    sna_error_log = yes
```

Having changed the SNA profile as illustrated above, import the profiles to include the changed definition.

A.1.4.2 Customizing the Profiles Using Token-Ring Adapter

Customize Service Point Profile Summary: Go to NetView Service Point Profile Summary using SMIT (selecting **Communication**, **Service Point**, **Configure**...). The appropriate panel is shown in Figure 156.

```
                NetView Service Point Profile Summary

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                  (Entry Fields)
* PU-SSCP Attachment                              NVIXTA01                  +
* SSCP Id                                        (05000000000B)            +
* CP Name                                        (RA62221A)
  FTS LU6.2 Logical Connection                    ()                        +
* Polling Period                                  (300)                      #
  Service Point Codepage                          ( )
  MDS LU6.2 Logical Connection                    (NVIXLCMDS1)              +
```

Figure 156. NetView Service Point Profile Summary for SNA Server

Before you start the Service Point, you have to start SNA without any attachment or connection. This can be done with the command `startsrc -s sna` or with SMIT. When Service Point is started it will start up the logical connection defined in the Service Point Profile Summary - in the example above the default NVIXLCMDS1 is used.

When the parameter MDS LU6.2 Logical Connection is filled in, the use of LU 6.2 connection is assumed. Then the fields PU-SSCP Attachment and SSCP ID are ignored although they do have to be filled in. As shown in Figure 157 on page 199, all other profiles are loaded by pointers.

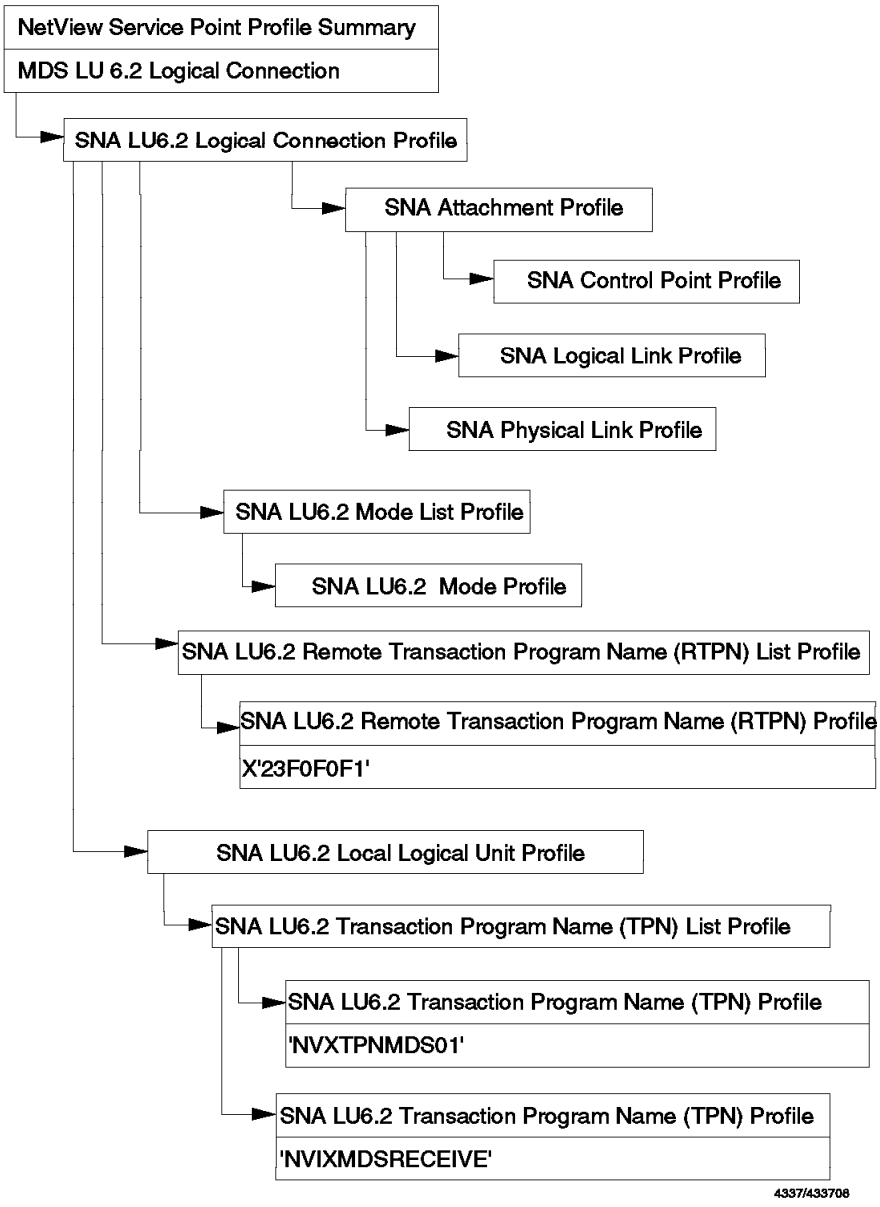


Figure 157. Structure of SNA Services Profiles

Note

All of the above profiles are provided as default profiles except for the TPN profile NVIXMDSRECEIVE, which you have to create manually. If you are using the default profile names, the logical connection profile name is NVIXLCMDS1. The CP Name should now be the VTAM name of the LU as also specified in the Local Logical Unit Profile. This name is used as the SP parameter in the RUNCMD. Defining anything other than the LU name in this field may lead to unpredictable results. No other parameters have to be changed.

The definitions are described below.

Configuring SNA Profiles: When you step through the Service Point SMIT menus, you will find an item Configure SNA Services. Service Point creates default profiles in the SNA section for the Service Point. These usually start with the prefixes NVIX or NVX. There are different profiles created for SSCP-PU and LU 6.2 session. The profiles for the LU6.2 session contain the string MDS.

We recommend using those default names. There are a lot of pointers to other profiles in the definitions that use these names as references. We found it helpful to stick with the samples as they are consistent and they work. Anyhow, the names, except for those of the Transaction Program Name profiles, do not have any other significance and may be changed. SNA Services also provides a tool called Quick Configuration, which gives you some LU 6.2 configuration and might be helpful for other occasions. As the profiles are built automatically, you don't know what has been done, which might lead to problems in tracking errors, unless you are experienced in using SNA Services.

As an active attachment is a prerequisite for any connection to become active the first step explained here is the customization of the attachment.

Note

If you are already running SNA on the machine and there is a PU in use (for example, for HCON), you must use this connection. One adapter can only have one physical link and represent one PU. It's no problem using the same attachment for both Service Point and HCON. You can use the LU 6.2 profiles as described below, but you have to change the fields referring to the profiles defining the PU.

Shown below are the profiles used for defining an SNA PU (extracted from Figure 157 on page 199):

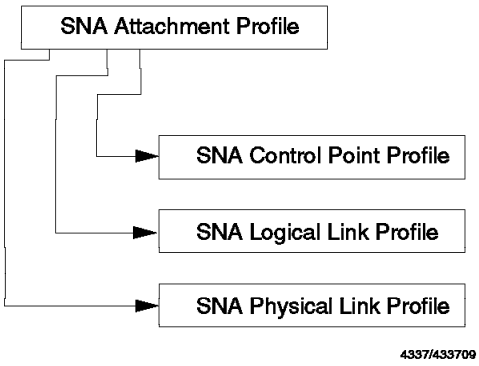


Figure 158. Structure of SNA Profiles

Start the process of defining a PU by selecting the following options: **Advanced SNA Configuration**, **Nodes** and **Control Point**. The resulting SNA Control Point Profile is shown below:

```
                Change / Show SNA Control Point Profile

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                  (Entry Fields)
  CURRENT profile name                           NVIXCP
  NEW PROFILE name                               ()
  XID node ID                                    (05D62221)                  X
  NETWORK name                                   (USIBMRA)
  CONTROL POINT name                             (SPCP)
```

The XID is composed of the IDBLK and IDNUM parameters in the VTAM PU definition statement; the first is IDBLK. This parameter only needs to match the VTAM definitions; you don't have to use any special value for Service Point. The Network Name and the CPNAME are optional fields. If they are specified, they are passed to VTAM; so they have to match VTAM naming rules. We used the network name as defined in the VTAM startlist ATCSTRxx and SPCP as control point name. If CPNAME was specified in VTAM, you should use this.

The SNA profile does not have to be customized.

The next screen shows the Attachment Profile, in our case a token-ring attachment, which is located under the SMIT entry Physical Units.

```
                    Change / Show SNA Token Ring Attachment Profile

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

(TOP)                                             (Entry Fields)
  CURRENT profile name                           NVIXTA01
  NEW PROFILE name                               ()
  CONTROL POINT profile name                     (NVIXCP)                    +
  LOGICAL LINK profile name                      (NVIXLLT1)                  +
  PHYSICAL LINK profile name                     (NVIXPLT1)                  +
  STOP ATTACHMENT on inactivity?                  no                         +
     If yes, inactivity TIMEOUT (0-10 minutes)   (0)                          #
  RESTART on deactivation?                        no                         +
  LU address REGISTRATION?                        no                         +
   If yes, LU address REGISTRATION PROFILE name  (LDEFAULT)                  +
  CALL type                                       call                       +
     If listen,
        AUTO-LISTEN?                              no                         +
        MINIMUM SAP address (hex 04-ec)          (04)                         X
        MAXIMUM SAP address (hex 04-ec)          (EC)                         X
     If call, ACCESS ROUTING                      link_address               +
        If link_name, REMOTE LINK name           ()
        If link_address,
           Remote LINK address                   (400001260000)             X
           Remote SAP address (hex 04-ec)        (04)                         X
```

You have to fill in your SNA Gateway's MAC address - in our case the token-ring adapter address of the 3745 token-ring interface coupler (TIC).

The next profile is the Physical Link Profile, which you will find by selecting the option **Data Link Control**.

```
                Change / Show SNA Token Ring Physical Link Profile

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                  (Entry Fields)
  CURRENT profile name                           NVIXPLT1
  NEW PROFILE name                               ()
  DATALINK device name                           (tok0)                    +
  LOCAL LINK name                                ()
  Maximum number of LOGICAL LINKS (1-255)        (32)                       #
  Local SAP address (hex 04-ec)                  (04)                       X
```

Make sure the DATALINK device name is the adapter you want to use. The Logical Link Profile needs no change.

A.1.4.3 Setting up the LU 6.2 session

Now customize the LU. You will find all the profiles by selecting the **Logical Units** option. Choosing the LU6.2 entry in this menu results in the following screen:

```
                                      LU6.2

Move cursor to desired item and press Enter.

  LU6.2 Local Logical Unit
  LU6.2 Logical Connection
  LU6.2 Mode
  LU6.2 Mode List
  LU6.2 Transaction Program Name (TPN)
  LU6.2 Transaction Program Name List
  LU6.2 Conversation Security Options
  LU6.2 Remote Transaction Program Name (RTPN)
  LU6.2 Remote Transaction Program Name List
  LU6.2 CPI Communications Side Information
```

As it is the central profile, referring to all others, the Logical Connection Profile will be discussed first. A sample listing of the profile input window is provided below.

```
        Change / Show SNA LU6.2 Logical Connection Profile

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

(TOP)                                          (Entry Fields)
  CURRENT profile name                         NVIXLCMDS1
  NEW PROFILE name                             ()
  ATTACHMENT profile name                      (NVIXTA01)                +
  LOCAL LU profile name                        (NVIXL62MDS1)             +
  NETWORK name                                 (USIBMRA)
  STOP CONNECTION on inactivity?               no                        +
     If yes, TIMEOUT (0-10 minutes)            (3)                        #
  REMOTE LU name                               (RABAN)
  SECURITY Accepted                            none                      +
     If conversation or already_verified,
     CONVERSATION SECURITY ACCESS LIST profile (CONVDEFAULT)
        (If no name entered, /etc/passwd used)
  REMOTE TPN LIST profile name                 (NVXRTPLMDS1)             +
  MODE LIST profile name                       (NVIXMLPMDS1)             +
  INTERFACE type                               extended                  +
     If extended, SESSION CONCURRENCY          parallel                  +
  Node VERIFICATION?                           no                        +
```

In the LU6.2 Logical Connection Profile window, enter the NETWORK name of the NetView/MVS you want to reach and its LU name. The LU name of NetView/MVS is defined in the VTAM APPL major node for NetView. Those parameters together build the fully qualified LU name of your partner LU. Now we will step through the various panels used for LU 6.2 definitions (see Figure 157 on page 199).

```
                  Change / Show SNA LU6.2 Local LU Profile

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                               (Entry Fields)
  CURRENT profile name                         NVIXL62MDS1
  NEW PROFILE name                             ()
  TPN LIST profile name                        (NVIXTPLMDS1)             +
  NETWORK name                                 (USIBMRA)
  Local LU NAME                                (RA62221A)
  INDEPENDENT LU?                              yes                       +
     If no,
        Local LU ADDRESS (1-255)               (1)                       #
        SSCP ID                                ()
```

Here you have to define your own fully qualified LU name, so fill in your own LU name, which you also used in the Service Point Profile Summary and your own network name.

Now, as you have defined the LUs, you have to define the transaction programs. There are lists for the local and the remote transaction profiles. You have to add the profile NVIXMDSRECEIVE to the provided local transaction program list. The List Profile should look like this:

```
                    Change SNA LU6.2 TPN List Profile

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

(TOP)                                                (Entry Fields)
  CURRENT profile name                                 NVIXTPLMDS1
  NEW PROFILE name                                     ()
  DELETE profile names from list (F4 to list)                                +
  Add profile names to list:
     Name  1                                  (NVXTPNMDS01)                  +
     Name  2                                  (NVIXMDSRECEIVE)               +
     Name  3                                  ()                             +
     Name  4                                  ()                             +
     Name  5                                  ()
```

No changes are required in the default transaction profiles NVXTPNMDS01. The transaction profile NVIXMDSRECEIVE has to be added manually, it is not provided as a default profile. It is just the same as NVIXTPNMDS01 except that the Transaction Program Name field is blank and the full path to TPN executable is /dev/null as shown below:

```
                    Change / Show SNA LU6.2 TPN Profile

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                      (Entry Fields)
  CURRENT profile name                               NVIXMDSRECEIVE
  NEW PROFILE name                                   ()
  Transaction program name is in HEXADECIMAL?         yes                    +
  TRANSACTION program name                           ()
  PIP data?                                           no                     +
     If yes, SUBFIELDS (0-99)                        (0)                     #
  CONVERSATION type                                   basic                  +
  RECOVERY level                                      no_reconnect           +
  SYNC level                                          confirm                +
  Full PATH to TPN executable                        (/dev/null)
  MULTIPLE INSTANCES supported?                       no                     +
  User ID                                            (0)                     #
  SERVER synonym name                                ()
  RESTART action                                      once                   +
  COMMUNICATION type                                  sockets                +
     If IPC, communication IPC queue key             (0)
  Standard INPUT file/device                         (/dev/null)
  Standard OUTPUT file/device                        (/dev/console)
  Standard ERROR file/device                         (/dev/console)
  SECURITY Required                                   none                   +
     If access,
        RESOURCE SECURITY ACCESS LIST profile        (RSRCDEFAULT)
        (If no name entered, /etc/passwd used)
```

The remote transaction profile list and the remote transaction profiles do not have be changed either, if you have used the default profiles.

The same is true for the Mode List Profile and the Mode Profile. The defaults should work fine.

Verify that the field MODE name is blank in the Mode Profile as shown below:

```
                    Change / Show SNA LU6.2 Mode Profile

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                      (Entry Fields)
  CURRENT profile name                               NVIXMOPMDS1
  NEW PROFILE name                                   ()
  MODE name                                          (        )
  Maximum number of SESSIONS (1-999)                 (8)                    #
  Minimum contention WINNERS (0-499)                 (1)                    #
  Minimum contention LOSERS (0-500)                  (0)                    #
  Auto ACTIVATIONS limit (0-500)                     (0)                    #
  RECEIVE pacing (0-63)                              (7)                    #
  SEND pacing (0-63)                                 (7)                    #
  Maximum RU SIZE (256,288,...,3840)                 (2816)                 #
  RECOVERY level                                      no_reconnect          +
```

Now you can leave the configuration panels and start SNA.

A.1.4.4 Customizing the Profiles Using Ethernet Adapter

No default profiles are provided for an Ethernet connection. In our test environment we used a 3172 as a gateway.

Activating Data Link Control: If SNA is being installed for the Ethernet adapter the first time, you will have to activate Data Link Control. To do this, do the following:

- Select option **Devices from SMIT**
- Select option **Communication**
- Select option **Ethernet**
- Select option **Services**
- Add (or you may first display) **Data Link Controls**
- Select **IEEE Ethernet (802.3)**
- Press Enter

For the SNA connection you have to use IEEE 802.3 Ethernet - standard Ethernet will not work.

Customizing the Profiles: We used most of the token-ring profiles described earlier. Only the profiles listed below had to be created for the Ethernet connection, and only minor changes had to be made compared to the Token Ring profiles:

- MDS LU 6.2 Logical Connection
- SNA Attachment Profile
- SNA Logical Link Profile
- SNA Physical Link Profile

The changes we made are described briefly below.

MDS LU 6.2 Logical Connection: We called this profile NVIXLCMDS2. The only thing different from the profile used for the token-ring connection was the Attachment Profile name, which was the name of our Ethernet attachment NVIXEA01.

SNA Attachment Profile: This profile we named NVIXEA01. You have to specify the MAC address of your gateway machine and the profile names of the logical and physical link profile. All other parameters are the same as described for the token-ring connection.

SNA Logical Link Profile: You have to create a Logical Link Profile for Ethernet with the name used in the attachment profile. We used NVIXLLE1.

SNA Physical Link Profile: Our Physical Link Profile was called NVIXPLE1, and the only thing changed was the DATALINK device name which referred to our Ethernet adapter.

To start the Ethernet connection you have to change the NetView Service Point Profile Summary. Just fill in the name of your new MDS LU 6.2 Logical Connection, which in our case was NVIXLCMDS2.

To define a connection using the multiprotocol adapter, similar changes have to be made to those profiles.

A.1.5 Start and Test Connectivity

After you have completed the SNA customization, you should complete the following steps:

- Check your language environment variable.
- Set up the applications (tralertd, spappld).
- Start up subsystems and processes.
- Control Status.
- Issue RUNCMD; send trap/alert to NetView/MVS.

Check Your Language Environment Variable: Use the command `ECHO $LANG`. If it is not En_US, change it with the command `export LANG=En_US`.

Set up the Applications (Spappld, Tralertd): There are two host connection daemons provided with NetView/6000, the trap to alert daemon (called tralertd) and the service point application daemon (called spappld). To configure them call SMIT nv6000 and select the following menu items from SMIT: **Configure**, **Set options for AIX NetView/6000 daemons** and **Set options for host connection daemons**. You will get a menu with two options: Set options for tralertd daemon and Set options for spappld daemon. You have to open both menus, although changes are only required in the spappld configuration. When you open those menus, a registration file for each of the daemons is created. These lrf files, which stands for local registration files, are necessary for the start up of the daemons. They are called /usr/OV/lrf/spappld.lrf and /usr/OV/lrf/tralertd.lrf. You should consider changing the application names, which have generic defaults. They are used to address the spappld in the RUNCMD and as a qualifier in the alert sent to NetView/MVS by tralertd. Using meaningful names here may help

you. Because our machine is called rs60001, we named both applications rs60001s. For MSM both applications *must* have the same name.

```
                        Set Options for tralertd daemon

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                    (Entry Fields)
  Tracing mask:                                    (0)
  Full path name of trace file:                    (/usr/OV/log/tralertd.t>
* Service point application name:                  (RS60005S)
  Service point host name:                         ()
* Are you using NETCENTER?                         no
       if yes:
     Domain name:                                  (SNMP)
     Standalone timeout:                           (90)
```

```
                         Set Options for spappld daemon

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                    (Entry Fields)
  Service point host name:                        ()
* Service point application name:                 (RS60005S)
  Execute shell state:                            bsh(Bourne)
  Execute shell path:                             (r/OV/bin:/usr/lpp/msmip)
  Log service point transactions?                 yes
  Full path name of log file:                     (/usr/OV/log/NV390.log)
  Tracing mask:                                   (0)
  Full path name of trace file:                   (/usr/OV/log/NV390.trac>
  Are you using NETCENTER:                        no
```

Note

We did not fill out the Service Point host name. It is only required if distributed Service Point is used. If Service Point and NetView/6000 are running on the same machine, filling in this parameter makes the processes communicate via TCP sockets, which is unnecessary. You have to add the PATH to MSM′s executables to the execute shell path. Shell scripts that are located in directories different from those specified here can only be executed if the path is specified with the command. As the RUNCMD command is considered to be a root user and therefore is authorized to issue any commands, this might be a way of reducing the commands that are allowed by default. Add `:/usr/lpp/msmip` to the PATH statement as shown above. The execute shell state requires no change. It specifies the shell used for the commands you send down with a RUNCMD command (bsh means bourne shell). Nevertheless AIX-skilled operators could bypass this restriction by specifying the full path name of the shell they want to use.

Startup: When everything is customized, you have to start up in the following order:

- Check portmap and start if it is not running with the commands `lssrc -s portmap` and `startsrc -s portmap`.
- Start SNA by issuing the command `startsrc -s sna` or using SMIT.
- Start Service Point by issuing the command `nvix_control start` or using SMIT.
- Start the host connection daemons by issuing the commands `ovstart spappld` and `ovstart tralertd` or using SMIT.

Note

The line commands only work if your current directory is */usr/lpp/nvix/scripts* for the Service Point commands and */usr/OV/bin* for the NetView/6000 commands unless you have issued the AIX *set PATH=* command or included those directories in your *.profile*.

Control Status: To be sure everything is fine, do the following:

- After you start SNA, check SNA status. It should be *sna active*.

  If you are using SNA Server, check if the CP-CP session is active. In SMIT select **Display SNA Resources**, **Display Active Link Information** and press Enter. Your output should look similar to this:

```
                                COMMAND STATUS

Command: OK            stdout: yes           stderr: no

Before command completion, additional instructions may appear below.

    Link           Adjacent      Node    Device             # of local  In
   station         CP name       type     name      State    sessions   use
-------------- ----------------- ----- --------- ---------- ---------- -----
@tok0.4                               tok0      Starting            0 No
RA60005        USIBMRA.RAK       NN    tok0      Active              8 Yes
```

Note: If you are using VTAM V3, the Node type will show LEN instead of NN. If the link is not active, activate it manually using the SMIT menus or with the command

`sna -s l -p linkstationname.`

Then check the status again. To start the link automatically when SNA is started, you have to set the parameter Activate link station at SNA start up? to yes in the Link Station Profile.

You can also check the status of the connection in VTAM. A display of the PU shows that the CP is active and in session:

```
IST075I  NAME = RA60005          , TYPE = PU_T2.1
IST486I  STATUS= ACTIV--L--, DESIRED STATE= ACTIV
IST1043I  CP NAME = RA6005CP, CP NETID = USIBMRA , DYNAMIC LU = YES
IST1105I  RESOURCE STATUS TGN CP-CP TG CHARACTERISTICS
IST1106I  RA60005  AC/R    21 YES   982D000000000000000000017100808080
IST136I  SWITCHED SNA MAJOR NODE = RS60005
IST081I  LINE NAME = JOOOOOOF, LINE GROUP = EG24LOO , MAJNOD = RAONCPA
IST654I  I/O TRACE = OFF, BUFFER TRACE = OFF
IST355I  LOGICAL UNITS:
IST080I  RA600052 PACTL      RA600053 PACTL      RA600054 PACTL
IST080I  RA600055 PACTL      RA600056 ACTIV      RA600057 ACTIV
IST080I  RA600058 ACTIV      RA600059 ACTIV
IST080I  RA6005CP ACT/S----Y
```

If you display the control point you will find the CP-CP session where ACTIV/CP is shown:

```
IST171I  ACTIVE SESSIONS = 0000000002, SESSION REQUESTS = 0000000000
IST206I  SESSIONS:
IST1081I  ADJACENT LINK STATION = RA60005
IST634I  NAME     STATUS         SID          SEND RECV VR TP NETID
IST635I  RAK      ACTIV/CP-S E09B58133C577D10 0002 0001  0  0 USIBMRA
IST635I  RAK      ACTIV/CP-P F8D3D1647961A2A2 0001 0001  0  0 USIBMRA
IST924I  -------------------------------------------------------------
```

- After you started the Service Point check SNA status again. If you use SNA Services now, the attachment and the connection you want to use with Service Point should be active. The default names are NVIXTA01/NVIXSA01 and NVIXLCMDS1.

  Then check the status of the Service Point. There are two processes which have to be active: *evp_nvixSrd* and *evp_nvixCrd* . Don't worry if the other processes are inoperative. With SNA Services you should also get a message:

  `MDS LU6.2 session is active using profile NVIXLCMDS1.`

  Using SNA Server check for the message:

  `MDS session is active at the Service Point.`

  This sounds good, but does not guarantee everything is OK. For SNA Services check the VTAM status of your PU now - the PU should be active and the LU 6.2 should be active and in session.

- After you started the host connection daemons, check their status. They should be running now. When you check the Service Point Status again, you should find your spappld application name registered under:

*** Applications registered to receive commands from Host: ***

Issue RUNCMD and Send Trap/Alert to NetView/MVS: The last step to do is to test the connection. To test the spappld connection, issue a RUNCMD command from NetView/MVS.

Note: You should send a RUNCMD command before sending the first trap.

One way to send commands to a NetView/6000 workstation is to type in the RUNCMD directly at the NetView command line (NCCF). A brief description of the command syntax is provided below to illustrate the information required as input to the RUNCMD.

```
RUNCMD SP=service_point_name,
   APPL=application name,
   NETID=netid,
   command
```

Where:

SP is the LU name for LU 6.2 session using SNA Services and the CP name using SNA Server.

APPL is the name of the Service Point application SPAPPLD as specified in the set options... menu for host connection daemons in NetView/6000 SMIT.

NETID is the NETID if the partner LU belongs to another SNA network.

command can be any AIX, SNMP or NetView/6000 command string. An AIX shell script may also be invoked. Verify that the path statement in the customization screen for spappld contains the path to the executable you want to trigger.

The next function to test is the tralertd connection. You can generate a trap to be sent with the nvevent command or from the NetView/6000 SMIT menus. Choose **Diagnose** and **Send event to trapd daemon**. Make sure there is no filter active which might block the trap you are sending. If everything works fine, you should be able to find the alert in NetView's Hardware Monitor (NPDA) as shown below:

```
N E T V I E W          SESSION DOMAIN: RABAN    STEFFES   05/12/94 17:50
NPDA-30A                      * ALERTS-DYNAMIC *

  DOMAIN RESNAME  TYPE TIME  ALERT DESCRIPTION: PROBABLE CAUSE
   RABAN PSAIX    DEV  17:50 NO COMM WITH REMOTE NODE: COMM/REMOTE NODE
   RABAN PSAIX    DEV  17:50 NO COMM WITH REMOTE NODE: COMMUNICATIONS I
   RABAN RS60006  DEV  17:45 NO COMM WITH REMOTE NODE: COMM/REMOTE NODE
   RABAN RS60006  DEV  17:45 NO COMM WITH REMOTE NODE: COMMUNICATIONS I
   RABAN RS60001  DEV  17:43 NO COMM WITH REMOTE NODE: COMM/REMOTE NODE
   RABAN RS60001  DEV  17:43 NO COMM WITH REMOTE NODE: COMMUNICATIONS I
   RABAN EAMON    DEV  17:39 PROBLEM RESOLVED: REMOTE NODE
   RABAN EAMON    DEV  17:39 PROBLEM RESOLVED: COMMUNICATIONS INTERFACE
   RABAN EAMON    DEV  17:34 NO COMM WITH REMOTE NODE: COMM/REMOTE NODE
   RABAN EAMON    DEV  17:34 NO COMM WITH REMOTE NODE: COMMUNICATIONS I
   RABAN RS60009A DEV  17:32 PROBLEM RESOLVED: REMOTE NODE
   RABAN RS60009A DEV  17:32 PROBLEM RESOLVED: REMOTE NODE
   RABAN RS60009A DEV  17:32 PROBLEM RESOLVED: REMOTE NODE
```

Before you start the NetView/6000 Host Application Daemons, you might want to check if the Service Point is operational. Service Point V1.2.1 provides two commands as test tools. To test the RUNCMD command, issue the following command from your AIX command line:

```
rs60005:/ > usr/lpp/nvix/bin/cmdappl &
```

You can issue a RUNCMD from the focal point NetView now using the following syntax:

```
RUNCMD SP=cpname APPL=cmdappl anycommand
```

The response should be:

```
* RAKAN    RUNCMD SP=RA6005CP APPL=CMDAPPL ANY
-          this is the response to command <ANY> from NetView
```

Note: The process cmdappl can only be stopped with an AIX kill command.

To test the alert forwarding function, issue the command:

```
rs60005:/ > /usr/lpp/nvix/bin/testa
status=00000000 for alert session status
status=00000000 for alert send
```

This sends an alert to the focal point NetView. To find the alert in NetView go to the NPDA ALERTS-DYNAMIC screen (npda ald):

```
NPDA-30A                      * ALERTS-DYNAMIC *

    DOMAIN RESNAME  TYPE TIME  ALERT DESCRIPTION: PROBABLE CAUSE
     RAKAN NVIXSP  *TP   14:46 OUT OF COINS: COIN DISPENSER
```

The alert detail looks like this:

```
NPDA-45A           * RECOMMENDED ACTION FOR SELECTED EVENT *
 RAKAN       RA6005CP     NVIXSP       TESTA678
            +---------+               +---------+
 DOMAIN     |  CP     |---<  PROG  >---|  TP     |
            +---------+               +---------+

USER    CAUSED - NONE

INSTALL CAUSED - NONE

FAILURE CAUSED -  FAILING COMPONENT IS IDENTIFIED BY:
                      money machine CARTRIDGE wallet in
                      CARTRIDGE my pocket
       ACTIONS - I148 - WAIT FOR ADDITIONAL MESSAGE BEFORE TAKING ACTION
```

A.2 VTAM Definitions for SNA Server Connectivity

For the CP-CP session used by SNA server with VTAM V4, no LU definitions are required. This is the minimum information required:

```
 BROWSE    RISC.VTAMLST(RS60005) - 01.03             Line 00000000 Col
******************************** Top of Data ***************************
RA6RS05 VBUILD MAXGRP=10,              REQUIRED                      * X
               MAXNO=18,               REQUIRED                      * X
               TYPE=SWNET              REQUIRED
RA60005  PU    ADDR=13,                COULD BE ANYTHING (NOT USED)  * X
               CPNAME=RA6005CP,        USED FOR NVIX                 * X
               ANS=CONTINUE,                                           *
               PUTYPE=2
RA600052 LU    LOCADDR=2,                                              *
               MODETAB=MODNDM12,                                       *
               DLOGMOD=AIXLGMD1,                                       *
               ISTATUS=ACTIVE
RA600053 LU    LOCADDR=3,                                              *
               MODETAB=MODNDM12,                                       *
               DLOGMOD=AIXLGMD1,                                       *
               ISTATUS=ACTIVE
******************************** Bottom of Data ************************
```

The LUs are used for HCON.

If you are using VTAM V3, you don't have to define the LU at the workstation as well, but you have to define a LU 6.2 in the major node with the name of the AIX control point. For testing we added the statement CONNTYPE=LEN, to simulate VTAM V3.4.

```
 BROWSE    RISC.VTAMLST(RS60005) - 01.03             Line 00000000 Col
******************************** Top of Data ************************
RA6RS05 VBUILD MAXGRP=10,              REQUIRED                      * X
               MAXNO=18,               REQUIRED                      * X
               TYPE=SWNET              REQUIRED
RA60005  PU    ADDR=13,                COULD BE ANYTHING (NOT USED)  * X
               CPNAME=RA6005CP,        USED FOR NVIX                 * X
               ANS=CONTINUE,                                           *
               PUTYPE=2,*
               CONNTYPE=LEN
RA6005CP LU    LOCADDR=0,MODETAB=AMODETAB,DLOGMOD=DSIL6MOD
RA600052 LU    LOCADDR=2,                                              *
               MODETAB=MODNDM12,                                       *
               DLOGMOD=AIXLGMD1,                                       *
               ISTATUS=ACTIVE
RA600053 LU    LOCADDR=3,                                              *
               MODETAB=MODNDM12,                                       *
               DLOGMOD=AIXLGMD1,                                       *
               ISTATUS=ACTIVE

******************************** Bottom of Data *********************
```

Appendix B. Customizing AIX for Topology Manager

B.1 Log Maintenance

NetView/6000 logfiles generally expand continuously until the disk is full. Especially the MSM heartbeat function, which checks if the Service Point and the MSM topology agent are still alive, fills up the NV390.log especially rapidly.

A procedure to do this automatically is considerable. For this you can use the NetView/6000 SMIT. Select **Maintain** and **Manage crontab entries for log, trace, or collector files**. You get a list of all log, trace and collector files that should be maintained regularly. When you choose **NV390.log** from that list, you get another list offering *set, clear* and *display*. Select **set** and press Enter. You get the default crontab entry for the logfile. Change it as you like. We did the following:

```
   Set crontab entries for log, trace, or collector files


Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                          (Entry Fields)
  Set crontab for...                  /usr/OV/log/NV390.log
* The minute:                        (0)
* The hour:                          (1)
* The day of the month:              (*)
* The month of the year:             (*)
* The day of the week:               (*)
* Shell command:                     (/usr/bin/cat /dev/null > /usr/OV/log/NV390.log
```

The shell command clears the logfile. It is issued every day in every month at 1:00 a.m. Because the heartbeat is running day and night, we found this helpful.

B.2 Maintaining the Databases

As the MSM topology agent retrieves information from the ovw database and from the topology database literally, you should watch the databases carefully! Inconsistencies in the NetView for AIX databases can lead to confusing results in RODM and NGMF or even cause the GETTOPO IPRES to fail with the message FLC070E, RODM PROCESSING ERROR. You should use NetView for AIX or NetView/6000 with latest maintenance level because there were some problems in earlier releases with resources that were initially discovered as routers and later changed to be hosts.

To avoid those problems, you should run the NetView for AIX ovtopofix command before you issue the first GETTOPO. To be sure your database is in good shape you might consider running the ovtopofix command regularly later as well. Inconsistencies can appear whenever PTFs are applied or different maps are edited.

This is a description of the *ovtopofix* command:

```
-----------------------------------------------------------------
ovtopofix
-----------------------------------------------------------------


Purpose

Corrects inconsistencies between ovtopmd and ovwdb


Description

The ovtopofix command is used to detect and correct
inconsistencies that might develop between the IP topology
database and the ovwdb database.  The default behavior is to
remove old hints from the ovwdb database and to verify the
managed and removed state of all objects.  As inconsistencies are
discovered, ovtopofix reports actions taken to the standard
output.

If updates to the databases are attempted, the ovtopofix command
verifies that no ipmap or netmon process is currently running.
```

To invoke the ovtopofix command start the NetView for AIX daemons using SMIT or with the command ovstart. Then do the following:

- stop netmon: ovstop netmon
- run ovtopofix: ovtopofix
- start netmon: ovstart netmon

Your output may look similar to this:

```
deleting object 620 (HINT).
deleting object 579 (HINT).
2 objects removed from ovwdb (2 hints, 0 old hints, 0 still valid)
```

The ovtopofix command corrects inconsistencies and recommends deleting resources that are only in some of the topology maps. This can be the case, if you delete resources on some submaps to manage only a certain part of your IP network. Objects are kept in the object database until they are deleted from all maps. As objects are not rediscovered until they are deleted from the object database, you might want to delete those objects from all maps. Otherwise ignore the messages.

To invoke the ovtopofix command regularly, you should consider setting up a crontab entry. This might be helpful if your topology databases change a lot. You can do this with the following command:

```
rs60005:/>  crontab (press enter)
0 1 * * 1 ovstop netmon ; ovtopofix ; ovstart netmon (enter and Ctrl D)
```

This crontab entry runs the ovtopofix every Monday morning at 1:00 a.m.

If you have problems with your databases, although you have run the ovtopofix, for example, some objects or links are not shown on NGMF, the only way to be

sure of fixing this problem is to clear out the NetView for AIX databases completely. The most common reason for corrupted or inconsistent databases is improper customization of objects in NetView for AIX. You should customize the map you plan to use for MSM by carefully following the cutting and pasting rules for NetView for AIX. The information was copied from the file README.Ipmap:

B.2.1 Cutting, Pasting, Adding and Copying Symbols

```
The ipmap application (the application that creates and maintains the
symbols that represent IP topology entities) contains code that controls
cutting and pasting symbols, adding objects, and copying symbols.
Sections 1a, 1b, and 1c describe the how to use these functions,
and Section 1d provides a sample exercise.

Because ipmap only interacts with IP topology objects, these rules
only correspond to the manipulation of symbols and objects representing
IP topology entities.

1. CUT and PASTE Rules.

    The CUT/PASTE operation allows you to MOVE symbols from one submap
    to another.  The CUT/PASTE functionality should not be used to
    COPY symbols.  See section 1c for rules about copying symbols.

    The way ipmap behaves when a symbol is moved (cut and pasted) depends
    upon many factors.  In some cases, ipmap will "support" the movement
    of a symbol from one submap to another, and in other cases, ipmap will
    not support the movement of a symbol.

    If ipmap supports a cut and paste operation, then the symbol that
    was cut and pasted will be placed in the application plane of the
    destination submap.  This means that ipmap will continue to manage
    the object represented by the symbol, and the symbol will accurately
    reflect the status of the object.  If ipmap does not support a
    cut and paste operation, then the symbol will be placed in the user
    plane of the destination submap.  This means that the symbol will no
    longer accurately reflect the status of the entity it represents.
    To maintain the accuracy of all maps, users should only execute
    cut and paste operations that are supported by ipmap.

    Which cut and paste operations are supported?  In general, ipmap
    supports operations that "makes sense".  For instance, it might
    make sense to move a network from one location to another, while
    it definitely makes no sense to move an interface card from one
    network to another (because the interface card's IP address will
    contain the network address of the network in which it previously
    resided).

    It would be impossible to list all possible cut and paste
    scenarios and whether or not they are supported, but it is possible
    to list all cut/paste restrictions (actions not supported by ipmap).
    If a cut and paste action does not match any of the restrictions
    listed below, then the action will be supported by ipmap.

    The most important restriction is that SYMBOLS CAN'T BE MOVED FROM
    A SUBMAP TO A SUBMAP OF A DIFFERENT TYPE.
    Here are two examples:
       - a bridge symbol on a network level submap can't be moved
         to a segment submap
```

- an interface card symbol on a node (computer) level submap
  can't be moved to an location level submap

This is the main restriction, but there are others that are important. Since moves can only be made across submaps of the same type, the remaining restrictions are listed by submap type.

a. Root Submap Restrictions:

   NO SYMBOLS CAN BE MOVED TO OR FROM THIS SUBMAP.
   Ipmap only has access to symbols on or below the submap accessible from the IP internet symbol on the root submap.

b. Internet/Location Submaps Restrictions:

   1. Connection symbols cannot be moved. Connection symbols are

      the lines that connect two symbols. Connection symbols should not be confused with connector symbols, which represent entities like gateways, bridges, and repeaters.

   2. As might be expected, an internet/location symbol cannot be moved into its own child submap, because this would create an infinite loop.

   3. Internet/location symbols cannot be moved if the submaps they represent have symbols in them. In other words, Internet/Location symbols must have empty child submaps in order to be moved.

c. Network Submap Restrictions:

   NO SYMBOLS CAN BE MOVED FROM A NETWORK SUBMAP TO ANOTHER NETWORK SUBMAP. This is because all symbols on a network submap (gateways, nodes, segments, and connections) all have interfaces that correspond to a unique network. Moving a symbol from one network submap to another means that an object is being moved into a different network. The network address in the interface's IP address would conflict with the network address of the destination network submap.

d. Segment Submap Restrictions:

   Nodes symbols cannot be moved from a segment in one network to a segment in another network. Nodes can be moved from segments within the same network, however.

e. Node Submap Restrictions:

   NO SYMBOLS CAN BE MOVED FROM A NODE SUBMAP TO ANOTHER NODE SUBMAP. Only interface card symbols can appear on the node level submap, and it usually isn't necessary to move interface cards from node to node. In the event that an interface card has been moved from one node to another, instead of trying to manually cut and paste the card symbol, simply do a demand poll on the two nodes in question, and the map will be updated automatically.

Basically, the Internet/Location and Segment submaps are the only

places where you can cut and paste. If you're on the root, network, or node level submaps, don't try to cut and paste.

2. Add Object Rules

   The way ipmap behaves when an object is added depends upon the type of object being added and the destination submap of the object's symbol. As with cutting and pasting symbols, ipmap will "support" some object additions, and in other cases, ipmap will not support the creation of an object.

   If ipmap supports an object addition, then the object's symbol icon will be placed in the application plane of the destination submap. This means that ipmap will continue to manage the object represented by the symbol, and the symbol will accurately reflect the status of the object. If ipmap does not support an object addition, then the object's symbol icon will be placed in the user plane of the destination submap and ipmap will not manage the object. This means that the symbol will not accurately reflect the status of the object. To maintain the accuracy of all maps, users should try to add objects in a manner that allows ipmap to manage the objects.

   One thing that makes adding objects different from moving symbols is that, in most cases, you must provide correct information (like IP addresses, subnet masks, etc.) when you add an object. If the information provided is not consistent with a real life object in your network, then ipmap will not manage the object. This information is entered by pressing the "IP Map - Set Object Attributes" push button on the "Add Object" dialog box.

   a. Root Submap

      NO OBJECTS CAN BE ADDED TO THIS SUBMAP. As with cutting and pasting, ipmap only has access to symbols on or below the submap accessible from the IP internet symbol on the root submap.

   b. Internet/Location Submap

      The following objects can be added:
      1. Internets/Locations
         - User must provide unique name
      2. Connectors (Gateways)
         - User must provide correct hostname, IP address, and subnet mask
      3. IP Networks
         - Must use IP Network icon! If "generic" or "regular" network icon is chosen, ipmap will not manage the network.
         - User must provide unique network name, IP address, and subnet mask
      4. Connections
         - Only certain objects can be connected. For instance, you can't connect two networks directly with a connection symbol. Instead, you must connect a network with a gateway, which is then connected to another network.
         - When adding a connection between two symbols, you are really adding an interface object. After drawing the connection between the two symbols, if the "Add Object" dialog box does not appear, then you have tried to connect

two symbols that cannot be connected.
- When the "Add Object" dialog comes up, you must specify information about the interface that you are adding. You must provide the IP address and subnet mask of the interface.
- Be careful when adding connections, because connection symbols have no "user plane" like other object symbols, so it impossible to tell just by looking at the connection symbol whether or not ipmap supports the connection.

c. Network Submap

The following symbols can be added:
1. Segments
   - User must provide unique name for segment
2. Connectors (Bridges)
   - User must provide correct hostname, IP address, and subnet mask
3. Connections
   - see notes for connections above

d. Segment Submap

The following symbols can be added:
1. Nodes (Computer, etc.)
   - User must provide unique hostname and IP address
2. Connections
   - see notes for connections above

e. Node Submap

Only interfaces can be added to the Node Submap. The user must provide the IP address and the subnet mask for the interface being added.

3. COPY and PASTE Rules

Symbols COPIED from one submap into another will not be managed by the ipmap application. This means that copied symbols will be placed in the user plane rather than in the application plane. In general, the COPY menu option on the user interface exists for use with other applications, and not with ipmap. Within ipmap, it is recommended that the COPY/PASTE function be used sparingly, if at all.

4. An Example

A common exercise using both the Add..Object and Cut/Paste functions is partitioning a submap in to smaller, more manageable units. For instance, to partition a Network submap into multiple Segments:

- Open the Network submap that contains the Segment submap which you want to partition.
- Add a new Segment symbol to that Network submap.
  Add a symbol which will represent the new Segment.
  Use "Edit->Add -> Object" menubar option to select a new symbol in the Network symbol class, and then drag one of its subclass symbols to the submap.
- Select IP Map, making sure that ipmap recognizes the new symbol in its application plane.

```
   To make sure that the ipmap recognizes the new symbol in its
   application plane, do the following:
   - In the "Add Object" dialog box, select the Object Attribute
     named 'IP Map' and press "Set Object Attributes" to set a
     name for the IP Map. Note that some of the symbol subclasses
     under the Network symbol class do not have the IP Map
     attribute.
   - When you have entered a name, press the Verify button to test
     your choice.
- Double-click on the segment.
- In the Network submap, double-click on the new segment symbol.
- Cut nodes from the Segment submap that you want to partition.
- Go back into the Network map where new Segment submap was
  created.
- Paste the nodes cut from the Segment map into the new Segment
  submap.
- Wait about an hour or more for paste to complete when pasting
  large numbers of nodes.  The EUI will be processing the changes
  during this time period.

In a similar manner, Internet/Location submaps can be partitioned
by adding a new Internet/Location symbol and pasting networks and
routers into it.

There is no way to partition the Network or Node submaps.
```

B.3 Setting up NetView for AIX Filters

This section describes trap to alert filtering in NetView for AIX.

B.3.1 Traps

In general a SNMP management station keeps itself up-to-date on the status of the nodes under its control by regular polling. However there are cases where the managed nodes may wish to inform of an extraordinary event without waiting to be polled. The mechanism for such communication is the trap.

There are seven generic trap types defined in RFC 1157:

- Trap type 0: coldStart
- Trap type 1: warmStart
- Trap type 2: linkDown
- Trap type 3: linkUp
- Trap type 4: authenticationFailure
- Trap type 5: egpNeighborLoss
- Trap type 6: enterpriseSpecific

A enterpriseSpecific (6) trap signifies that the SNMP agent has recognized that some enterprise-specific event has occurred. The specific-trap field then identifies the particular trap. The manager should be able to interpret the enterprise specific traps defined in agents it manages.

Traps are often thought of as the IP equivalent to the alert of SNA network management architecture. However, whereas the structure of an SNA alert has many fields, prompting the encoder to describe a problem in detail, a trap has a

limited number of field types and usually carries a limited amount of data. It contains information about the source agent, trap information, a time stamp and optional interesting information as a reference to the MIB variable. The intention of a trap is to inform a managing node that there has been some change of status or other unusual condition in the managed node.The managing node may then chose to use SNMP commands to retrieve relevant additional data from the managed node using whatever automation capabilities the managing node has.

Most traps you will find in NetView for AIX are enterpriseSpecific traps generated by NetView for AIX itself. For example, if a node goes down, it doesn′t send a node down trap by itself! This trap is generated by NetView for AIX as a specific trap on behalf of the node.

B.3.2 Using the Trap to Alert Filter in NetView for AIX

NetView for AIX provides a filter editor to edit filters. Those filters may be activated for different reasons, for example:

- To select which events are displayed in the dynamic events window in NetView/6000
- To select which events are converted into alerts and sent to NetView for MVS.

The filters configuration files are located in the directory /usr/OV/filters. The default file is called filter.samples. It contains the Trap_to_Alert_Filter. This filter is activated when tralertd is started.

The default filter specifies which traps are converted to alerts and forwarded to NetView for MVS. You can look at it using the Filter Editor. Select **Tools** from the menu bar to find it. You will see a window like the following:

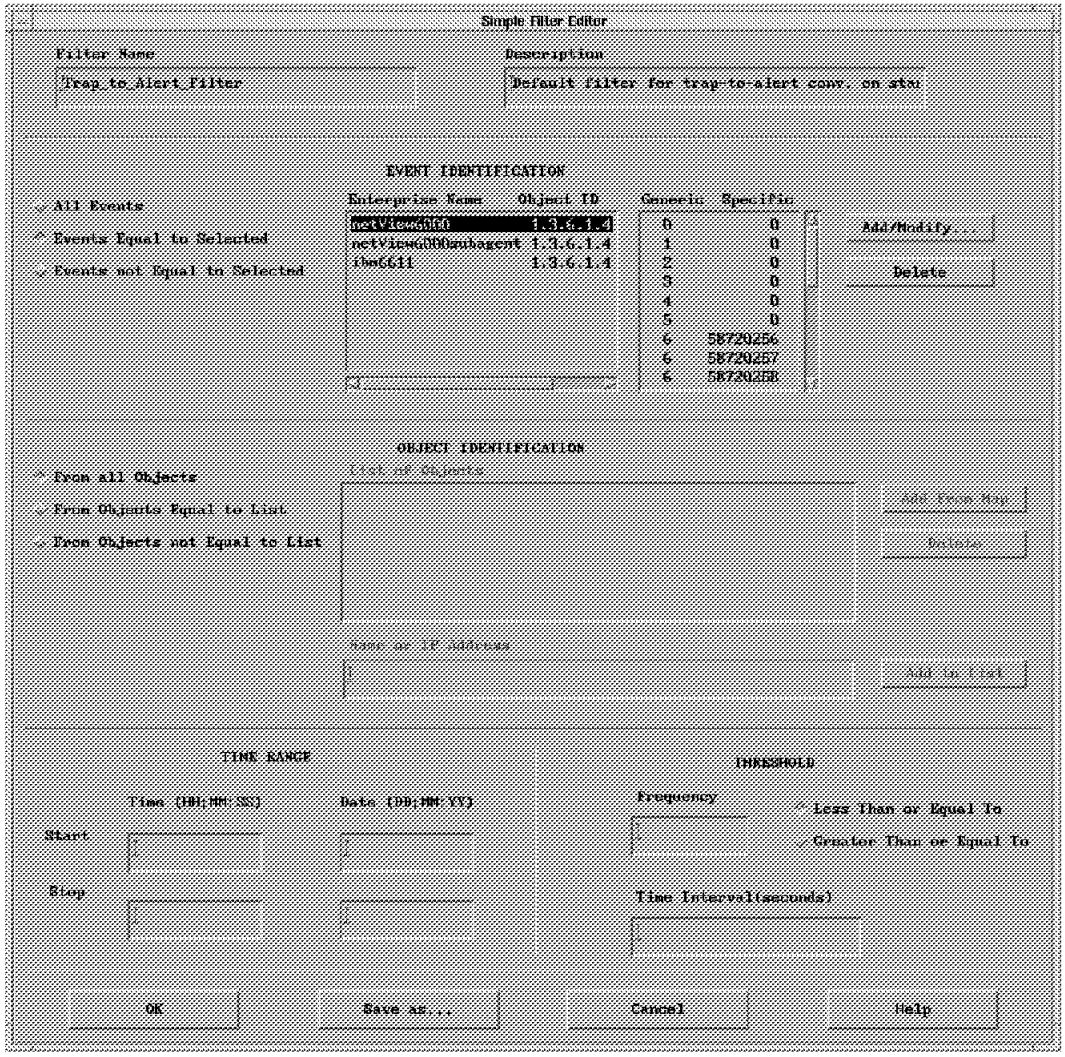


Figure 159. Trap_to_Alert Default Filter

The traps forwarded are:

- **NV/6000**:
  - Generic traps type 0-5
  - Sixteen of the enterpriseSpecific traps (type 6)
- **NV/6000 subagent** (trapgend):
  - All traps
- **IBM 6611**:
  - All traps

You can edit this filter to make it fit your environment by adding or deleting traps in the list. This filter was built as a sample regarding NetView/MVS operator requirements.

Note: You should use a filter specifying the traps that should be forwarded. As not all traps can be handled with the filter editor provided by NetView/6000 you might get unexpected alerts when you try to specify the traps to be filtered out.

Below you will find a list of all NetView for AIX enterpriseSpecific traps. Those traps forwarded by the default filter are **highlighted**. Traps created only by NetView/6000 are underlined. The last three traps are NetView for AIX only. The trap_to_alert filter was not changed.

event name	number	description
LLAC_EV	0058982400	Link Level Address Changed
MLLA_EV	0058982401	Mismatch of Link Level Address
ULLA_EV	0058982402	Undetermined Link Level Address
OIC_EV	0058982403	Object Identifier Change
SDC_EV	0058982404	System Descr Change
SNC_EV	0058982405	System Name Change
SMC_EV	0058982406	Subnet Mask Change
FSC_EV	0058982407	Forwarding status change
FTH_EV	0058982408	Forwarding to a host
NS_EV	0058982409	No SNMP Response
SCC_EV	0058982410	System Contact Change
SLC_EV	0058982411	System Location Change
ITC_EV	0058982412	Interface Type Change
IDC_EV	0058982413	Interface Descr Change
BSM_EV	0058982414	Bad Subnet Mask
IADD_EV	0058785792	Interface Added
IDEL_EV	0058785793	Interface Deleted
NADD_EV	0058785794	Node Added
NDEL_EV	0058785795	Node Deleted
NUP_EV	**0058916864**	**Node Up**
NDWN_EV	**0058916865**	**Node Down**
IUP_EV	**0058916866**	**Interface Up**
IDWN_EV	**0058916867**	**Interface Down**
SC_EV	**0058916868**	**Segment Critical**
NC_EV	**0058916869**	**Network Critical**
CMIS_EV	0058916870	CMIS Status Event
SNMP_EV	0058916871	SNMP Status Event
CPUL_EV	**0058720256**	**CPU Load**
DSPU_EV	**0058720257**	**Disk Space Percentage Used**
IPD_EV	**0058720258**	**Interface Percent Deferred**
IPC_EV	**0058720259**	**Interface Percent Collisions**
ICE_EV	**0058720260**	**Interface CRC Errors**
IPIE_EV	**0058720261**	**Interface Percent Input Errors**
IPOE_EV	**0058720262**	**Interface Percent Output Errors**
DCOL_EV	**0058720263**	**Data Collector detected threshold**
DCRA_EV	**0058720264**	**Data Collector re-arm event**
WARN_EV	0050462720	Warnings
ERR_EV	0058851329	Non Fatal Errors
FERR_EV	**0058851330**	**Fatal Errors**
AA_EV	0059047936	Application Alert
NM_EV	0050790400	Node Marginal
SN_EV	0050790401	Segment Normal
SM_EV	0050790402	Segment Marginal
NETN_EV	0050790403	Network Normal
NETM_EV	0050790404	Network Marginal
SA_EV	0050790405	Segment Added
SD_EV	0050790406	Segment Deleted
NETA_EV	0050790407	Network Added
NETD_EV	0050790408	Network Deleted
CA_EV	0050790409	Connection Added
CD_EV	0050790410	Connection Deleted
CPP_EV	0050790411	Change Polling Period

FP_EV	0050790412	Forced Poll
CFP_EV	0050790413	Cancel Forced Poll
ST_EV	0050790414	Set Threshold
DT_EV	0050790415	Delete Threshold
MNET_EV	0050790416	Manage Network
UNET_EV	0050790417	Unmanage Network
MN_EV	0050790418	Manage Node
UN_EV	0050790419	Unmanage Node
MSEG_EV	0050790420	Manage Segment
USEG_EV	0050790421	Unmanage Segment
NMTF_EV	0050790422	Netmon Change trace file
NMTM_EV	0050790423	Netmon Change trace mask
NMDN_EV	0050790424	Netmon Dump node
NMDI_EV	0050790425	Netmon Dump interface
NMAC_EV	0050790426	Netmon Action
CIS_EV	0050790427	Change Interface Segment
FMTCHG	0050790438	trapd.conf format changed
MIBCHG	0050790439	ASN.1 mib definition file format changed
COLCHG	0050790440	SNMP data collector file format changed
MI_EV	0050790441	Manage Interface
UI_EV	0050790442	Unmanage Interface
NETFC_EV	0050790443	Network Flags changed
SEGFC_EV	0050790444	Segment Flags changed
NFC_EV	0050790445	Node Flags changed
IFC_EV	0050790446	Interface Flags changed
IPOS_EV	0050790447	Interface position changed
APUP_EV	0059179056	Application Up Event
APDN_EV	0059179057	Application Down Event
TATM_EV	0059179068	Tralert change tracemask Event
SPTM_EV	0059179069	Service point appl. changed Mask
NMCR_EV	0059179070	Change netmon retry count
MCHG_EV	0059113474	Map Change event
SUGUP_EV	0058916872	Systems Monitor Mid Level Manager UP
SUGDN_EV	0058916873	Systems Monitor Mid Level Manager UP
DUPIP_EV	0058982415	Duplicate IP Address

NetView for AIX provides a catalog of NetView for MVS code points. It allows you to define the way some of the subvectors present in the alert major vector should be constructed. The customization of the alert data is performed from the window presented when the Alert Editor bar is selected from the Event Configuration panel. The text associated with the codes is presented for selection, but only the two-byte codes will be carried in the alert. The customization for the traps present in the Trap_to_Alert_Filter has already been performed. This means you get some helpful information in the Event Detail screen in the NetView for MVS Hardware Monitor NPDA. These may be examined as examples of how the customization is performed.

To control the trap to alert filters select **Options** from the NV/6000 menu bar, **Event Customization** and then **Trap to Alert filter control**. You can activate and deactivate filter in the window displayed.

B.3.3 Sample Filter

Below you will find the trap_to_alert default filter as provided by by NetView for AIX. It's an extract of /usr/OV/filters/filter.samples.

```
RuleName=Trap_to_Alert_Filter
RuleDescription=Default filter for trap-to-alert conv. on startup of tralertd
RuleContent=((CLASS=1.3.6.1.4.1.2.6.3 && (SNMP_TRAP=0 || SNMP_TRAP=1 ||
SNMP_TRAP=2 || SNMP_TRAP=3 || SNMP_TRAP= || SNMP_TRAP=5 ||
SNMP_SPECIFIC=58720256 || SNMP_SPECIFIC=58720257 || SNMP_SPECIFIC=5872028 ||
SNMP_SPECIFIC=58720259 || SNMP_SPECIFIC=58720260 || SNMP_SPECIFIC=58720261 ||
SNMP_SPECIFIC=58720262 || SNMP_SPECIFIC=58720263 || SNMP_SPECIFIC=58720264
|| SNMP_SPECIFIC=58851330 || SNMP_SPECIFIC=58916864 ||
SNMP_SPECIFIC=58916865 || SNMP_SPECIFIC=58916866 || SNMP_SPECIFIC=58916867 ||
SNMP_SPECIFIC=58916868 || SNMP_SPECIFIC=58916869))
|| (CLASS=1.3.6.1.4.1.2.6.4) || (CLASS=1.3.6.1.4.1.2.6.2))
```

Note: The traps listed in the filter rule above are those forwarded to NetView/MVS, not those filtered out!

B.3.4 MSM Trap to Alert Filter

Because only some of the converted traps are used for MSM automation, you can filter the rest out. The traps used for MSM automation are:

```
The NetView for AIX enterprise id traps (enterprise id=1.3.6.1.4.1.2.6.3)

# event name   number       description

MI_EV        0050790441     Manage Interface     <=== new trap
UI_EV        0050790442     Unmanage Interface   <=== new trap
NADD_EV      0058785794     Node Added
NDEL_EV      0058785795     Node Deleted
IUP_EV       0058916866     Interface Up
IDWN_EV      0058916867     Interface Down


The enterprise "netviewMSM"  traps (enterprise id=1.3.6.1.4.1.2.6.67)

# event name    number    description

MSMAGNT_START  565504401  MultiSystem Manager IP Agent Started/Waiting
MSMAGNT_UP     565504402  MultiSystem Manager IP Agent Up/Ready
MSMAGNT_STOP   565504403  MultiSystem Manager IP Agent Down
```

Note: Those traps are created by the map with the topology agent attached.

To make sure you do not filter out any of the alerts that the MSM IP agent sends to MSM, use the sample filter provided by the topology agent. The default filter provided by MSM is autoactivated in the installation process. After it has been included once, it will become active every time the TRALERTD daemon starts. The filter is shown below:

```
RuleName=MultiSystem_Manager_Alert_Filter
RuleDescription=MultiSystem Manager trap-to-alert filter conversion
RuleContent=(
(CLASS=1.3.6.1.4.1.2.6.67 && (
SNMP_SPECIFIC=565504401
|| SNMP_SPECIFIC=565504402
|| SNMP_SPECIFIC=565504403
)) ||
(CLASS=1.3.6.1.4.1.2.6.3 && (
SNMP_SPECIFIC=58785794
|| SNMP_SPECIFIC=58785795
|| SNMP_SPECIFIC=58916866
|| SNMP_SPECIFIC=58916867
|| SNMP_SPECIFIC=50790441
|| SNMP_SPECIFIC=50790442
)))
```

This filter describes the traps that pass through to NetView for MVS, in addition to those specified in the default filter. If the default filter was not changed, the IUP_EV and the IDWN_EV pass anyhow (those are the trap IDs 58916866 and 58916867). In the filter above you find the six NetView for AIX traps and the three MultiSystem Manager traps that have been added by during the agents installation process.

The installation process also updates the tralertd.conf file, which contains the rules for the trap-to-alert conversion. It provides definitions for all the MSM added traps to give the alerts meaningful contents. Because they are used for automation in NetView for MVS, they should not be changed!

The summary lines for the alerts as they appears in NetView for MVS Hardware Monitor are as follows:

```
Manage Interface:              Problem Resolved: personnel
Unmanage Interface:            Operator Notification: personnel
Node Added:                    Problem Resolved: communication interface
Node Deleted:                  Unable to communicate with remote node: c
Interface Up:                  Problem Resolved: communication interface
Interface Down:                Unable to communicate with remote node: c
MSM IP Agent Started/Waiting:  Operator Notification: Software Program
MSM IP Agent Up/Ready:         Problem Resolved: Software Program
MSM IP Agent Down:             Operator Notification: Software Program
```

If you want additional traps to pass the filter, you have to add them manually. If you want to pass the trap 123456, for example, do the following:

- Open the Filter Editor.
- Select the default trap to alert filter and click on **Modify**.
- Select **netView6000** and click on **Add/Modify...**.
- Select the specific trap **123456** from the list of available traps and select **>>Select>>**. If they are not in the list you have to add them to the list of selected trap types manually as shown in Figure 160 on page 228.
- Select **OK**
- Finally, inactivate and activate the filter.

The trap now should be passed to NetView for MVS. You can test this with the command:

```
event -E 123456
```

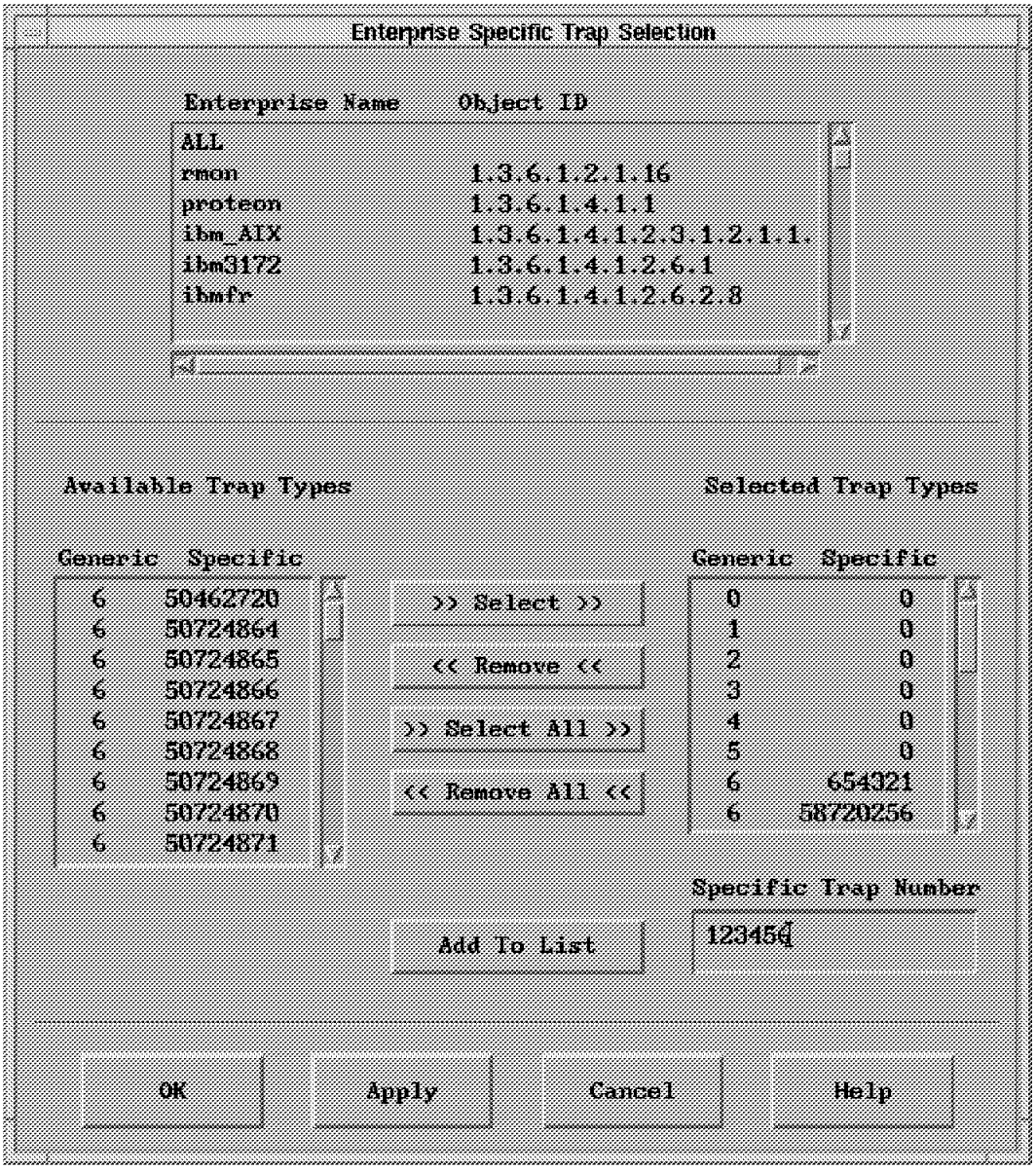


Figure 160. Adding a Specific Trap Type

B.4 Recycle Shell Script for Service Point

As we found that the Service Point went inoperative for some reason quite frequently, we decided to set up a simple shell script to make the recycle process more convenient. During testing, this might be helpful. This might, for example, be necessary if the VTAM major node has been down for a while. As the attachment for SNA Services was started automatically by the Service Point, you can change the SNA start command to sna -s.

```
#####################################################################
#     This Script recycles the NV/6000 Host connection Daemons      #
#     and the NetView Service Point for RS6000.                     #
#     Raleigh, 5/26/94, Rita Steffes-Hollaender                     #
#     RA60005 is the link used, RS60005S is the APPL                #
#####################################################################


ovstop spappld
ovstop tralertd
nvix_control stop 1> /dev/null
sleep 10
sna -stop sna -t forced 1> /dev/null
sna -s l -p RA60005
nvix_control start 1> /dev/null
sleep 10
ovstart spappld
ovstart tralertd
nvix_control status > /tmp/status
print 'Service Point is operative now for your application:'
cat /tmp/status | grep RS60005S
rm /tmp/status
```

The output should be:

```
The "RA60005" Link Station has been started"
Service Point is operative now for your application:
RS60005S
```

We found that if the switched major node was recycled, SNA on the RISC/6000 also has to be deactivated and activated, if you are using SNA Services. You can configure SNA Server to retry establishing the session up to 500 attempts.

Appendix C. Installing NetView Graphic Monitor Facility on the PC Workstation

C.1 The Platform Used in the ITSO LAB

We used a minimal configuration to enable NGMF, PMX and 3270 emulation on the PC.

C.1.1 Hardware Used

- 8580-321 16M (386Mhz, 320MB Disk)
- 4 Mbps Token Ring Card
- 8514/a Video Adapter + 8514 Screen

C.1.2 Software Used

- OS/2 V2.11
- CM/2 V1.11

C.1.3 Configuration

- NGMF Workstation is standalone, therefore it is both the server and the client.
- NGMF will be installed on drive D.
- The host PDS that contains the code to be downloaded is

  'NETVIEW.V2R4M0.SEGVPS21'
- The toolkit will also be installed, allowing you to customize NGMF.

C.2 Summary of Installation Procedure

- Install the Software Installer for OS/2.
- Install NGMF using the Software Installer for OS/2.
- Perform Host Definitions.
- Customize CM/2.

C.3 Installing the Software Installer for OS/2

1. Log on to TSO Host.
   - Check to see whether you have the 'NETVIEW.V2R4M0.SEGVPS21' data set.
   - Ensure the cursor is at the READY prompt for downloading.
2. Go to OS/2 Window Command Line.

- Change to D drive.
- Download the DUIHGETE.CMD file:

```
RECEIVE D:\DUIHGETE.CMD A:'NETVIEW.V2R4M0.SEGVPS21(DUIHGETE)' ASCII CRLF
```

  (Where D is your target drive and A is your TSO session ID)
- Run the DUIHGETE.CMD file to download the rest of the package:

```
DUIHGETE D: NETVIEW.V2R4M0.SEGVPS21 A:
```

  (Where D is your target drive and A is your TSO session ID)

C.4 Installing NetView Graphic Monitor Facility

You will use the Software Installer for OS/2 to install NetView Graphic Monitor Facility.

- If you have previously installed NGMF and/or CT/2, you must shutdown NGMF and CT/2 in order for the installation to be successful.
- Ensure you are logged on to the MVS system and you are at the READY prompt.
- Go to an OS/2 window command line prompt.
- Change to the IBMDUI directory:

```
CD\IBMDUI
```

- Enter the following to start the Software Installer for OS/2:

```
DUIINSTS /S:NETVIEW.V2R4M0. /O:MVS
```

  The following screen appears:

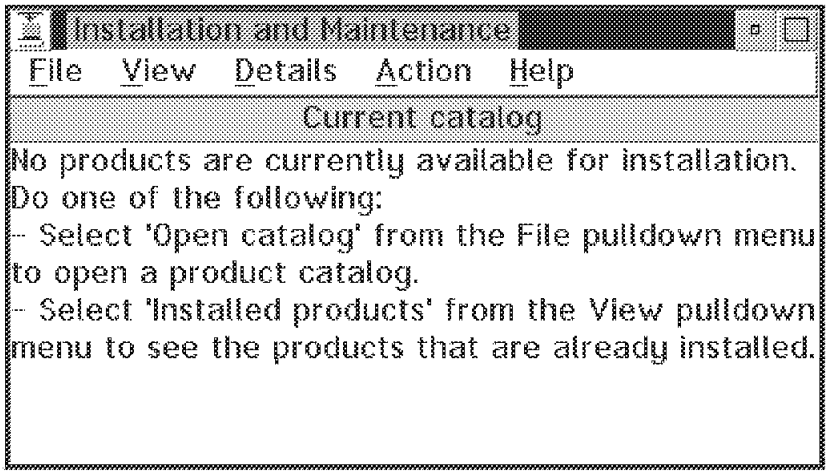


Figure 161. Installation and Maintenance Window

Do the following:

- Select **File**, then **Open Catalog**, then **Host** from the menu bar.

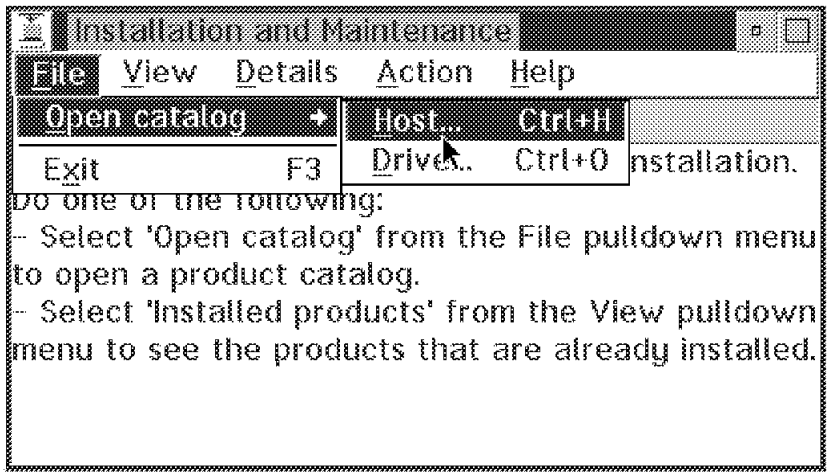


Figure 162. Selecting Host Catalog

- The following panel appears:

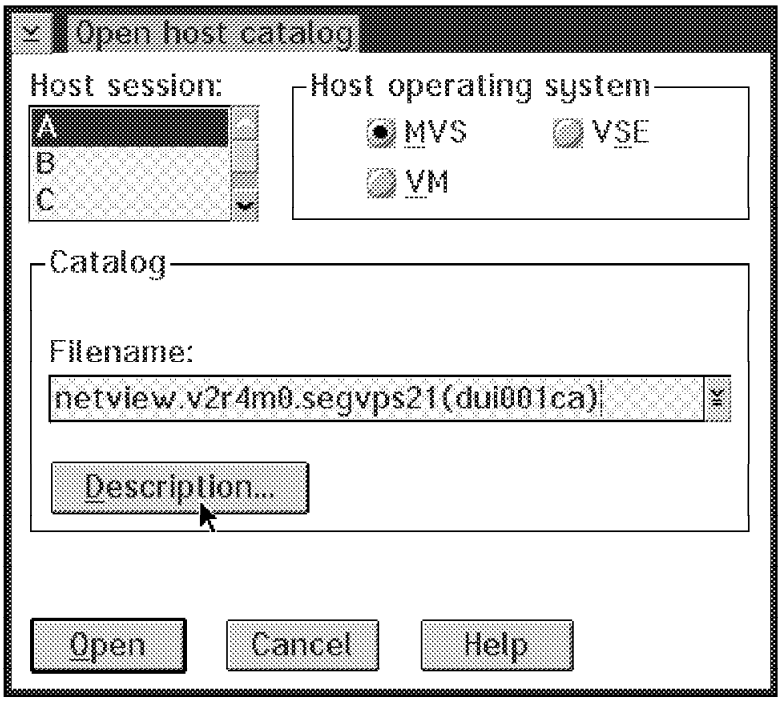


Figure 163. Open Host Catalog Panel

- In the Open host catalog panel, enter the following in the filename field:

  `NETVIEW.V2R4M0.SEGVPS21(DUI001CA)`

- Select your **Host** session and then click on **Open**.
- On the next panel (Figure 164 on page 234) click on **Select all**.

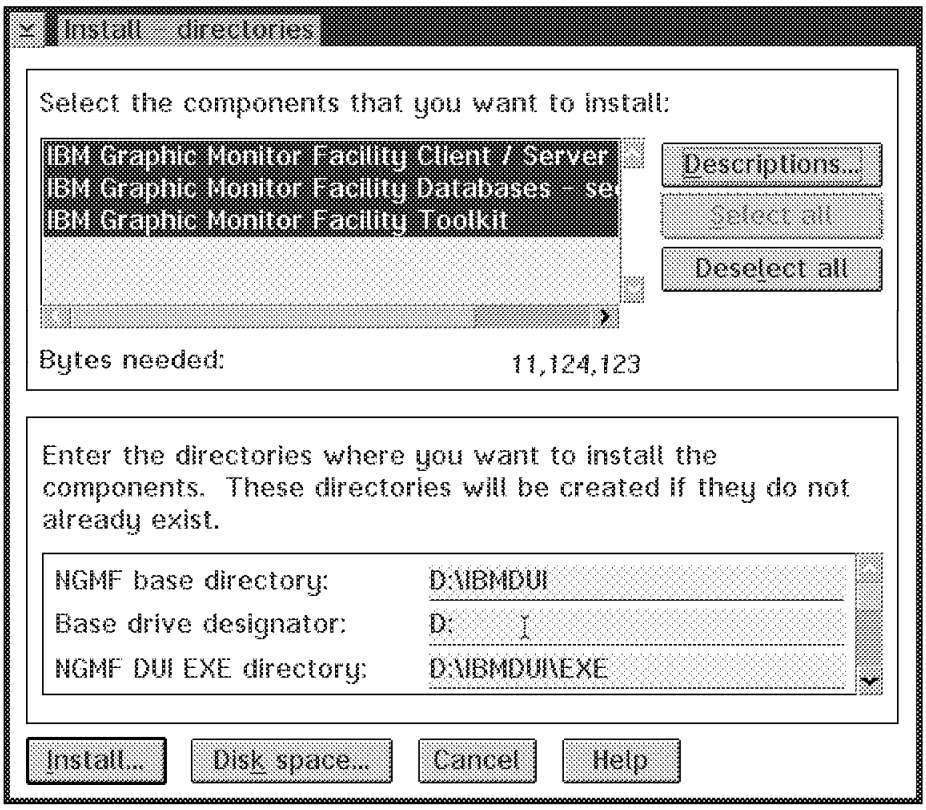


Figure 164. Install - Directories Panel

- Select **Disk space**, to verify if NGMF will fit on your hard disk and to optionally change your drive letter.

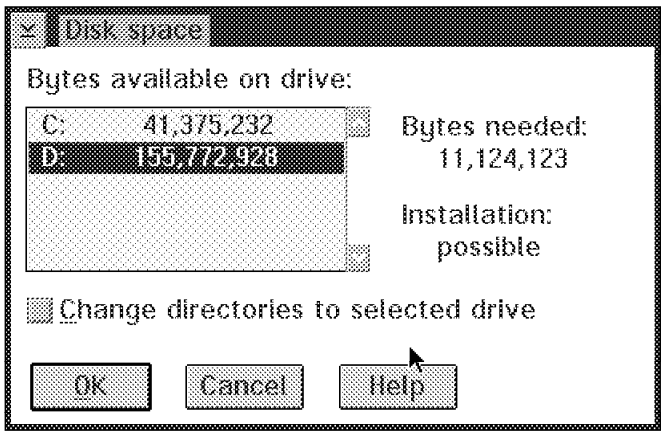


Figure 165. Disk Space Panel

- If that's what you want, select **OK**.
- You get back to panel Figure 164 and select **Install**.
- The following panel appears:

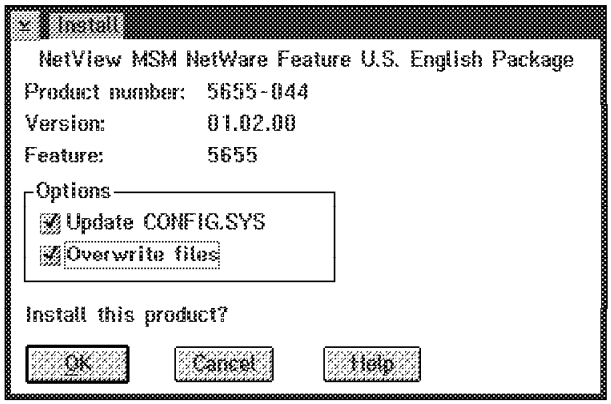


Figure 166. Install Panel

- Select **Update CONFIG.SYS**, **Overwrite files** and **OK**.
- The following panel appears:

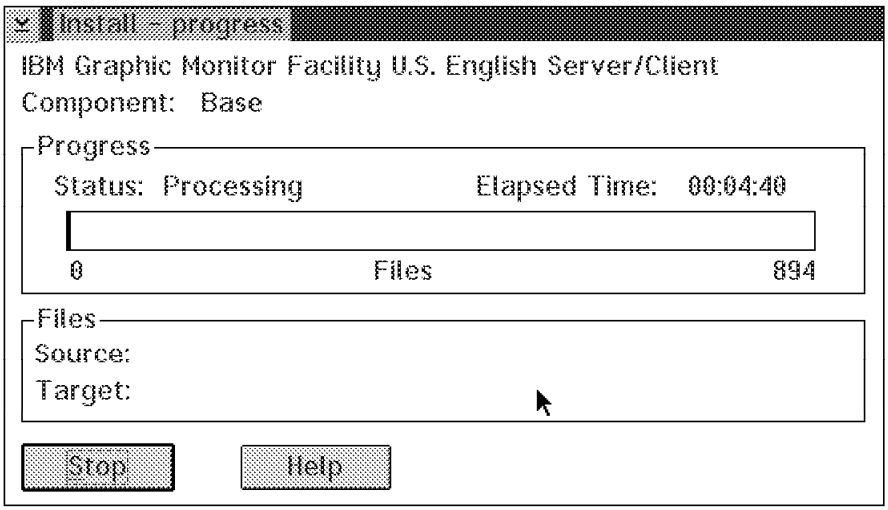


Figure 167. Install - Progress Panel. This step took 30 minutes on our PC.

C.5 Host Definitions Sample

Below is a sample VTAM switched major node for a token-ring-attached NGMF workstation:

```
*************************************************************************
*                                                                       *
*         VTAM SWITCHED MAJOR NODE FOR ITSC OFFICES                     *
*                                                                       *
*************************************************************************
        VBUILD MAXGRP=25,                                              X
               MAXNO=25,                                               X
               TYPE=SWNET
*************************************************************************
* NGMF WORKSTATIONS FOR RESIDENTS (KARL)
*************************************************************************
RAGMF9   PU    ADDR=01,                                                X
               CPNAME=WTR33301,                                        X
               IDBLK=05D,                                              X
               IDNUM=33301,                                            X
               DISCNT=NO,                                              X
               ISTATUS=ACTIVE,                                         X
               MAXDATA=1033,                                           X
               MAXOUT=7,                                               X
               DLOGMOD=D4C32XX3,                                       X
               MODETAB=ISTINCLM,                                       X
               USSTAB=US327X,                                          X
               PASSLIM=7,                                              X
               MAXPATH=8,                                              X
               PACING=0,                                               X
               PUTYPE=2
RANGMF9  LU    LOCADDR=0,DLOGMOD=DSIL6MOD,MODETAB=AMODETAB
RAGMF902 LU    LOCADDR=2
RAGMF903 LU    LOCADDR=3
RAGMF904 LU    LOCADDR=4
RAGMF905 LU    LOCADDR=5
```

C.6 Customizing Communications Manager/2

There are two ways to customize Communications Manager/2 for NGMF. However you do it, you have to edit some of the definitions afterwards - see C.6.3, “Important Things to Do” on page 250 for details.

C.6.1 The Easy Way - Using the NGMF CM/2 Configuration Utility

1. Type EGVNCFG on an OS/2 window.
2. Fill in the fields for your environment.
3. Select the **Configure** button.

C.6.2 The More Complicated Way

1. Start the Communications Manager/2 Installation and Setup utility and click on the **OK** push button.

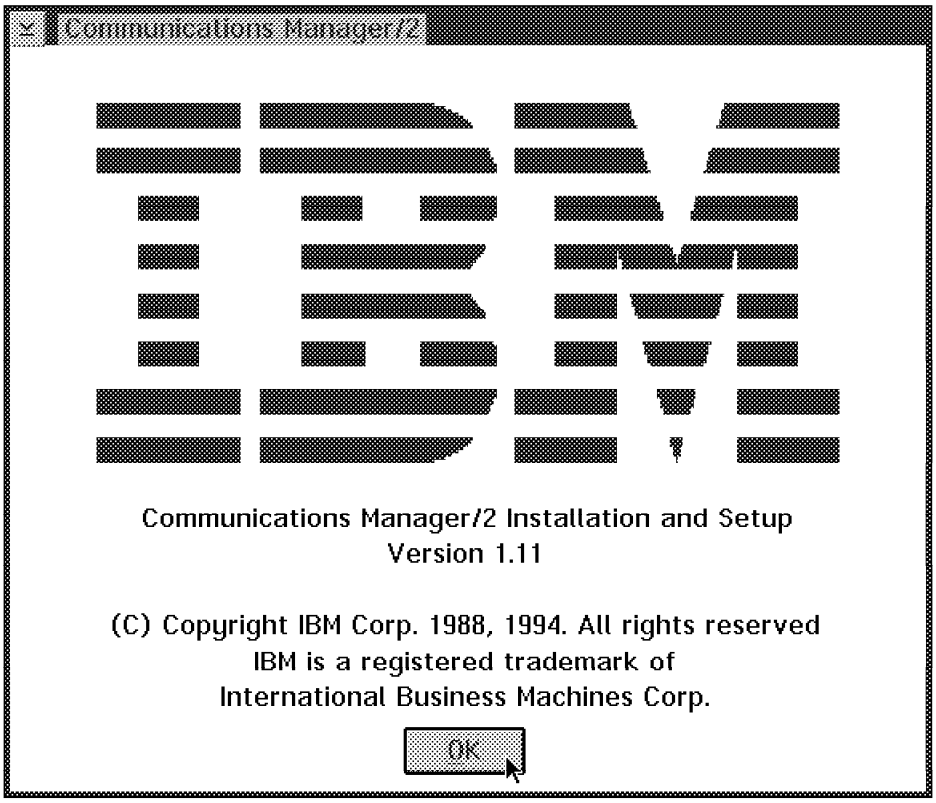


Figure 168. Logo Window

2. Click on the **Setup** push button on Figure 169 on page 238 to modify a configuration.

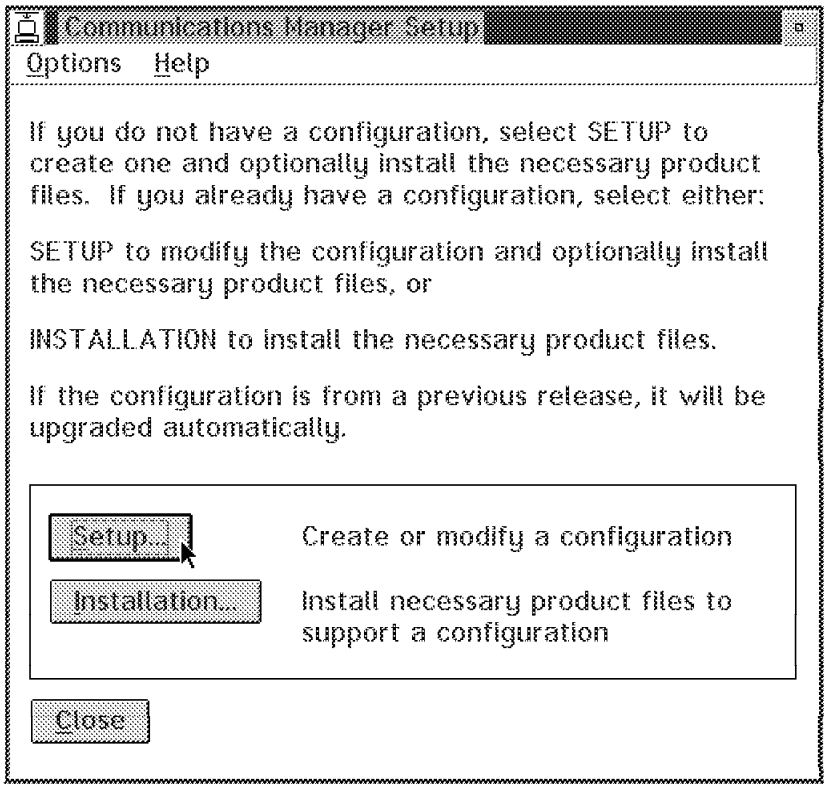


Figure 169. Setup/Installation Window

3. Select the configuration file you wish to modify from the *Configurations* list box on Figure 170 and click on the **OK** push button.

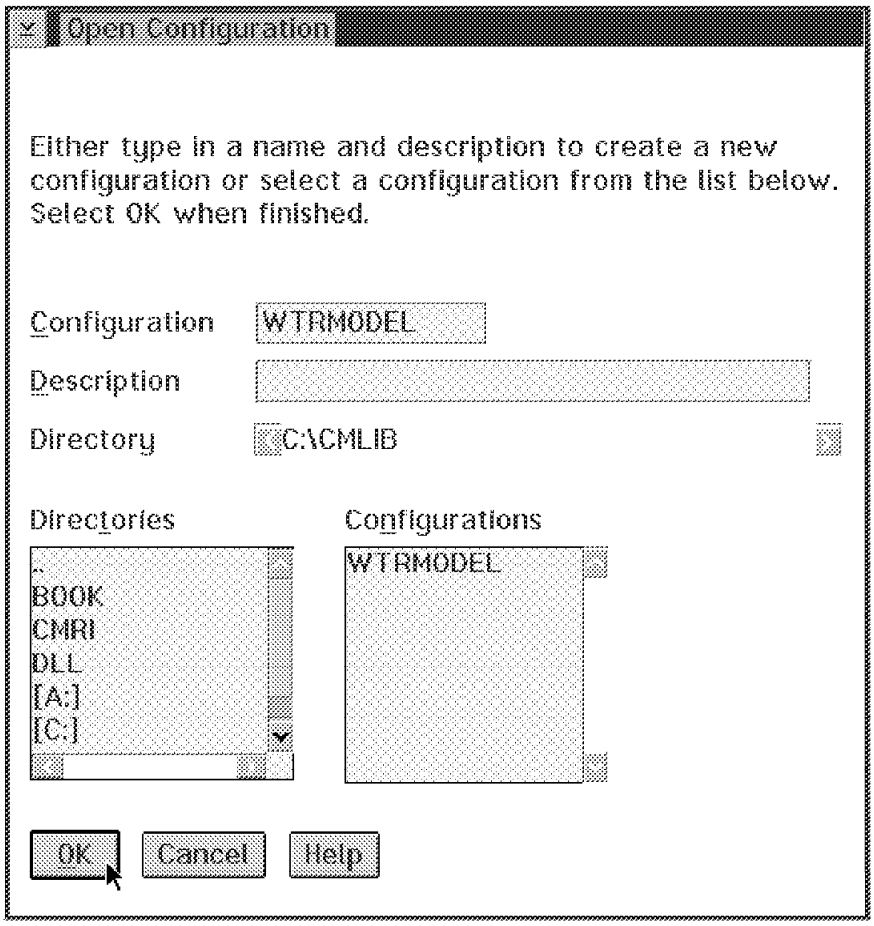
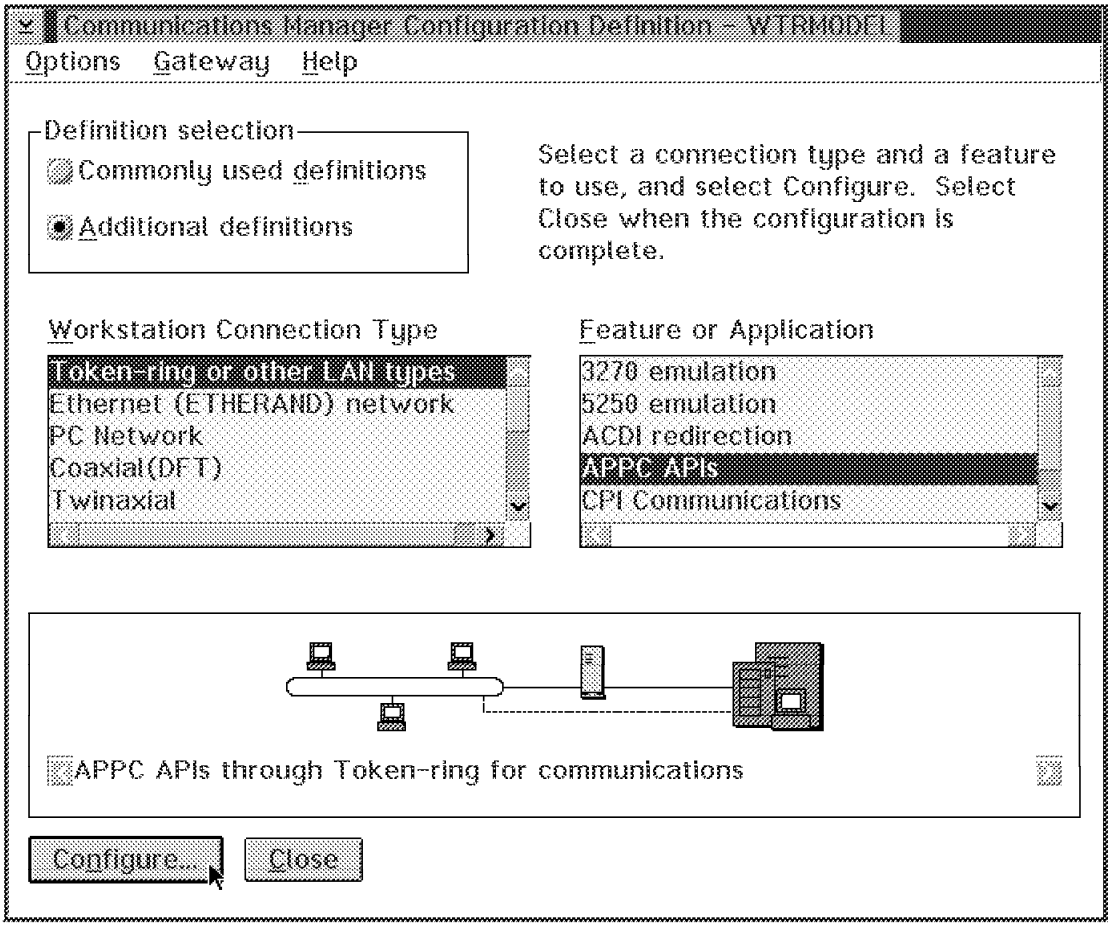


Figure 170. Open Configuration Window

4. Assuming your NGMF workstation is LAN attached to your SNA gateway and your Token-Ring Data Link Control is already configured, then go ahead and select **Additional definitions**, **Token-ring or other LAN types** and **APPC APIs** and click on the **Configure** push button:



5. Enter your:
   - Network ID
   - Local node name (CPNAME or PUname)

   Select your node type as an **End node-no network node server** and click on the **Advanced** push button.

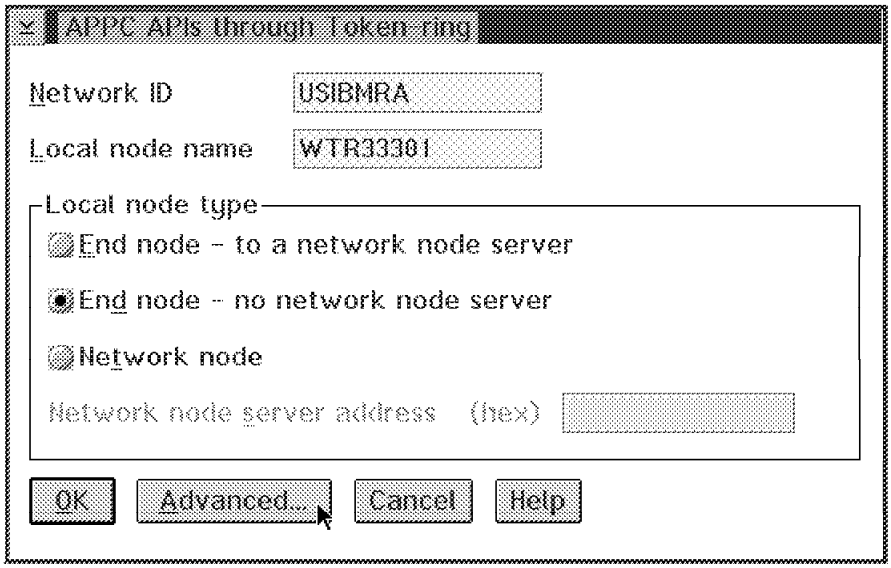


Figure 171. Local Node Characteristics Window

6. Select **SNA connections** from the list box and click on the **Configure** push button.

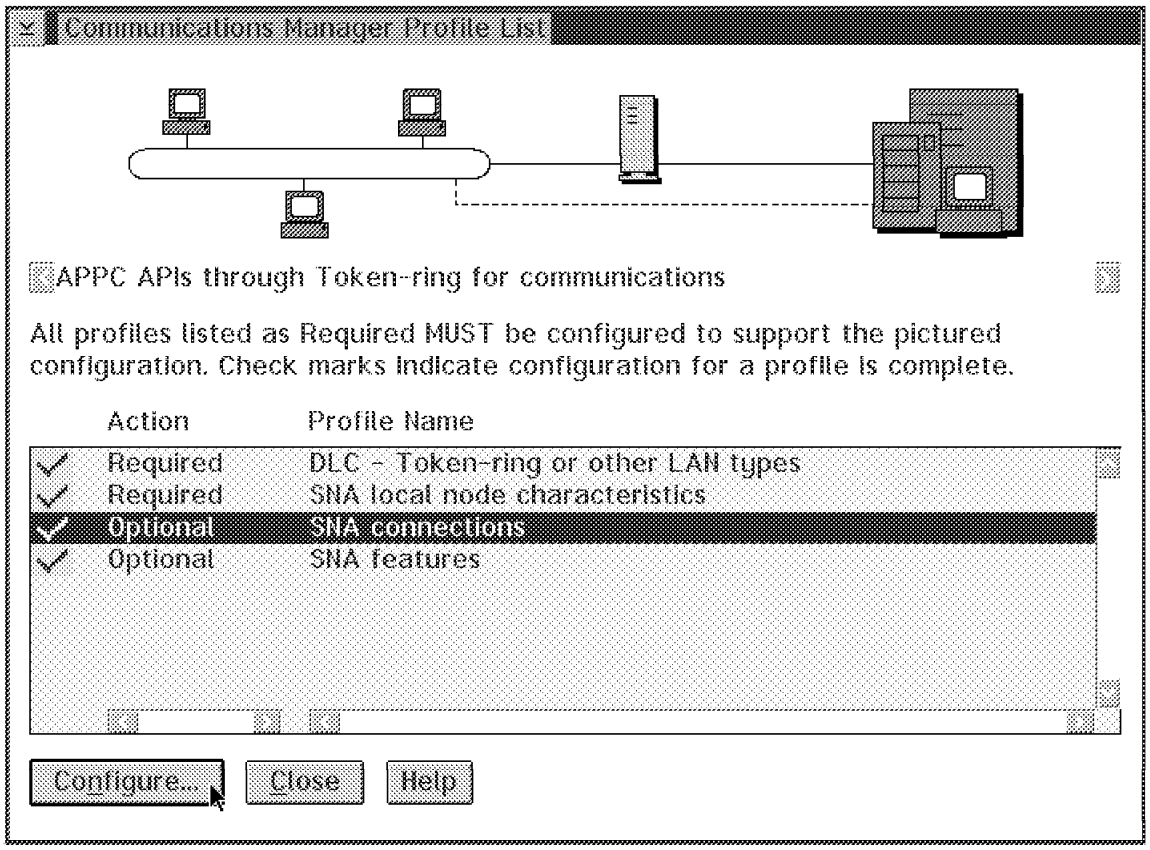


Figure 172. Profile List Feature Window

7. Select **To host** from the partner type box and click on the **Create** push button to make a new link. If you already have a link, select it from the list box and click on the **Change** push button to verify its contents.

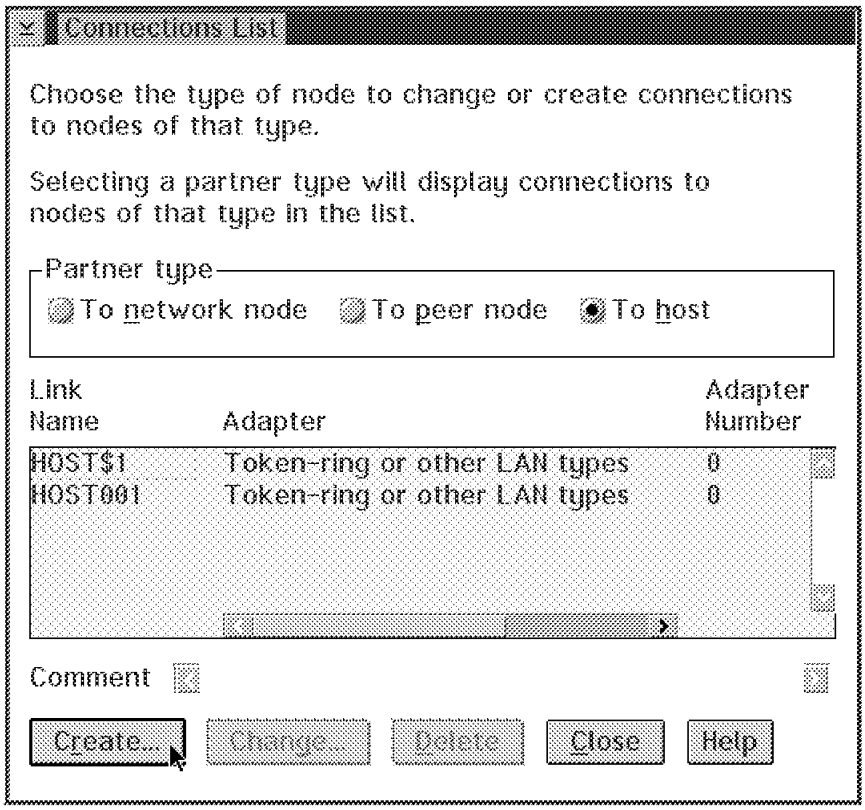


Figure 173. Connections List Window

8. Select **Token-ring or other LAN types** from the list box and click on the **Continue** push button.

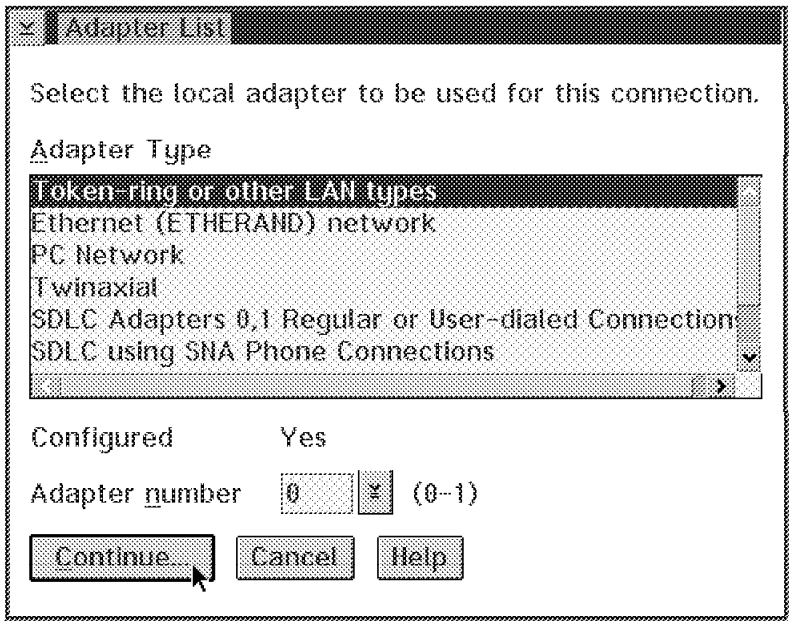


Figure 174. Adapter List Window

9. Enter your:
   - LAN destination address - the MAC address of the adapter which provides a gateway to the SNA network.
   - PU name or CPNAME
   - Node ID - IDBLK IDNUM in the VTAM switched major node. These are not required if a CPNAME is used above.

   and press the **OK** push button.

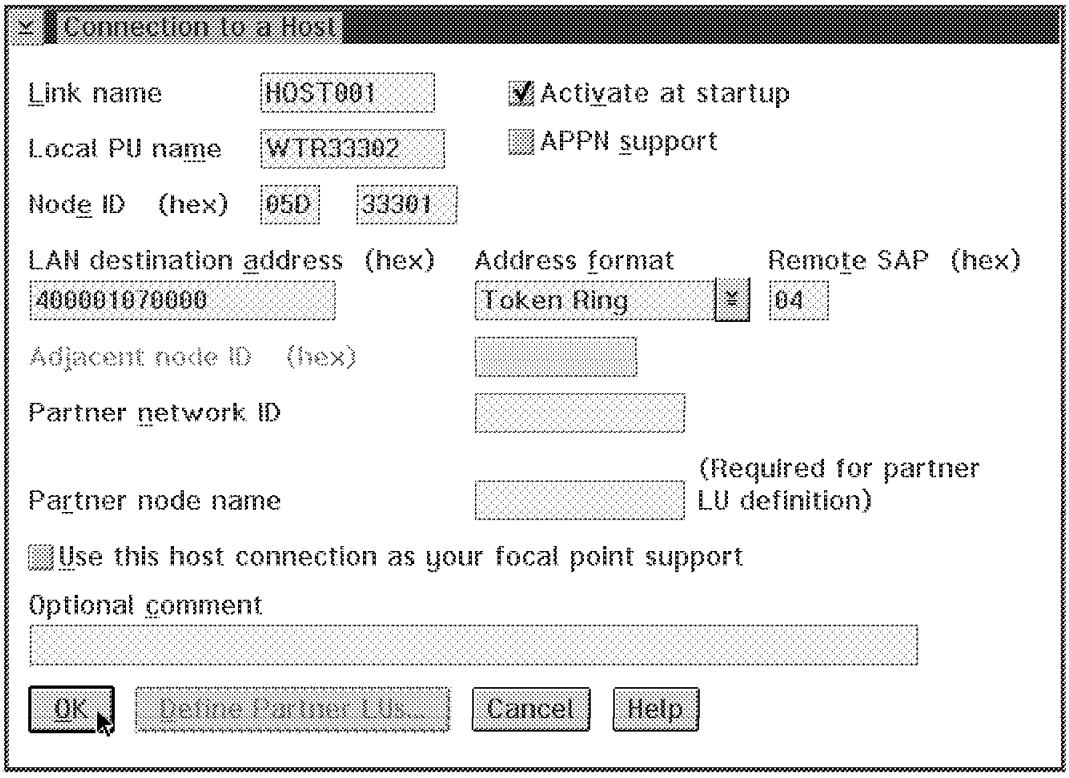


Figure 175. Connection to a Host Window

10. Select *SNA features* from the list box and press the **Configure** push button.

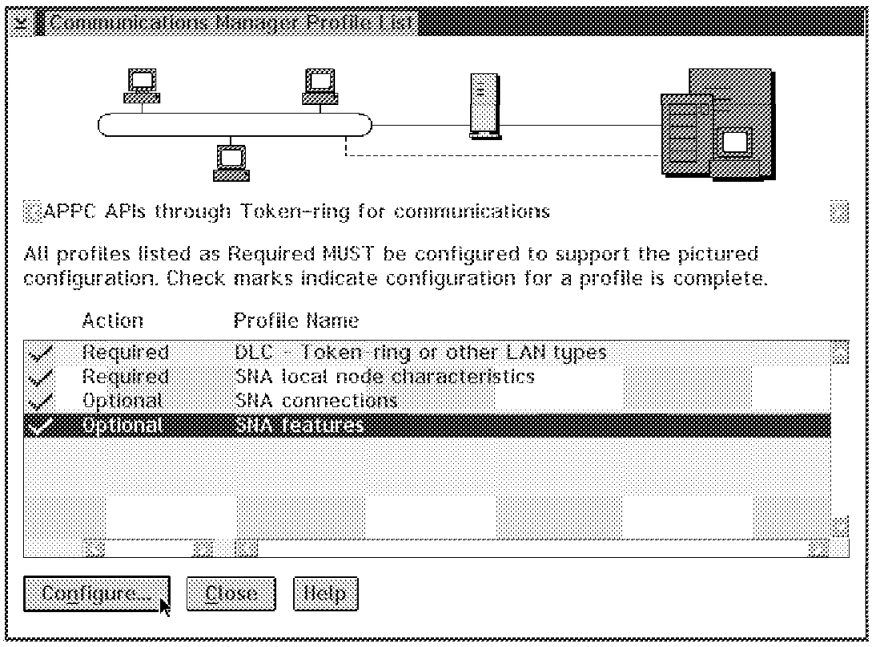


Figure 176. Profile List Window

11. Select **Local LUs** from the list box and click on the **Create** (or the **Change**) push button.

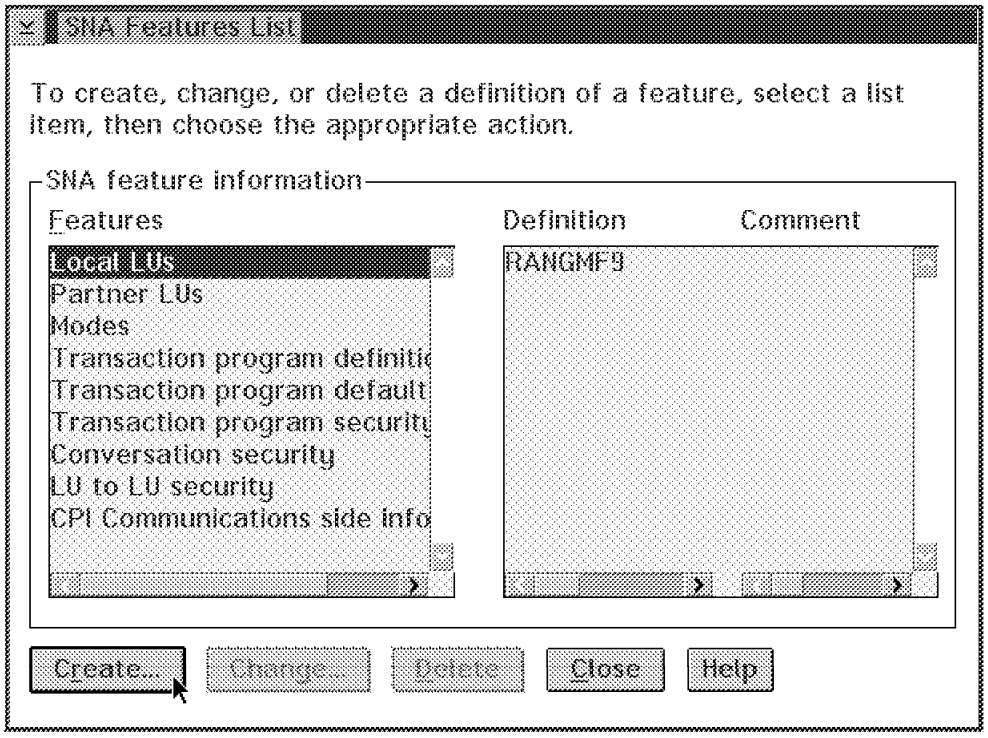


Figure 177. SNA Features List Window

12. Enter the:
    - Independent LU name - as defined in the VTAM switched major node.
    - Alias egvpc
13. Select **Independent LU** in the NAU address box. Click on the **OK** push button.

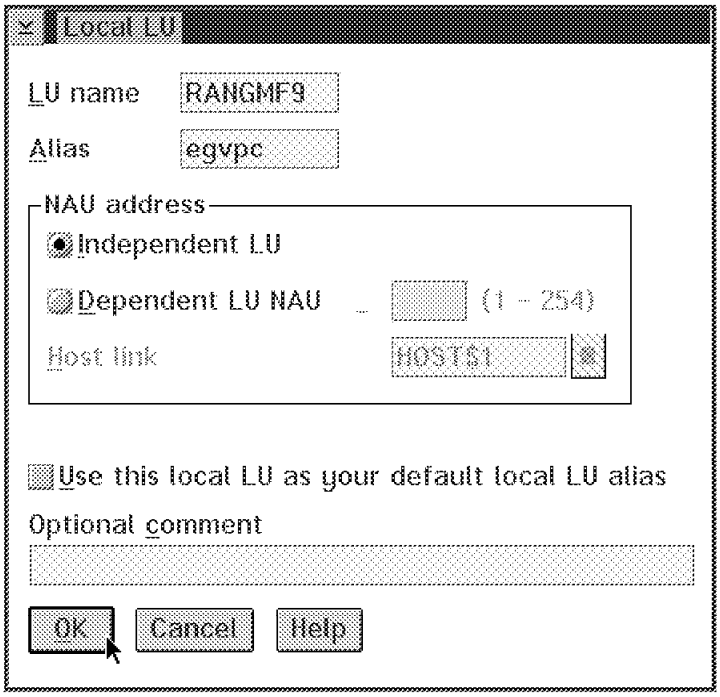


Figure 178. Local LU Definition

14. Select **Modes** from the list box and click on the **Create** (or the **Change**) push button.

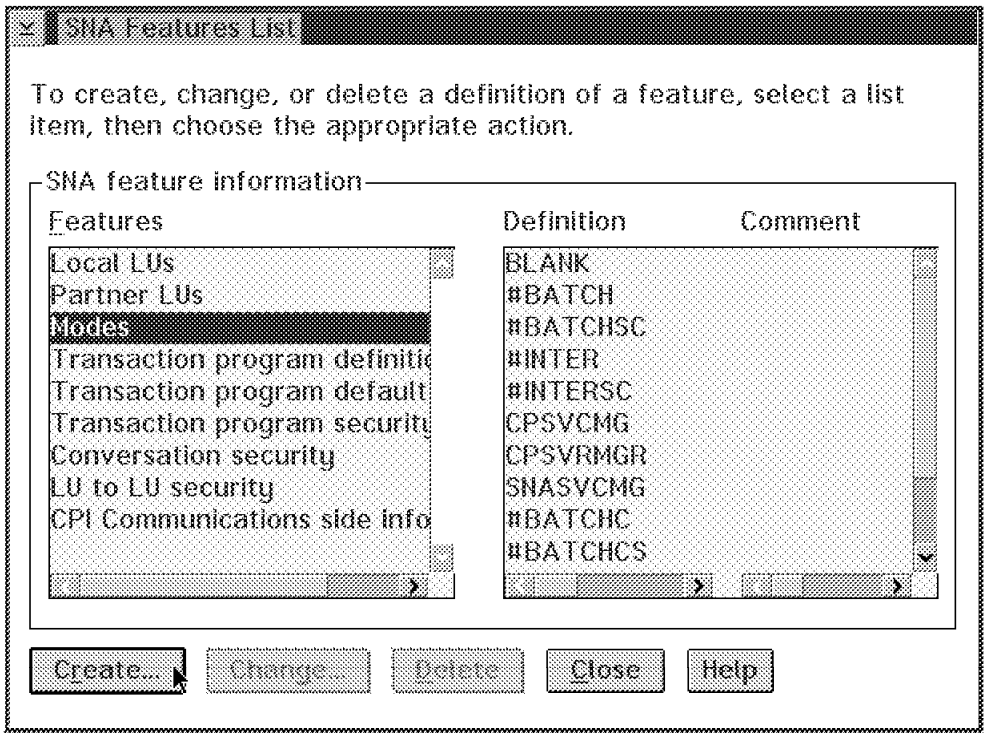


Figure 179. SNA Features List Window

15. Enter the mode name as DSIL6MOD and accept the defaults for the other options on the screen and click on the **OK** push button.

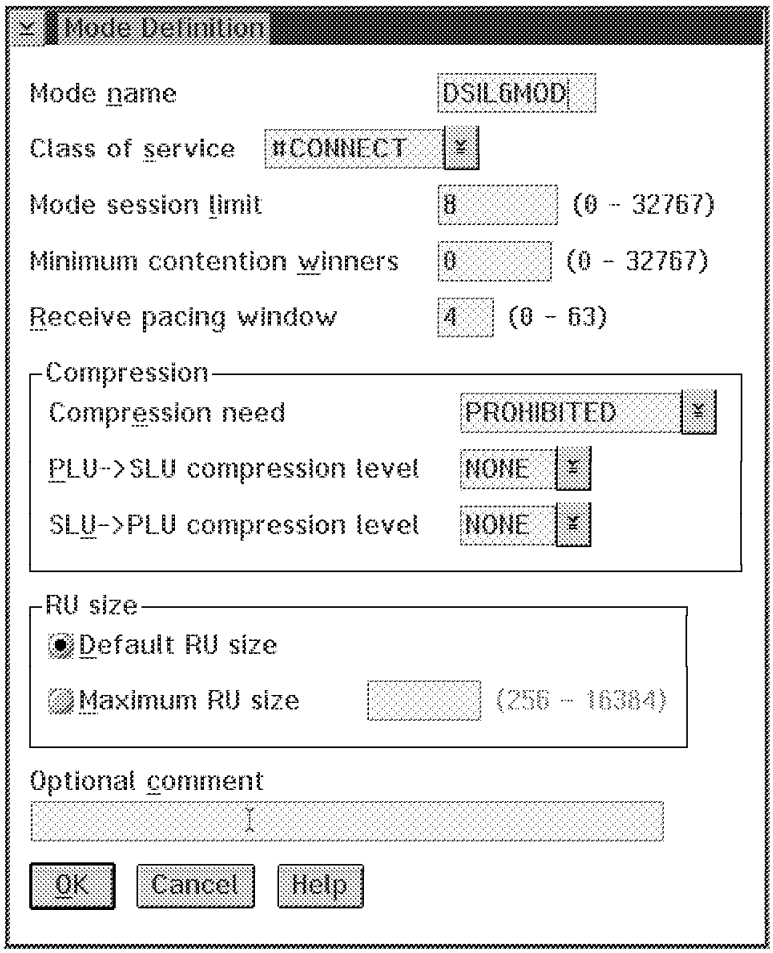


Figure 180. Change a Mode Definition

16. Select **Transaction program definitions** from the list box and click on the **Create** (or the **Change**) push button.

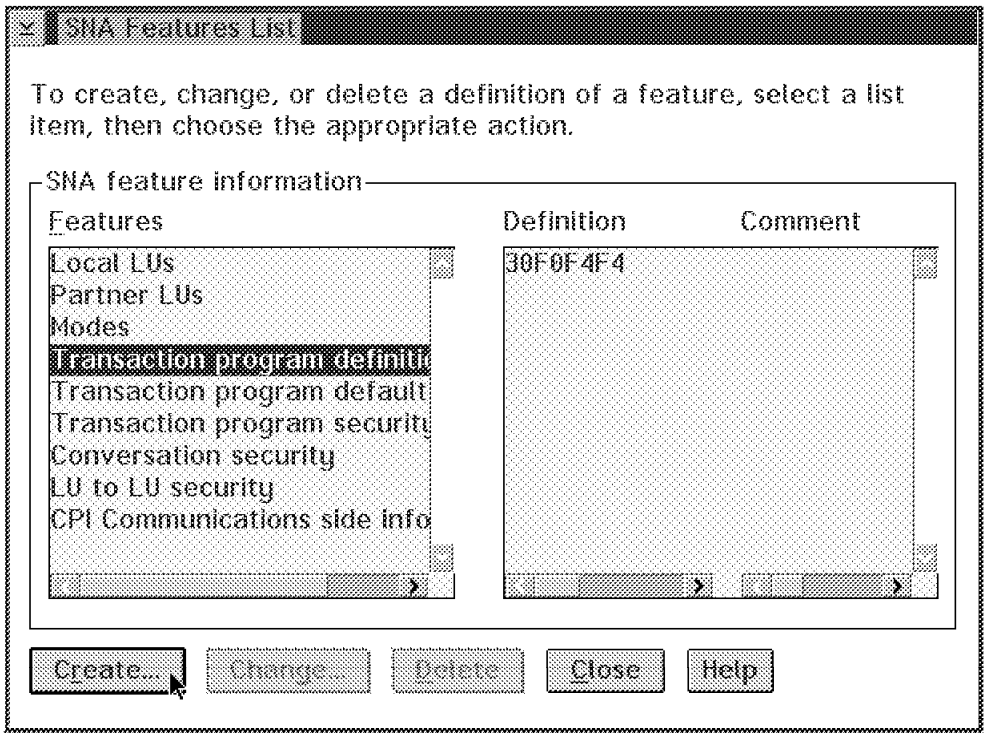


Figure 181. SNA Features List Window

17. Enter the:

    - Transaction program (TP) name as 30F0F0F4. The F must be in uppercase.
    - OS/2 program path and file name. This is, in our case, `d:\ibmegv\exe\egvctp.exe`

    and click on the **Continue** push button.

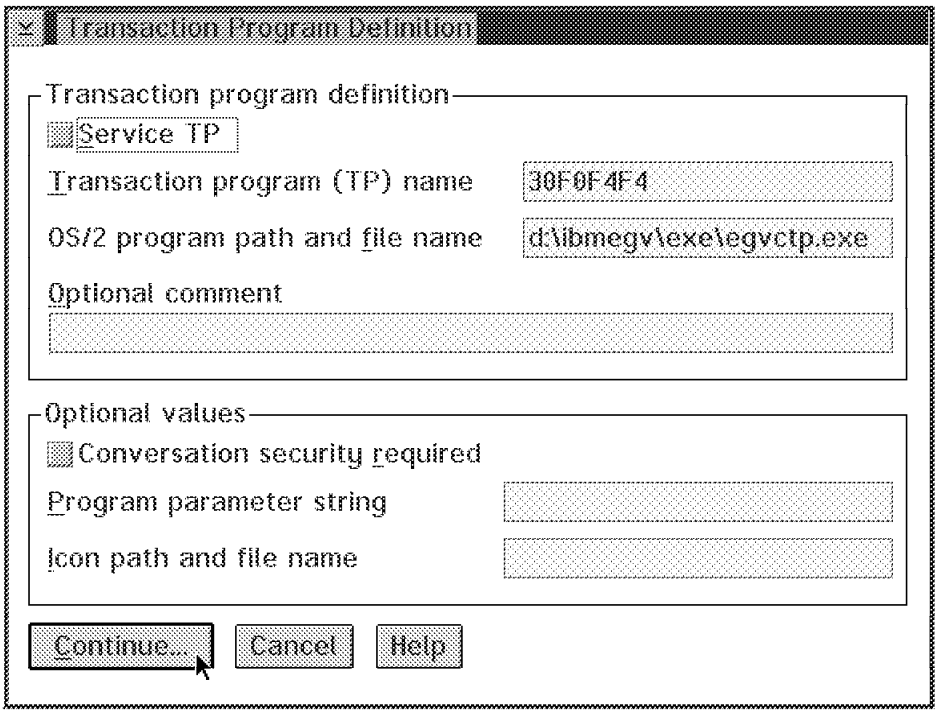


Figure 182. Transaction Program Definition

18. Select **Background** from the Presentation type box.
19. Select **Queued, Attach Manager started** from the Operation type box.
20. Click on the **OK** push button.

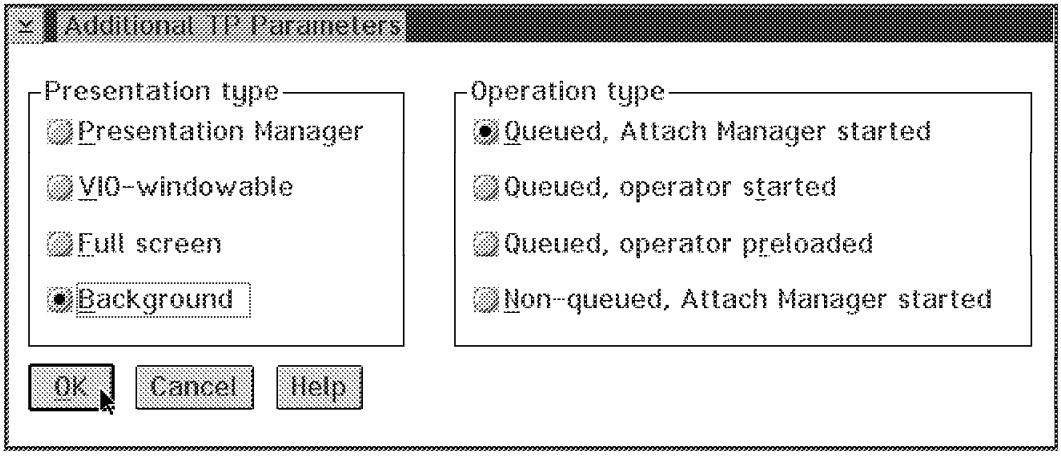


Figure 183. Additional TP Parameters

21. Click on the **Close** push button until you exit Communication Manager Setup.

C.6.3 Important Things to Do

After the configuration has been done the Communications Manager needs some tuning. Without this, the shutdown of NGMF may not work properly.

Edit your NDF file. The file is in the CMLIB directory and has a file name of your configuration.NDF.

- Find *DEFINE_TP*.
- Change the following values
  - INCOMING_ALLOCATE_QUEUE_DEPTH to (4)
  - INCOMING_ALLOCATE_TIMEOUT to (60)
  - RECEIVE_ALLOCATE_TIMEOUT to (1)
- Save the file.
- Run CMVERIFY for your configuration.NDF, from the OS/2 prompt.

C.6.4 Sample NDF File

Your NDF file should look like the following:

C.6.4.1 Local CP

```
DEFINE_LOCAL_CP  FQ_CP_NAME(USIBMRA.WTR33301 )
                 CP_ALIAS(WTR33301)
                 NAU_ADDRESS(INDEPENDENT_LU)
                 NODE_TYPE(EN)
                 NODE_ID(X'05D33301')
                 NW_FP_SUPPORT(NONE)
                 HOST_FP_SUPPORT(YES)
                 HOST_FP_LINK_NAME(HOST$1  )
                 MAX_COMP_LEVEL(NONE)
                 MAX_COMP_TOKENS(0);
```

C.6.4.2 Logical Link

```
DEFINE_LOGICAL_LINK  LINK_NAME(HOST001 )
                     ADJACENT_NODE_TYPE(LEN)
                     DLC_NAME(IBMTRNET)
                     ADAPTER_NUMBER(0)
                     DESTINATION_ADDRESS(X'40000107000004')
                     ETHERNET_FORMAT(NO)
                     CP_CP_SESSION_SUPPORT(NO)
                     SOLICIT_SSCP_SESSION(YES)
                     PU_NAME(WTR33302)
                     NODE_ID(X'05D33301')
                     ACTIVATE_AT_STARTUP(YES)
                     USE_PUNAME_AS_CPNAME(NO)
                     LIMITED_RESOURCE(USE_ADAPTER_DEFINITION)
                     LINK_STATION_ROLE(USE_ADAPTER_DEFINITION)
                     MAX_ACTIVATION_ATTEMPTS(USE_ADAPTER_DEFINITION)
                     EFFECTIVE_CAPACITY(USE_ADAPTER_DEFINITION)
                     COST_PER_CONNECT_TIME(USE_ADAPTER_DEFINITION)
                     COST_PER_BYTE(USE_ADAPTER_DEFINITION)
                     SECURITY(USE_ADAPTER_DEFINITION)
                     PROPAGATION_DELAY(USE_ADAPTER_DEFINITION)
                     USER_DEFINED_1(USE_ADAPTER_DEFINITION)
                     USER_DEFINED_2(USE_ADAPTER_DEFINITION)
                     USER_DEFINED_3(USE_ADAPTER_DEFINITION);
```

C.6.4.3 Local LU

```
DEFINE_LOCAL_LU  LU_NAME(RANGMF9 )
                 LU_ALIAS(egvpc   )
                 NAU_ADDRESS(INDEPENDENT_LU);
```

C.6.4.4 Partner LUs

```
DEFINE_PARTNER_LU  FQ_PARTNER_LU_NAME(USIBMRA.RABAN    )
                   PARTNER_LU_ALIAS(egvpart)
                   PARTNER_LU_UNINTERPRETED_NAME(RABAN   )
                   MAX_MC_LL_SEND_SIZE(32767)
                   CONV_SECURITY_VERIFICATION(NO)
                   PARALLEL_SESSION_SUPPORT(YES);
```

C.6.4.5 Mode Tables

```
DEFINE_MODE  MODE_NAME(DSIL6MOD)
             COS_NAME(#CONNECT)
             DEFAULT_RU_SIZE(YES)
             RECEIVE_PACING_WINDOW(4)
             MAX_NEGOTIABLE_SESSION_LIMIT(32767)
             PLU_MODE_SESSION_LIMIT(8)
             MIN_CONWINNERS_SOURCE(0)
             COMPRESSION_NEED(PROHIBITED)
             PLU_SLU_COMPRESSION(NONE)
             SLU_PLU_COMPRESSION(NONE);
```

C.6.4.6 Defaults

```
DEFINE_DEFAULTS  IMPLICIT_INBOUND_PLU_SUPPORT(YES)
                 DEFAULT_MODE_NAME(BLANK)
                 MAX_MC_LL_SEND_SIZE(32767)
                 DIRECTORY_FOR_INBOUND_ATTACHES(*)
                 DEFAULT_TP_OPERATION(NONQUEUED_AM_STARTED)
                 DEFAULT_TP_PROGRAM_TYPE(BACKGROUND)
                 DEFAULT_TP_CONV_SECURITY_RQD(NO)
                 MAX_HELD_ALERTS(10);
```

C.6.4.7 Transaction Program

```
DEFINE_TP  TP_NAME(30F0F4F4)
           PIP_ALLOWED(NO)
           FILESPEC(d:\ibmegv\exe\egvctp.exe)
           CONVERSATION_TYPE(ANY_TYPE)
           CONV_SECURITY_RQD(NO)
           SYNC_LEVEL(EITHER)
           TP_OPERATION(QUEUED_AM_STARTED)
           PROGRAM_TYPE(BACKGROUND)
           INCOMING_ALLOCATE_QUEUE_DEPTH(4)
           INCOMING_ALLOCATE_TIMEOUT(60)
           RECEIVE_ALLOCATE_TIMEOUT(1);
```

C.6.4.8 Attach Manager

```
START_ATTACH_MANAGER;
```

Appendix D. ITSO IP Environment

This is a picture of the ITSO Raleigh IP environment.

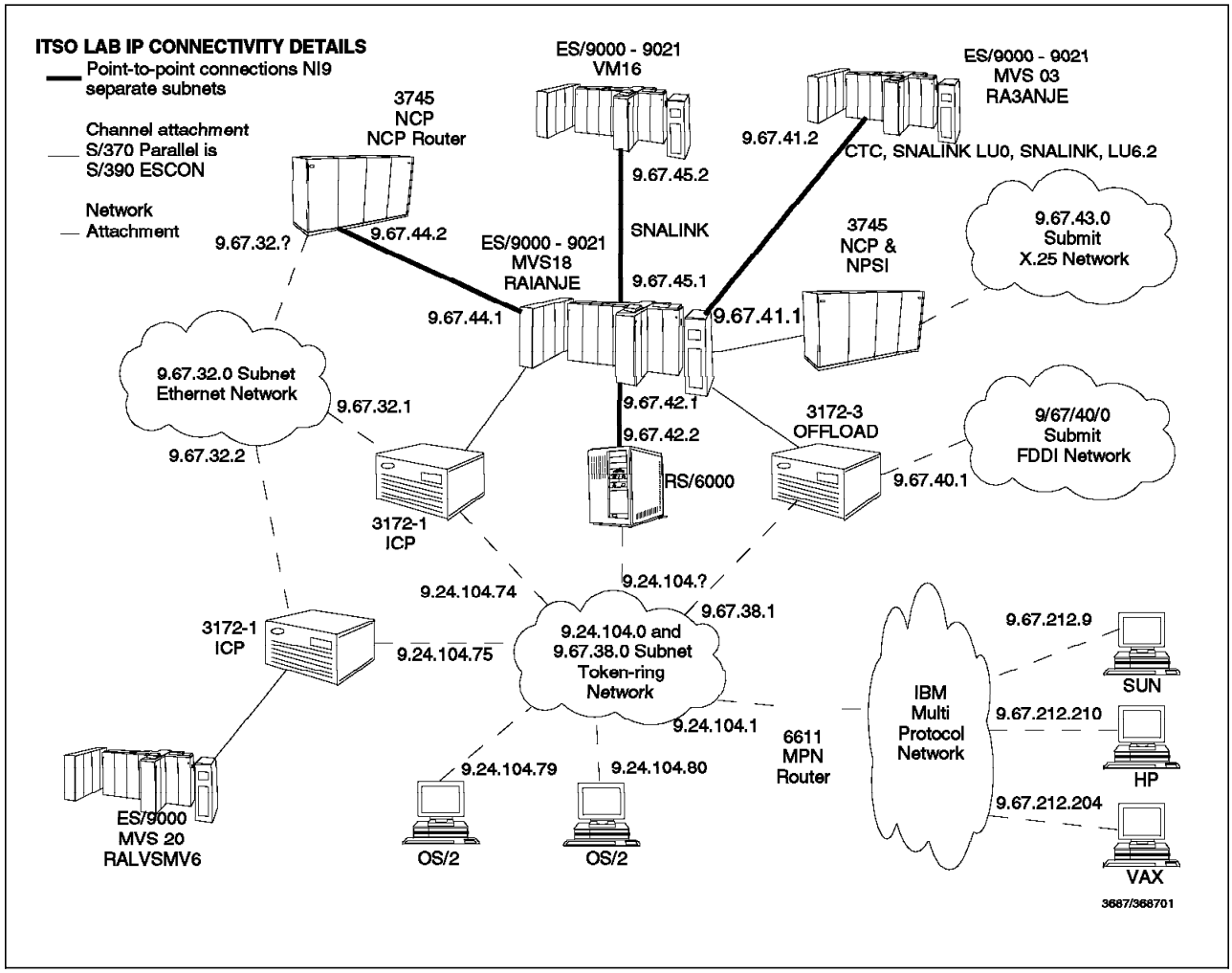


Figure 184. ITSO IP Network Configuration Diagram

Appendix E. MSM Host Samples

E.1 Sample NetView Procedure

```
//NETCA11I PROC Q1=NETVIEW.NV24,     ** USER DSN HIGH LEVEL QUALIFIER
//         U23=NETVIEW.NV23.RABAN,   ** OLD NV 2.3 PARMS
//         DOMAIN=RABAN,        ** NETVIEW DOMAIN NAME
//         PROG=BNJLINTX,       ** PGM USED TO START NETVIEW
//         SQ2=SYS1.NETVIEW.V2R4M0,
//         SQ1=NETVIEW.V2R4M0,
//         MQ1=NETVIEW.NV24.MSMIP, MSM DATA SETS            <===========
//         OQ1=NETVIEW.NV24.MSMIP, MSM DATA SETS            <===========
//         VQ1=NETVIEW.NV24,    ** HIGH LVL DSN QUALIFIER-VSAM DSNS
//         SOUTA='*',           ** DEFAULT PRINTED OUTPUT CLASS
//         REG=4096,            ** REGION SIZE(IN K) FOR MAIN TASK
//         BFSZ=24,             ** BUFFER SIZE(IN K)
//         SLSZ=200             **
//NETVIEW  EXEC PGM=&PROG,TIME=1440,
//         REGION=&REG.K,PARM=(&BFSZ.K,&SLSZ),
//         DPRTY=(13,13)
//STEPLIB  DD   DSN=&SQ2..CNMLINK,DISP=SHR
//         DD   DSN=&SQ2..SEKGMOD1,DISP=SHR
//         DD   DSN=&SQ1..SEKGMOD2,DISP=SHR
//         DD   DSN=&MQ1.SFLCLINK,DISP=SHR               <=============
//         DD   DSN=NETVIEW.NV24.RODMVIEW.LOAD,DISP=SHR
//         DD   DSN=NETVIEW.NV23.USER.CNMLINK,DISP=SHR,
//         UNIT=3390,VOL=SER=WT8043
//         DD   DSN=NPM.V2R1M0.SFNMLMD1,DISP=SHR
//         DD   DSN=PLI.V2R3M0.SIBMLINK,DISP=SHR
//         DD   DSN=PLI.V2R3M0.PLILINK,DISP=SHR
//         DD   DSN=C370.V2R1M0.SEDCLINK,DISP=SHR
//         DD   DSN=NETVIEW.NV24.CWSM.REXX120.SEAGALT,DISP=SHR
//DSICLD   DD   DSN=&Q1..&DOMAIN..DSICLD,DISP=SHR
//         DD   DSN=&MQ1..SFLCCLST,DISP=SHR              <=============
//         DD   DSN=&OQ1..SFLCREX1,DISP=SHR              <=============
//         DD   DSN=NETVIEW.RODMTOOL.CLISTS,DISP=SHR
//         DD   DSN=NETVIEW.LANRODM.CLISTS,DISP=SHR
//         DD   DSN=&SQ1..CNMCLST,DISP=SHR
//         DD   DSN=&Q1..CNMCLST,DISP=SHR
//         DD   DSN=SAO1.CLISTS,DISP=SHR
//         DD   DSN=NETVIEW.NV23.USER.CLISTS,DISP=SHR
//         DD   DSN=NETVIEW.NV23.USER.CLIST2,DISP=SHR
//         DD   DSN=ITSC.COMMON.CLISTS,DISP=SHR,
```

Figure 185 (Part 1 of 2). Sample NetView Procedure

```
//DSIPARM  DD   DSN=ITSC.DSIOPF,DISP=SHR
//         DD   DSN=&MQ1..SFLCSAMP,DISP=SHR               <=============
//         DD   DSN=&Q1..&DOMAIN..DSIPARM,DISP=SHR
//         DD   DSN=&SQ1..DSIPARM,DISP=SHR
//         DD   DSN=&Q1..DSIPARM,DISP=SHR
//         DD   DSN=RISC.VTAMLST,DISP=SHR
//         DD   DSN=RISC.PROCLIB,DISP=SHR
//         DD   DSN=&U23..DSIPARM,DISP=SHR
//DSILIST  DD   DSN=&Q1..&DOMAIN..DSILIST,DISP=SHR
//DSIVTAM  DD   DSN=ITSC.VTAMLST,DISP=SHR
//         DD   DSN=RISC.VTAMLST,DISP=SHR
//DSIPRF   DD   DSN=&Q1..&DOMAIN..DSIPRF,DISP=SHR
//         DD   DSN=&SQ1..DSIPRF,DISP=SHR
//         DD   DSN=ITSC.DSIPRF,DISP=SHR,
//         UNIT=3380,VOL=SER=WTL852
//FLBDAT1  DD  DSN=NETVIEW.NV24.SFLBDAT1,DISP=SHR
//DSIMSG   DD   DSN=&SQ1..SDSIMSG1,DISP=SHR
//         DD   DSN=&Q1..SDSIMSG1,DISP=SHR
//         DD   DSN=&MQ1..SFLCMSGU,DISP=SHR               <=============
//BNJPNL1  DD   DSN=&SQ1..BNJPNL1,DISP=SHR
//BNJPNL2  DD   DSN=&SQ1..BNJPNL2,DISP=SHR
//CNMPNL1  DD   DSN=&SQ1..CNMPNL1,DISP=SHR
//         DD   DSN=NETVIEW.NV24.RODMVIEW.PANEL,DISP=SHR
//         DD   DSN=&MQ1..SFLCPNLU,DISP=SHR
//         DD   DSN=NETVIEW.NV23.USER.PANEL,DISP=SHR
//CNMMSGF  DD   DSN=&VQ1..&DOMAIN..CNMMSGF,DISP=SHR,
//         AMP='AMORG,BUFNI=10,BUFND=5'
//CNMCMDF  DD   DSN=&VQ1..&DOMAIN..CNMCMDF,DISP=SHR,
//         AMP='AMORG,BUFNI=10,BUFND=5'
//DSILOGP  DD   DSN=&VQ1..&DOMAIN..DSILOGP,
//         DISP=SHR,AMP='AMORG,BUFNI=10,BUFND=5'
//DSILOGS  DD   DSN=&VQ1..&DOMAIN..DSILOGS,
//         DISP=SHR,AMP='AMORG,BUFNI=10,BUFND=5'
//DSITRCP  DD   DSN=&VQ1..&DOMAIN..DSITRCP,
//         DISP=SHR,AMP=AMORG
//DSITRCS  DD   DSN=&VQ1..&DOMAIN..DSITRCS,
//         DISP=SHR,AMP=AMORG
//AAUVSPL  DD   DSN=&VQ1..&DOMAIN..AAUVSPL,
//         DISP=SHR,AMP='AMORG'
//AAUVSSL  DD   DSN=&VQ1..&DOMAIN..AAUVSSL,
//         DISP=SHR,AMP='AMORG'
//BNJLGPR  DD   DSN=&VQ1..&DOMAIN..BNJLGPR,
//         DISP=SHR,AMP='AMORG'
//BNJLGSE  DD   DSN=&VQ1..&DOMAIN..BNJLGSE,
//         DISP=SHR,AMP='AMORG'
//BNJ36PR  DD   DSN=&VQ1..&DOMAIN..BNJ36PR,
//         DISP=SHR,AMP=AMORG
//DSISVRT  DD   DSN=&VQ1..&DOMAIN..DSISVRT,
//         DISP=SHR,AMP=AMORG
//SYSPRINT DD   SYSOUT=&SOUTA
//RORGNLDM DD DSN=&SQ1..CNMSAMP(CNMSJV03),DISP=SHR,
//         UNIT=3380,VOL=SER=WTL660
//RORGNPDA DD DSN=&SQ1..CNMSAMP(CNMSJV04),DISP=SHR,
//         UNIT=3380,VOL=SER=WTL660
```

Figure 185 (Part 2 of 2). Sample NetView Procedure

E.2 Sample NetView SSI Procedure

```
//NETCS11 PROC SQ1='SYS1.NETVIEW.V2R4M0',
//       PROG=CNMINIT,        ** PGM USED TO START NETVIEW SUBSYSTEM
//       REG=1250,            ** REGION SIZE(IN K)
//       MBUF=4000,           ** NUMBER OF MESSAGE BUFFERS TO USE
//       CBUF=200,            ** NUMBER OF COMMAND BUFFERS TO USE
//       DSIG='%',            ** SUBSYSTEM COMMAND DESIGNATOR CHARACTER
//       MSGIFAC='SYSTEM',    ** SSI/Extended console override switch
//       PPIOPT='PPI'          ** PPI options switch
//NETVIEW  EXEC PGM=&PROG,TIME=1440,REGION=&REG.K,
//         PARM=(&MBUF,&CBUF,'&DSIG','&MSGIFAC','&PPIOPT'),
//         DPRTY=(13,13)
//STEPLIB  DD   DSN=&SQ1..CNMLINK,DISP=SHR
```

Figure 186. Sample NetView SSI Procedure

E.3 Sample RODM Procedure

```
//RODM11I  PROC SQ1=SYS1.NETVIEW.V2R4M0,
//         VQ1=NETVIEW.NV24.RABAN,   ** HIGH LVL DSN Q'FIER-VSAM DSNS
//         TYPE=W,              ** SELECT A COLD OR WARM START
//         NAME=RODM11,INIT=,CLRSSB=NO,CUST=EKGCUST
//*****************************************************************
//START    EXEC PGM=EKGTC000,REGION=0K,TIME=1440,
//           PARM='&TYPE,&NAME,&INIT,&CLRSSB,&CUST'
//STEPLIB  DD DSN=&SQ1..SEKGMOD1,DISP=SHR
//         DD DSN=NETVIEW.V2R4M0.SEKGMOD2,DISP=SHR
//         DD DSN=PLI.V2R3M0.PLILINK,DISP=SHR
//         DD DSN=PLI.V2R3M0.SIBMLINK,DISP=SHR
//         DD DSN=C370.V2R1M0.SEDCLINK,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSABEND DD SYSOUT=*
//SYSDUMP  DD SYSOUT=*
//SYSTERM  DD SYSOUT=*
//EKGLOGP  DD DSN=&VQ1..EKGLOGP,DISP=SHR,
//         AMP=('BUFND=10')
//EKGLOGS  DD DSN=&VQ1..EKGLOGS,DISP=SHR,
//         AMP=('BUFND=10')
//EKGCUST  DD DSN=&VQ1..SEKGSMP1,DISP=SHR
//EKGLANG  DD DSN=NETVIEW.V2R4M0.SEKGLANG,DISP=SHR
//EKGMAST  DD DSN=&VQ1..EKGMAST,DISP=SHR
//EKGTRAN  DD DSN=&VQ1..EKGTRAN,DISP=SHR
//EKGD001  DD DSN=&VQ1..EKGCK001,DISP=SHR
//EKGD002  DD DSN=&VQ1..EKGCK002,DISP=SHR
```

Figure 187. Sample RODM Procedure

E.4 Sample GMFHS Procedure

```
//GMFHS11I PROC Q1=NETVIEW.V2R4M0,
//             SQ1=SYS1.NETVIEW.V2R4M0,
//             VQ1=NETVIEW.NV24, ** HIGH LVL DSN Q'FIER-VSAM DSNS
//             DOMAIN=RABAN,  ** NETVIEW DOMAIN NAME
//             PROG=DUIFT000, ** PGM USED TO START GMFHS HOST MAIN TASK
//             REG=0K,        ** REGION SIZE IN K FOR MAIN TASK
//             AGGRST=        ** RUN AGG CALCULATION ON STARTUP
//STEP1    EXEC PGM=&PROG,REGION=&REG,PARM='&AGGRST',TIME=1440
//STEPLIB  DD DSN=&SQ1..CNMLINK,DISP=SHR
//         DD DSN=&SQ1..SEKGMOD1,DISP=SHR
//         DD DSN=PLI.V2R3M0.PLILINK,DISP=SHR
//         DD DSN=PLI.V2R3M0.SIBMLINK,DISP=SHR
//*   INITIALIZATION PARAMETERS DATA SET
//CNMPARM  DD DSN=&VQ1..&DOMAIN..DSIPARM,DISP=SHR
//         DD DSN=&Q1..DSIPARM,DISP=SHR
//*   GMFHS MESSAGES DATA SET
//CNMMSG1  DD DSN=&Q1..SDUIMSG1,DISP=SHR
//CNMDB    DD DSN=&VQ1..&DOMAIN..DUIDB,DISP=SHR
//CNMM     DD SYSOUT=L
//CNMD     DD SYSOUT=L
//CNMI     DD SYSOUT=L
//CNMO     DD SYSOUT=L
//CNMF     DD SYSOUT=L
//CNME     DD SYSOUT=L
//CNMV     DD SYSOUT=L
//CNMC     DD SYSOUT=L
//CNMS     DD SYSOUT=L
//CNMT     DD SYSOUT=L
//*   RUNTIME LIBRARY MESSAGES
//SYSTERM  DD SYSOUT=L
//*   THE FOLLOWING ARE FOR THE RODM LOAD UTILITY
//EKGLANG  DD DSN=&Q1..SEKGLANG,DISP=SHR
//EKGLUTB  DD DSN=&Q1..SEKGLUTB,DISP=SHR
//EKGPRINT DD SYSOUT=L
//EKGIN3   DD DUMMY,DCB=BLKSIZE=80
```

Figure 188. Sample GMFHS Procedure

E.5 Sample GMFHS Data Model Load Job

```
//GEORGESY JOB O-111111,MSGCLASS=O,MSGLEVEL=(1,1),REGION=4M,CLASS=I     00001002
//EKGLOADP PROC SQ1='SYS1.NETVIEW.V2R4MO',
//            Q1='NETVIEW.V2R4MO',
//            RODMNAME=RODM11,
//            EKGIN1='NETVIEW.V2R4MO.CNMSAMP(DUIFSTRC)',
//            EKGIN3='NETVIEW.V2R4MO.CNMSAMP(DUIFSNET)',
//            LOAD=STRUCTURE,
//            OPER=LOAD,
//            LISTL=ERRORSYNTAX,
//            SEVERITY=WARNING,
//            COPIES=1,
//            CODEPAGE=EKGCP500
//*
//LOADRODM EXEC PGM=EKGLOTLM,
//         PARM=('OPERATION=&OPER,LOAD=&LOAD,NAME=&RODMNAME',
//    'CODEPAGE=&CODEPAGE,LISTLEVEL=&LISTL,SEVERITY=&SEVERITY')
//STEPLIB  DD  DSN=&SQ1..SEKGMOD1,DISP=SHR
//         DD  DSN=PLI.V2R3MO.PLILINK,DISP=SHR
//         DD  DSN=PLI.V2R3MO.SIBMLINK,DISP=SHR
//*
//EKGLANG  DD  DSN=&Q1..SEKGLANG,DISP=SHR
//EKGLUTB  DD  DSN=&Q1..SEKGLUTB,DISP=SHR
//EKGPRINT DD  SYSOUT=*,COPIES=&COPIES
//SYSPRINT DD  SYSOUT=*
//EKGIN1   DD DSN=&EKGIN1,DISP=SHR
//EKGIN2   DD DSN=&Q1..SEKGCAS1,DISP=SHR
//EKGIN3   DD DSN=&EKGIN3,DISP=SHR
//PLIDUMP  DD  SYSOUT=*
//*
//         PEND
//S1  EXEC EKGLOADP
```

Figure 189. Sample GMFHS Data Model Load Job

E.6 Sample MSM Data Model Load Job

```
//WOZABAL1 JOB O-111111,MSGCLASS=O,MSGLEVEL=(1,1),REGION=4M,CLASS=I,
// NOTIFY=WOZABAL
//EKGLOADP PROC SQ1='SYS1.NETVIEW.V2R4MO',
//            Q1='NETVIEW.V2R4MO',
//            MQ1='MSM.V1R2MO',
//            RODMNAME=RODM11,
//            LOAD=STRUCTURE,
//            OPER=LOAD,
//            LISTL=ERRORSYNTAX,
//            SEVERITY=ERROR,
//            COPIES=1,
//            CODEPAGE=EKGCP500
//*
//LOADRODM EXEC PGM=EKGLOTLM,
//         PARM=('OPERATION=&OPER,LOAD=&LOAD,NAME=&RODMNAME',
//    'CODEPAGE=&CODEPAGE,LISTLEVEL=&LISTL,SEVERITY=&SEVERITY')
//STEPLIB  DD  DSN=&SQ1..SEKGMOD1,DISP=SHR
//         DD  DSN=PLI.V2R3MO.PLILINK,DISP=SHR
//         DD  DSN=PLI.V2R3MO.SIBMLINK,DISP=SHR
//*
//EKGLANG  DD  DSN=&Q1..SEKGLANG,DISP=SHR
//EKGLUTB  DD  DSN=&Q1..SEKGLUTB,DISP=SHR
//EKGPRINT DD  SYSOUT=*,COPIES=&COPIES
//SYSPRINT DD  SYSOUT=*
//EKGIN1   DD DUMMY
//EKGIN2   DD DSN=&Q1..SEKGCAS1,DISP=SHR
//EKGIN3   DD DUMMY
//PLIDUMP  DD  SYSOUT=*
//      PEND
//LOAD EXEC EKGLOADP
//         DD  DSN=&MQ1..SFLCSAMP(FLCSDM1),DISP=SHR
//         DD  DSN=&MQ1..SFLCSAMP(FLCSDM2),DISP=SHR
//         DD  DSN=&MQ1..SFLCSAMP(FLCSDM3),DISP=SHR
//         DD  DSN=&MQ1..SFLCSAMP(FLCSDM4),DISP=SHR
//         DD  DSN=&MQ1..SFLCSAMP(FLCSDM5),DISP=SHR
//         DD  DSN=&MQ1..SFLCSAMP(FLCSDM64),DISP=SHR
//         DD  DSN=&MQ1..SFLCSAMP(FLCSDM7),DISP=SHR
//         DD  DSN=&MQ1..SFLCSAMP(FLCSDM8),DISP=SHR
//         DD  DSN=&MQ1..SFLCSAMP(FLCSDM9),DISP=SHR
//         DD  DSN=&MQ1..SFLCSAMP(FLCSDM10),DISP=SHR
```

Figure 190. Sample MSM Data Model Load Job

E.7 Sample MSM Initialization File FLCAINP

```
*********************************************************************
*    5655-044 (C) COPYRIGHT IBM CORPORATION 1993                    *
*     ALL RIGHTS RESERVED.                                          *
*********************************************************************
* Description: Sample initialization file for MultiSystem Manager.  *
*              This file specifies the necessary information required *
*              by MultiSystem Manager.                              *
*              Note that the statements are currently commented (as *
*              denoted by the asterisk in the first column).        *
*              Remove the comments from the lines containing the    *
*              keywords that apply to your environment and fill in  *
*              the values for the keywords as appropriate.          *
*********************************************************************
* DEF_AUTOTASK is used to specify the name of the default autotask. *
* This autotask is used if the AUTOTASK keyword is NOT specified on *
* the GETTOPO command.  This keyword is required.                   *
*********************************************************************
DEF_AUTOTASK=AUTOMSM
*********************************************************************
* The RODMNAME statement is required.                               *
*********************************************************************
RODMNAME=RODM11
*********************************************************************
* The RODMRETRY statement is optional.                              *
*********************************************************************
*RODMRETRY=xx
*********************************************************************
* The RODMINT statement is optional.                                *
*********************************************************************
*RODMINT=xx
*********************************************************************
* The RUNCMDRETRY statement is optional.                            *
*********************************************************************
*RUNCMDRETRY=x
*********************************************************************
* DEF_NETWORK_VIEW allows you to provide a specific name for the    *
* default network view name and associated annotation.  If not      *
* specified, the default network view name and annotation will be   *
* used.                                                             *
*********************************************************************
DEF_NETWORK_VIEW=MSM_REDBOOK/Default_name
*********************************************************************
* Include the initialization statements for NetWare, LNM and NV6000 *
*********************************************************************
%INCLUDE FLCINW
%INCLUDE FLCILNM
%INCLUDE FLCIIP
```

Figure 191. Sample MSM Initialization File

E.8 Sample MSM Initialization File FLCIIP

```
GETTOPO,
IPRES,
SP=RA6OO5CP,
MAP=msm,
NETWORK_AG_OBJECT=LAB_IP,
NETWORK_VIEW=MSM_Views/IP,LNM_and_NetWare_Views,
APPL=RS6OOO5S,
AUTOTASK=AUTOIPA,
HEARTBEAT=3O,
TRACE=YES
GETTOPO,
IPRES,
SP=RA6O1OCP,
AUTOTASK=AUTORAY,
NETWORK_AG_OBJECT=LAB_IP,
NETWORK_VIEW=MSM_Views/IP,LNM_and_NetWare_Views,
APPL=RS6OO1OS,
HEARTBEAT=3O,
TRACE=YES
```

Figure 192. Sample MSM Initialization File for IP

Appendix F. Mibappl Shell Script

```
#-------------------------------------------------------------------------
#
# mibappl - This AIX Shell script allows you to "execute" MIB
#           applications remotely via RUNCMD from host NetView.
#
#           It "reads" the specified MIB application and then
#           issues SNMPWALKs for the MIB variables specified in
#           the MIB application.
#
# Syntax:   mibappl  mib_application host [community_name]
#
#
#-------------------------------------------------------------------------


#-------------------------------------------------------------------------
#
# getmib - This function gets called when the specified MIB application
#          contains a statement which begins with ' -mib' which contains
#          a list of mib variables to be displayed.
#
# Syntax:  getmib host community list_of_mib_variables
#
#-------------------------------------------------------------------------

function getmib {

host=$1

community=$2

mibvars=$3

let varnum=1

mibvar=$(print $mibvars | cut -f$varnum -d',' | cut -f1 -d':')

while [[ -n $mibvar ]]; do

      snmpwalk -c $community $host $mibvar

      let varnum="varnum+1"

      mibvar=$(print $mibvars | cut -f$varnum -d',' | cut -f1 -d':')
done

return

}


#-------------------------------------------------------------------------
#
# getobj - This function gets called when the specified MIB application
#          contains a statement which begins with ' -obj' which contains
```

```
#          a list of mib variables to be displayed.
#
# Syntax:  getobj host community list_of_mib_variables
#
#-------------------------------------------------------------------------

function getobj {

host=$1

community=$2

mibvars=$3

let varnum=2

mibvar=$(print $mibvars | cut -f$varnum -d'=' | cut -f1 -d',')

while [[ -n $mibvar ]]; do

      snmpwalk -c $community $host $mibvar

      let varnum="varnum+1"

      mibvar=$(print $mibvars | cut -f$varnum -d'=' | cut -f1 -d',')
done

return

}


#-------------------------------------------------------------------------
#
# getfield - This function gets called when the specified MIB application
#            contains a statement which begins with ' -table' and a
#            statement which begins with ' -fields'.  The 2 statements
#            define mib variables to be displayed.
#
# Syntax:    getfield host community table list_of_mib_variables
#
#
#-------------------------------------------------------------------------

function getfield {

host=$1

community=$2

table=$3

mibvars=$4

let varnum=2

mibvar=$(print $mibvars | cut -f2 -d"'" | cut -f1 -d'\' | cut -f$varnum -d'=' |
                                                              cut -f1 -d':')
```

```
while [[ -n $mibvar ]]; do

        snmpwalk -c $community $host $table".".$mibvar

        let varnum="varnum+1"

        mibvar=$(print $mibvars | cut -f2 -d'"' | cut -f1 -d'\' |
                                    cut -f$varnum -d'=' | cut -f1 -d':')

done

return

}


#--------------------------------------------------------------------
#
# mibappl - This is the main line shell script.  It gets passed 3
#           parameters: mib application, host, and an optional community
#           name.  It reads the mib application searching for statements
#           which begin with ' -mib', ' -obj' or ' -table' and then
#           calls the appropriate functions identified above to retrieve
#           the mib variables and display them.
#
# Syntax:   mibappl  mib_application host [community_name]
#
#--------------------------------------------------------------------

mibappl=$1

if [[ -z $mibappl ]]; then
   print "MIBAPPL Syntax error: mib application was not specfied."
   print " "
   print "MIBAPPL Syntax: mibappl mib_application host_name [community]"
   exit 1
fi

filename='/usr/OV/registration/C/ovmib/'$mibappl

if [[ ! -s $filename ]]; then
   print "MIBAPPL error: $filename does not exist or is empty."
   exit 1
fi

host=$2

if [[ -z $host ]]; then
   print "MIBAPPL Syntax error: host_name was not specfied."
   print " "
   print "MIBAPPL Syntax: mibappl mib_application host_name [community]"
   exit 1
fi

community=${3:-"public"}

getmib $host $community $(grep -h ' -mib' $filename | cut -f2 -d'"' | cut -f1 -d'\')

getobj $host $community $(grep -h ' -obj' $filename | cut -f2 -d'"' | cut -f1 -d'\')
```

```
getfield $host $community $(grep -h ' -table' $filename | cut -f2 -d'"'  |
cut -f1 -d'\') $(grep -h ' -fields' $filename | cut -f2 -d'"' | cut -f1 d'\')

exit
```

List of Abbreviations

APAR	authorized program analysis report
APPN	Advanced Peer-to-Peer Networking
CLIST	command list
CT/2	Command Tree/2
GMFHS	Graphic Monitor Facility Host Subsystem
IBM	International Business Machines Corporation
ITSO	International Technical Support Organization
LAN	local area network
LAPS	LAN Adapter and Protocol Support
LNM	LAN Network Manager
LU	logical unit
MSM	MultiSystem Manager
MVS	multiple virtual storage
NCCF	network command and control facility
NCP	network control program
NGMF	NetView Graphic Monitor Facility
PTF	program temporary fix
RC	resource compiler
REXX	restructured extended executor language
RODM	Resource Object Data Manager
RT/2	RODMTool/2
SMIT	System Management Interface Tool
SNA	systems network architecture
SNMP	simple network management protocol
SSCP	systems services control point
VTAM	virtual telecommunications access method

Index

Numerics

A

B

C

D

E

F

G

I

L

M

N

O

P

R

S

T

V

ITSO Technical Bulletin Evaluation RED000

International Technical Support Organization
Managing IP Networks
Using NetView MultiSystem Manager R2
December 1994

Publication No. GG24-4337-00

Your feedback is very important to help us maintain the quality of ITSO Bulletins. **Please fill out this questionnaire and return it using one of the following methods:**

- Mail it to the address on the back (postage paid in U.S. only)
- Give it to an IBM marketing representative for mailing
- Fax it to: Your International Access Code + 1 914 432 8246
- Send a note to REDBOOK@VNET.IBM.COM

Please rate on a scale of 1 to 5 the subjects below.
(1 = very good, 2 = good, 3 = average, 4 = poor, 5 = very poor)

Overall Satisfaction	____		
Organization of the book	____	Grammar/punctuation/spelling	____
Accuracy of the information	____	Ease of reading and understanding	____
Relevance of the information	____	Ease of finding information	____
Completeness of the information	____	Level of technical detail	____
Value of illustrations	____	Print quality	____

Please answer the following questions:

a) If you are an employee of IBM or its subsidiaries:

Do you provide billable services for 20% or more of your time? Yes____ No____

Are you in a Services Organization? Yes____ No____

b) Are you working in the USA? Yes____ No____

c) Was the Bulletin published in time for your needs? Yes____ No____

d) Did this Bulletin meet your needs? Yes____ No____

If no, please explain:

_____

_____

What other topics would you like to see in this Bulletin?

_____

_____

What other Technical Bulletins would you like to see published?

_____

Comments/Suggestions: (THANK YOU FOR YOUR FEEDBACK!)

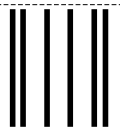
_____ _____
Name Address

_____ _____
Company or Organization

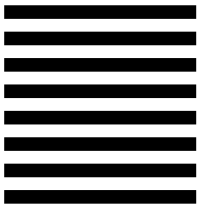
_____ _____
Phone No.

Cut or Fold
Along Line

Fold and Tape **Please do not staple** Fold and Tape



NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES



BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM International Technical Support Organization
Department 545, Building 657
P.O. BOX 12195
RESEARCH TRIANGLE PARK NC
USA 27709-2195

Fold and Tape **Please do not staple** Fold and Tape

Cut or Fold
Along Line

Printed in U.S.A.

GG24-4337-00