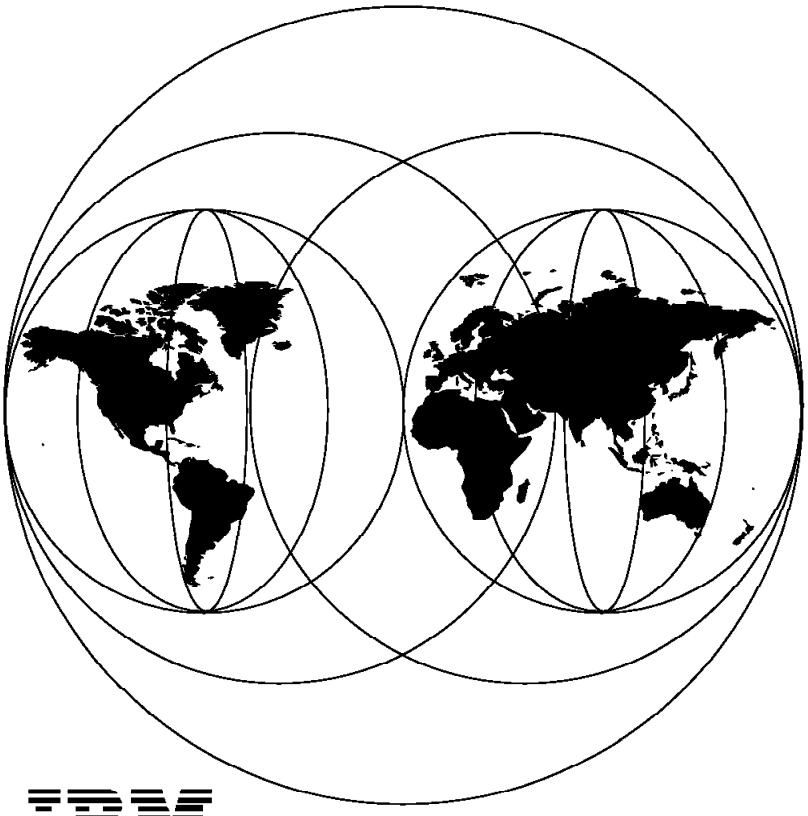
International Technical Support Organization

SG24-4517-00

LAN Management Processes (Alerts/Monitoring) Using NetFinity

December 1995



IBM

International Technical Support Organization
Raleigh Center

International Technical Support Organization

SG24-4517-00

LAN Management Processes (Alerts/Monitoring) Using NetFinity

December 1995

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 1995)

This edition applies to Version 3.0 of NetFinity Manager and NetFinity Services Program Numbers 41H6272 and 41H6273 for use with OS/2 V2.11 and OS/2 V3.0.

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. HZ8 Building 678
P.O. Box 12195
Research Triangle Park, NC 27709-2195

Abstract

This document is unique in its detailed coverage of NetFinity and its interactions with its agents on the OS/2, DOS/Windows and NetWare platforms. In addition, it shows how to exchange information with NetView for AIX and NetView for MVS. It provides information about LAN systems management. It focuses on how to manage and monitor different systems management components and take corrective action when it is needed.

This document was written for technical professionals who have some knowledge of LAN systems management but have not used NetFinity to assist them with it. Some knowledge of systems management is assumed.

(174 pages)

Contents

Figures

Tables

Special Notices

This publication is intended to help technical support personnel implement LAN systems management using NetFinity V3.0. The information in this publication is not intended as the specification of any programming interfaces that are provided by NetFinity. See the PUBLICATIONS section of the IBM Programming Announcement for NetFinity for more information about what publications are considered to be product documentation.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM′s product, program, or service may be used. Any functionally equivalent program that does not infringe any of IBM′s intellectual property rights may be used instead of the IBM product, program or service.

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

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, 500 Columbus Avenue, Thornwood, NY 10594 USA.

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

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

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

AIX	DB2
FFST	IBM
Micro Channel	MVS/ESA
OS/2	PS/2
VTAM	

The following terms are trademarks of other companies:

Windows is a trademark of Microsoft Corporation.

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

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

C-bus is a trademark of Corollary, Inc.

Lotus Notes	Lotus Development Corporation
IPX, NetWare	Novell, Incorporated
NFS	Sun Microsystems, Incorporated
EtherLink/MC, 3Com	3Com Corporation
SCSI	Security Control Systems, Incorporated

Other trademarks are trademarks of their respective companies.

Preface

This document is intended to show how to implement the systems management functions that are part of NetFinity V3.0. This is done by showing examples of how the functions work. It contains examples for multiple platforms as well as interactions with higher level systems managers such as NetView for AIX and NetView for MVS.

This document is intended for use by persons who are involved with distributed systems management using NetFinity.

How This Document is Organized

The document is organized as follows:

- Chapter 1, “Installation and Configuration of NetFinity for OS/2”

  This chapter provides an overview of the book and shows how to install the base product NetFinity.

- Chapter 2, “Alert Management Functions”

  This chapter provides insight into how to set up alert management in a NetFinity environment that includes managers and clients.

- Chapter 3, “Monitoring Functions”

  This chapter provides details on how to use NetFinity services to monitor resources and components of NetFinity.

- Chapter 4, “Remote Management Functions”

  This chapter shows examples of how to set up remote management of NetFinity clients as well as how to set thresholds.

- Chapter 5, “Hardware Manager Functions”

  This chapter provides examples of the hardware monitoring capabilities that are built into NetFinity.

- Chapter 6, “NetFinity and NetView for AIX”

  This chapter describes how to set up the exchanges between NetFinity and NetView for AIX.

- Chapter 7, “NetFinity and NetView for MVS”

  This chapter describes how to set up the exchanges between NetFinity and NetView for MVS.

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 NetFinity Manager for Windows*, S41H-6267-00
- *IBM NetFinity Manager for OS/2*, S41H-6268-00
- *IBM NetFinity Services for Windows*, S41H-6269-00
- *IBM NetFinity Services for OS/2*, S41H-6270-00

- *IBM NetFinity Services for NetWare*, S41H-6271-00

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

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

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

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

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

How to Order ITSO Redbooks

IBM employees in the USA may order ITSO books and CD-ROMs using PUBORDER. Customers in the USA may order by calling 1-800-879-2755 or by faxing 1-800-445-9269. Most major credit cards are accepted. Outside the USA, customers should contact their local IBM office. For guidance on ordering, send a PROFS note to BOOKSHOP at DKIBMVM1 or E-mail to bookshop@dk.ibm.com.

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

ITSO Redbooks on the World Wide Web (WWW)

Internet users may find information about redbooks on the ITSO World Wide Web home page. To access the ITSO Web pages, point your Web browser to the following URL:

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

IBM employees may access LIST3820s of redbooks as well. The internal Redbooks home page may be found at the following URL:

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

Acknowledgments

This project was designed and managed by:

Barry D. Nusbaum
International Technical Support Organization, Raleigh Center

The author of this document is:

Hermann Braun
IBM Germany

Assistance was provided from a residency that ran in parallel from:

Becky Anderson
IBM US

P. Kastrup Ferreira
IBM Brazil

Dirk Oppenkowski
IBM Germany

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

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

Allison Farley, Susan Holahan, Bill Piazza
Gregg Primm, Jeff Cripe, Wade Mahan
IBM PC Company

Chapter 1. Installation and Configuration of NetFinity for OS/2

This chapter describes the installation and configuration of the following components of NetFinityfor OS/2:

- NetFinity Manager for OS/2
- NetFinity for OS/2 Passive Client
- NetFinity for OS/2 Active Client

There is also a NetFinity for Windows Manager and client and a NetFinity for NetWare client.

1.1 Installation and Configuration of NetFinity Manager for OS/2

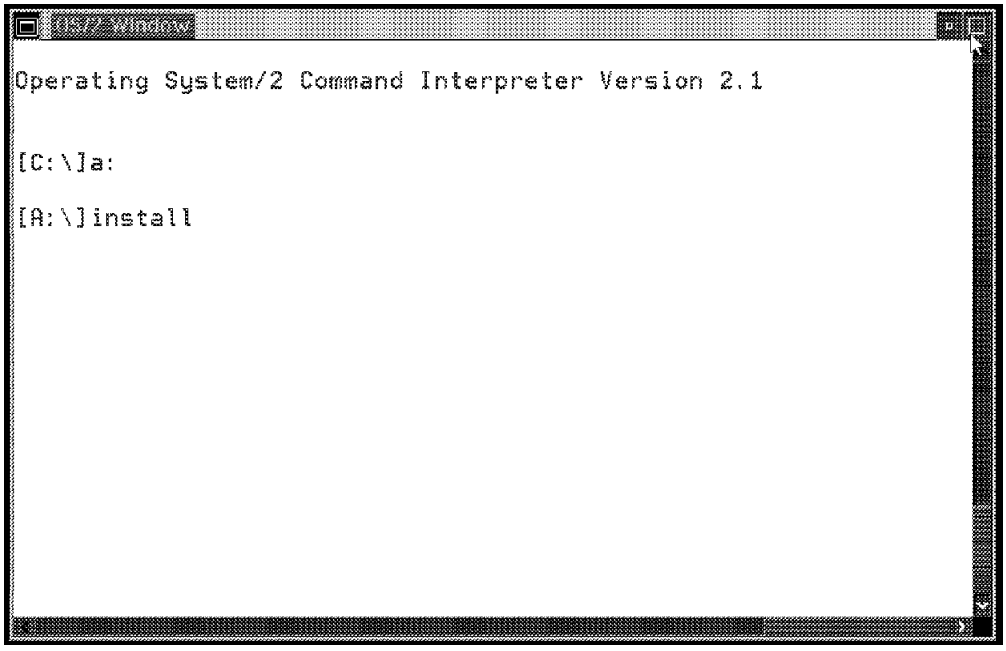


Figure 1. Start the Installation of NetFinity Manager for OS/2 from an OS/2 Window

Figure 1 shows the installation of NetFinity V3.0 from a diskette. We also installed it from a LAN drive and from a CD-ROM.

The levels of OS/2 that we used in this residency were OS/2 Warp Fullpack and OS/2 Warp Connect. To install NetFinity Manager for OS/2:

- Start your OS/2 system and open an OS/2 window.
- Insert the diskette labeled *NetFinity Manager for OS/2 Diskette # 1* into the A drive and enter `A:\INSTALL`.

Note

If you are installing NetFinity Manager for OS/2 on a system on which you previously installed the NetFinity Services for OS2, you must reinstall all of the NetFinity Services. Any previously configured system information (such as network configuration or incoming user ID/password combinations) will remain intact. Close any NetFinity windows that are currently open and shut down all NetFinity programs that might be running, using the command: \NETFBASE SHUTDOWN.

After you enter the A:\INSTALL command, you will see the following window:

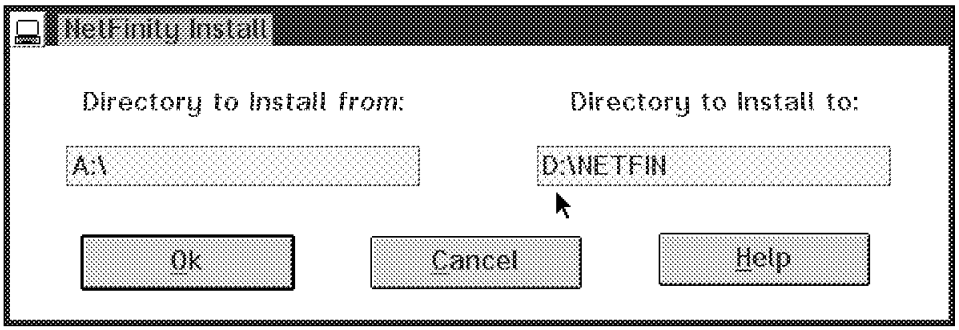


Figure 2. NetFinity Manager for OS/2 Install Window

- Indicate which directory the NetFinity Manager for OS/2 code should be installed in. The default is C:\NETFIN, but we placed the code on another drive.

  The directory it is installed from in this case is the A drive since we are using diskettes.

- Press **OK** to continue with the installation process.

If the directory D:\NETFIN does not already exist, you will get the following pop-up window:

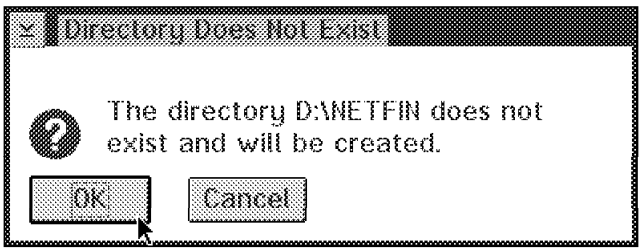


Figure 3. NetFinity Manager for OS/2 Directory Does not Exist

- When you click on the **OK** button, the NetFinity Manager for OS/2 window will pop up.

If the directory already exists, you will get a different pop-up window that will confirm that it's okay to overwrite the contents of the directory.

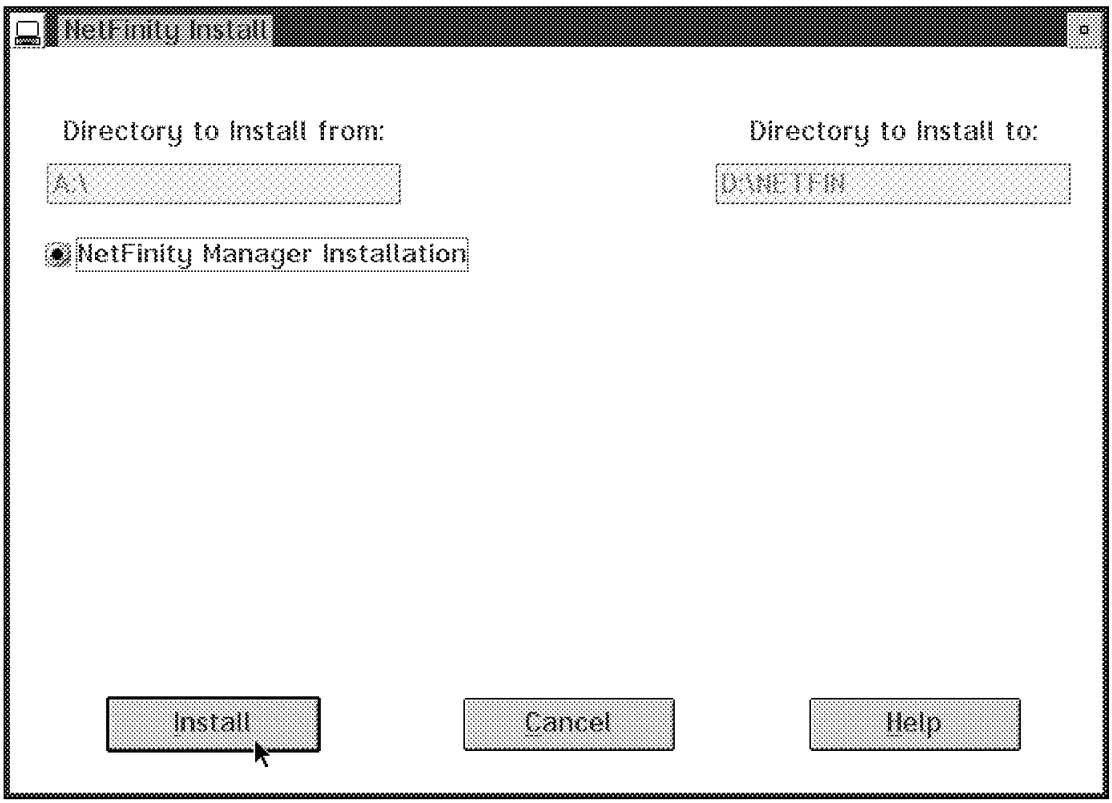


Figure 4. NetFinity Installation Panel

- Click on **Install** to begin the installation of the code.

During the installation, NetFinity indicates how far in the process it has gone towards full installation. Select the **Cancel** button if you want to stop the installation process.

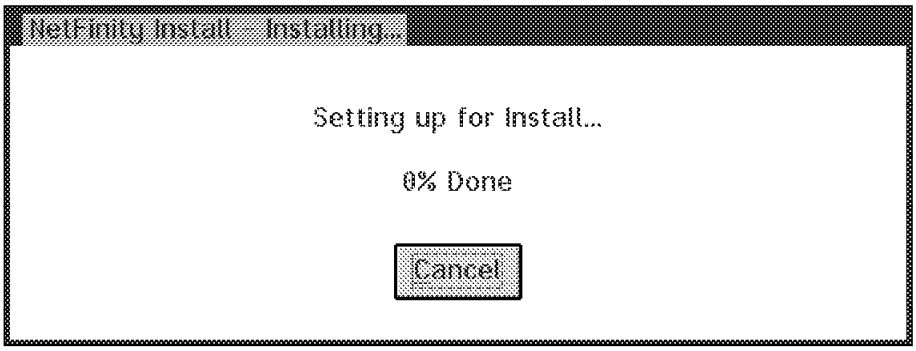


Figure 5. NetFinity Manager for OS/2 Installing Progress Window

You will be prompted for the following diskettes:

- NetFinity Manager for OS2, Diskette #2
- NetFinity Services for OS2, Diskette #1
- NetFinity Services for OS2, Diskette #2
- NetFinity Services for OS2, Diskette #3
- NetFinity Services for OS2, Diskette #4

When the installation process is complete, the Network Driver Configuration window will appear, and will need to be customized.

1.2 NetFinity Manager for OS/2 Configuration

When you set up the Network Driver Configuration panel, you need to think about the importance of a good naming convention. Since you have eight system keywords to choose from you will want to group your users based upon these fields. For example, you might have a keyword called Accounting, or another called TCP/IP. These fields are important when we use the Remote Systems Manager feature of NetFinity to remotely discover and manage clients.

In addition to the naming convention being important in the Network Driver Configuration panel, as shown in Figure 6, you will need to specify the transport protocols that the client can be managed with. During the installation process, NetFinity will detect what is installed on your machine. If you do not have IPX, then it will not end up being a choice on the panel. Therefore, if you add other protocol stacks after the installation, you will need to re-install NetFinity to add the additional protocols. You can select an individual protocol, or all of the protocols. The choices will be from the following:

- NetBIOS
- TCP/IP
- IPX
- Serial NetFinity

The support for a serial connection will show up in all configurations.

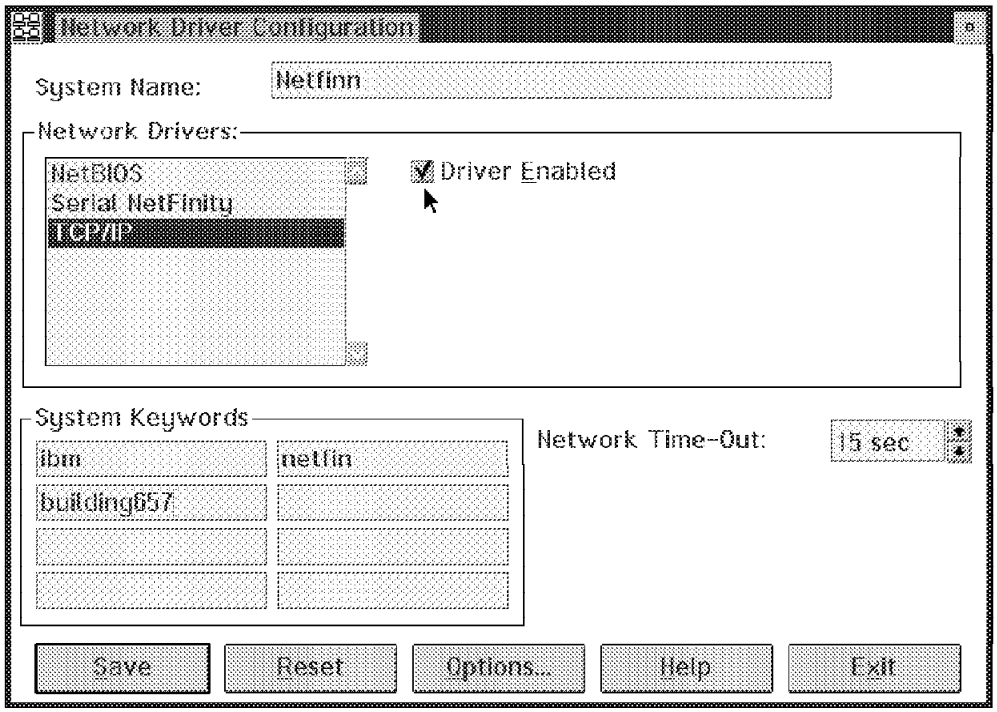


Figure 6. NetFinity Manager for OS/2 Network Driver Configuration Window for TCP/IP

Figure 6 shows the configuration for a system that we have called Netfinn and we have enabled the TCP/IP protocol stack. In addition, you can see that we

have said that this system will be known by several keywords (ibm, netfin and building657), when NetFinity performs its broadcast discovery.

A summary of the fields that you can fill in follows:

- System Name

  This name usually is the same as the NetBIOS or TCP/IP host name, but it is not required to be so. You might select the name based upon some other local naming convention. The name you pick for the system name will be the name that is displayed in the Remote Systems Manager, as well as the title bar of the OS/2 windows that are used for local management of this NetFinity system.

- Select Network Driver

  Select one network driver at a time. Click on the Driver Enabled button to enable that protocol. You can select one or all of the network drivers. When you select a network driver, a network address is assigned to your system. If you are enabling TCP/IP or an IPX Network Driver you cannot alter its name and it will not appear on the screen. The Network address is assigned from your TCP/IP or IPX Configuration. If you are enabling the NetBIOS Network Driver, a default address is either your LAN Requester workstation name or the last eight numbers of your adapter address (MAC Address). It finds your workstation name in your IBMLAN.INI file.

  Figure 7 shows a Network Driver Configuration window with the NetBIOS driver selected and the Network Address field available. This value can be changed. We would also need to click on the Driver Enabled button to enable the NetBIOS protocol.

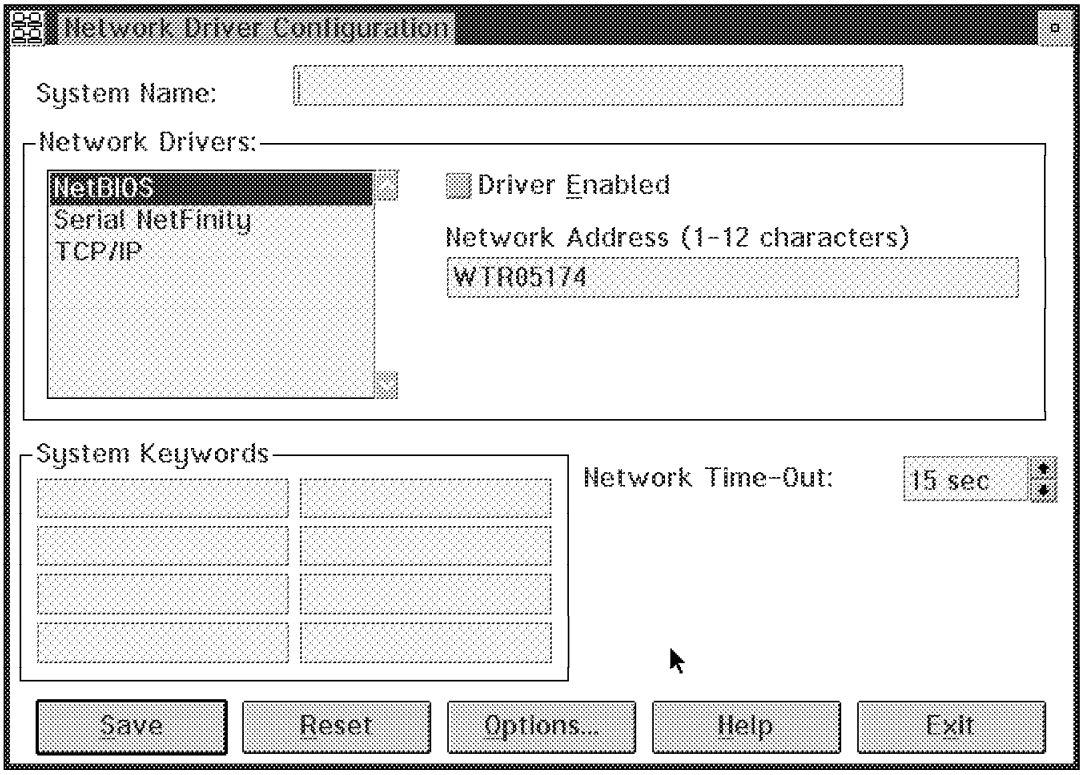


Figure 7. NetFinity Manager for OS/2 Network Driver Configuration for NetBIOS

- Enter one or more keywords to represent this system.

To take advantage of the Remote System Manager′s discovery process, you must identify your system and each of the NetFinity systems that are on your network with descriptive system keywords.

- The Network Time-Out field shows the number of seconds that NetFinity will attempt to communicate with a remote system. If NetFinity does not establish contact with the remote system within this time, it stops trying to connect to the system. The network time-out default is 15 seconds. If you find your connections timing out often, due to heavy traffic, you should increase the value.
- Click on the **Options** button in Figure 7 on page 5 and you will get the following pop-up window:

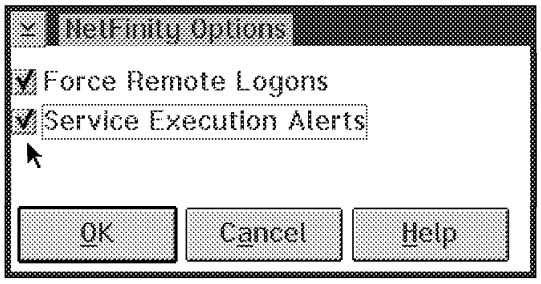


Figure 8. NetFinity Manager for OS/2 NetFinity Options Screen

- **Force Remote Logon** - This option will force you to manually log on each time you want to access a remote system. Your system will not be able to save the user ID/password combination that you use when accessing a remote system.

  Note

  This option is not available from a NetFinity client.

- **Service Execution Alerts** - The NetFinity Service Manager will generate a NetFinity alert whenever one of the NetFinity services is started by a remote user. The alert includes the name of the service that was requested and details about the user that started the service.

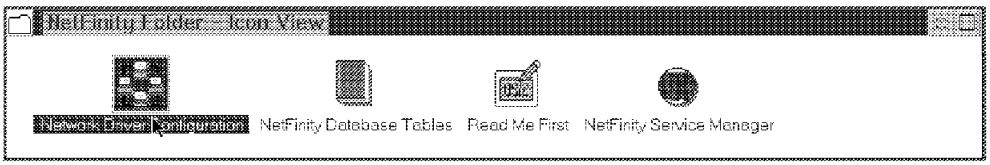
  For example, if a remote user starts your NetFinity Screen View application, which enables the remote NetFinity manager to capture a snapshot of your screen contents, you will get an alert with the system name that started this service. This way you are always aware of who is controlling your system remotely using NetFinity.

- Select **OK** to exit the Option window.

  After you have made those changes, you are back in the Network Driver Configuration window.

- Click on **Save** to save your configuration.
- Select **Exit** to finish up the customization.

All the parameters you just configured can be changed after installation by selecting the **Network Driver Configuration** object from your NetFinity folder on the OS/2 desktop shown below:



Remember to stop and restart NETFBASE.EXE after any changes, otherwise the new configuration will not be active. One way to do this is:

- Enter NETFBASE SHUTDOWN in an OS/2 Window.
- To restart it enter: NETFBASE.

Another way this can be done is to:

- Select **NetFinity Network Interface** or **NetFinity Network Support** from the OS/2 tasklist.
- Click it on with the right mouse button.
- Select **Close** and then **YES**.
- Enter NETFBASE or NETFIN in an OS/2 Window.

If you make any changes to the Network Configuration Driver you will get a pop-up window asking you to confirm your changes. An example of this follows:

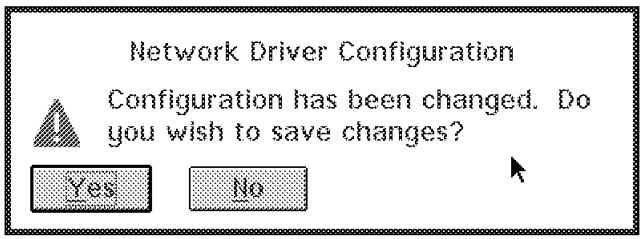


Figure 9. Network Driver Configuration Saved

- Click **Yes** to continue.

  After you have performed all of the installation customization, you will get another pop-up window asking you to confirm all the changes to CONFIG.SYS. The installation program can update it for you. You will need to reboot your system to have these changes take effect.

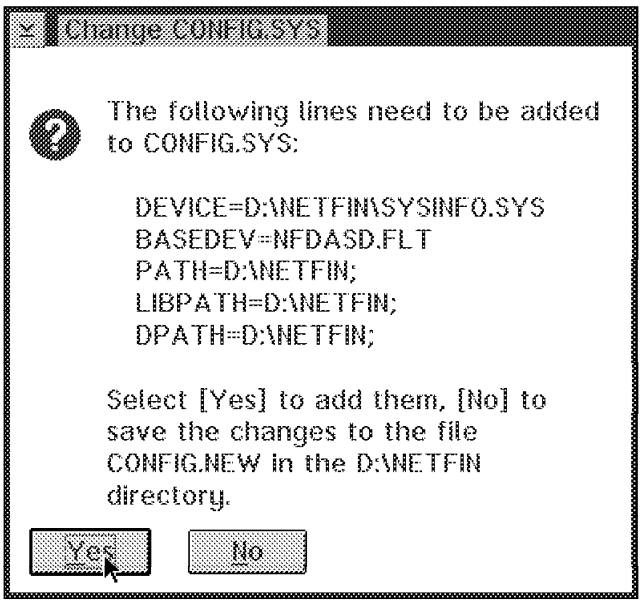


Figure 10. NetFinity Manager for OS/2 Change the CONFIG.SYS Window

- Click on the **Yes** button.

  The next window you get only if C:\CONFIG.RPS already exists.

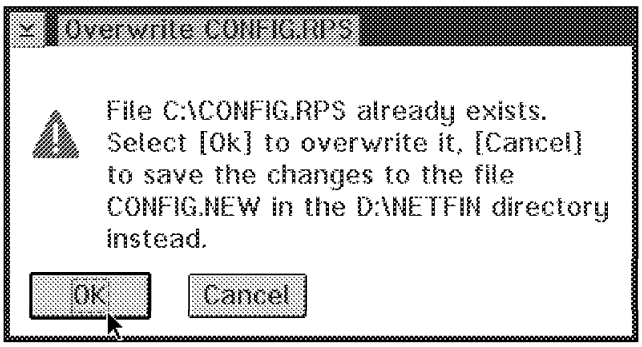


Figure 11. NetFinity Manager for OS/2 Overwrite CONFIG.RPS Window

- Click on **OK** and the last Installation Window appears.

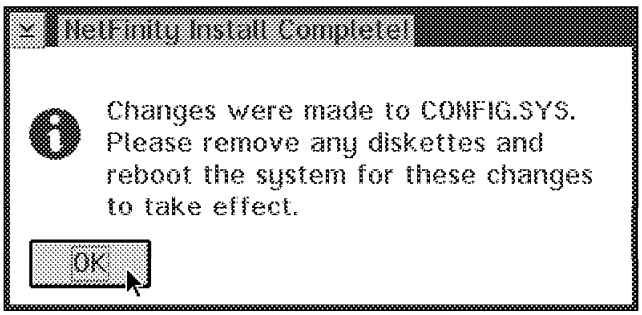


Figure 12. Installation Completed

Your installation is now complete. Make sure you remove the installation diskettes from the diskette drive before you restart your system.

Chapter 2. Alert Management Functions

This chapter describes the management functions that can be performed using NetFinity V3.0 that are related to alerts. These alerts can be issued from any client or manager:

- Alert Manager
- Critical File Monitor
- Event Scheduler

2.1 Alert Manager

Figure 13. Alert Manager View Icon

The *Alert Manager* is an application that allows you to transmit or receive application or user generated alerts. Many different actions can be taken as a result of the alerts, including just logging the alerts to a file. The most powerful feature is the ability to run a command as a result of the alert. In addition to that, the alert manager provides the following options:

- Send the alert as TCP/IP mail
- Send an SNMP alert through TCP/IP to another manager like NetView for AIX
- Send an SNMP reset alert
- Send an alert to an alphanumeric pager
- Activate a numeric pager
- Forward the alert to FFST/2
- Export to a Lotus Notes database
- Export to a DB2 database
- Send E-mail using the Vendor Independent Mail interface
- Clear error condition for sending system
- Set error condition for sending system
- Execute minimized command
- Notify user with a pop-up window
- Forward the alert to another manager
- Add the alert to a log file
- Play a waveform (WAV) file
- Send DMI indication to DMI service layer
- Print the alert

It is possible that not all of the options will show up in your list. For example, if you haven't installed OS/2 multimedia support, you won't have the option to play a waveform file.

You can start the Alert Manager service by double-clicking on it from the NetFinity Service Manager folder which is shown in Figure 14.

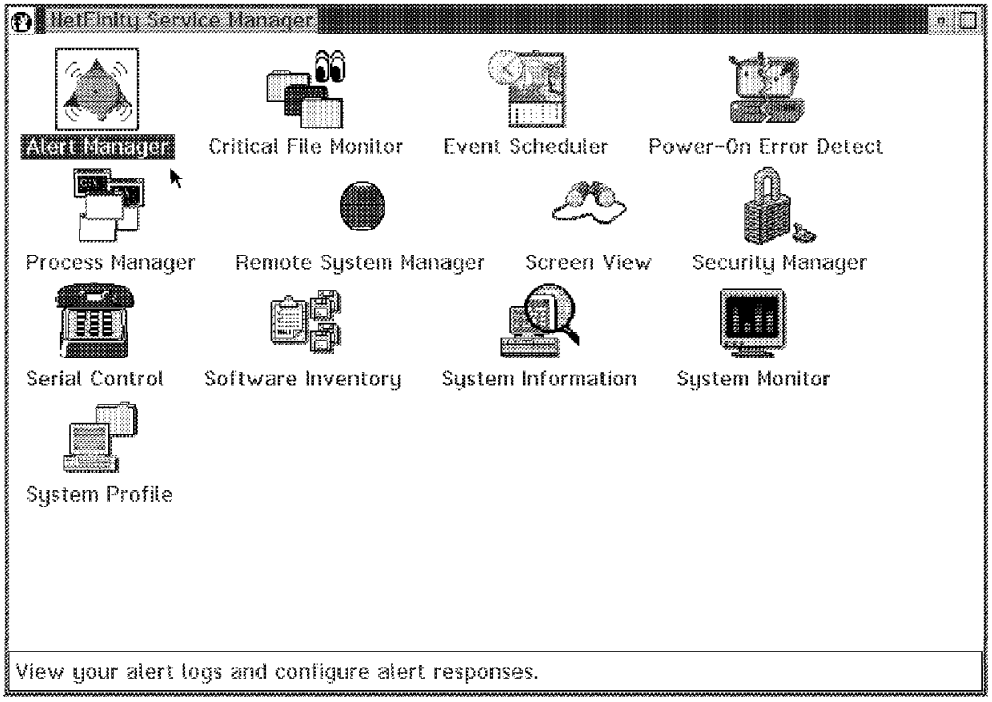


Figure 14. NetFinity Service Manager Folder

- When you double-click on the **Alert Manager** icon the first thing you will see is the Alert Manager Log. This shows you all of the alerts in the log, as well as provides you with an interface to configure the Alert Manager for alerts that will flow to and from this NetFinity Service manager. Most likely, you will not have any alerts in the log until you configure a component to send you one. An easy example to test would be to set the CPU monitor threshold to a low value and cause an alert to be logged. For now, we will take a look at a log that has been in service for awhile and has many alerts in it. Looking at Figure 15 on page 11 we can see that the alert that is highlighted is described in the top half of the Alert Log window. We can see all of the fields broken out (for example, Severity 7).

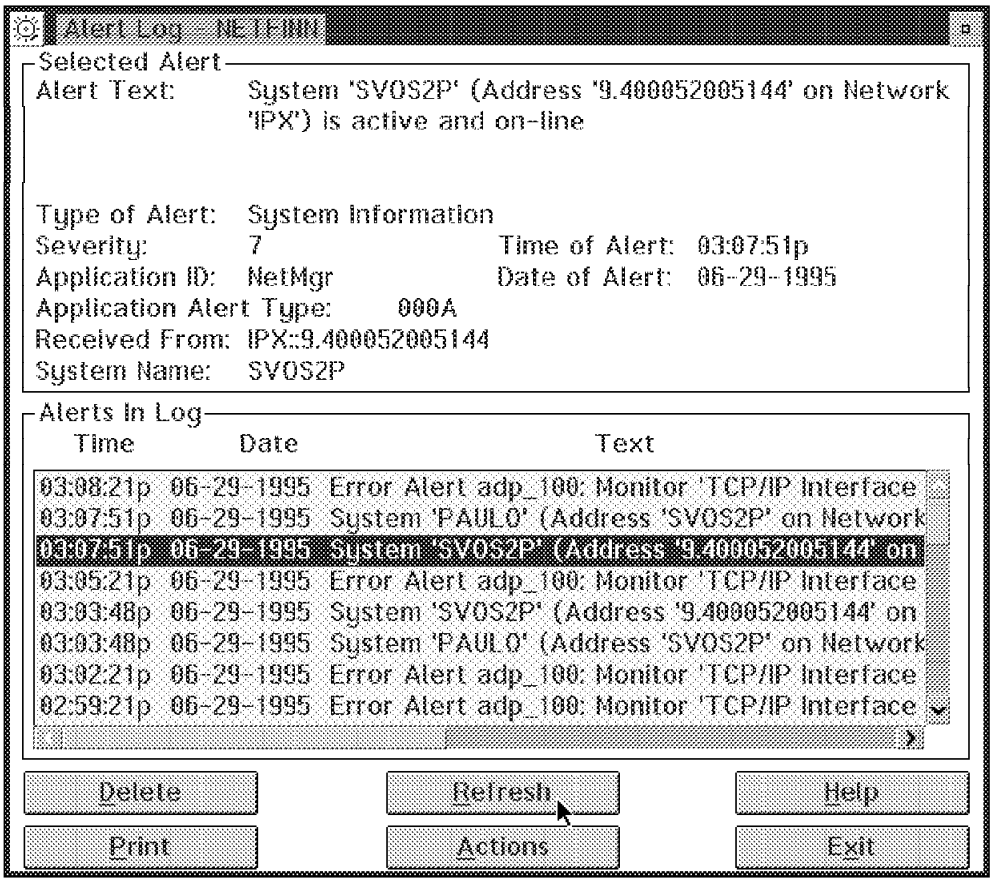


Figure 15. Alert Log Window

- Select the **Refresh** push button to update the alert log since the Alert Manager does not add alerts that it receives while the alert log is being accessed by a user until the Refresh Log button is selected.
- If you want to print or delete multiple alerts at the same time it is possible to do so.

  To select more than one at a time, hold the Ctrl key down and click on the additional alerts you want selected, or if they are next to each other, just drag the mouse down holding the left mouse button down.
- If you click on **Actions** it will bring up a list of already configured actions for alerts to this manager. You can edit these or you can create new actions by clicking on **New** as shown in Figure 16 on page 12.

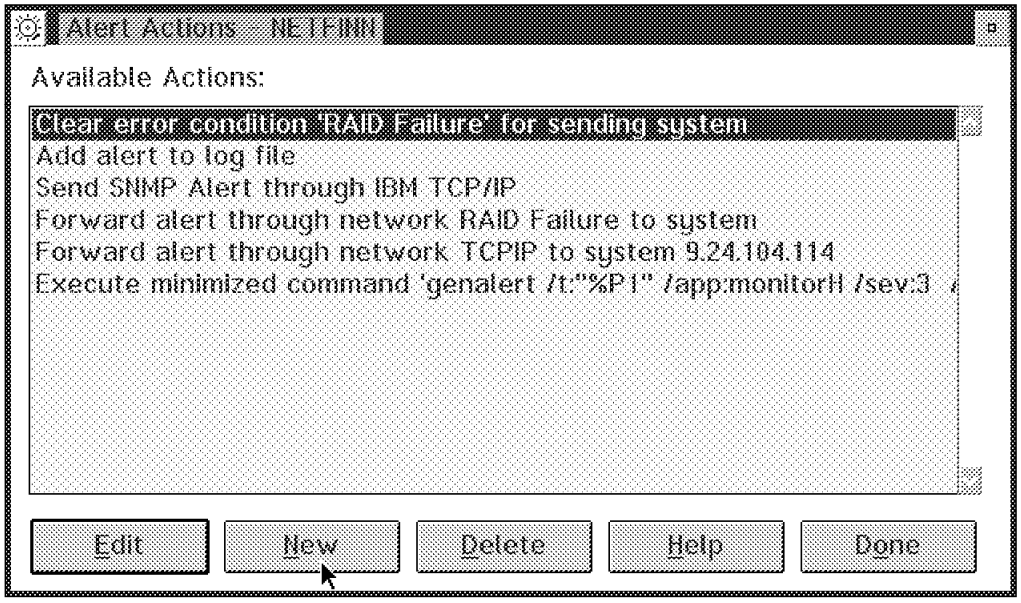


Figure 16. Alert Action Window

- Select the action you wish to edit or delete by highlighting it with the left mouse button or use the up and down arrow keys.
- Select the appropriate action button at the bottom of the Alert Actions window with the mouse, or tab to the button and press Enter.

  Note: Double-clicking on an action in the Available Actions List will move you to the Action Editor. You can also get to the Action Editor if you click on an item and press Enter.

  Reminder

  It is not possible to copy an action or get a comment, so it can be that several actions with the same text appears in the Available Actions list. You cannot differentiate without going into the next window and finding out in detail definitions that are configured differently, so this isn't user friendly.

2.1.1 Alert Manager Configuration

- Double-click on the **New** button to create a new action for use by the Alert Manager.

  The following Action Editor Window will appear.

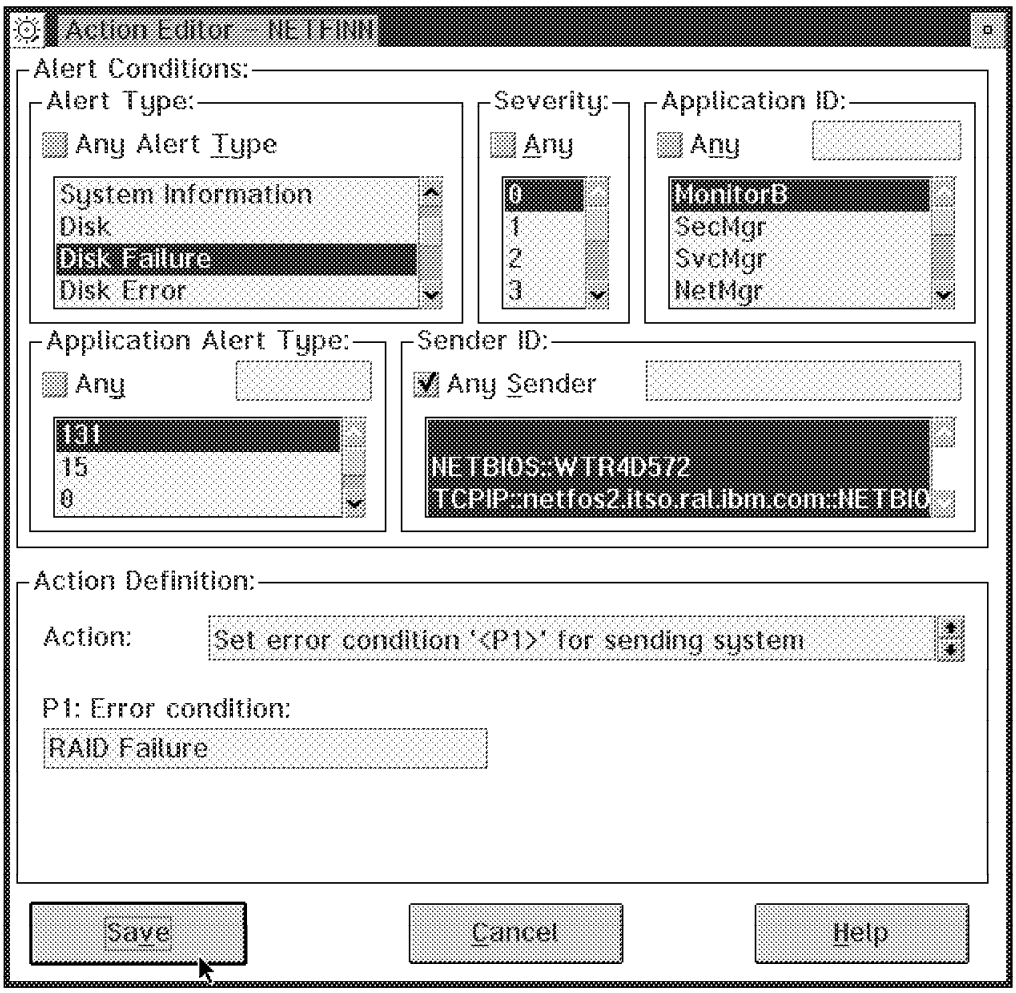


Figure 17. Action Editor Window

The Action Editor enables the user to create and configure actions that the Alert Manager can take in response to specific alerts.

It uses a series of user-defined alert conditions to determine which alerts will trigger a defined action. In order to trigger an action, you should make sure the alert coming in is for the problem that you wish to address. This means you should rarely select a category of Any from Figure 17.

To configure an action:

1. Set the Alert Conditions

   When defining an action, you must first specify the alert conditions that must be met for the Alert Manager to execute a defined action. As alerts are received, the Alert Manager checks each of these conditions to see if they meet the specifications for a defined action. If all alert conditions are met, the defined action is executed. The specific action is in the Action field in the Action Definition part of Figure 17.

   To specify the Alert Conditions:

   – Select an Alert Type.

     If you wish to filter incoming alerts for specific alert types, select one or more alert types from the selection list. If you do not wish to look for specific alert types, select the Any check box in the selection list.

– Select a Severity.

  If you wish to look for incoming alerts for specific severity values, select one or more values from the selection list. If you do not wish to look for specific values, select the Any check box above the selection list.

  The severity is a value from 0 to 7, with 0 being the most severe.

  For example, an alert severity of 0 might be assigned to a disk failure, while a value of 7 might represent a system coming online at the start of a day. Alert severity is determined by the application that generates the alert. The severity helps to determine the actions that the Alert Manager will then take, from advising a user of a disk drive that is nearly full to launching applications to deal with the disk errors.

  By default, alerts with severity values from 0 to 5 will be logged in the alert Log. Alerts with severity values from 0 to 3 will also be displayed in a pop-up window.

  When you are using the Action Editor and defining a new action, the severity field is the only field where the check box isn′t checked off by default. You will always need to specify the severity or it will match the alert when the severity value is between 0 and 3.

– Select an Application ID.

  If you wish to screen incoming alerts for specific application IDs, you may choose one or more from the application ID selection list. If an application ID that you require is not available from the list, you may add it to the list by entering the ID in the entry field above the selection list and pressing enter.

  If you do not wish to look for specific application IDs, select the Any check box.

  The application ID for the alert can be up to eight characters long.

  Following are some NetFinity applications:

  - MonitorB - System Monitor Service
  - SecMgr - Security Manager Service
  - ProcMgr - Process Manager Service

Note

With the GENALERT.EXE command you can also define your own NetFinity alert. But you must use following rules:

GENALERT /T:″text″ < /APP:id_name > < /PRI:<0..7> >
</TYPE:sssttt >
< /ATYPE:hexnum >, where:
/T:″text″ - Defines the text message describing the alert
/APP:id_name - Defines the application ID for the alert (1-8 characters)
/SEV:<0..7> - Defines the severity of the alert (0 = max, 7=min)
/TYPE:sssttt - Defines the standard type of alert. The ′sss′ field describes the ID of the alert:
UNK - Unknown
SYS - System
DSK - Disk or DASD
NET - Network
OS_ - Operating System
APP - Application
DEV - Device
SEC - Security
The ′ttt′ field describes the class of the alert:
UNK - Unknown
FLT - Fault or Failure
ERR - Error
WRN - Warning
INF - Information
/ATYPE:hexnum - Defines the application-specific alert type as a hexadecimal value between 0000 and FFFF.

– Select an Application Alert Type

  If you wish to screen incoming alerts for specific application alert types, you may choose one or more from the Application Alert Type selection list. If an application alert type that you require is not available from the list, you may add it to the list by entering it in the entry field above the selection list and pressing Enter. If you do not wish to look for specific application alert types, select the Any check box above the selection list.

– Select a Sender ID

  If you wish to filter incoming alerts for specific sender IDs, you may choose one or more from the Sender ID selection list. If a sender ID that you require is not available from the list, you may add it to the list by entering it in the entry field above the selection list and pressing enter.

  If you do not wish to look for specific sender IDs, select the Any check box above the selection list.

2. Set an Action Definition

   Based upon the action that you want to take, you will need to specify an action and possibly some additional information.

– Select an Action

  Use the spin buttons at the right of the Action field to see the available actions. Some actions will require that you enter additional information in an Action Definition Parameter field.

– Enter additional information, if necessary

  If additional information is required, the parameter will be displayed in the Action field as <P#>, where # is the number of the parameter. An Action Definition Parameter field will appear for each required parameter, along with a brief description of the information that is required. Enter the appropriate information in each field.

  When you have updated all of the fields:

– Click on the **Save** button to save the actions and parameters you just configured

  This action will now appear in the Available Actions window of the Alert Actions window.

  The following confirmation window will also appear:

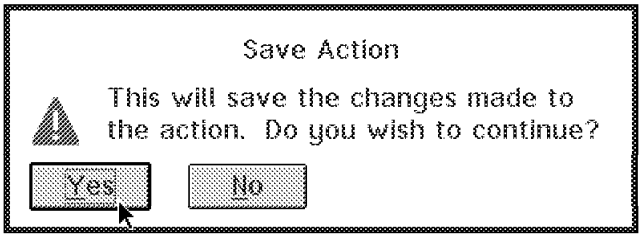


Figure 18. Save Action Window

– Click on **Yes** and the Alert Action window pops up showing the Action item you just saved

  At this point in time, if the alert flows to this manager and the conditions you specified for the alert are met, then the action you defined for the alert will be taken.

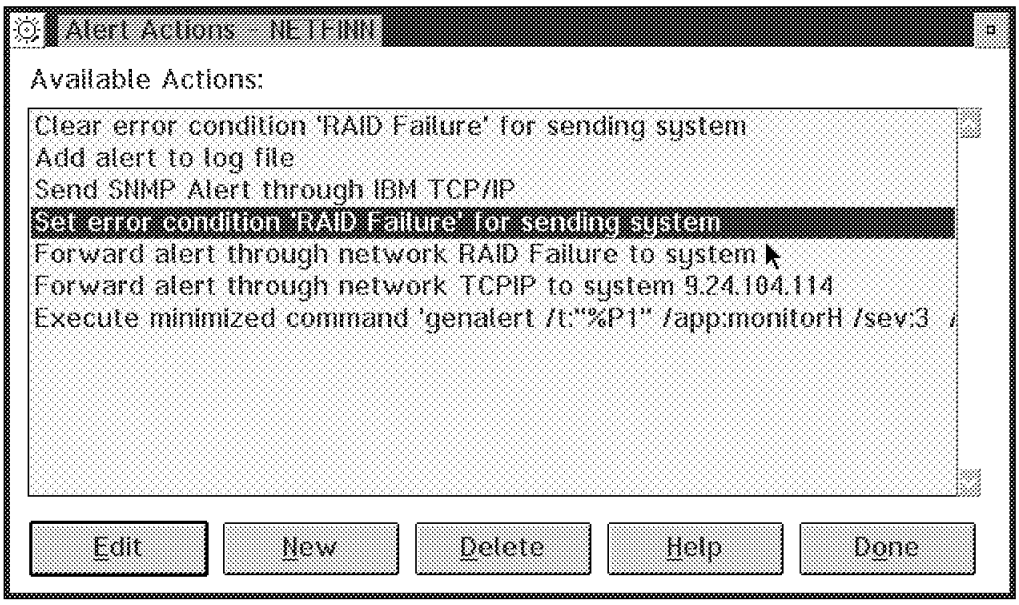


Figure 19. Alert Action Window

- Click on **Done** and the Alert Log: window will appear
- Click on **Exit** and you are done with the Alert Manager for now

2.2 Critical File Monitor

Figure 20. Critical File Monitor Icon

The NetFinity *Critical File Monitor* service can be used to monitor system files or any other user defined files. For example, critical user application files residing on a NetFinity system might be monitored, or files containing payroll information. When the Critical File Monitor is configured to monitor files, and one of those files are changed in some way, NetFinity will generate an alert that will be sent to the Alert Manager. At that point the Alert Manager can take a predefined action. Examples of this might be to:

- Notify a supervisor.
- Set up an automated process to replace the file that was just monitored.
- FTP a new CONFIG.SYS to that machine to disable it and shut it down until someone can check it out.
- Pop up a window on the remote machine warning them that they shouldn't have made that change.
- Log the incident in a file.

The alert condition is met when the date or time the file was originally saved gets altered. If the size of the file changes, this will cause an alert to flow. In addition, if the file gets created or deleted it will cause an alert to flow.

The Critical File Monitor service object is in the NetFinity Service Manager folder.

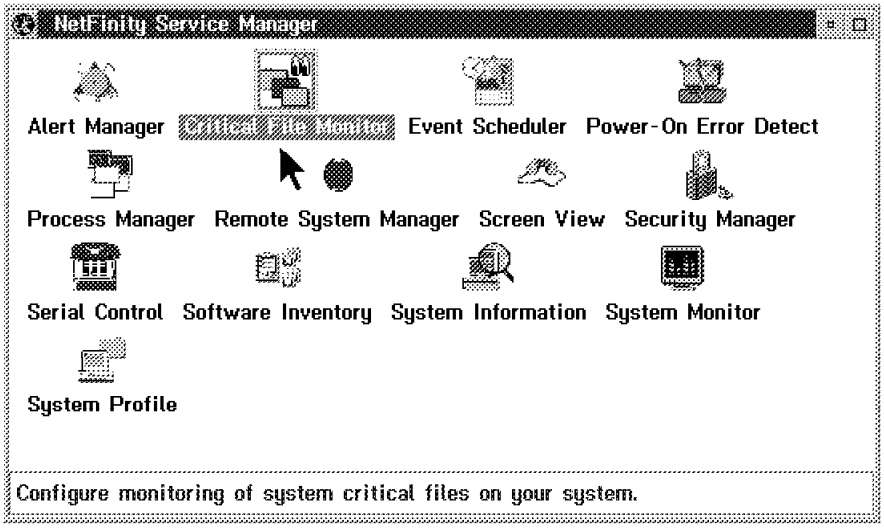


Figure 21. NetFinityService Manager Folder

- To start the Critical File Monitor, double-click on the **Critical File Monitor** object in the NetFinity Service Manager folder.

  This will cause the following window to appear:

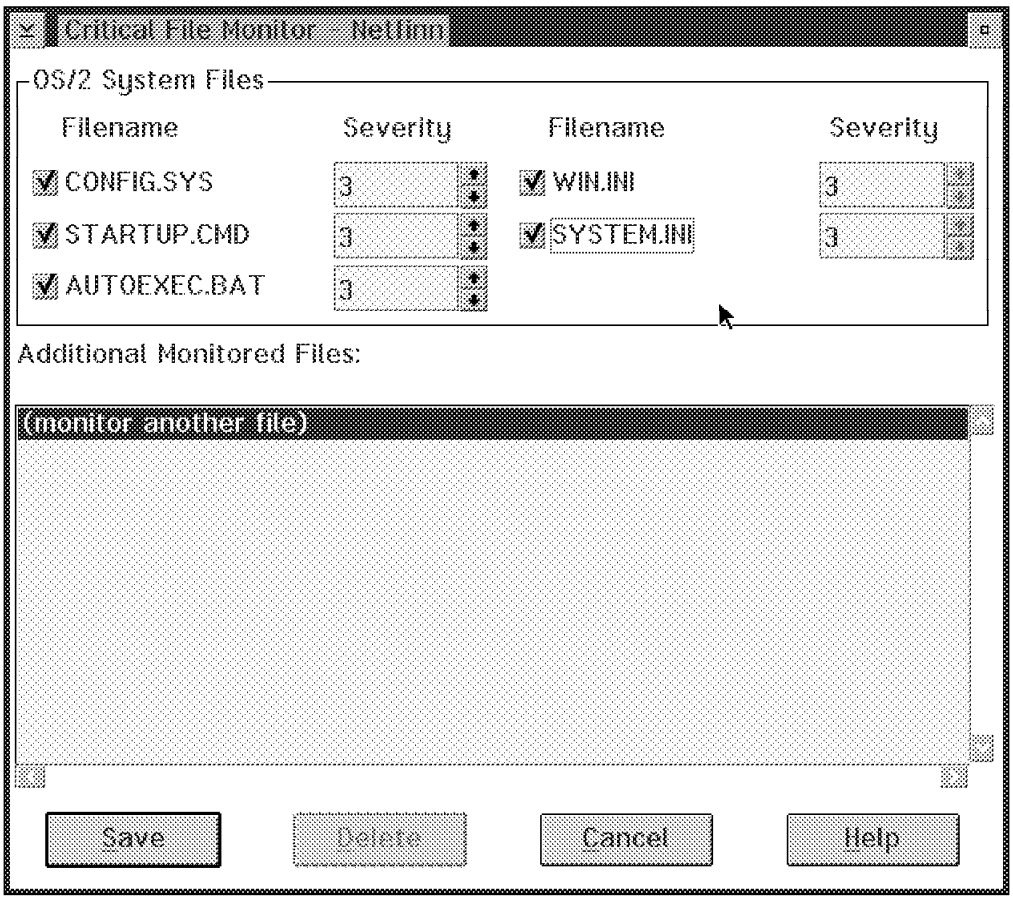


Figure 22. Critical File Monitor Window for OS/2

If you are running the Critical File Monitor on an OS/2 system you will see certain files always show up in the OS/2 system files list. You can add any other files to the list. They can be on FAT or HPFS or LAN drives. You will notice that the name of the system you are configuring the Critical File Monitor for appears in the title bar that you are working on. For systems that are running OS/2, the following files automatically appear in the list, and are enabled if you click in the check box to the left of the file name:

- CONFIG.SYS
- STARTUP.CMD
- AUTOEXEC.BAT
- WIN.INI
- SYSTEM.INI

  If you are using the Critical File Monitor on a Windows Manager or client, you will see the following window:

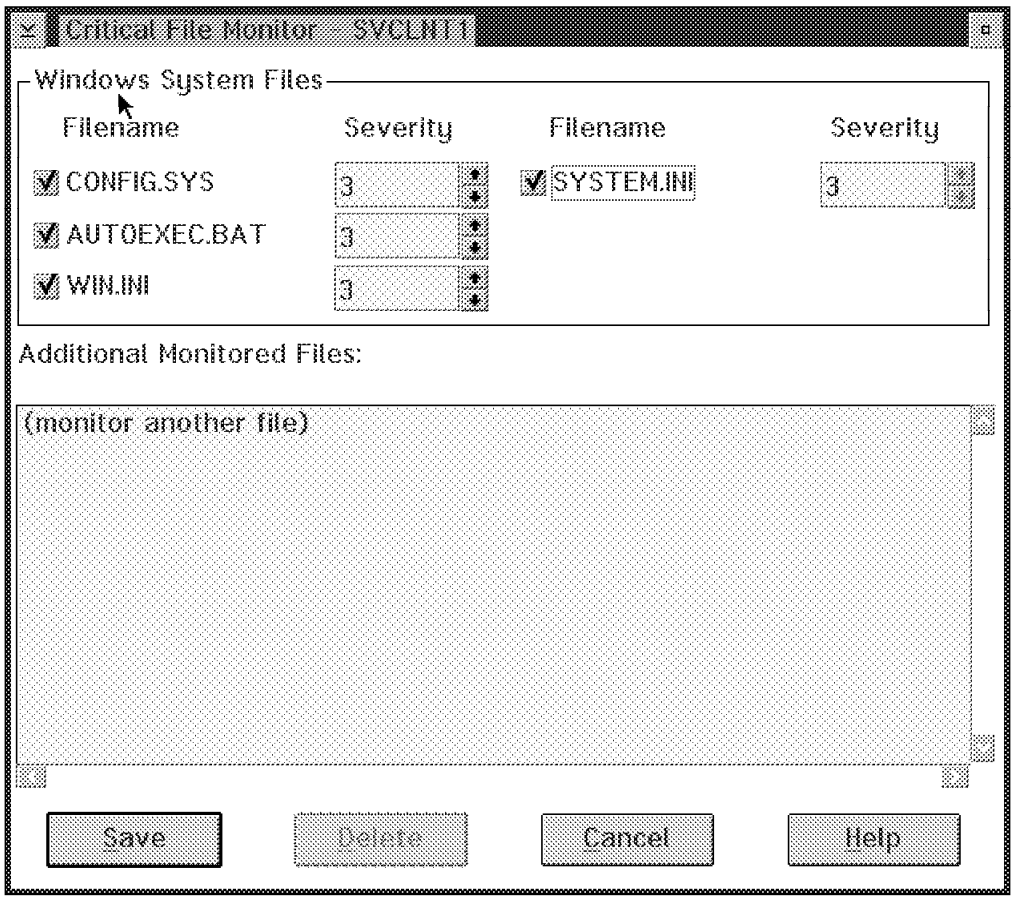


Figure 23. Critical File Monitor Window for DOS/Windows 3.1

As in the OS/2 window, the below files are always in the list but you can add as many other files to be monitored as you would like.

- CONFIG.SYS
- STARTUP.CMD
- AUTOEXEC.BAT
- WIN.INI
- SYSTEM.INI

If you are using the Critical File Monitor on a NetWare server, you will see the following window:

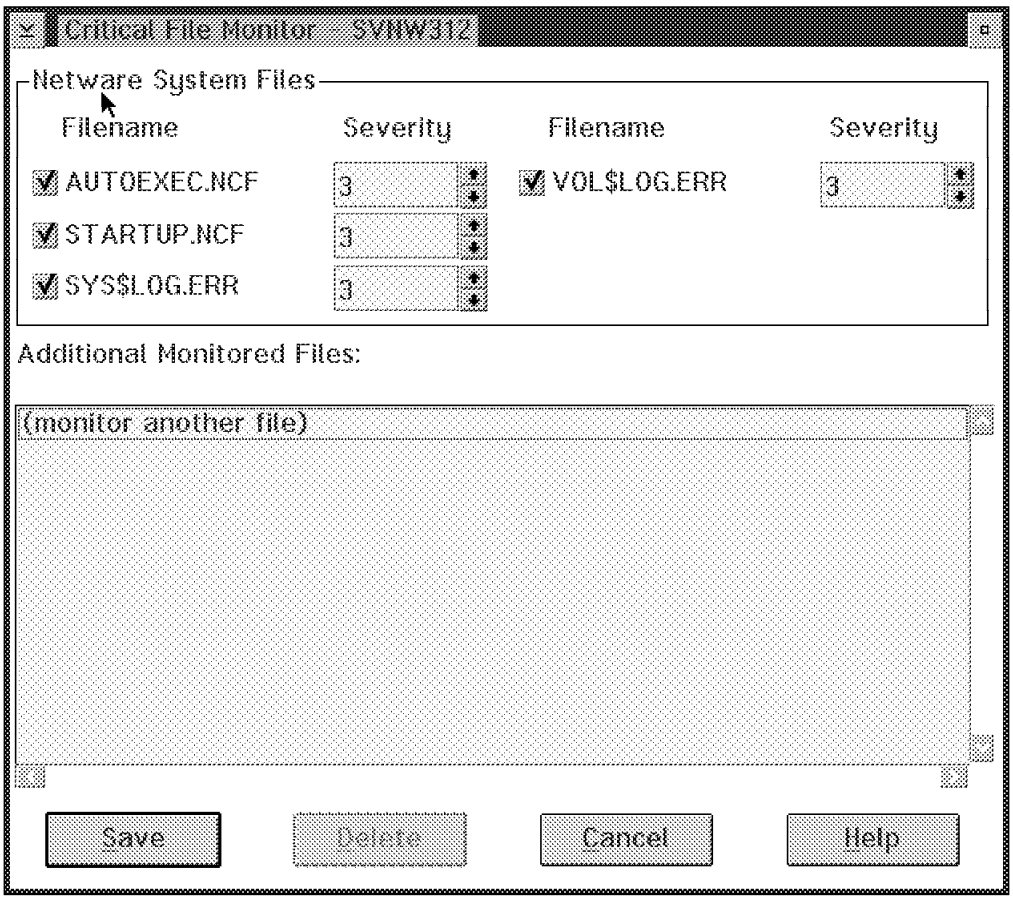


Figure 24. Critical File Monitor Window for NetWare

For systems running NetWare the following files are in the system list:

- AUTOEXEC.NCF
- STARTUP.NCF
- VOL$LOG.ERR
- SYS$LOG.ERR

2.2.1 Monitoring Files

The following is an example of how to set up the Critical File Monitor to monitor an OS/2 file that is a user file. In Figure 22 on page 19 we double-clicked on the field monitor another file. Figure 25 on page 22 appeared and we scrolled down the file list until we came to STARTCM.CMD. We selected this file and left the Alert Severity field at its default value of 3. The we clicked on the **Monitor** option.

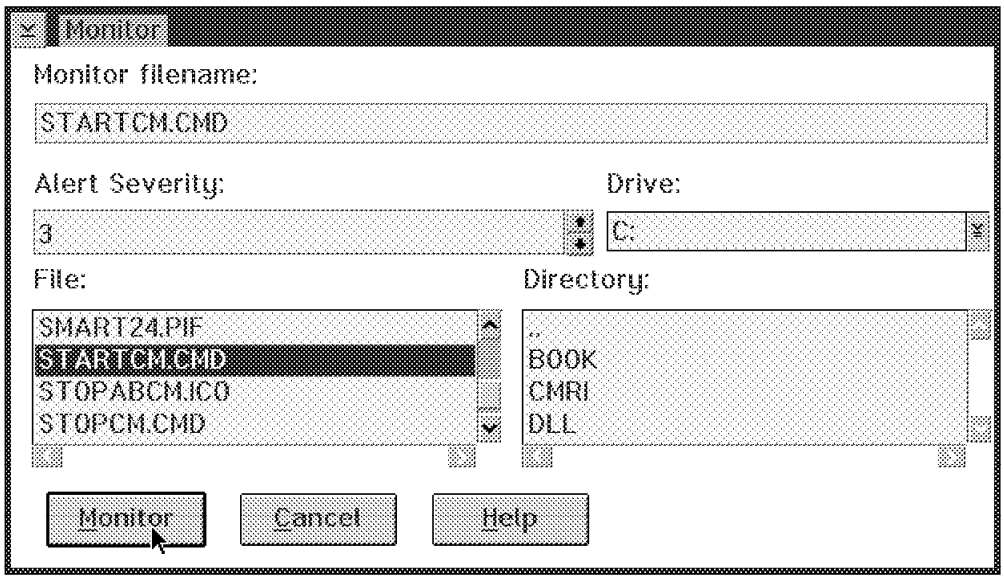


Figure 25. Monitor Screen

There is a predefined interval of time when NetFinity checks to see whether a file has been altered. This is not a file you can customize. When the file change was detected, we configured an alert to pop up on the screen similar to the following:

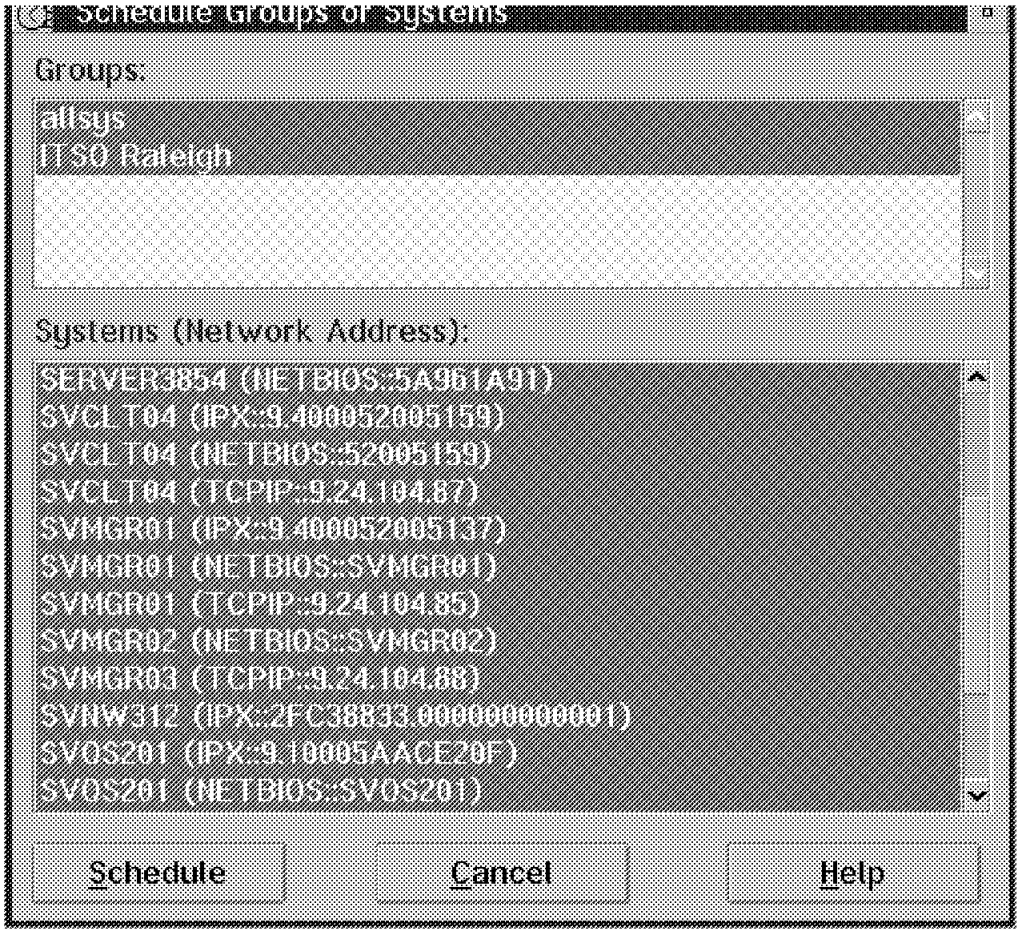


Figure 26. Alert When Critical File Monitor Detected a Change

Notice that the Application ID is MonCritF, the Severity field has a value of 3, and the Application Alert Type is 0000. They are all fields that you can customize in the Alert Manager.

You can add additional files to be monitored at any point in time, or remove files from the list.

Note

There is no check box for a local notify or a general notify option when configuring the NetFinity alert. This means that when you use the Critical File Monitor function on a remote machine using the Remote System Manager, both the local system and the remote system will receive a copy of the alert. This is important if you are going to run any commands (automation).

2.3 Event Scheduler

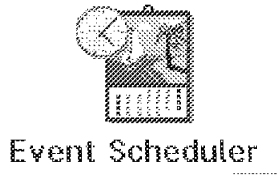


Figure 27. Event Scheduler Icon

The Event Scheduler service enables you to easily automate many hardware systems management tasks. You can use the Event Scheduler to schedule specific actions and execute these events automatically on a local or remote system. You can also schedule the events to execute against a group of systems that have been defined in the Remote Systems Manager. A log will be maintained showing the results of the scheduled events. You can also update or delete scheduled events.

The Event Scheduler Object is in the NetFinity Service Manager folder shown below:

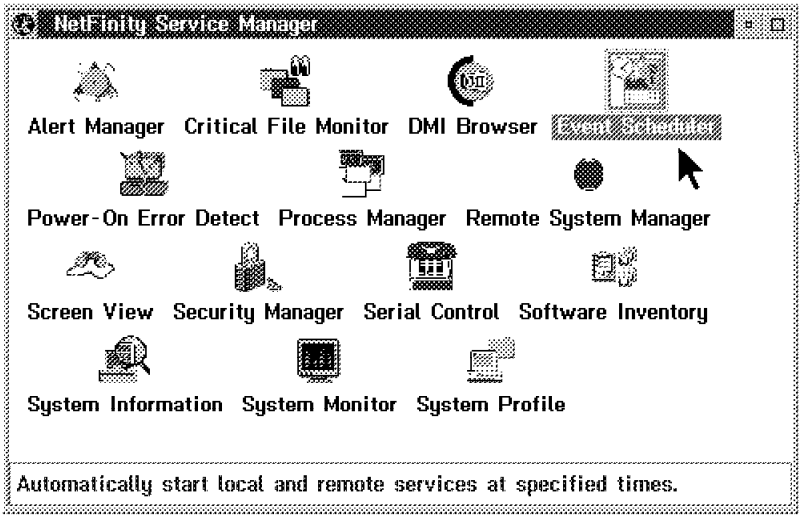


Figure 28. NetFinity Service Manager Folder

- Double-click on the **Scheduler Event** icon and the following window will appear.

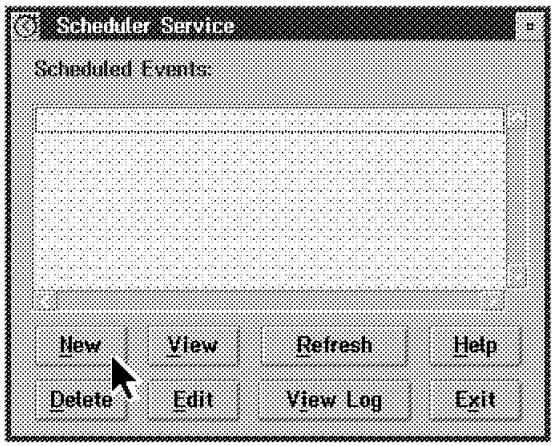


Figure 29. Scheduler Service Window

To create a new event:

- Select **New** to open the Schedule New Event window.

Figure 30. Scheduler New Event

- Enter a **New Event Name** (Here: DBEXP_SYS Group ITSO Raleigh).
- Select the action to be performed from the Tasks selection list.

2.3.1 Event Scheduler Task Configuration

2.3.1.1 System Information Export to a DB/2 Database

- We clicked on the **System Information Tool** to schedule this to be automatically run. We will gather the information from several systems and then export that information to a DB2 /2 database. After selecting the task you will need to specify which system or systems you wish to run this task for.
- Select **Groups** to perform the selected task on all of the system groups.

In this example we highlighted both the allsys and the ITSO Raleigh groups. All of the systems in these groups show up in the Systems list.

If you want to select a single system you must select Systems to perform the selected task on individual systems.

Selecting either of these buttons opens the Schedule Groups or Systems window.

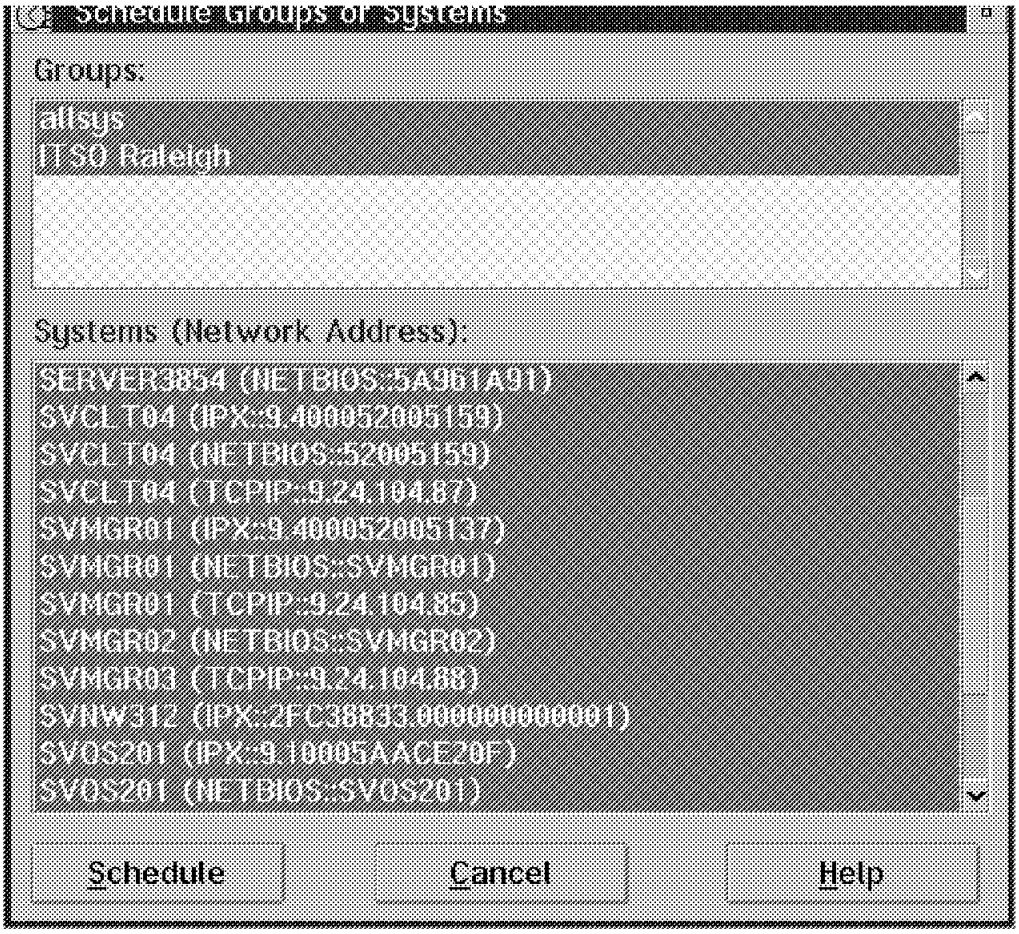


Figure 31. Scheduler Groups or Systems

- Select the system groups or systems on which the scheduled event will be performed.

  We selected both of the groups in the list.

- Then, select **Schedule** to save this information and open the task-specific window.

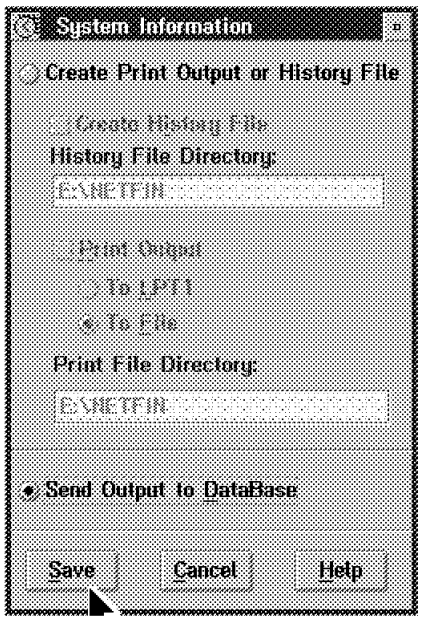


Figure 32. Scheduler Event: System Information Window

- Enter any information required by the specific task that will be performed by the scheduled event. We clicked on **Send Output to Database**.
- Then, select **Save**. In this example the Database Entry Selection window appears. Since we had Lotus Notes and DB2 installed on this system, it came up with options to write to either.

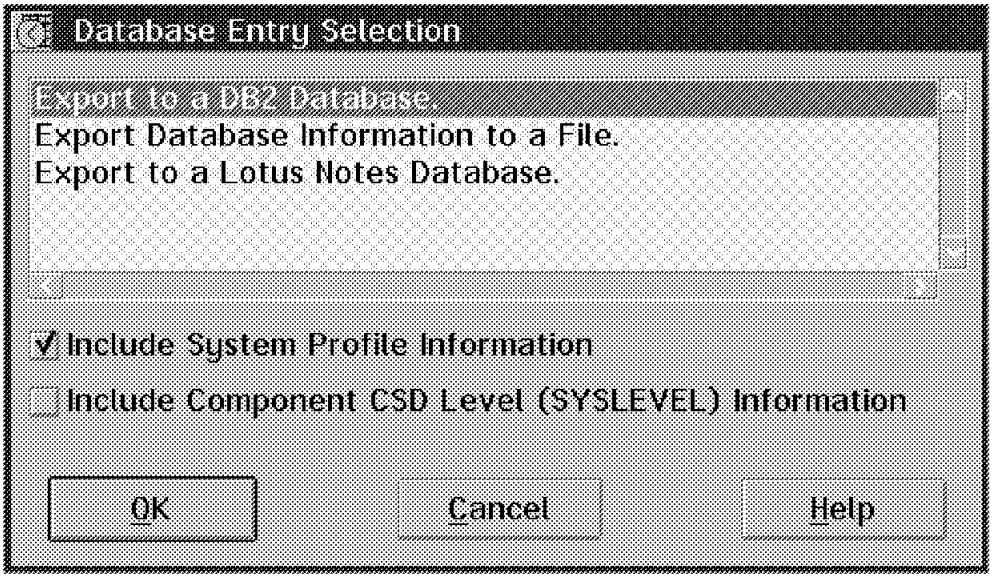


Figure 33. Database Entry Selection Window

- You can choose to include System Profile Information and/or the CSD Level in the DB2 or Lotus databases.

Note

The option to export to a DB2 database only appears if a NetFinity database was successfully installed earlier.

- Select **Export to a DB2 Database**.
- Click on **OK** and the Database Selection window appears.

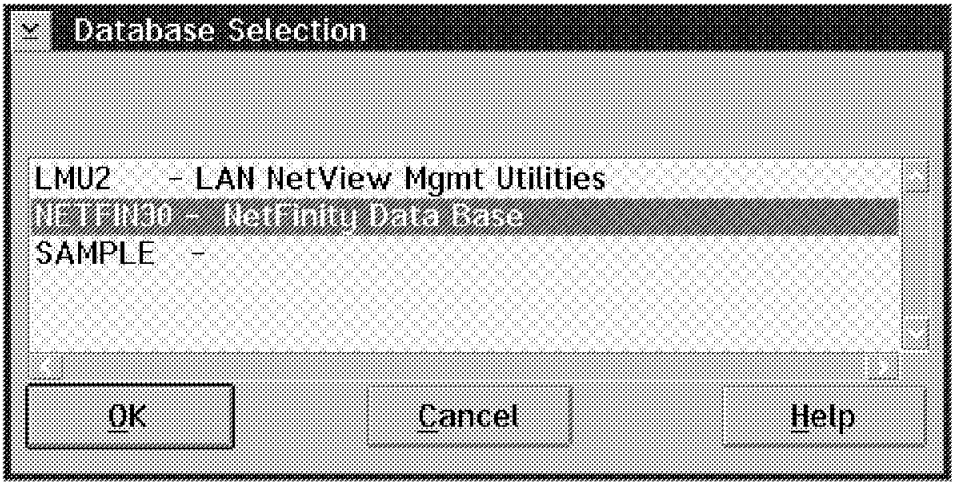


Figure 34. Database Selection Window

- The Database Selection screen lists all of the DB2 /2 databases.
- We chose to write to the NETFIN30 database.
- Click on **OK** and the Schedule Time and Date window appears.

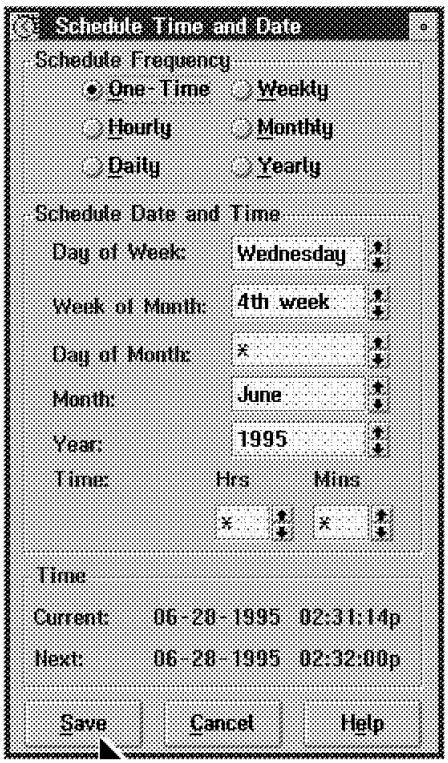


Figure 35. Schedule Time Date for the Database Export

You can specify that this only gets executed once, or you can ask that it gets scheduled on a regular basis. You should note that if you are going to run it only once, the Current time and the Next time fields are only a minute (or less) apart. This means that you have to click on the Save button right away, or change the time you wish to execute the task. In terms of how often it can be executed, you have a choice of any of the following:

- One time
- Hourly
- Daily
- Weekly
- Monthly
- Yearly

The Schedule Date and Time field group contains fields that enable you to set date and time-specific information that, when combined with your selected Schedule Frequency, will determine the dates and times at which the scheduled event will be executed. The fields that are active depends on which Schedule Frequency you selected. Each field features a wildcard value (a "*"). If you select this value, the Schedule Date and Time information is created for you based on the current date and time.

Note

If you alter the Schedule Date and Time values, the Next value at the bottom alters as well. That is useful if you are going to run the task again.

After you finished the Schedule Time and Date configuration:

- Select **Save** to save the scheduled event. You are then back at the Scheduler Service window.

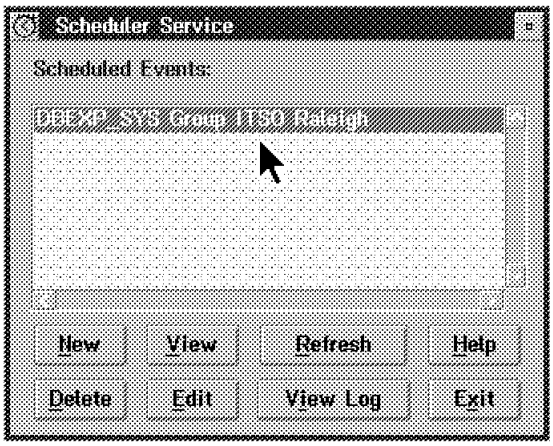


Figure 36. Scheduler Service Window

After the task is performed you can check if the task was completed successfully.

- Click on **View Log** and the following window appears:

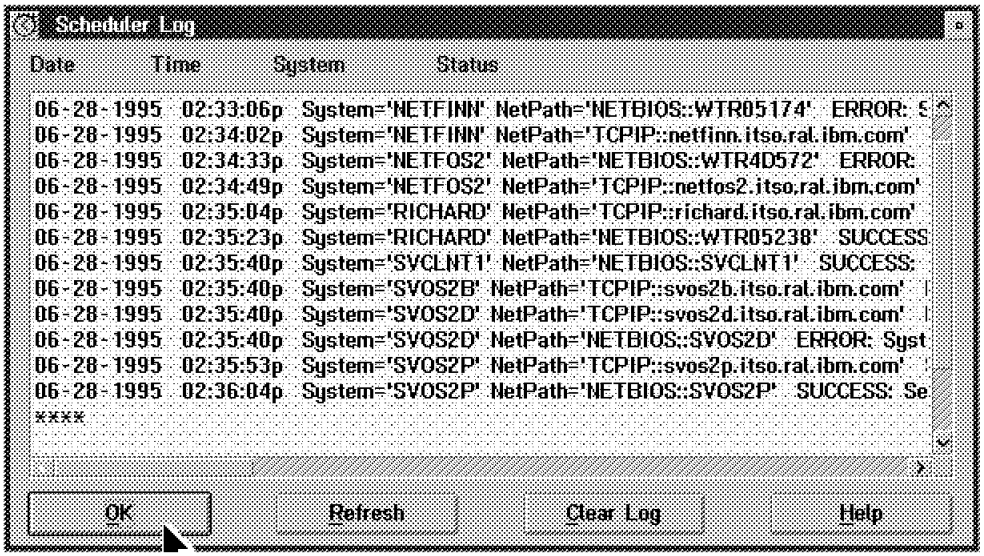


Figure 37. Scheduler Log Window

- Scroll the window to the right that you can see the feedback messages.

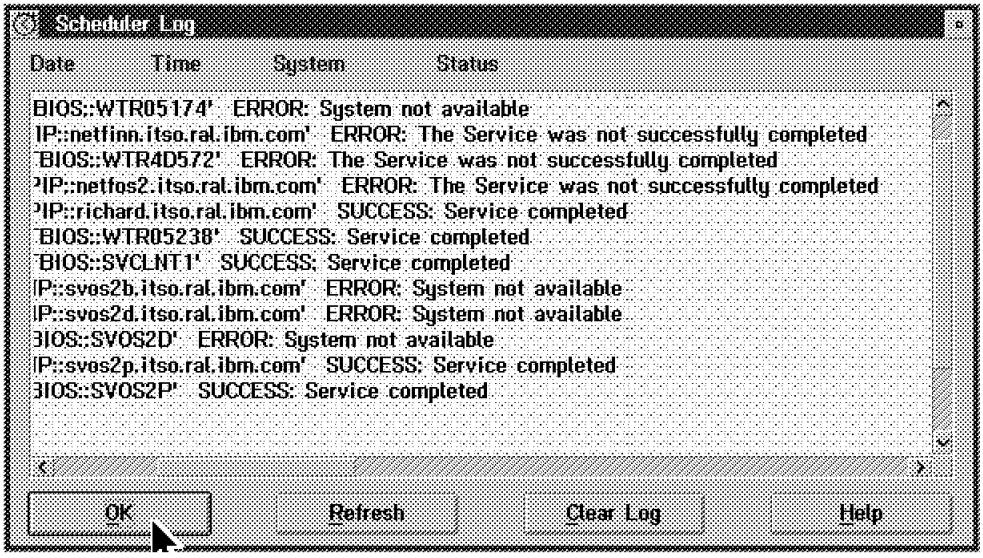


Figure 38. Scheduler Service Window

- Click on **OK**, to go back to the Scheduler Service window.

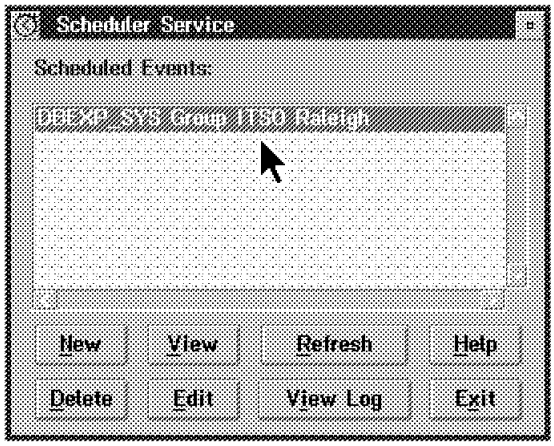


Figure 39. Scheduler Service Window

- If the task was not completed successfully or if you want to run the task for other systems:
- Click on **Edit** and the following window appears:

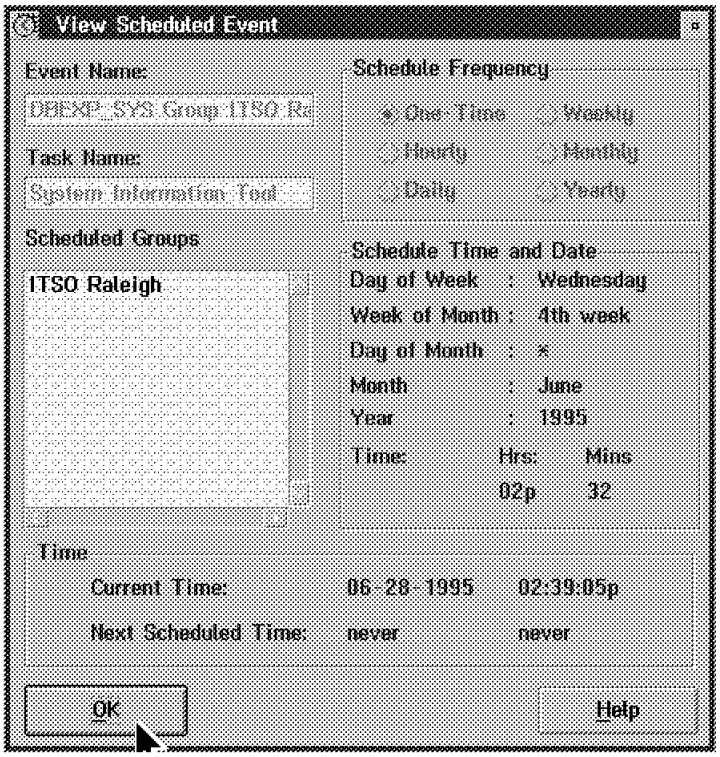


Figure 40. View Scheduled Event Window

Chapter 3. Monitoring Functions

This chapter describes the NetFinity services that can be performed from NetFinity managers and clients, using NetFinity V3.0. The clients can be OS/2, DOS/Windows, or NetWare. The services are:

- Process Manager
- System Monitor

3.1 Process Manager

Figure 41. Process Manager Icon

You can use the NetFinity Process Manager service to view detailed information about all processes that are currently active on a local or a remote system. Process Manager enables you to execute commands on the system and to close individual processes by initiating a Ctrl-C, Ctrl-Break, or Kill Process command. Finally, Process Manager will monitor any process that you have specified and can generate a NetFinity Process Alert if it is started, stops, or fails to start within a specified amount of time from startup. You can then define actions through the Alert Manager service that could automatically execute when these alerts are generated. This feature ensures that your environment is running exactly the programs it should be. This is very important on server machines, especially when they run unattended.

3.1.1 Local Configuration of the Process Manager

The Process Manager object is in the NetFinity Service Manager folder.

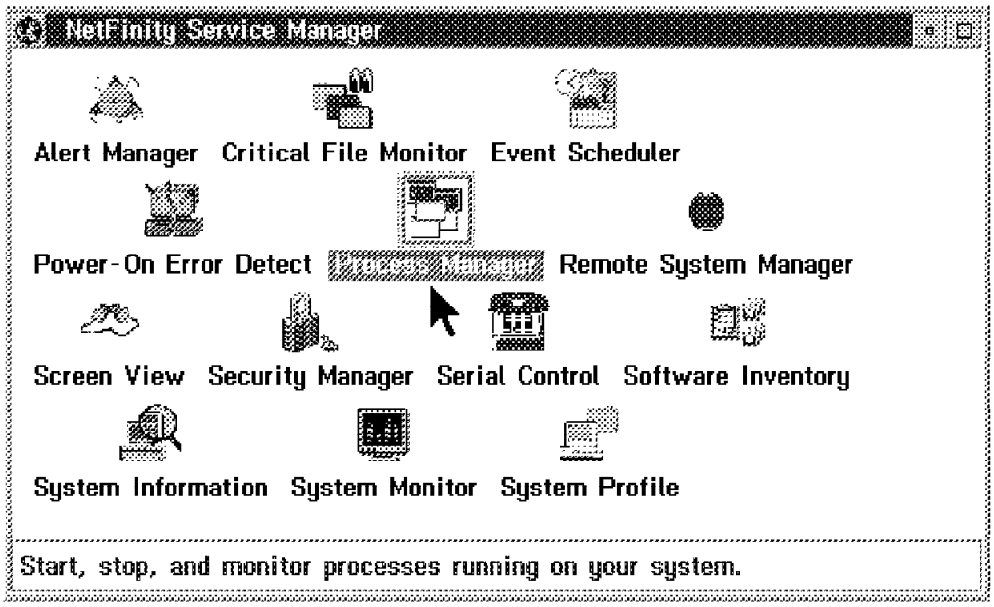


Figure 42. NetFinity Service Manager Folder

- Double-click on the **Process Manager** object in the NetFinity Service Manager folder, and the following NetFinity Process Manager window appears.

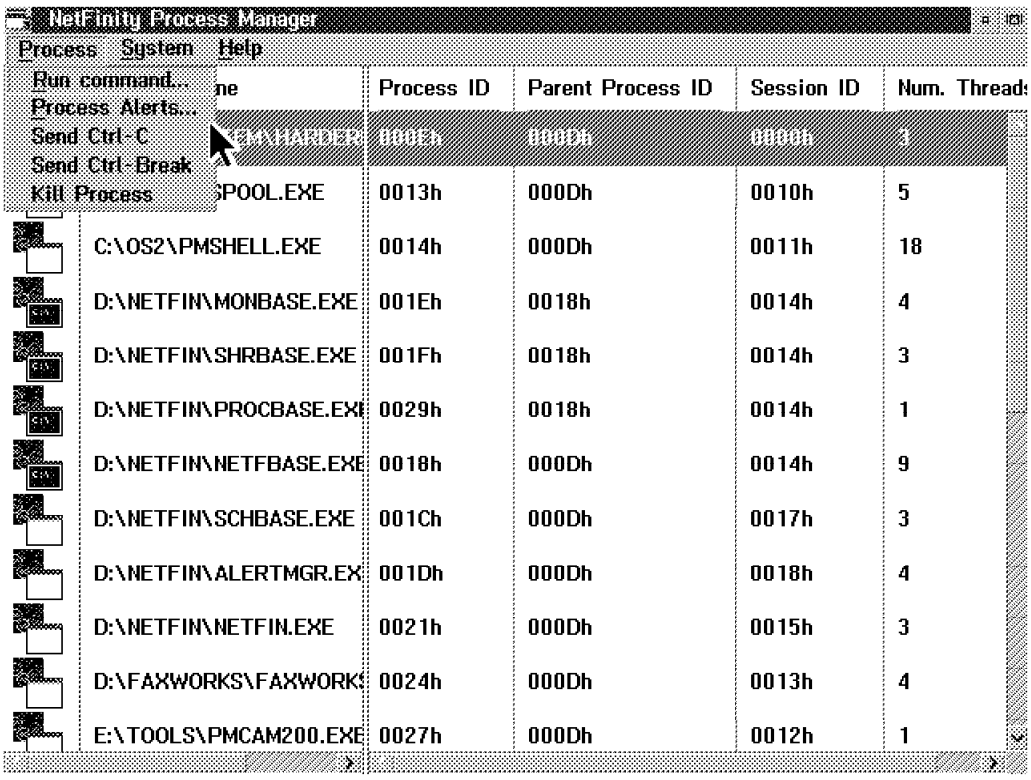


Figure 43. NetFinity Process Manager

The NetFinity Process Manager window shows all of the running programs in the monitored NetFinity system with some additional details about the program. Remember this can be your local system, or if you are using the

Remote Systems Manager, it can be the processes on the remote client. Those systems can be OS/2, DOS/Windows, or NetWare clients.

- Click on **Process** in the title bar and you get a pull-down menu with the following options:
  - Run Command
  - Process Alerts
  - Send Ctrl-C
  - Send Ctrl-Break
  - Kill Process

To start a process from the Process Manager service, on the system where the Process Manager resides:

- Click on **Run Command** in the Process pull-down menu in Figure 43 on page 34 and the Run Command window appears.

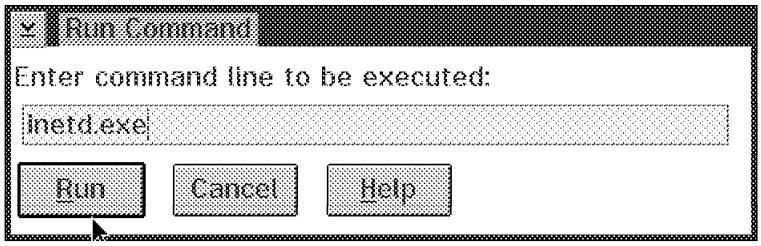


Figure 44. Run Command Window

- Enter the process name you want started and click on **Run** to start the process. You may notice at the end of the process list a new task appearing. This is the task that you entered in the Run Command line.

  To stop a process using the Process Monitor Service select the process and click on one of the following from the pull-down menu in Figure 43 on page 34:
  - Ctrl-C
  - Ctrl-Break
  - Kill Process
- If you click on one of these options, one of the commands Ctrl-C, Ctrl-Break, or Kill Process will be sent to try and terminate the process.

  Before the terminate function gets executed, a window appears asking for confirmation. This protects you from stopping a process by accident.

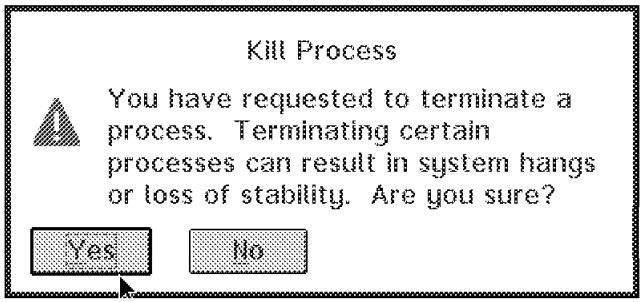


Figure 45. Kill Process Warning

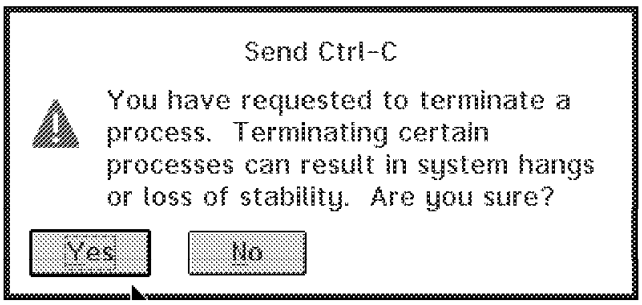


Figure 46. Send Ctrl-C Warning

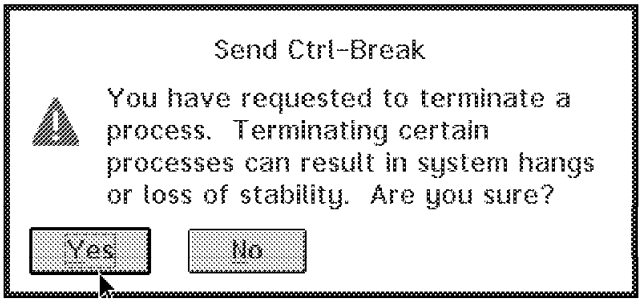


Figure 47. Send Ctrl-Break Warning

Select **Process Alerts** from the pull-down menu in Figure 43 on page 34 to configure the Process Manager service to generate a NetFinity alert when a specified program:

- Starts running
- Stops running
- Fails to start running within a specified time

To define Process alerts:

- Click on **Process Alerts...** from the Process pull-down menu.

  The Process Alerts window appears:

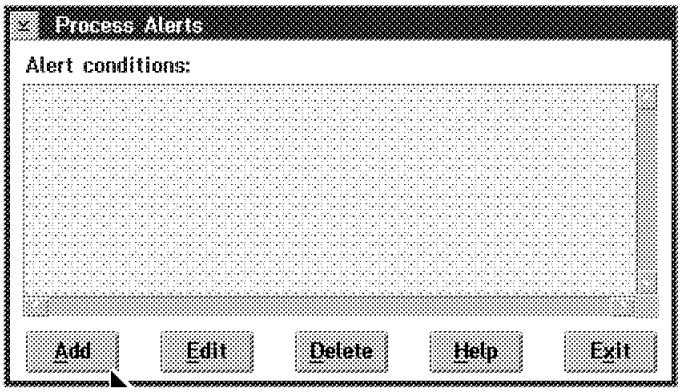


Figure 48. Process Alerts

- Click on the **Add** button to create a new Process Alert definition.

  The Add Process Alert window appears:

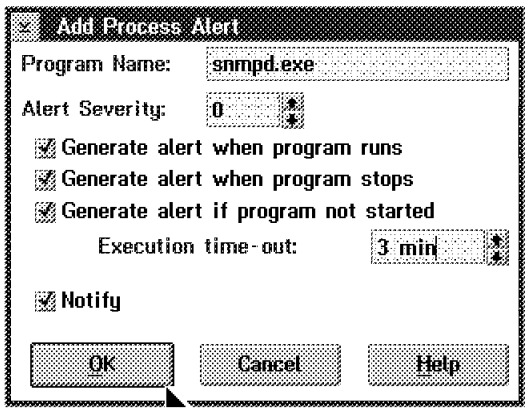


Figure 49. Add Process Alert

To add a new Process Alert:

- Enter a Program Name.
- The default severity is 0, but it can be changed.
- Select the **Generate alert** check boxes that you need.

  The Process Manager service can generate three different NetFinity alerts concerning the status of the specified program. These alerts will notify you when:

  – The specified program starts running.

  – The specified program stops running.

  – The specified program fails to start executing within a specified amount of time from startup.

- Set an execution time-out value. The default is one minute.

  This is the time NetFinity will wait before generating an alert. The execution time-out is measured from the time the NetFinity support program or NetFinity network interface is started.

  In our test case we had many different applications running on our system. Therefore, the system reboot took several minutes. We needed to specify a monitoring time that would give the system a chance to start everything up. In this case, it took two minutes to start. If you had selected one minute, an alert would have been generated.

- Select the **Notify** check box to cause alerts to be sent to your system′s alert manager.
- Select **OK** to save the Process Alert configuration and close this window.

  After filling in all the parameters, click on the **OK** button to have this alert added to the Alert Conditions list.

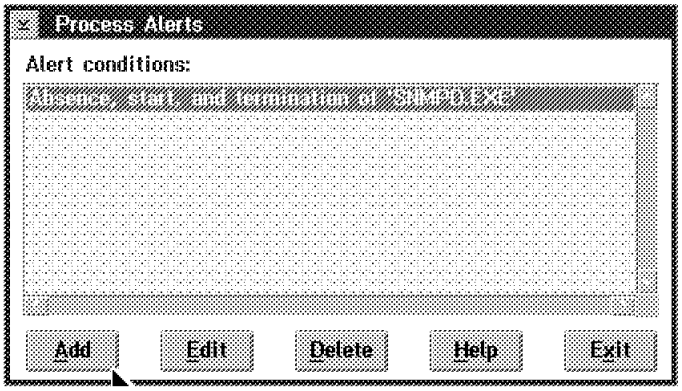


Figure 50. Process Alerts Screen with the First Alert Added

The alert you would see when SNMPD.EXE starts looks like the following:

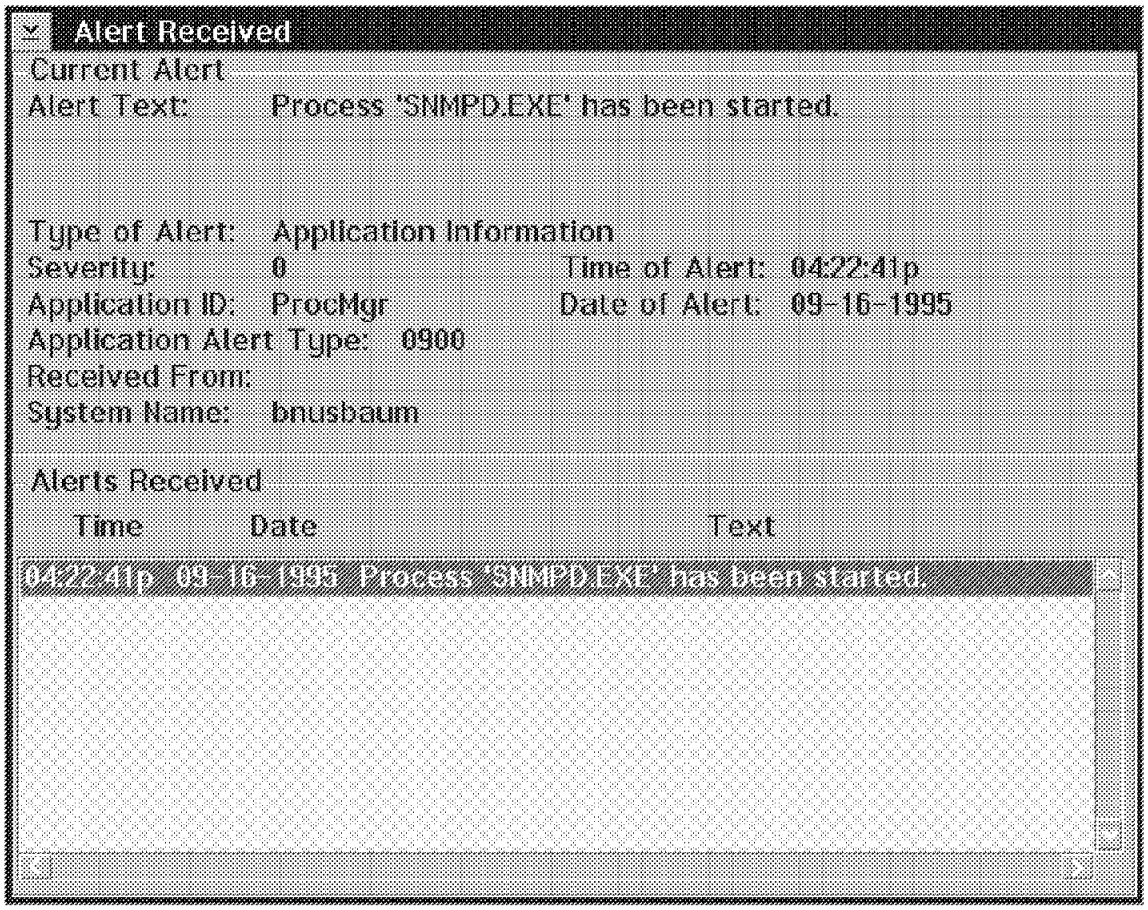


Figure 51. SNMPD.EXE Started Execution

The alert you would see when SNMPD.EXE stops looks like the following:

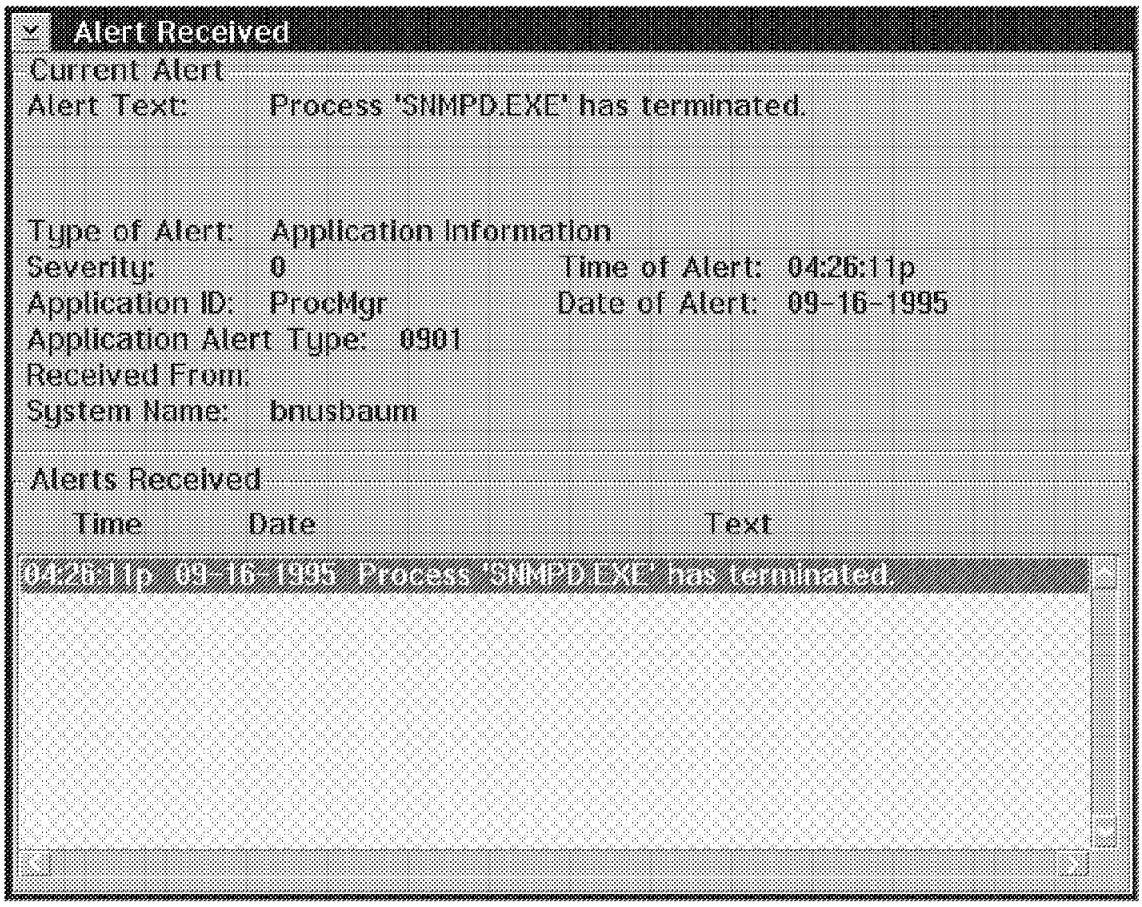


Figure 52. SNMPD.EXE Started Execution

After including all the programs you want to monitor, click on the **Exit** button to go back to the Process Manager screen.

3.1.2 Remote Configuration of the Process Manager

The Process Manager application can also be executed from a remote NetFinity managers system.

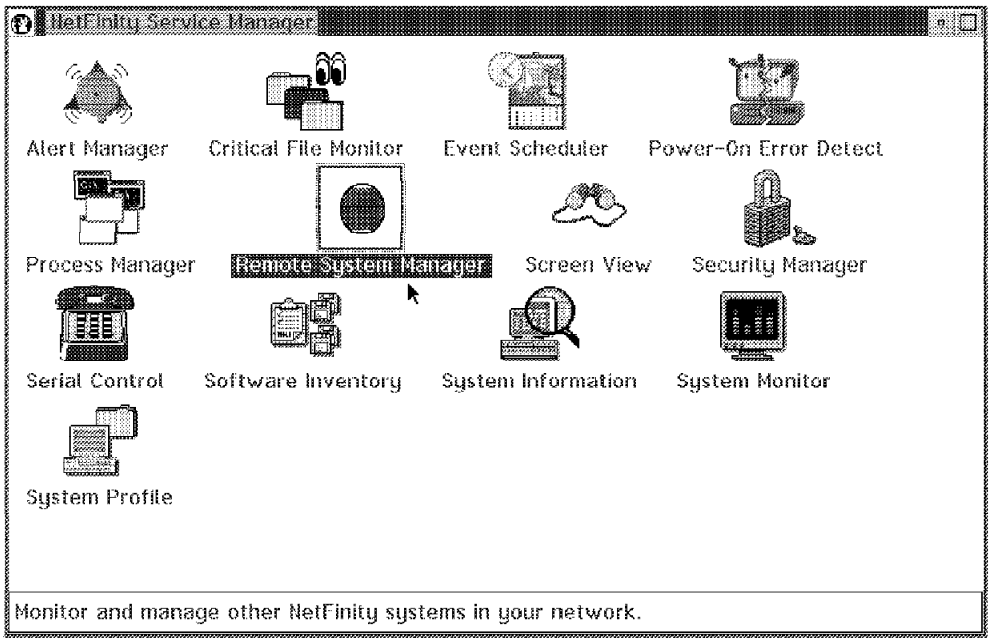


Figure 53. NetFinity Service Manager

- Double-click on the **Remote System Manager** object in the NetFinity Service Manager Folder.

  The System Group Management window with predefined groups is shown in:

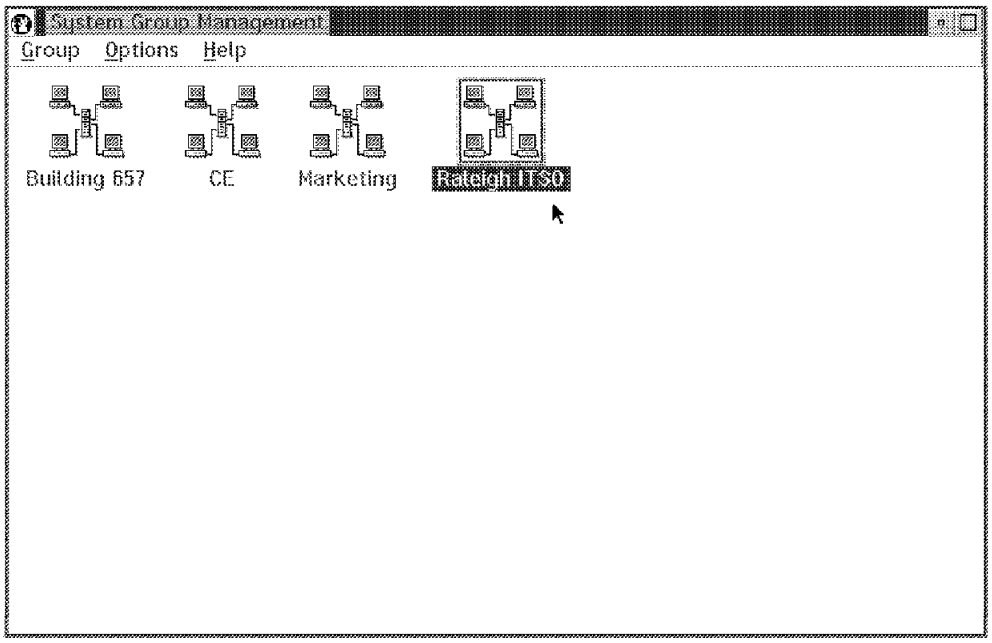


Figure 54. System Group Management

- Double-click on the remote system group that contains the system you want to monitor. In this case the system group ITSO Raleigh was selected.

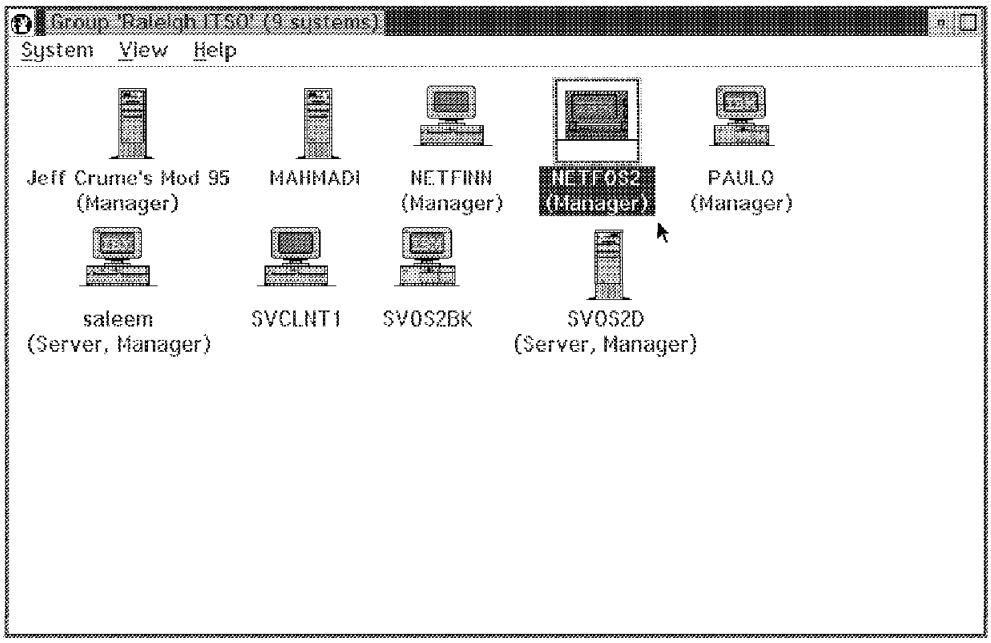


Figure 55. Remote Systems Group Raleigh ITSO

- In this example the system with the system name NETFOS2 is selected.
- Double-click on the system **NETFOS2** object and the NetFinity Service Manager from NETFOS2 window will appear. In the title bar of the NetFinity Service Manager window it shows which system the NetFinity Service Manager window is assigned. Only the functions that are supported on the remote system show up in the window.

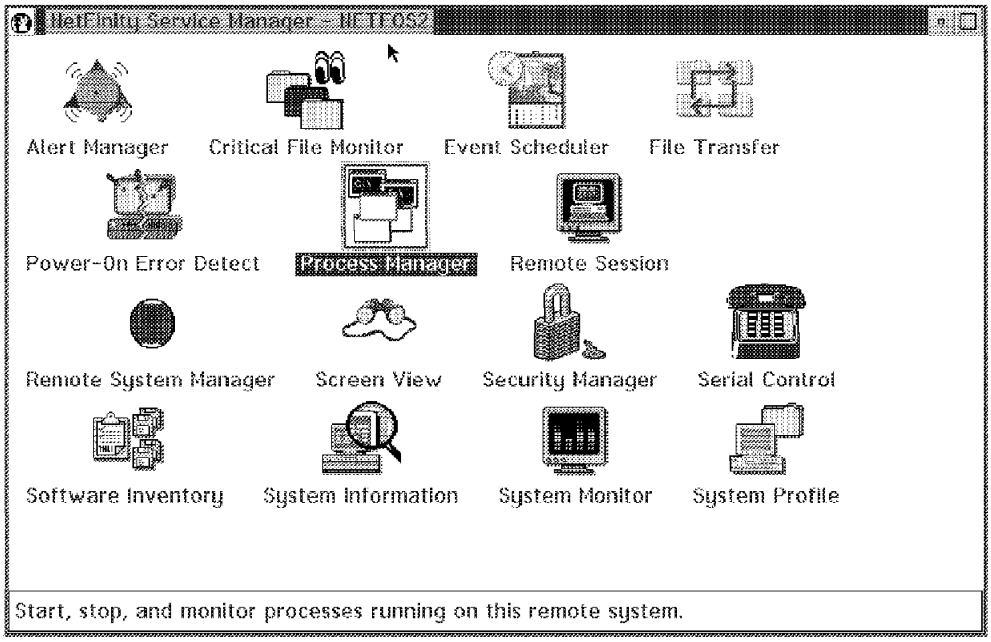


Figure 56. NetFinity Service Manager Window from NETFOS2

- Double-click on the **Process Manager** object in the NetFinity Manager folder for system NETFOS2. The following NetFinity Process Manager window from NETFOS2 appears:

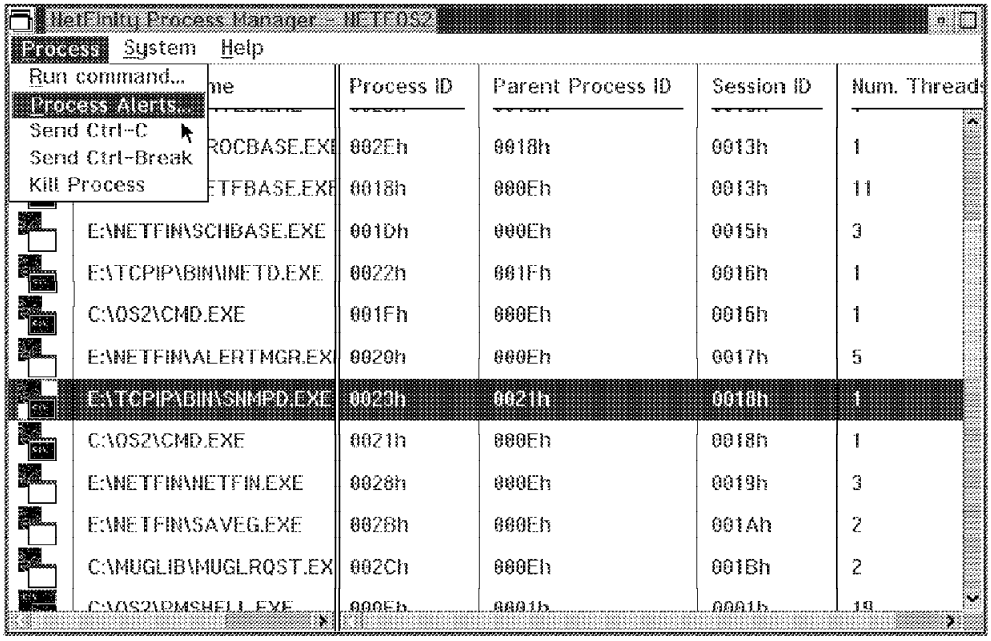


Figure 57. NetFinity Process Manager Window from NETFOS2

The Process Manager window from NETFOS2 shows all of the running programs in the monitored NetFinity system NETFOS2 with detailed description.

- Click on **Process** in the title bar and you get a pull-down menu with following options:
  - Run Command
  - Process Alerts
  - Send Ctrl-C
  - Send Ctrl-Break
  - Kill Process

  The last three Options relate to the process that is highlighted. If you click on one of these options, the command Ctrl-C or Ctrl-Break will be sent or the process will be killed. Before the command gets executed you will get a confirmation window that protects you for stopping a process by accident.
- Select **Process Alerts...** to configure the Process Manager to generate a NetFinity Alert when a specified program:
  - Starts running
  - Stops running
  - Fails to start running within a specified time
- To define Process alerts click on **Process Alerts...** from the Process pull-down menu.

  The Process Alerts screen appears as follows:

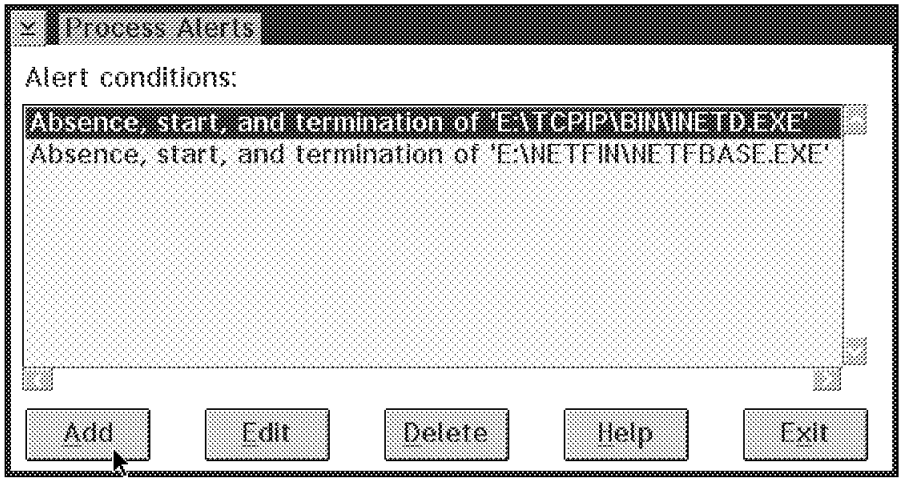


Figure 58. Process Alerts Window from NETFOS2

- Click on the **Add** button to create a new Process Alert definition.

  The Add Process Alert window appears.

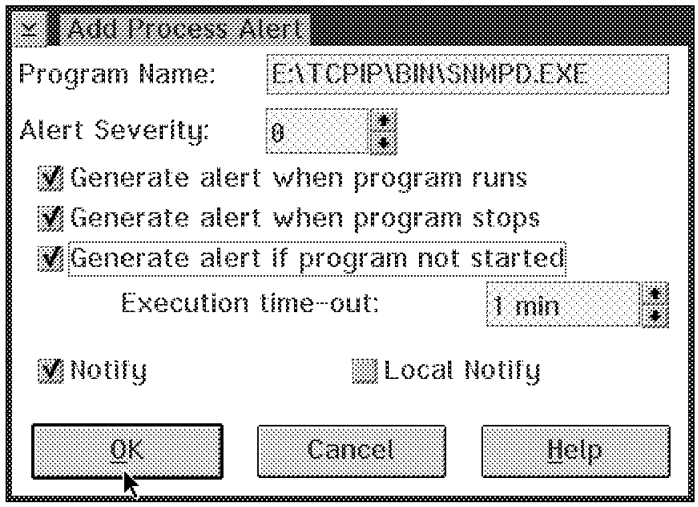


Figure 59. Add Process Alert Window from NETFOS2

  To add a new Process alert:

  - Type in the program name
  - Select in the alert severity field a severity value for the NetFinity alert. The default value is 0.

- Select one or more **Generate alert** check boxes.

  The Process Manager service can generate three different NetFinity alerts, reflecting the status of the specified program. These alerts will notify you when:

  - The specified program starts running.
  - The specified program stops running.
  - The specified program fails to start running within a specific amount of time from startup.

- Set an execution time-out value. The default value is 1 minute.

Execution time is the time NetFinity has to wait before generating an alert. The execution time-out is measured from the time at which the NetFinity support program or NetFinity Network Interface is started.

- Select the Notify checkbox to send the generated alerts to the Remote NetFinity Manager.
- Select the **Local Notify** checkbox to send the generated alerts to the local system as well.

> **Note**
>
> The check box Local Notify only appears on the Alert Process window on a NetFinity monitored system which will be remotely configured. If you don't select Notify or Local Notify, the NetFinity Process Manager Alerts will not get generated.

After filling in all the parameters click on the **OK** button to have this alert added to the alert conditions list.

You get a process specific pull-down menu when you click on the process you want to monitor in the NetFinity Process Manager window with the right mouse button.

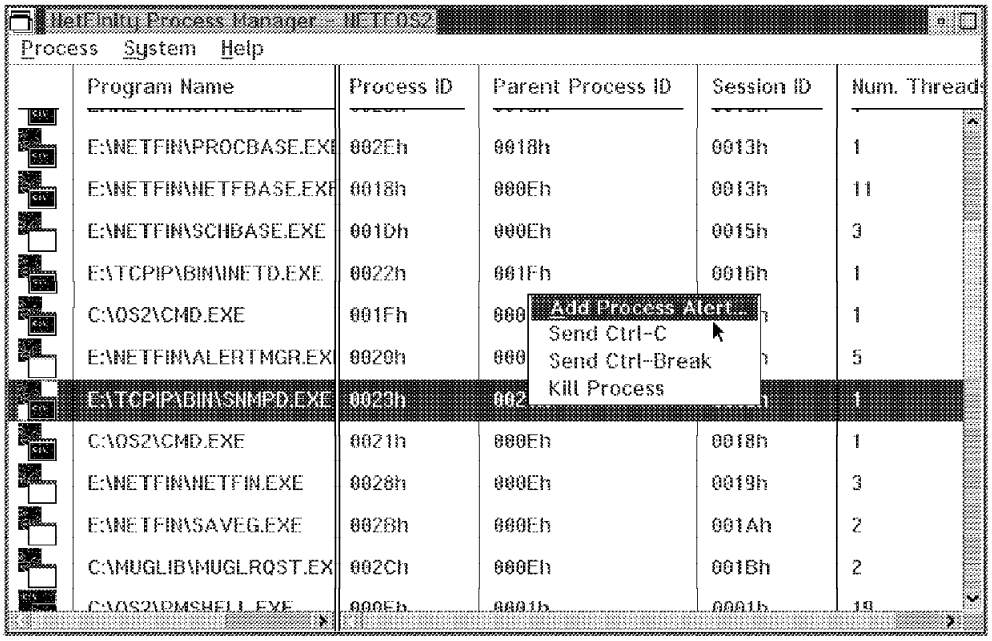


Figure 60. NetFinity Process Manager Window

- Click on **Add Process Alert...** and the following window appears:

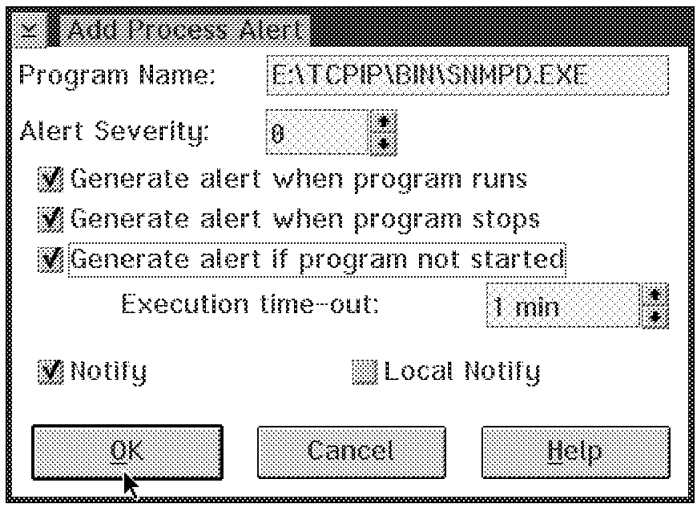


Figure 61. Add Process Alert Window

- The highlighted process name will appear automatically in the Program Name field.

  Define all parameters as described before.

- Click on **OK** and the Process Alert goes in the Process Alert List without showing the result through a following Process Alert window.

  If you want to see the list of process alerts, you need to go to the process pull-down menu shown in Figure 43 on page 34 and Click on **Process Alerts...**.

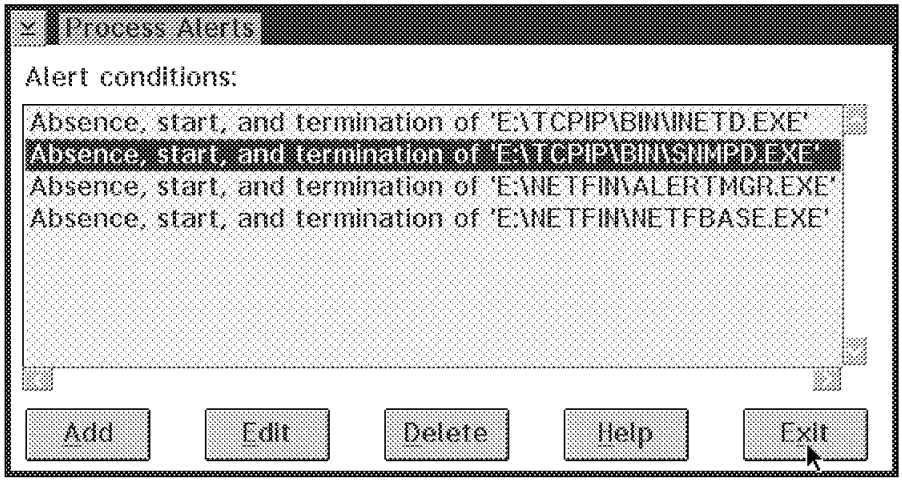


Figure 62. Process Alerts Screen from NETFOS2

After including all the programs you want to control, click on the **Exit** button to go back to the Process Manager screen.

3.2 System Monitor Services

Figure 63. System Monitor Icon

The System Monitor object is imbedded in the NetFinity service manager folder on the OS/2 desktop.

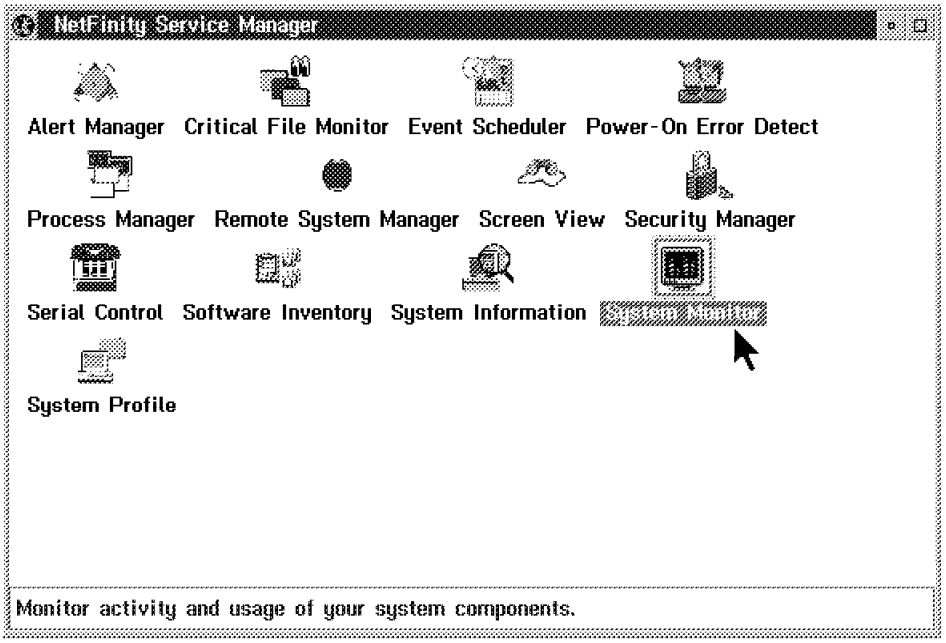


Figure 64. NetFinity Service Manager Window

The System Monitor provides an easy way of displaying and monitoring the current activity of components in a system.You can choose line graphs, textual representations, or real time graphs to represent system activity. All of the monitors are detachable, scalable and user customizable. You have the ability to export the System Monitor data to any of the databases that are defined to NetFinity. This includes DB2 /2 and Lotus Notes databases. One of the most important functions is the ability to set user defined thresholds that can generate NetFinity alerts. This helps you monitor the health of your system. You can generate these alerts when you low as well as high-water thresholds. This means you can send an alert when activity returns to normal.

There are a lot of default monitors that come with NetFinity. During the installation of NetFinity, it determines which monitors can be installed on the system, based upon its configuration. For example, if the Serverguard adapter is installed and the NetFinity Serverguard module is added to the NetFinity directory, it is possible to monitor the voltage and temperature of the system. Also, if you use an APC Un-interruptible Power Supply (UPS) and add the UPS

NetFinity module to the NetFinity directory you can monitor the same UPS Activity.

In addition to the monitors that are provided with NetFinity there is a developer's kit that you can use to develop your own monitors. Some of the standard monitors that come with NetFinity are:

- CPU Utilization
- Processes Count
- Thread Count
- Integer Instructions Rate
- Memory I/O Rate
- CPU Cache Hit Rate
- Drive x: space used or Remaining
- Print Jobs Queued
- Swap Space Remaining
- RAID Device Attributes
- Many TCP/IP monitors

You start the System Monitor by doing the following:

- Double-click on the object in the NetFinity Service Manager folder.

  This will cause all the monitors that you had previously set up to run (if any) to start up on your display. In addition, the following window will appear:

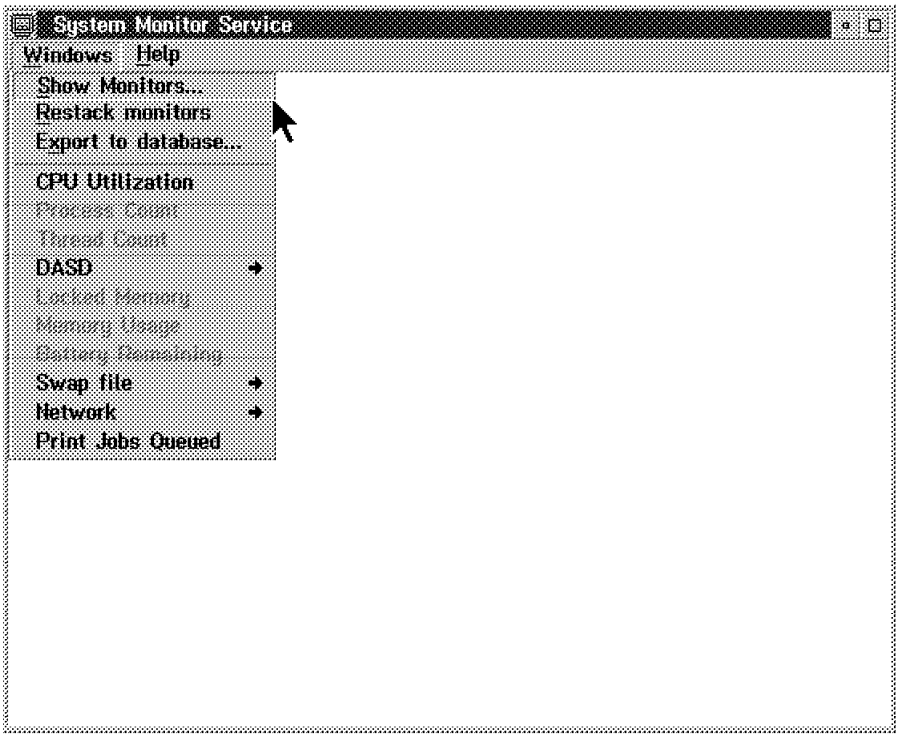


Figure 65. System Monitor Service Window

  When you are navigating backwards from one of the monitors to the Systems Monitor service window, you will see it referred to as the *Main Menu*. If you close the System Monitor service window all of the monitors will close as well.

- Click on **Windows** to get a list of all the options.

- The option Export to database lets you send information from the monitor to a NetFinity database. If you use the right mouse button on one of the monitors you will see this option.

  If you want to send information from all of your monitors to your database, then you will need to select the Export option from the System Monitor main menu option.

  When you look at the list of monitors that are available to you, you may see some of the monitors have an arrow pointing to the right. This is just a logical grouping of monitors together. There are many monitors that come standard with NetFinity but you also have the ability to use the System Developer Kit (SDK) to extend the number of monitors by writing your own. We did not write any new monitors during this project.

  To select monitors to use for capturing information or just for displaying on your EUI, all you need to do is click on any or all of the monitors from the Select Visible Monitors window, as shown in Figure 66. Once you click on **Accept** the monitors will appear on your display.

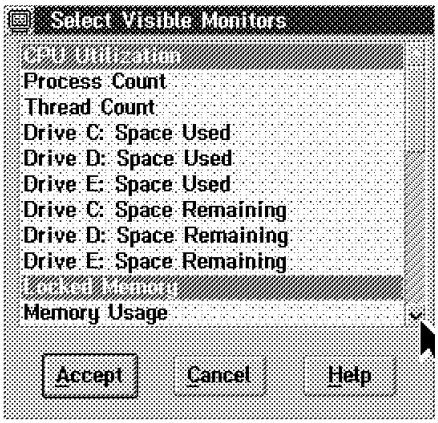


Figure 66. Select Visible Monitors Window

After you have clicked on the Accept button, you will see a monitor similar to Figure 67 on page 49 appear on the display. The default attributes are for the window to appear as a graphic. We made one change to the window you see. We requested that the title bar show up in the window. You can see an example of the OS/2 window settings by using the right mouse button within the monitor window, then click on **open** and **settings**. An example of this is shown in Figure 72 on page 53.

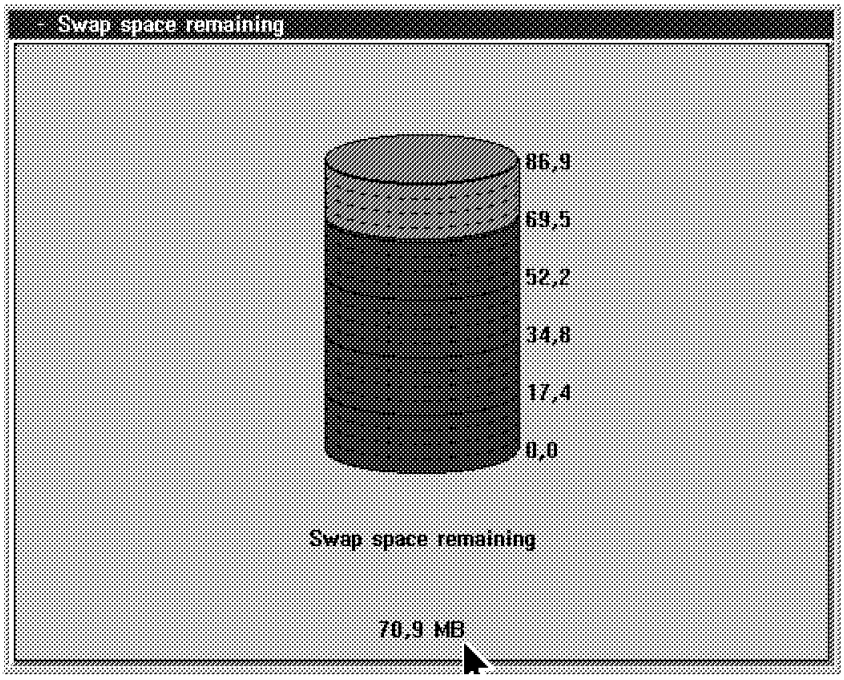


Figure 67. Graphic in Real-Time Mode

- Figure 67 shows the real time graphical representation of the Swap space remaining on the system.
- If you use the right mouse button and click on **View** you will see that you can see the swap space represented as:
  - A line graph
  - A real time display
  - A text display

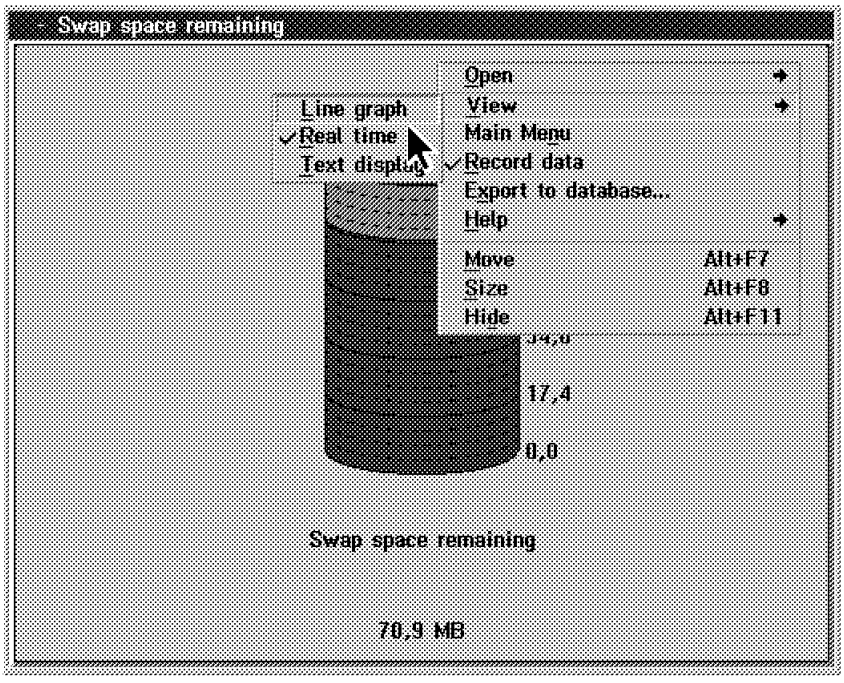


Figure 68. System Monitor Pull-Down Menu

In Figure 68, notice that the Record data field has a check mark to its left. This means that the historical data for this monitor is being saved. If you are going to export the data to a database on a regular basis, you will want to have the record feature turned on. If you are not going to do any analysis of the data, you should not turn recording on, as you will only waste disk space and some CPU cycles.

Note

If you disable Record data all of your historical data for the monitor is erased. When you re-enable the field, it will restart recording but not recover the old data.

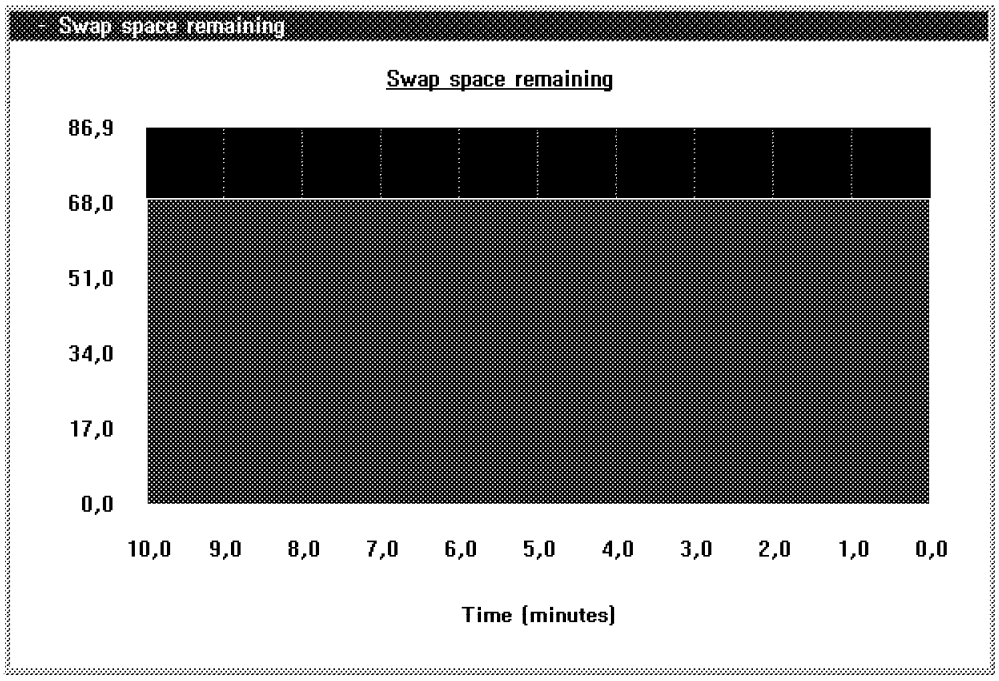


Figure 69. Swap Space Remaining Window in Line Graph Mode

1. Line Graph mode is a heartbeat-style chart of the system component's activity. The parameters that determine the length of the graph and the units to be used (for example, seconds or weeks) can be set in the Settings window, as shown in Figure 72 on page 53.

3.2.1 Setting Thresholds

One of the more powerful functions that the monitors provide is the ability to set thresholds (high and low) and issue alerts if they are reached. If you double-click on any of the monitors in text, graphic or line graph mode, you will get the threshold settings window, as shown in Figure 70 on page 51. Remember that these monitors can be configured both locally on your manager and remotely on your clients if you are using the Remote Systems Manager function of NetFinity.

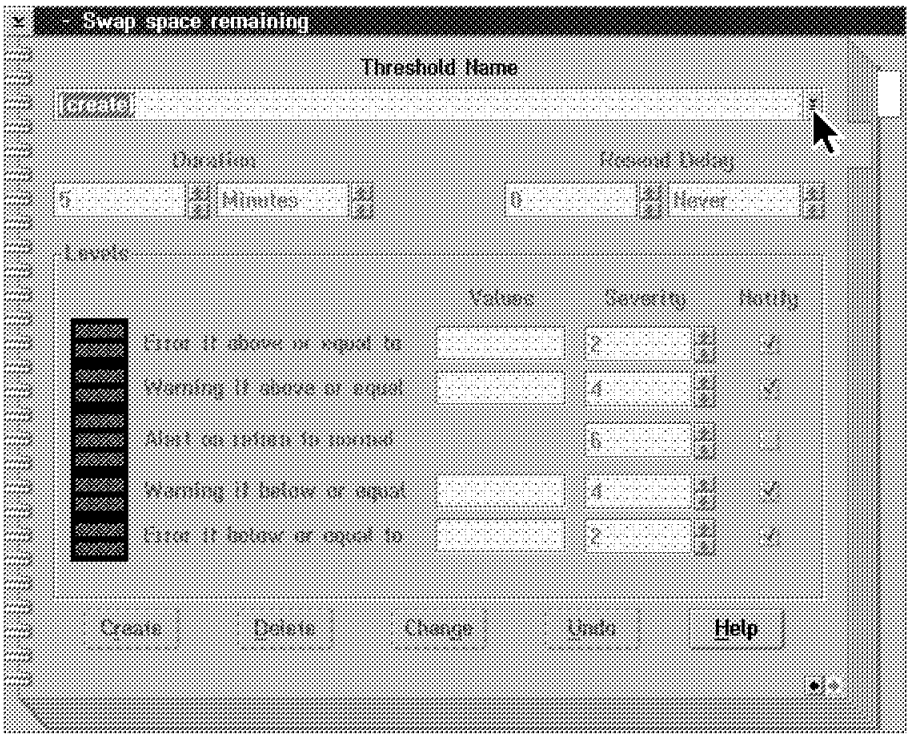


Figure 70. Threshold Window

All of the monitors are configured in the same way. It is only the value of the fields that will vary. As an example, we have configured the Swap space remaining threshold. The process requires you to:

- Enter a Threshold Name.

  You click on the arrow on the right side of the Threshold Name box. If there are any previously defined thresholds, they will appear in a list just below the box. You can either select an existing one to modify, or just type a new one in that you will configure.

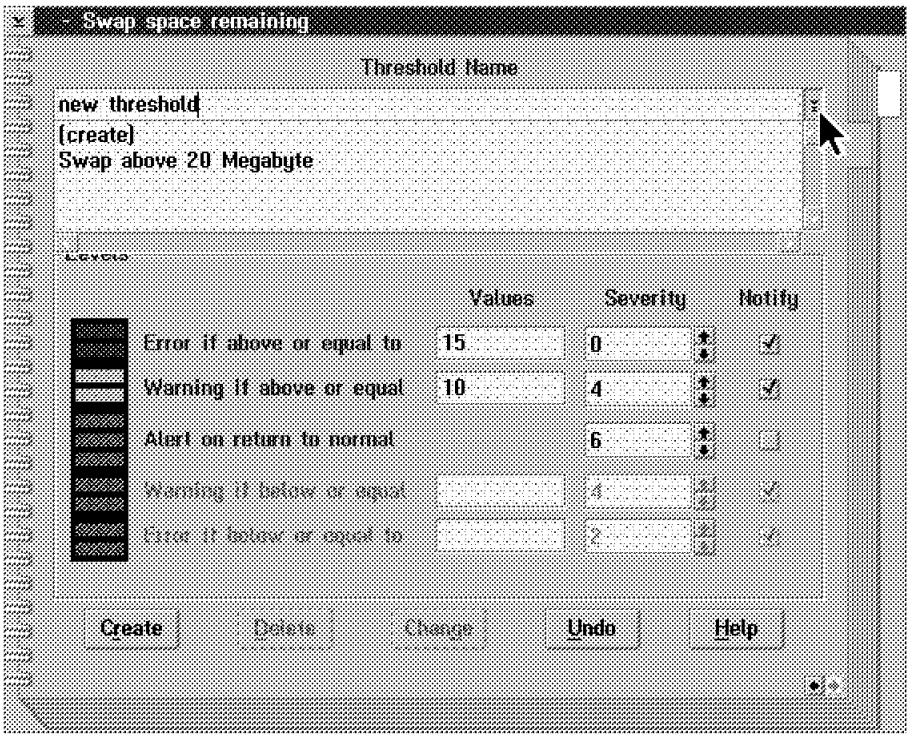


Figure 71. Threshold Window

- Set the values in the field called Duration Time.

  If the threshold is exceeded for a period of time that is longer then what is defined in this field an alert will get generated.

- Set the value in the field called Resend Delay.

  This means that if an alert gets sent due to a threshold being reached, the clock will get reset and wait for the resend delay period of time to pass before a second alert of the same type can be issued. This cuts down on duplicate alerts when a problem continues to occur over a period of time.

- Enter the threshold values and select the alert severity value that is to its right.

- Specify if you want an alert to flow by clicking on the **Notify** box.

  If you are setting up the threshold on your local system and you don't check the Notify box, you will not generate an alert. If you are on a NetFinity Manager station and you are accessing the systems monitor through the Remote Systems Manager, you can specify that alerts flow directly to the manager and not to the local system by clicking on the Notify box. If you want the local system to get notified you will see a check box called Local Notify that only appears on the threshold window if you are accessing it from the Remote System Manager.

  The actual thresholds that you can set are:

  - Error if above or equal to.
  - Warning if above or equal.
  - Alert on return to normal.
  - Warning if below or equal.
  - Error if below or equal to.

Each of the values and severities depend on the local criteria you have set up for each system.

If you click on the left arrow in the bottom right part of the window, you will go back to the Settings window as shown in Figure 72.

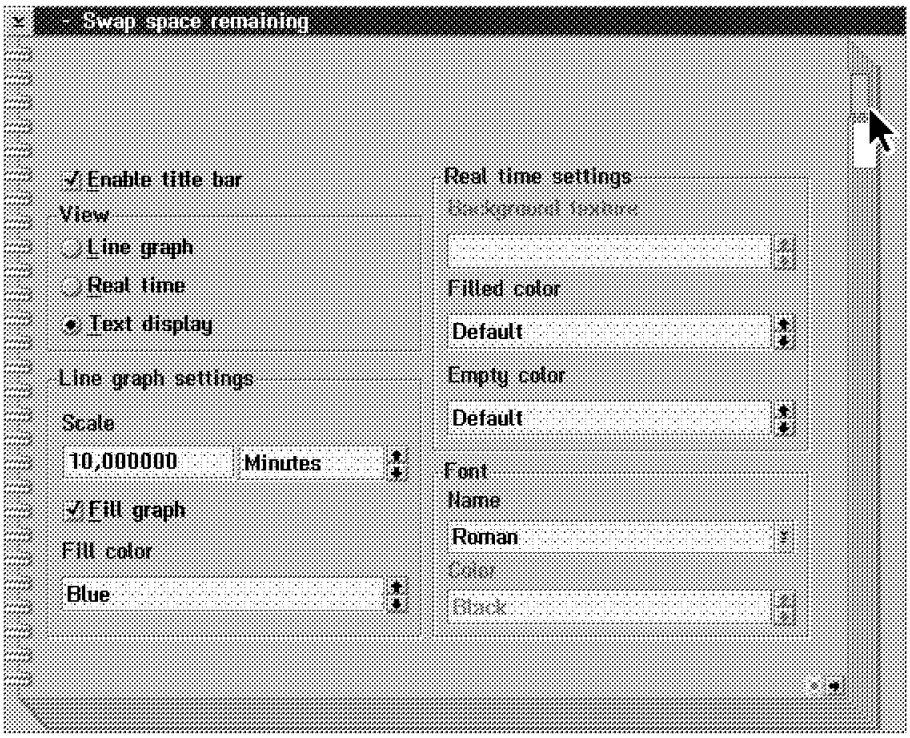


Figure 72. System Monitor Settings Window

Now that we have set some thresholds and collected some data using the monitor, we will want to save it in a database for further analysis. If you go back to the monitor window, single-click and use the right mouse button, you will see the option to click on to **Export to database** as shown in Figure 73 on page 54.

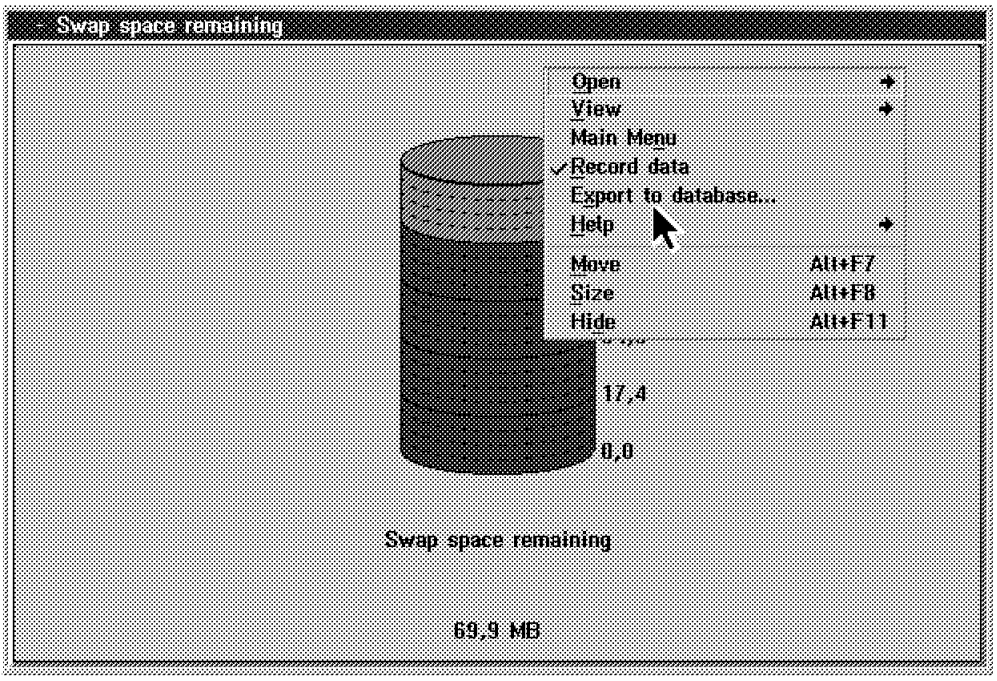


Figure 73. System Monitor Individual Pull-Down Menu

If you select **Export to database** in the pull-down menu on any of the monitors you will see a list of databases that you can export the data to, as shown in Figure 74.

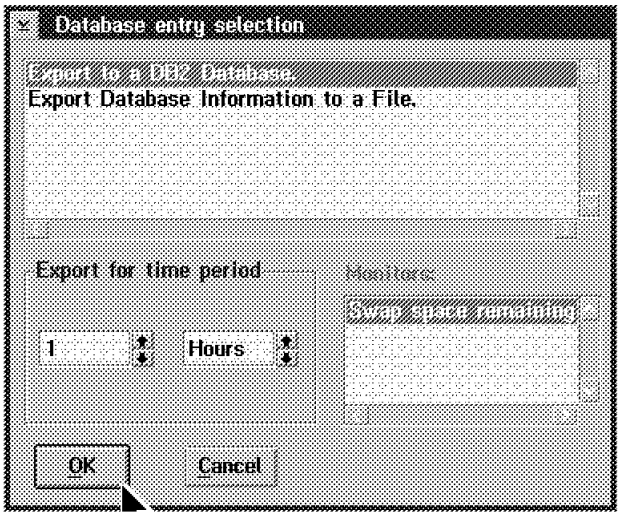


Figure 74. Databases for Export

You can export the data that you have been collecting to DB2 /2 databases, a flat file, or a Lotus Notes database. You can also specify how much data you wish to export by setting the values in the field Export for time period.

In Figure 74 there is also a field called Monitors. This will contain a list of monitors that you can click on to have their data exported to the database.

- Click on **OK**.

  The Server Selection window appears.

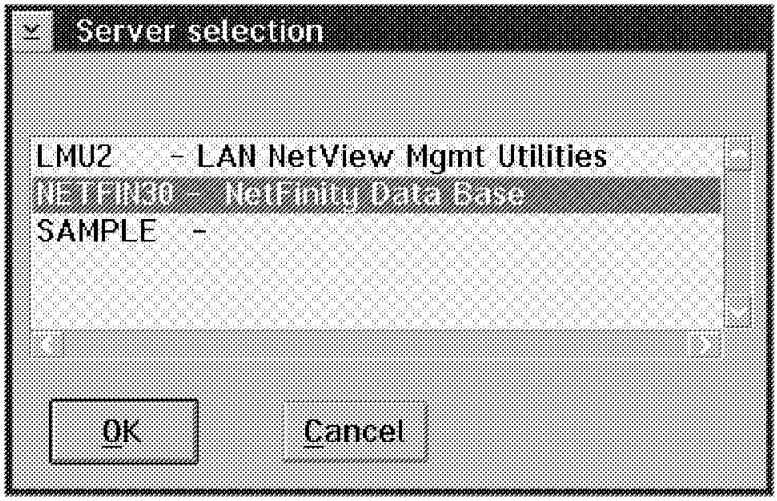


Figure 75. Choice of Databases

- Select a database. In this case we will use the NetFinity database.

  While it is writing the data, an option appears to cancel it. This window will stay on your display until the database is updated.

Figure 76. Updating the Database

Chapter 4. Remote Management Functions

This chapter describes the NetFinity services that relate to remote management. The following services can be performed at the NetFinity manager, but they require interaction with the NetFinity clients:

- Remote Systems Manager
- Security Manager
- Screen View

4.1 Remote Systems Monitor

NetFinity has the ability to manage remote systems using its standard graphical interface. It is as easy to manage a remote system as it is to manage your local system. The Remote Systems Manager icon is located in the NetFinity folder, as shown in Figure 77. There is a small amount of setup work that you need to do to manage the remote systems. If you have connectivity to the remote systems, you should be able to manage them. It can be done over TCP/IP, IPX, NetBIOS, or if you are dialing into the network using a serial connection, you can manage the environment that way as well. You will manage the remote machine based upon its hardware and software configuration. Even if you do not have some of the features on your local system (for example, RAID devices, or ECC memory), if the remote system has them, you can manage them.

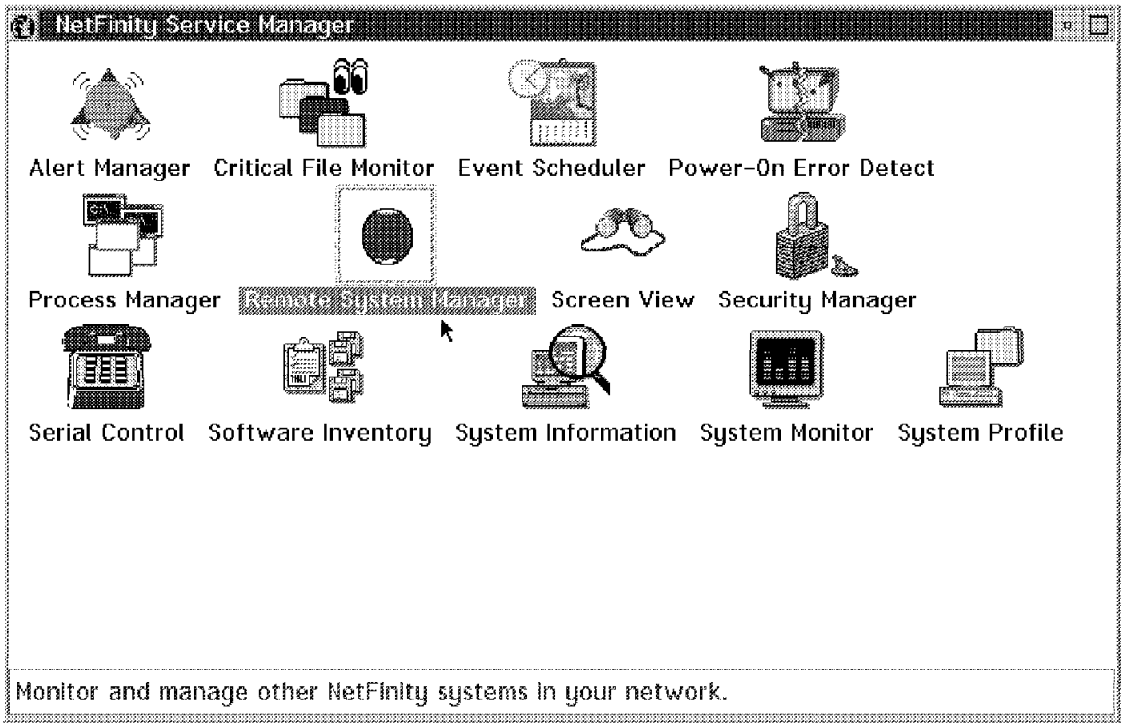


Figure 77. NetFinity Folder / Remote Systems Monitor

The first time you go into the Remote Systems Manager service you will need to set up which systems you want to monitor. When NetFinity was installed on any of your clients there was a set of keywords that were defined using the NetFinity

Driver Configuration on the client. You will classify your groups based upon those keywords. Managing stations have the same rules for having keywords associated with their system.

Before you can discover systems you will need to set up the groups. Using the pull-down menu under Group, select **Add Group**.

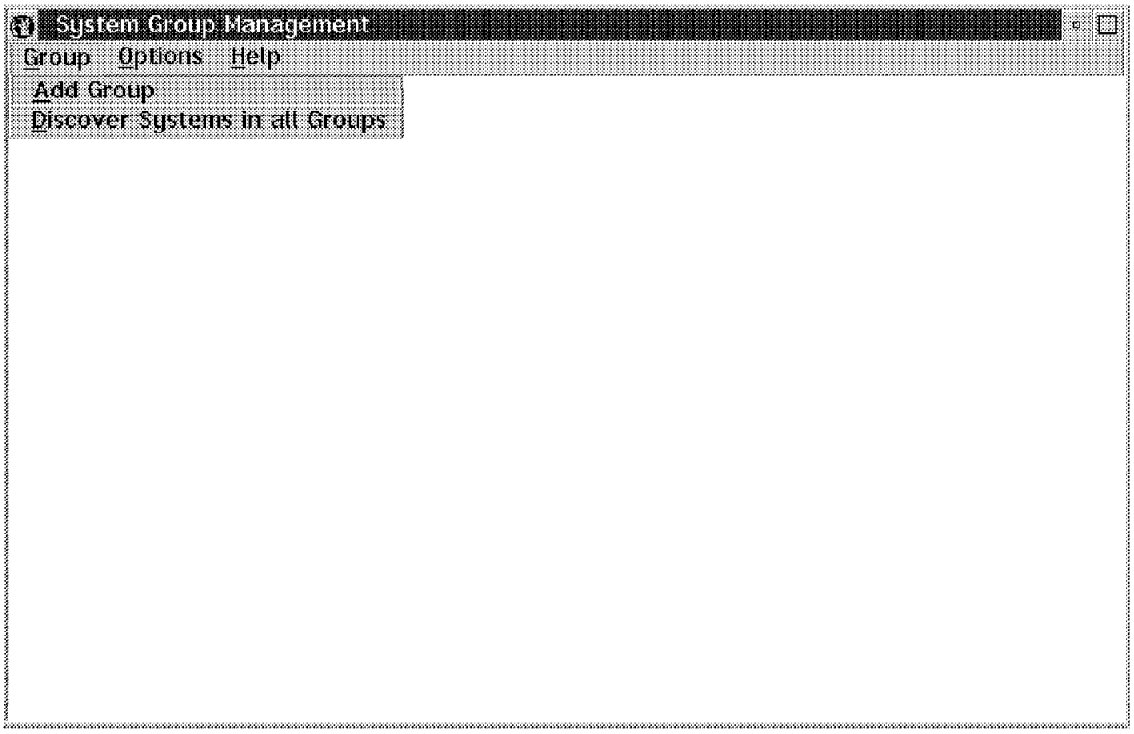


Figure 78. Setting Up Remote Management Folders

The group name can be any name that will help you remember what the group is. You can use special characters if you wish. For the example shown in Figure 79 on page 59, we called one of our groups all_sys. As you can see from the figure, we did not put any keywords in and we selected **Systems with any of the keywords**. That combination will create a search for any NetFinity system regardless of the keywords specified in its configuration file. NetFinity will do a broadcast using all of the protocols that are supported on the manager (for example, TCP/IP, NetBIOS and IPX), and build its remote systems folder based upon that discovery.

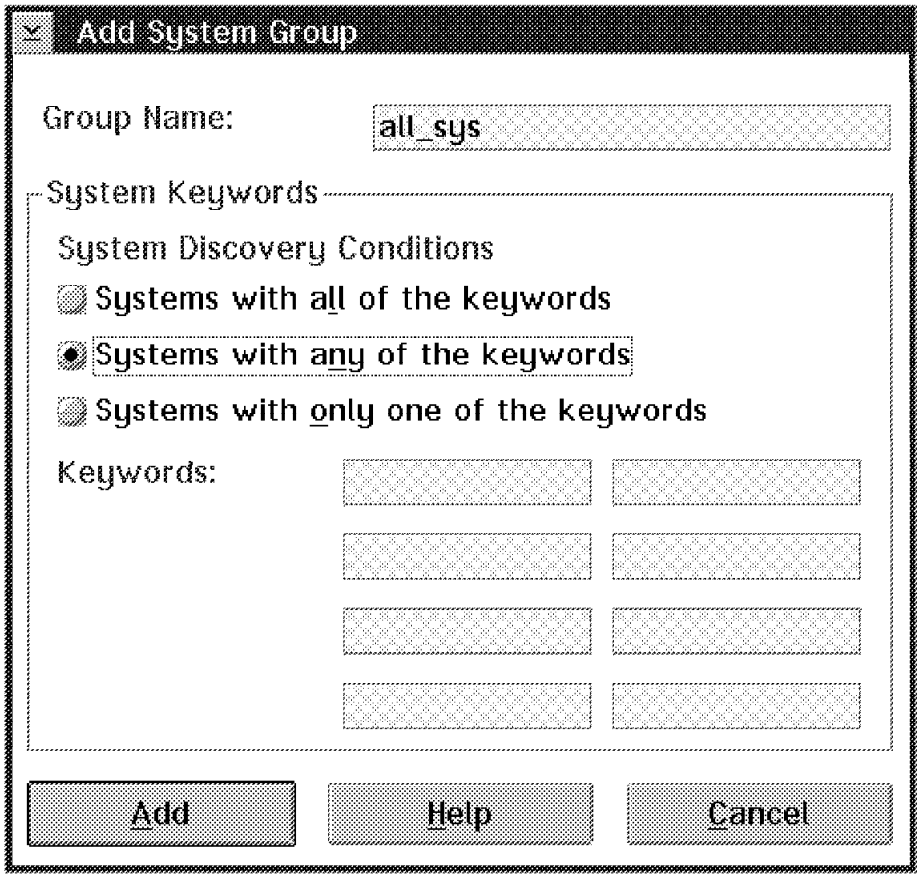


Figure 79. All Systems Discovery

In Figure 80 on page 60 we built several systems management groups. The names that we used are typical names that you might use in setting up your systems. You would probably want to discover systems based upon site-specific criteria:

- Transport Protocol
- Building Location
- Department Location
- Department Function

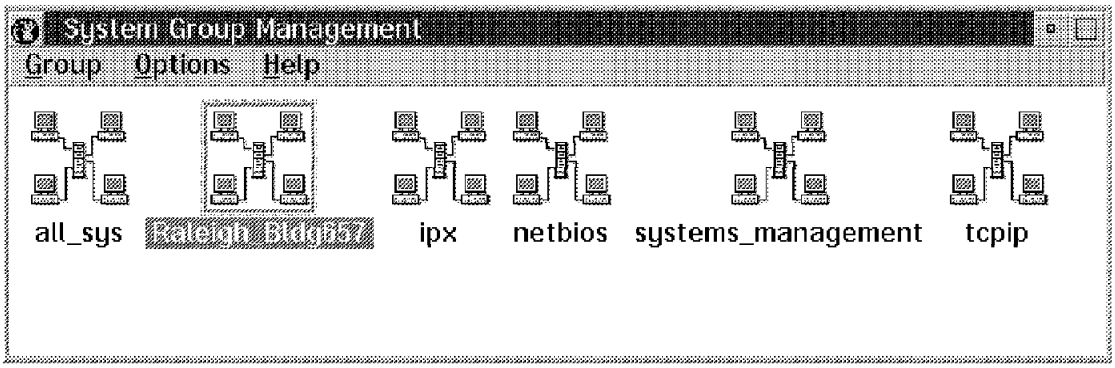


Figure 80. Logical Groups Set Up in the Remote Systems Manager

If you have a default user ID and password that is set up for the systems in your environment, you can set it up using the pull-down menus in the Remote Systems Manager group definitions. Most likely you will have a different user ID and password for each system and this function will not have any use in your network.

The other pull-down option, System Notification Defaults, is used to inform the managing system when NetFinity systems in the group go online or offline. If you are going to use the Alert Manager to automate any functions based upon that, you can change the default Severity value.

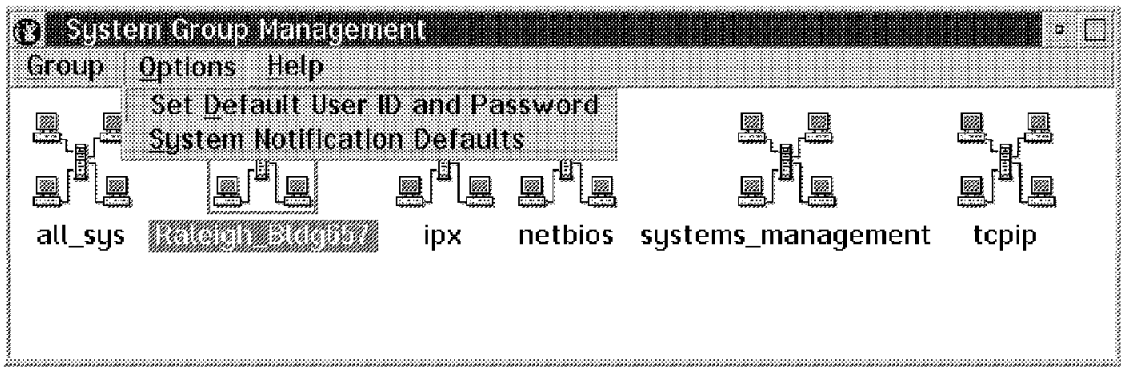


Figure 81. Security and System Notifications

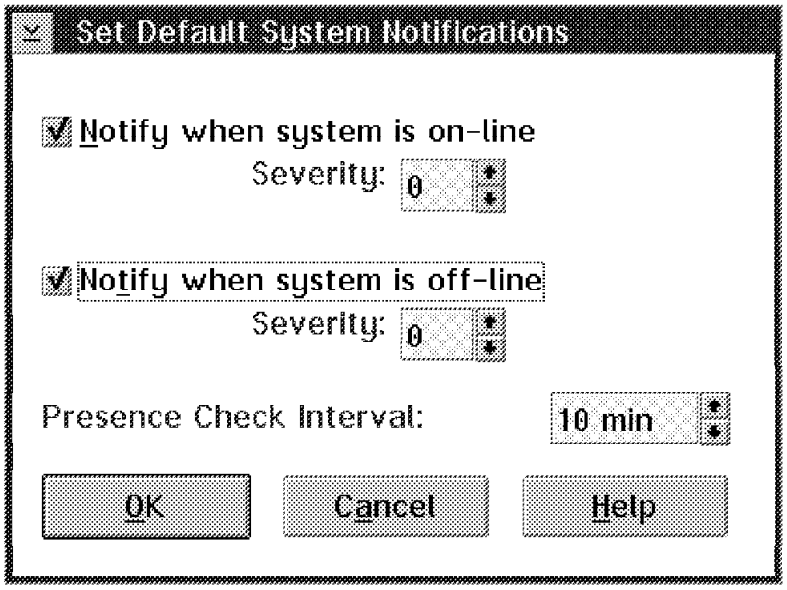


Figure 82. Alerts When Systems Come Online or Go Offline

Once you have set up the criteria for how you are going to discover the NetFinity clients and managers in your network you can also set up some filters to further narrow down the search patterns for determining which systems get placed in the discovered folder.

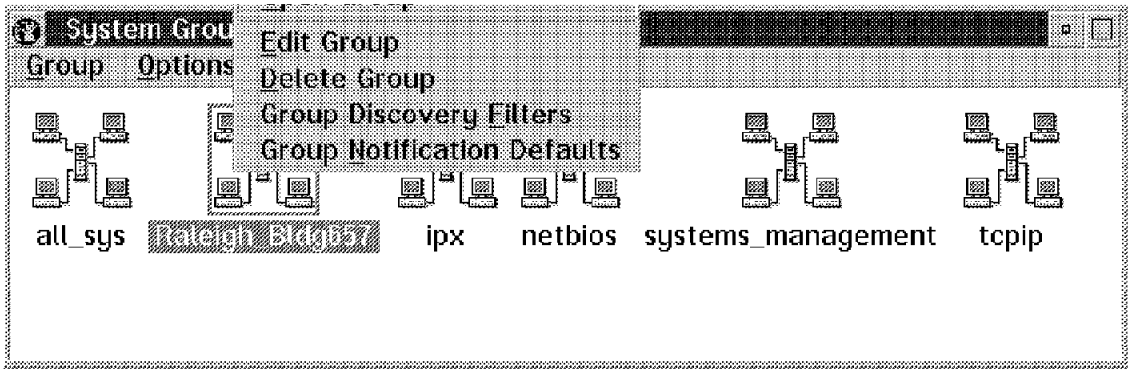


Figure 83. Editing Remote System Groups

In Figure 84 on page 62 you can see that filters can be set up for discovery of systems by transport protocol as well as operating system.

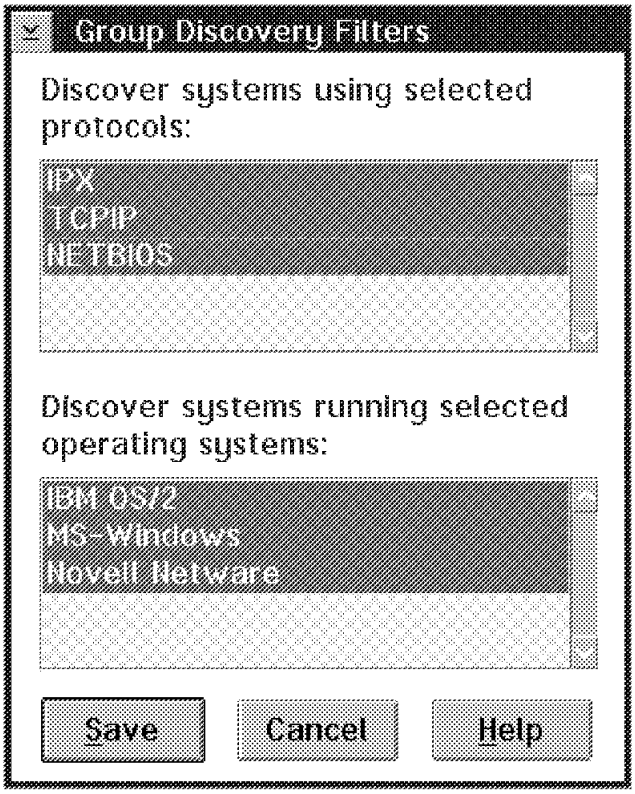


Figure 84. Discovery Filters

In Figure 85 on page 63 we found systems that have NetFinity and IPX. There are other transport protocols on those systems as well, and therefore they show up in the group window. In addition to the system name discovered, NetFinity resolves:

- Network transport protocol
- Network address
- System model type and number

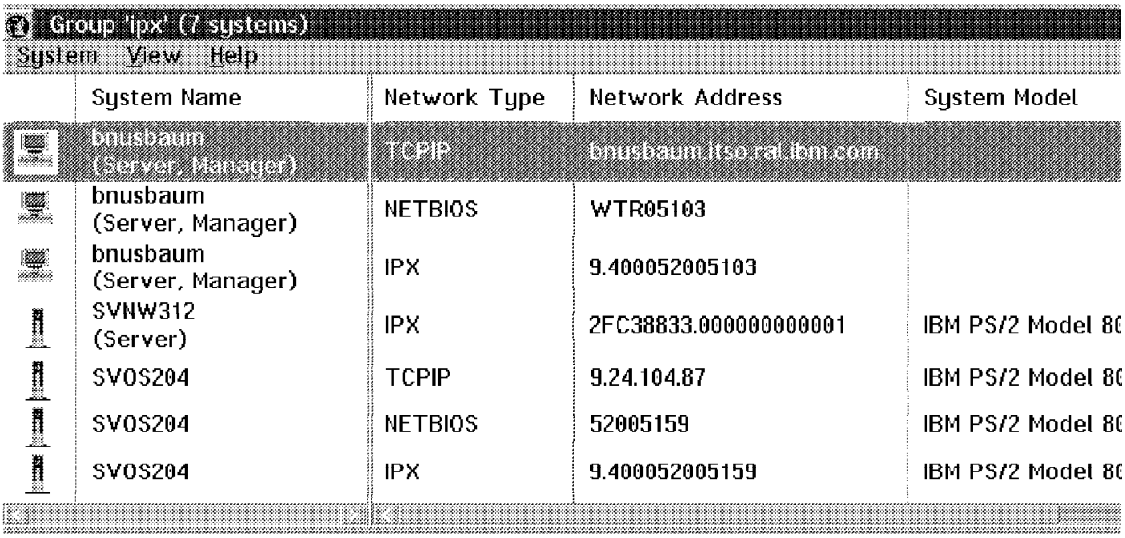


Figure 85. Discovered Systems

If we look in the all_sys folder we see all of the systems that NetFinity has discovered over all of its transport protocols. We will try and manage an OS/2 system called svos2d. The way to begin that process is to double-click on the icon.

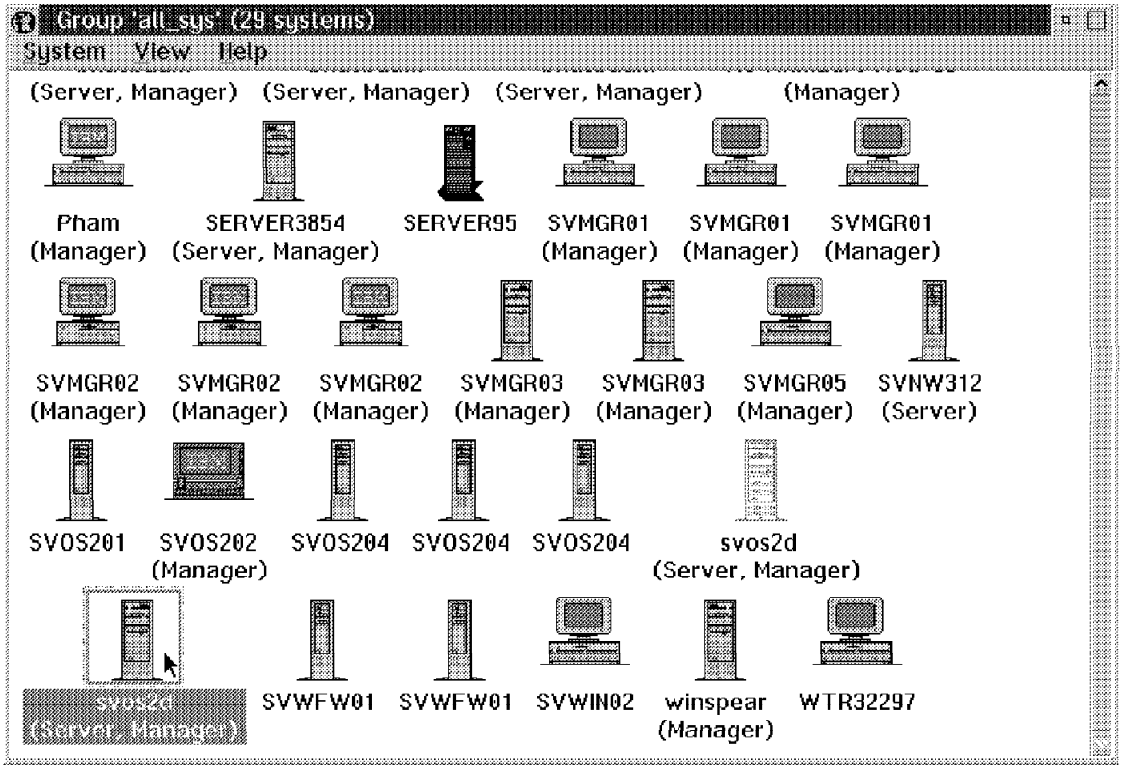


Figure 86. Discovery of All Systems

We have set up a user ID and password for all of our systems, so when the Remote Systems Manager tries to connect and manage any system it will receive a pop-up window requesting a user ID and password.

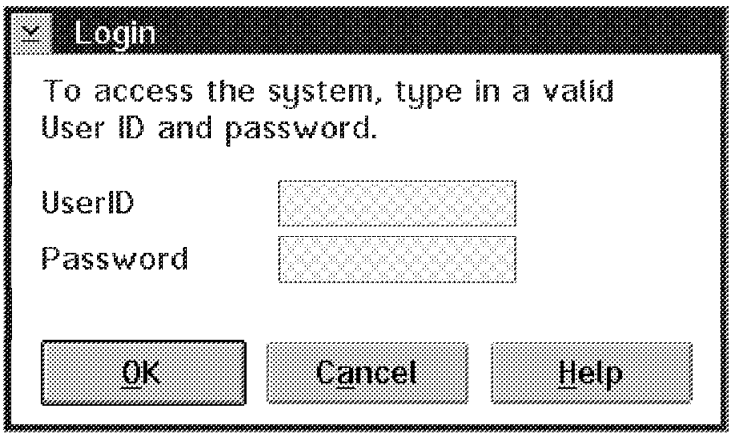


Figure 87. Remote Login Security

Figure 88 shows us what services we can manage in svos2d. The title bar on the figure lets us know which system we are managing. This is helpful when you are trying to manage more then one system at a time.

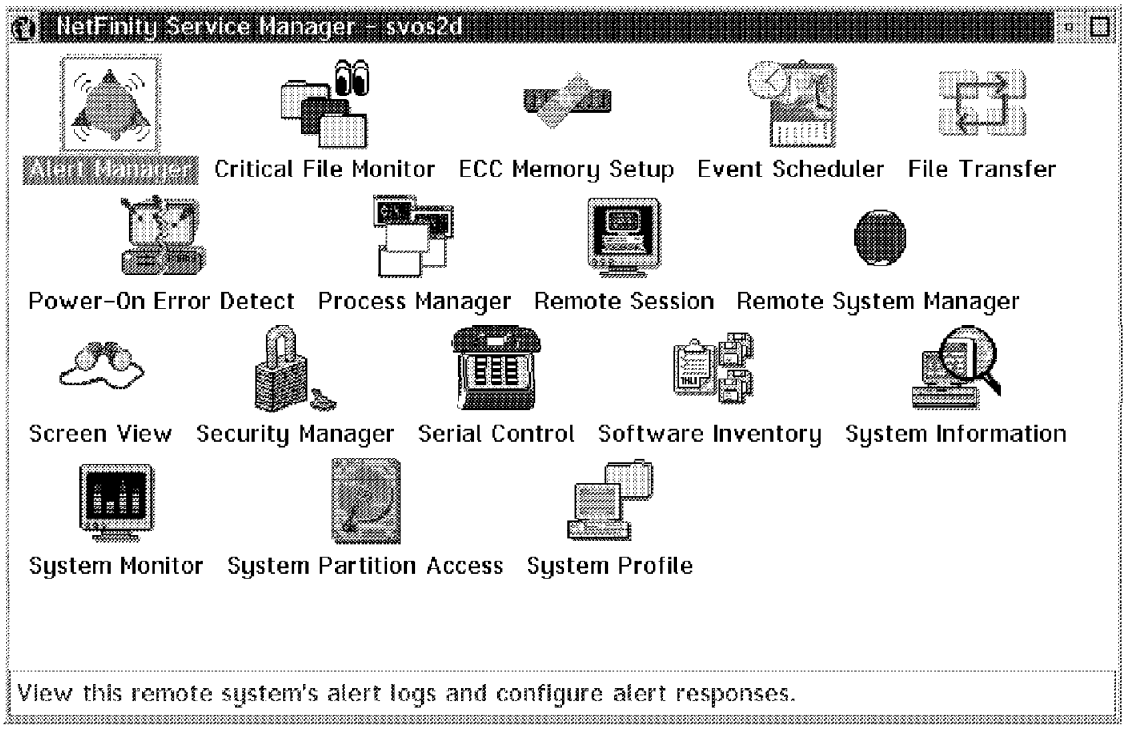


Figure 88. Remote Services Available to the NetFinity Manager

You will never see the file transfer function on the main window of the NetFinity manager, but when you try to manage any OS/2 or DOS/Windows client, you will see this icon appear. This is true even if the system you are going to manage is another manager. The file transfer function will let you send files or directories

between the two systems. You can send them from any drive. This includes NFS and LAN connected drives to any drive at the remote location. You can also delete files from the remote system using the file transfer window.

You can not send or receive files to the NetWare Server. You would want to send them to the NetWare client.

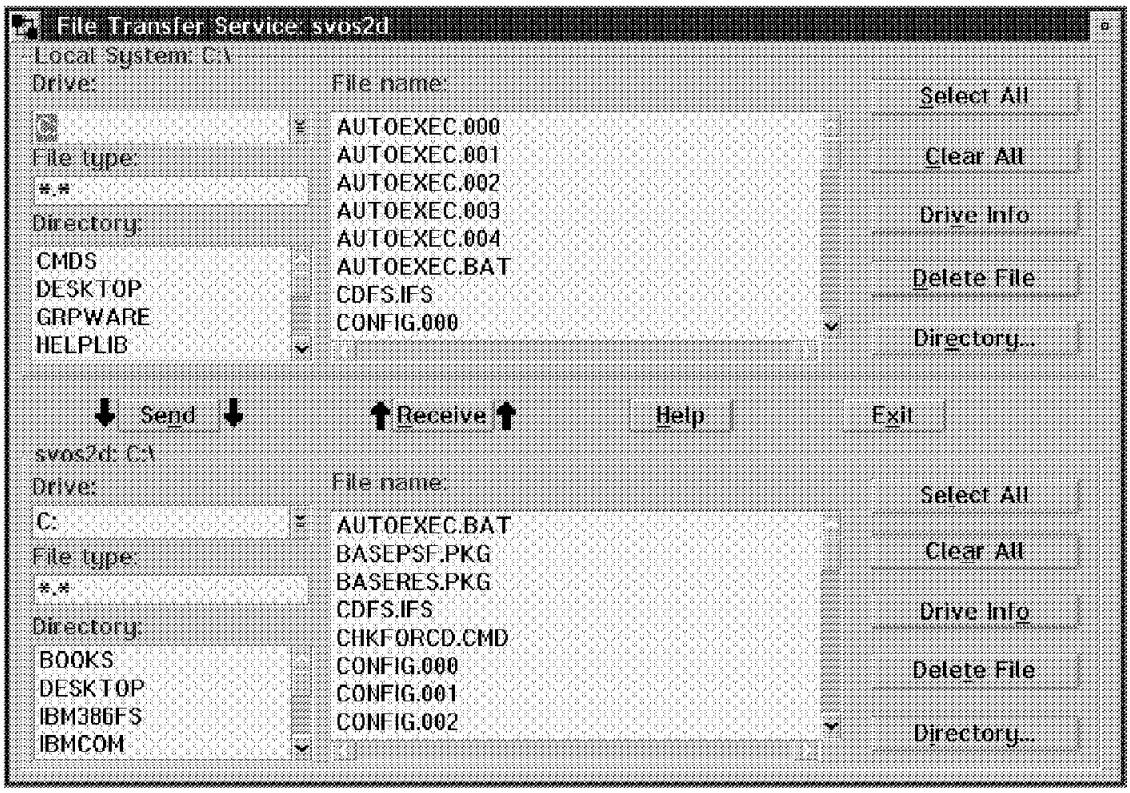


Figure 89. File Transfer

In addition to being able to use lots of services, you can also open up a remote window to the OS/2 client. Figure 90 on page 66 shows us an OS/2 window that is running on svos2d. Any command that you issue in that window will be run on the remote machine. You won't have access to Presentation Manager, but you can run commands and see the results in the window.

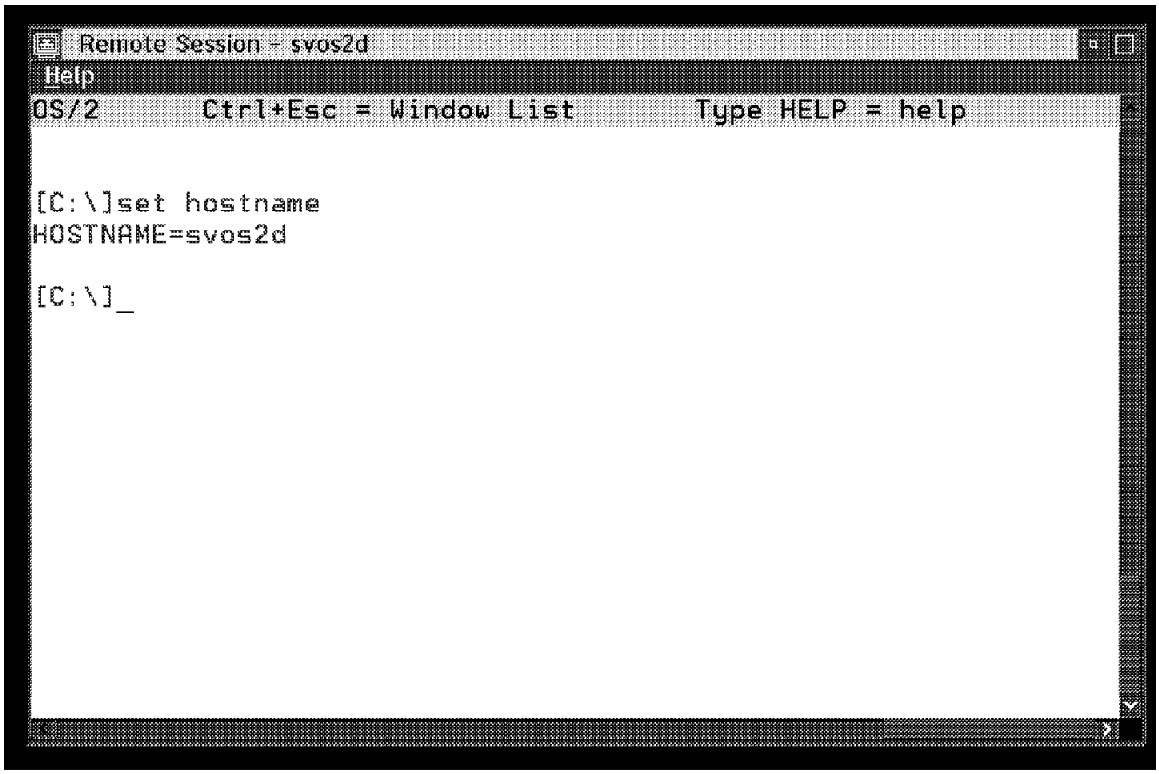


Figure 90. Remote Window

The system, svos2d, is a PS/2 Model 9595. It has a system partition that can be managed from the NetFinity manager.

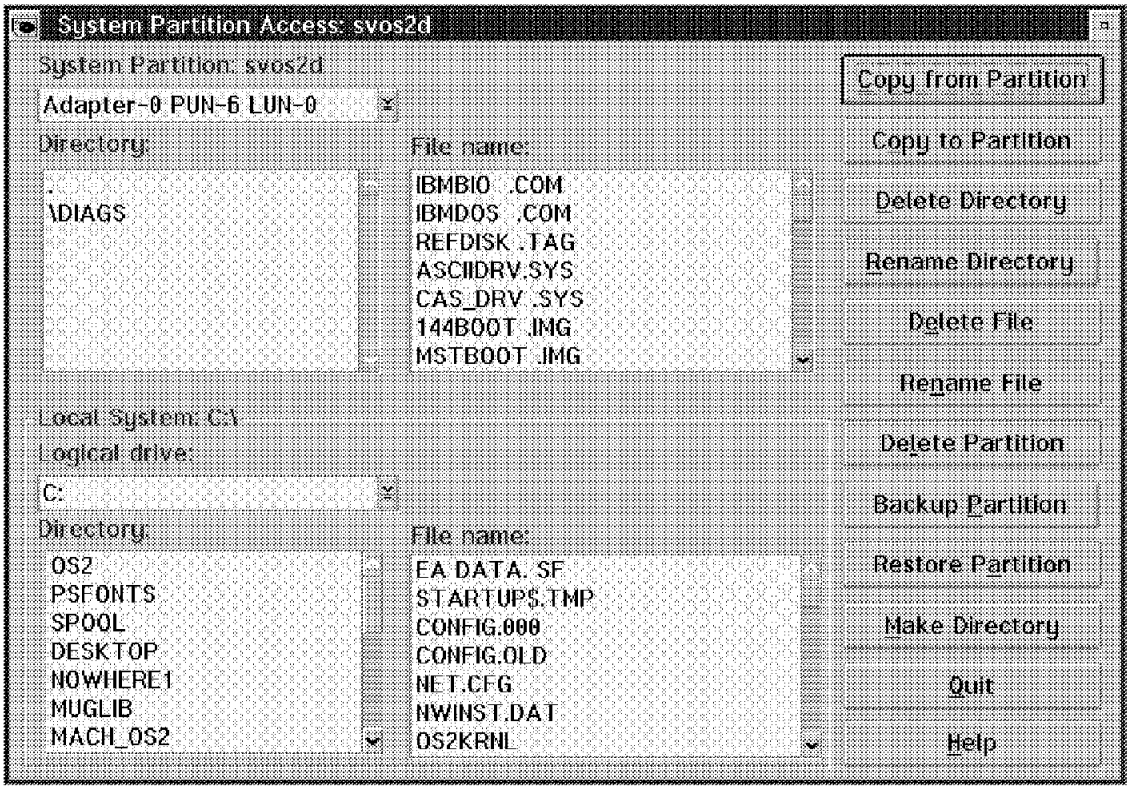


Figure 91. System Partition Access

If the remote user did not use NetFinity to set up their system profile, you can do this administrative function from your NetFinity manager. This helps you manage your assets.

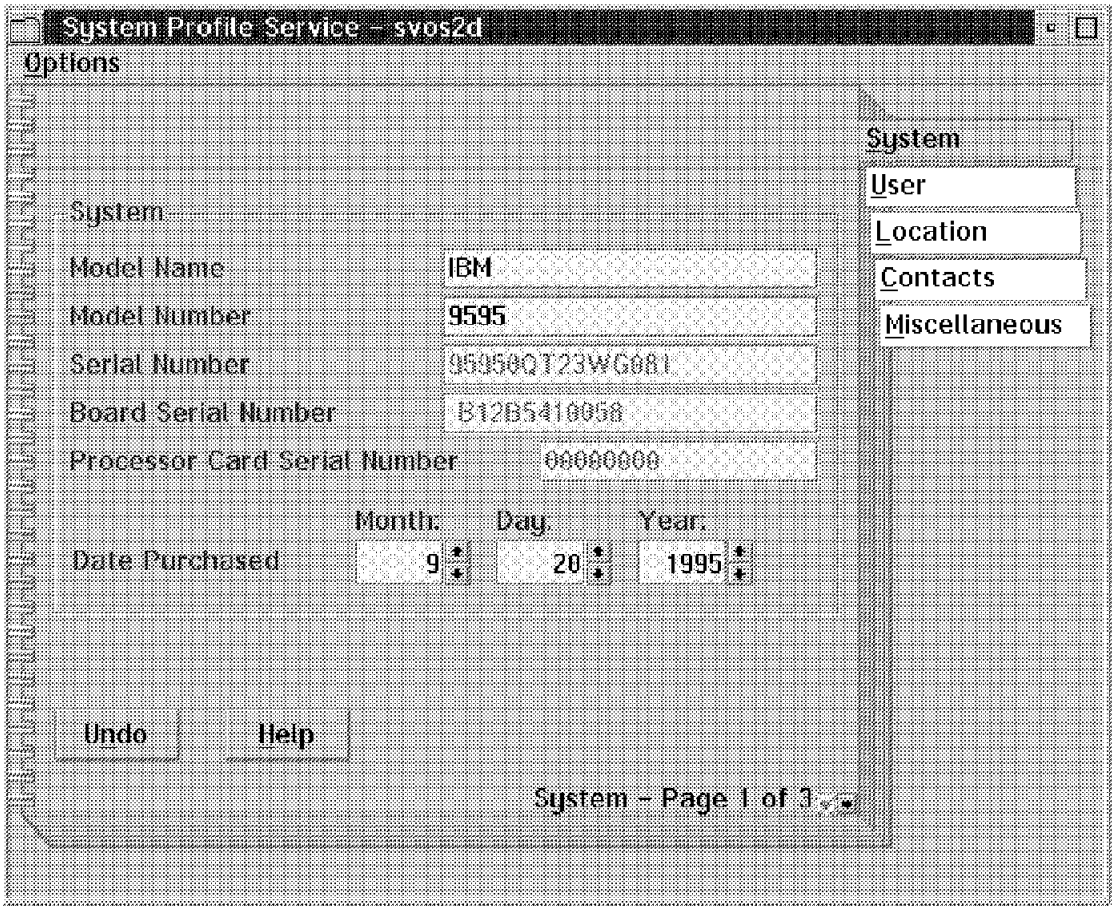


Figure 92. System Profile

By double-clicking on the **Software Inventory** icon on the Remote Systems Manager Services folder for svos2d, and using the pull-down option to discover the software inventory, we can see what software was installed on the OS/2 system. The inventory function does not discover all of the software, only software that matches patterns that have been set up already. You can expand the pattern matching by using the Dictionary pull-down menu.

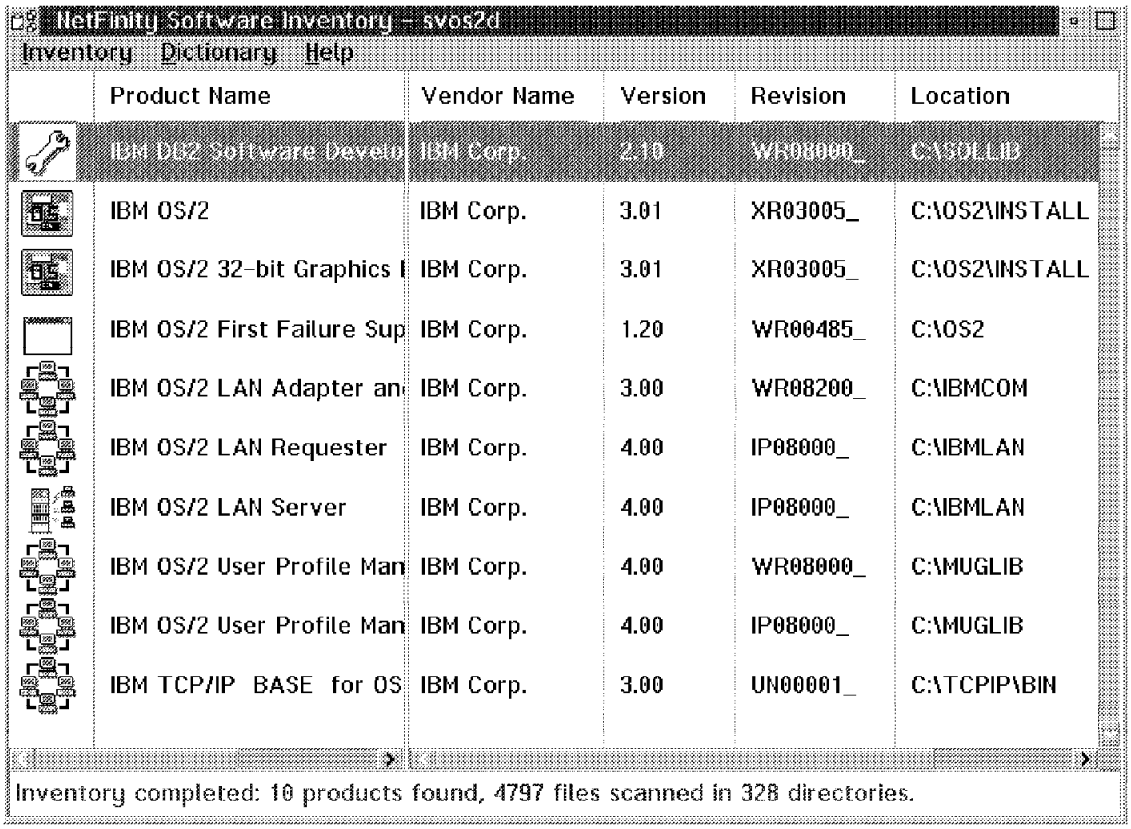


Figure 93. Software Inventory

Using the process manager remotely, we can list all of the tasks that are running in that OS/2 system. You can also do the same thing for DOS/Windows and NetWare systems. In Figure 94 on page 70 if you use the Process pull-down menu, you will see that you can run remote commands, send alerts, and kill tasks that are executing on the remote client.

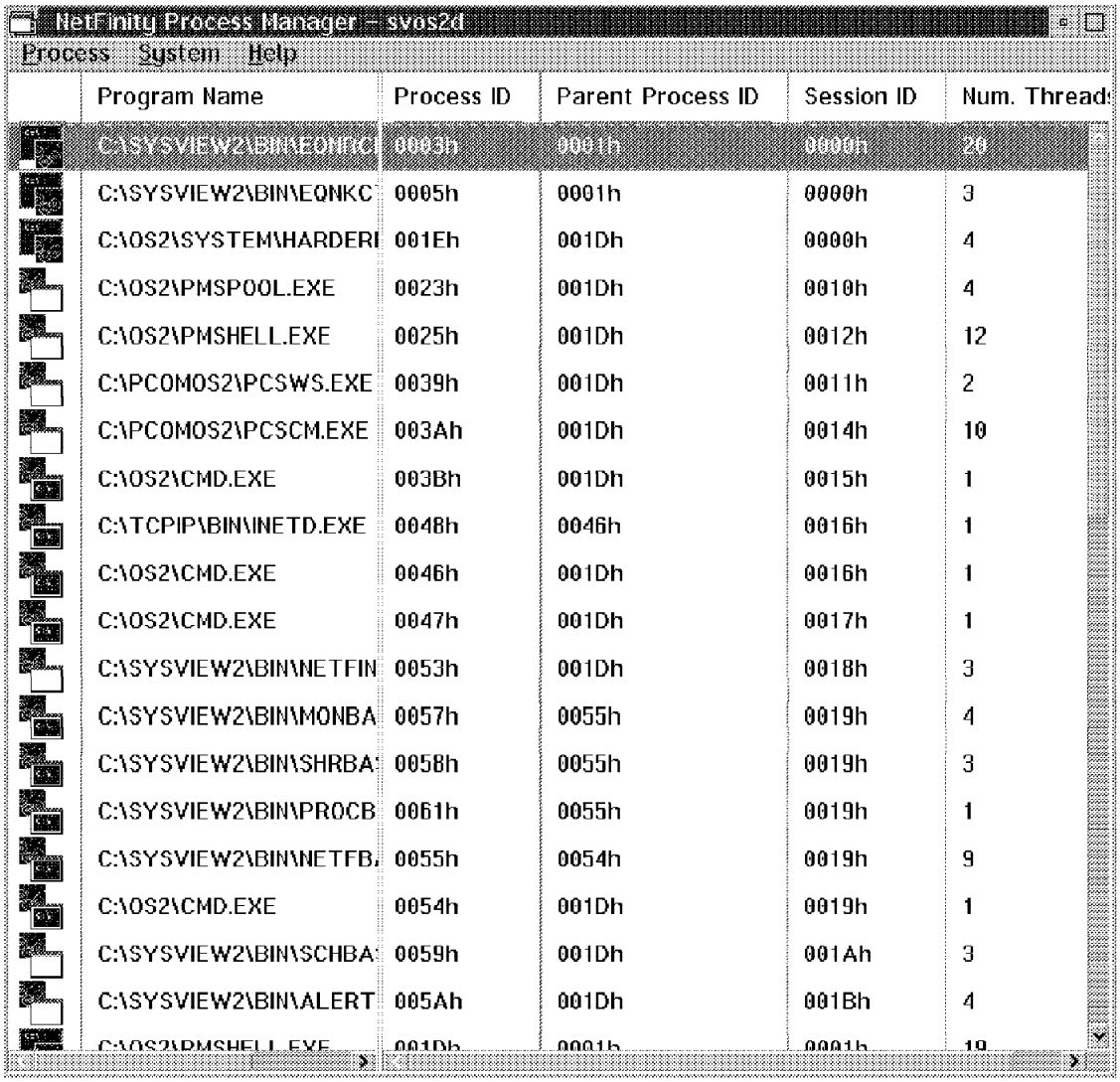


Figure 94. OS/2 Process Manager

In addition to managing OS/2 sessions, we can manage NetFinity DOS/Windows clients. Figure 95 on page 71 is an example of a remote session established through the Remote Systems Manager to the system called SVWIN02. The functions that are supported on this remote session are the icons that show up in the window.

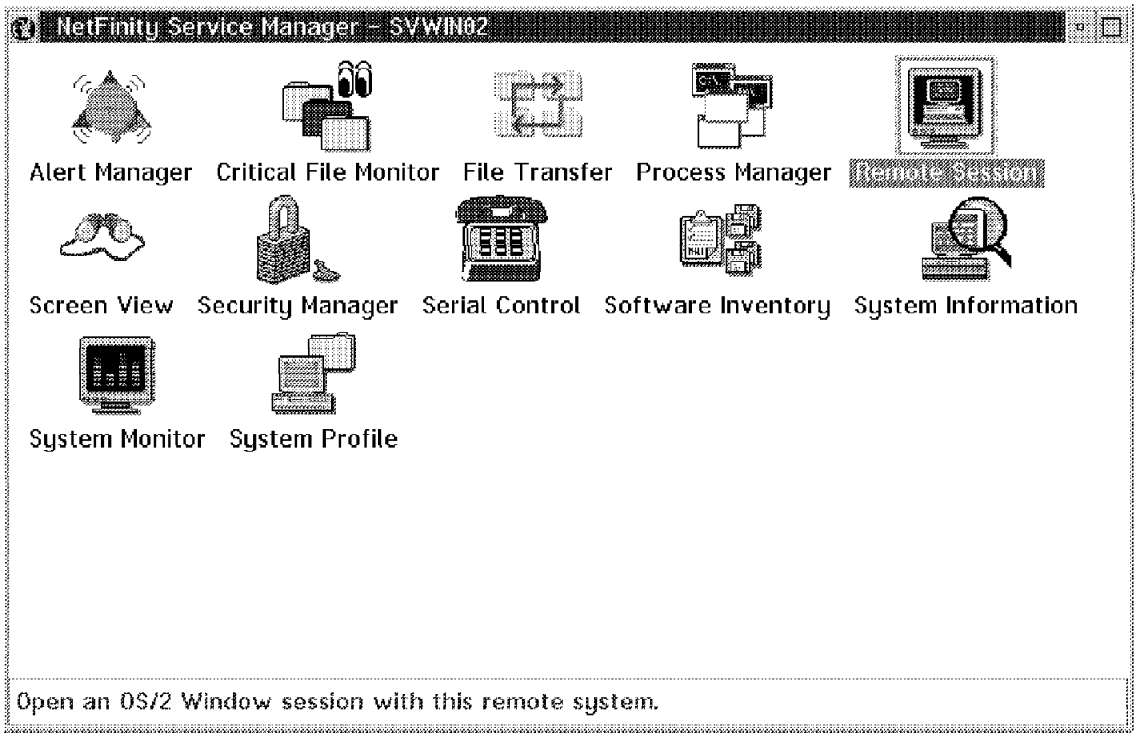


Figure 95. Managing a Remote Windows Client

You can manage remote tasks in a DOS/Windows environment just like you can manage the OS/2 tasks using the Process Manager.

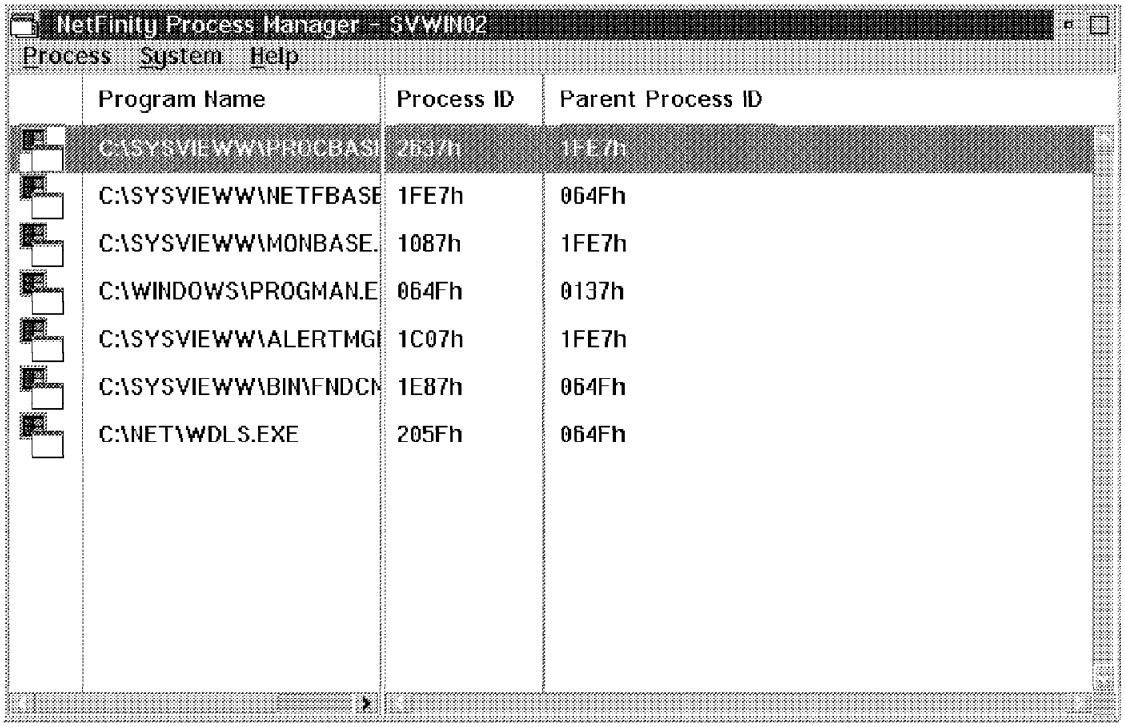


Figure 96. Remote Windows Processes

If at any time you get a call from a remote user who is having a problem with their system, you can use the Screen View function to capture an image of what is on their screen and have it show up on the NetFinity managing station. Figure 97 on page 72 is an example of the remote NetFinity DOS/Windows client. You can see the minimized icon for NetFinity in the lower left corner of the screen image.

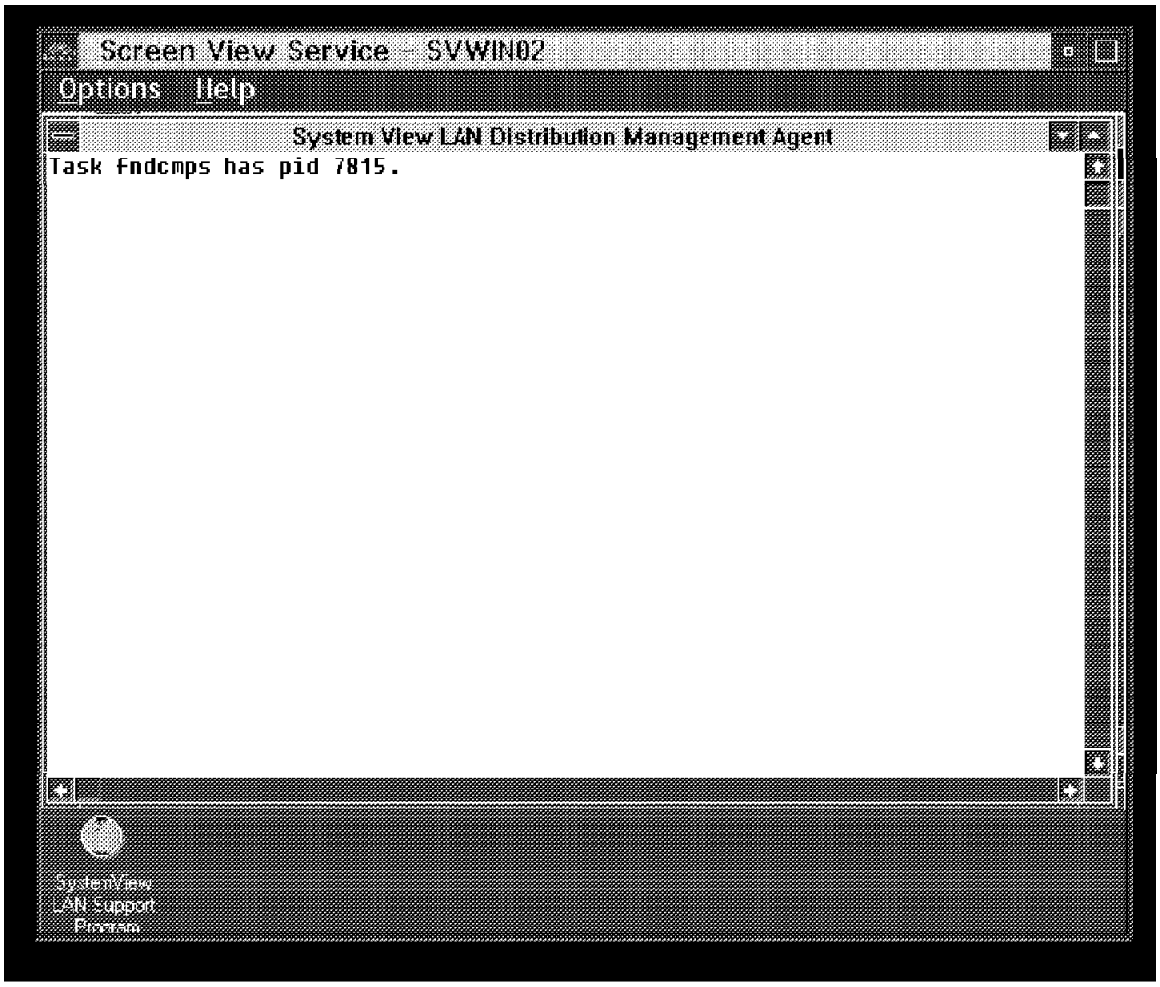


Figure 97. Screen View

Finally, from a client perspective, we can manage NetWare Servers. The example in Figure 98 on page 73 is for a NetWare V3.12 server. A lot of the services that are available in this folder are the same ones that were available for OS/2 and for DOS/Windows.

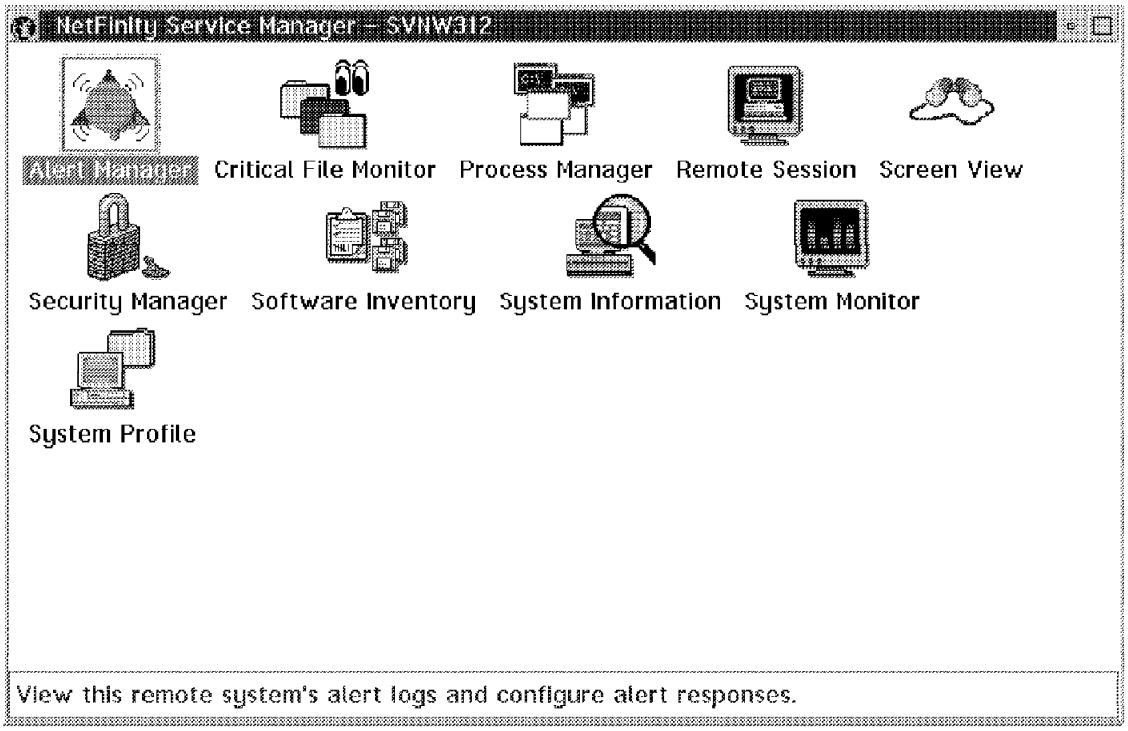


Figure 98. NetWare Clients

By clicking on the **Remote Session** icon in the NetFinity folder we can establish a remote session to the NetWare console and view information or issue commands. Figure 99 on page 74 is an example of looking at the NetWare Monitor NLM that we loaded using the remote window.

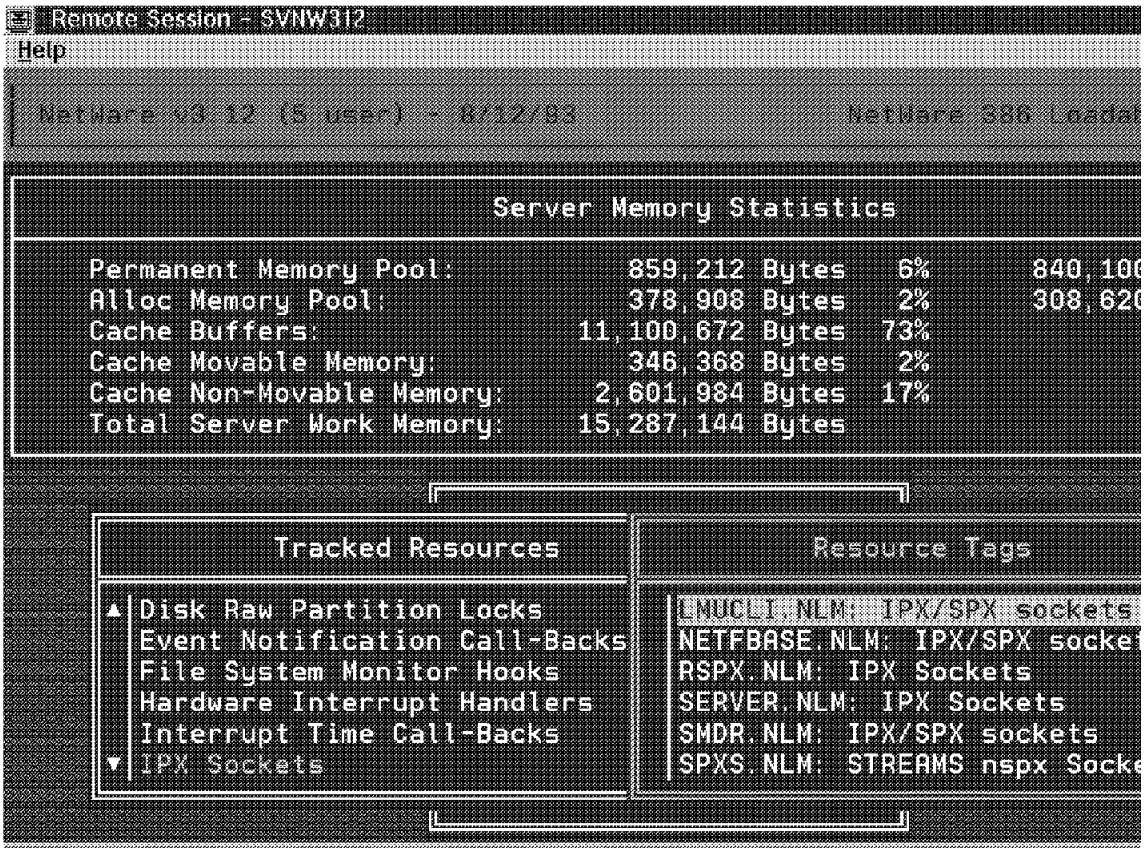


Figure 99. NetWare Console

Using the Remote Systems Manager and the Process Manager, we can get a list of all of the NLMs that are loaded on the server. We can unload the NLMs at any time.

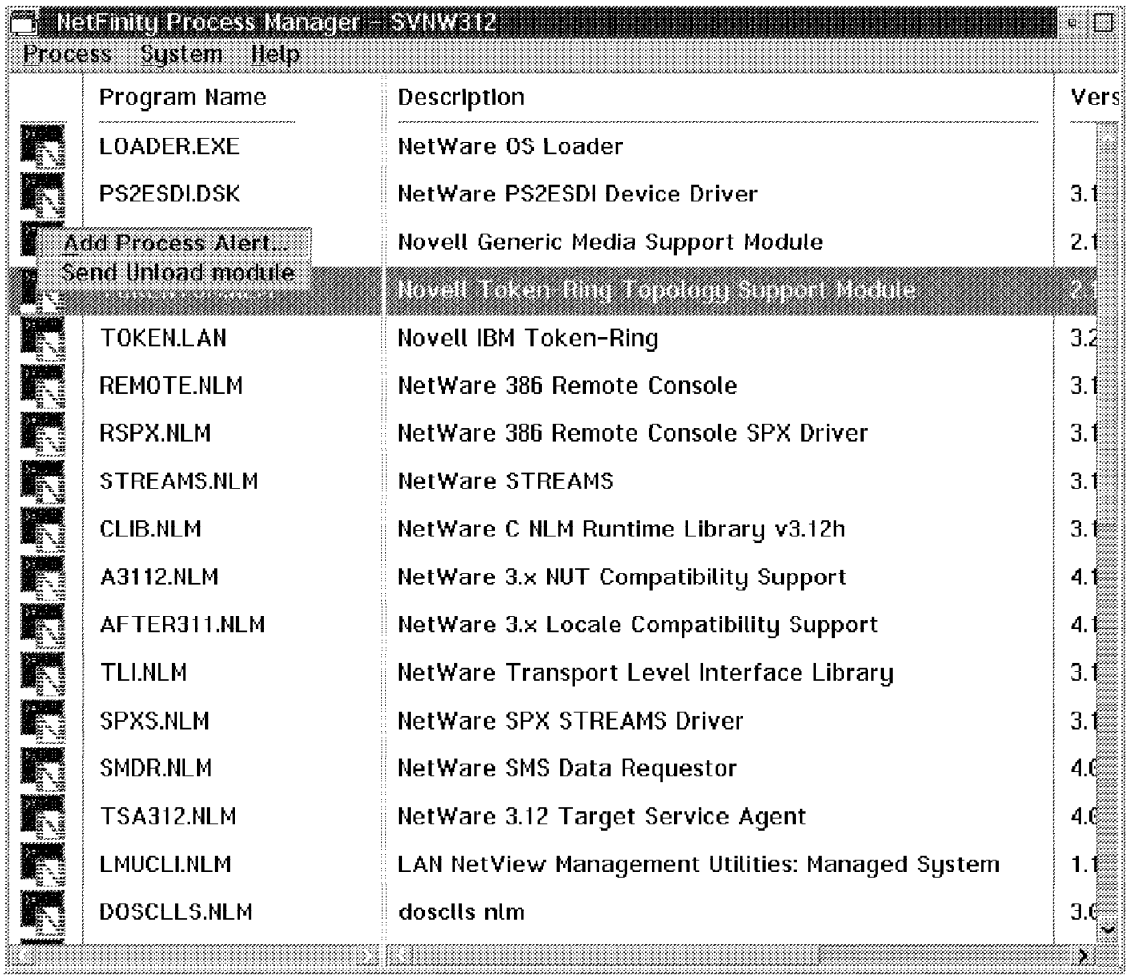


Figure 100. Process Manager for NetWare

We can also cause an alert to flow when the NLM gets loaded or unloaded. In addition, we can have an alert flow if the NLM doesn't load within a predefined period of time after the startup of NetFinity on the NetWare console. Any of the alerts can be sent back to the manager and can also show up on the local client.

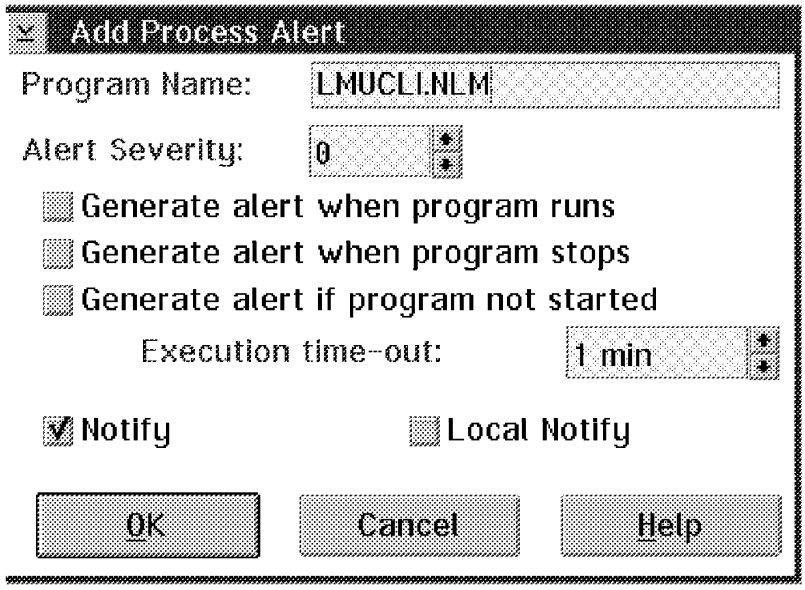


Figure 101. Process Alerts for the NetWare Client

You can monitor critical files that are on the NetWare server just like you can for an OS/2 and DOS/Windows client. Figure 102 on page 77 show you the default files that can be monitored. You can add any other files you wish to monitor by clicking on the button to the right of (monitor another file).

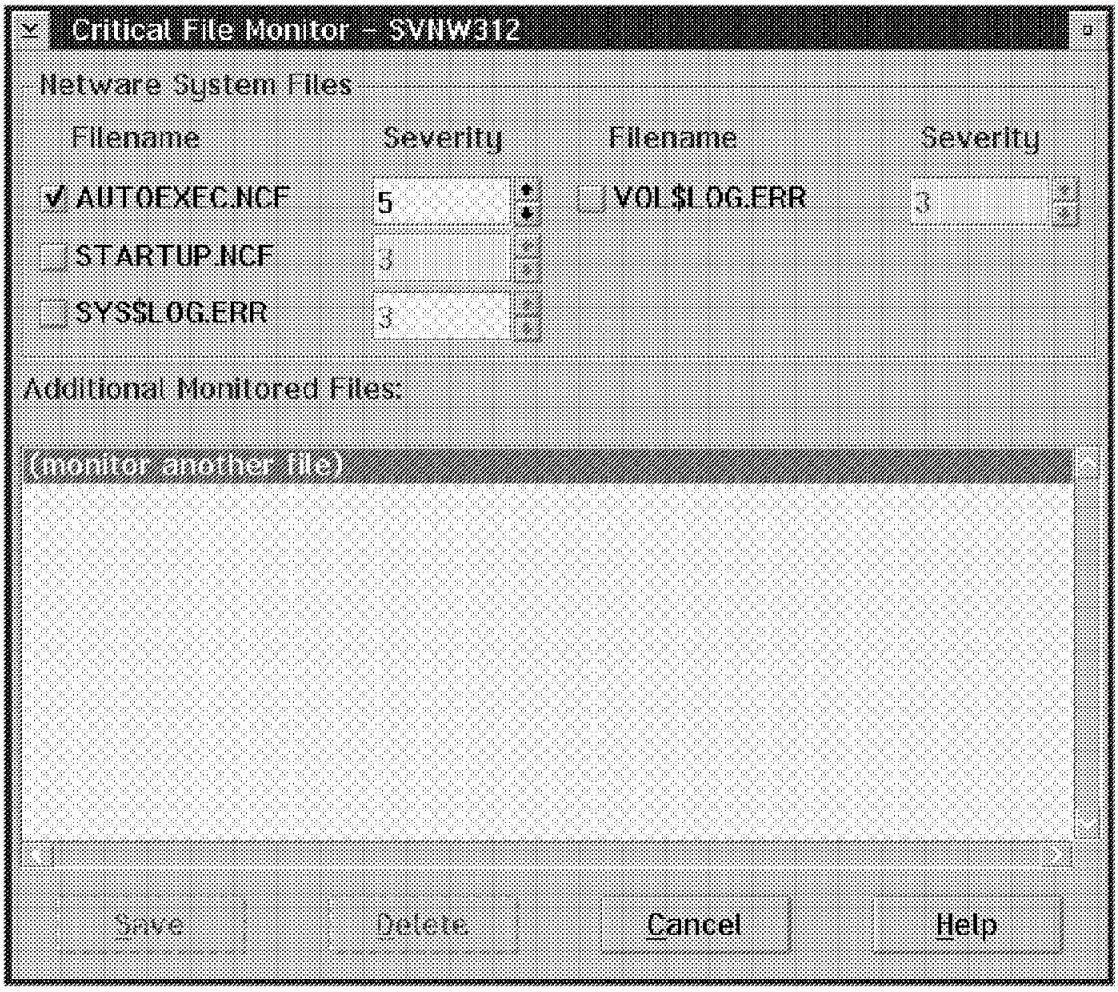


Figure 102. NetWare Critical Files

The monitors from the System Monitor service for NetWare are not the same that are on either OS/2 or DOS/Windows. Figure 103 on page 78 shows the default monitors that can be used on our NetWare V3.12 server. The monitors installed were determined by what we had installed on that system. Other monitors can be created using the NetFinity software developer's kit (SDK).

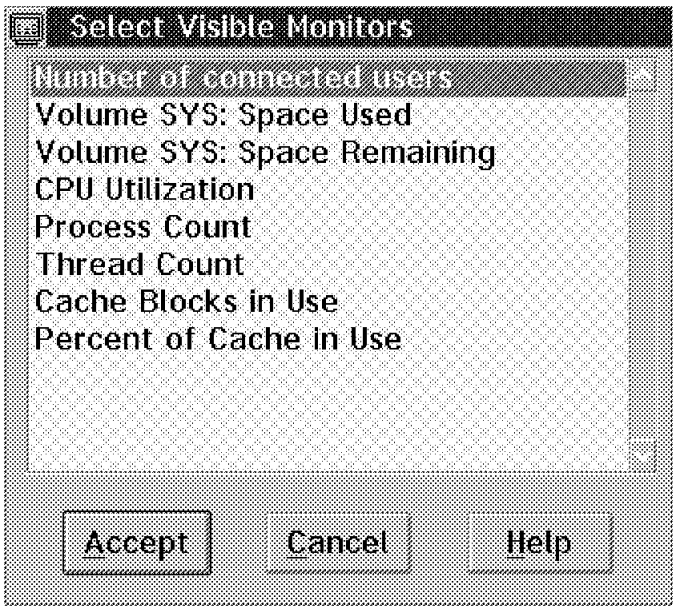


Figure 103. System Monitor for NetWare

4.2 Security Manager

Figure 104. Security Manager Icon

The Security Manager enables you to control who has remote access to the NetFinity services on your system. This is done by assigning passwords to specific user IDs, and then specifying which services each user ID has access to.

If an unauthorized remote user attempts to access your system, a screen will appear asking for a valid user ID and password. If a valid user ID and password are not provided, remote access to the system will not be granted.

Either during the installation of NetFinity, or after the installation you can specify that alerts will flow every time a remote NetFinity manager starts a session with your system. This is done by first double-clicking on the Network Driver Configuration window, then selecting **Options** and **Service Execution Alerts**. You will get an alert every time a remote NetFinity manager starts a NetFinity service at your NetFinity system.

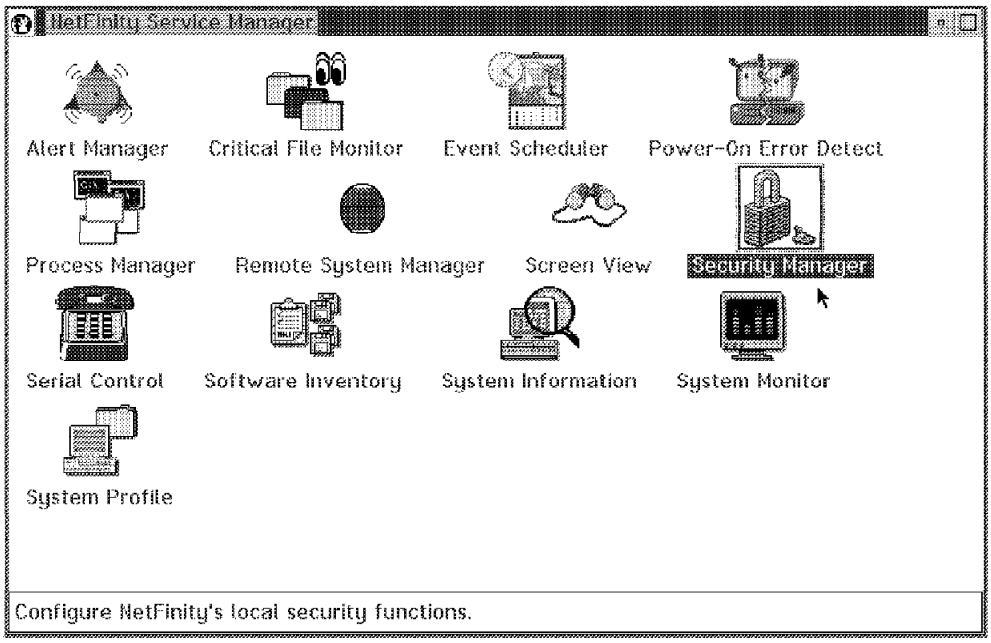


Figure 105. NetFinity Service Manager Folder

Double-click on the **Security Manager** object in the NetFinity service manager folder.

The following screen appears:

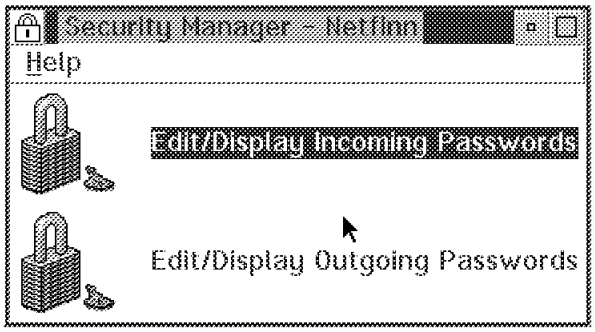


Figure 106. Security Manager Screen

Double-click on **Edit/Display Incoming**.

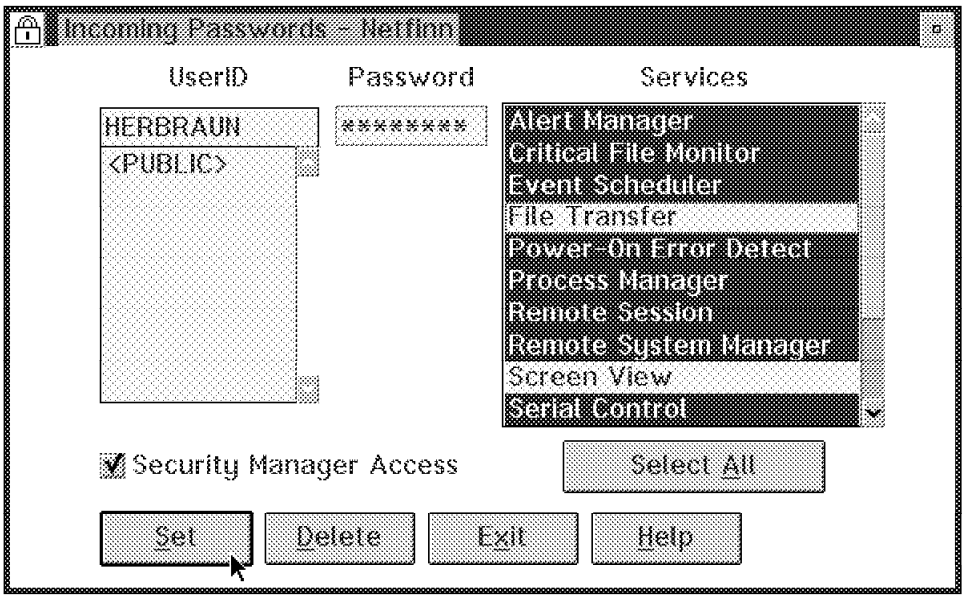


Figure 107. Incoming Password Window

If the Security Manager has not been pre-configured, there will be a user ID called <PUBLIC>. This is a general security access default setting. It enables any system using the corresponding outgoing user ID and password default combination to access all NetFinity Services on your system. Also, when a remote system user attempts to use the Remote System Manager′s icon to access your system and fails to match a corresponding incoming user ID and password, the remote user will receive access to any services allowed according to your <PUBLIC> configuration by default.

You can edit the list of services available from the <PUBLIC> user ID and password combination by selecting <PUBLIC> from the user ID selection list, selecting the services you wish to make available for public access, and then selecting **Set** to save your configuration. After setting the default services available to users (this might mean setting the default to no services), you should set up other user IDs for access to specific services, and an administration user ID with access to all services.

Attention

If you are in a production environment, change the default user ID PUBLIC to have no services, or change its password. Since the default is for PUBLIC to not require a password, and for it to have access to all of NetFinity′s services, there is a big security exposure if you don′t change the password. You are advised to do this at the end of the installation process, but it is very easy to miss that information on the screen.

Note

Before you remove the PUBLIC user ID and password, you should define another user ID and password with access to the Security Manager and its services. If you forget to do this, and you remove the PUBLIC user ID and password, you will have no remote access to the system.

To create a new manager user ID:

- Fill in the new user ID in the User ID field.
- Fill in the new password in the Password field.
- Click on the **Select All** button, or select the specific services available to this new user.
- Click on the **Security Manager Access** check box. If you are finished with the selection of the services,
- Click on the **Set** button.

  The steps to remove access for the <PUBLIC> user are as follows:

- Click on <**PUBLIC**>.
- Click on each service until none of them are highlighted.
- Click on the **Security Manager Access** check box so that it de-selects the box (the checkbox will now be empty).
- Click on the **Set** button.

> **Note**
>
> This grants access to the Security Manager configuration for this user ID. If you do not want to enable this function for this user ID, do not click on this check box. If this function is on, it will let this user reboot your system. So be careful with who can use this service. If you don't want to let users reboot your system or execute similar commands, you should also disable the access to the Remote System Manager. Otherwise, the user can start the commands from a remote session command.

Now the new user ID is created and the user ID PUBLIC is disabled for access your system.

The outgoing passwords window contains a list of all network addresses and user IDs that your Security Manager is currently configured to use when attempting to connect with a remote system. Use the outgoing password window to:

- Add a new outgoing password.
- Delete a previously configured outgoing password.
- Edit a previously configured outgoing password.

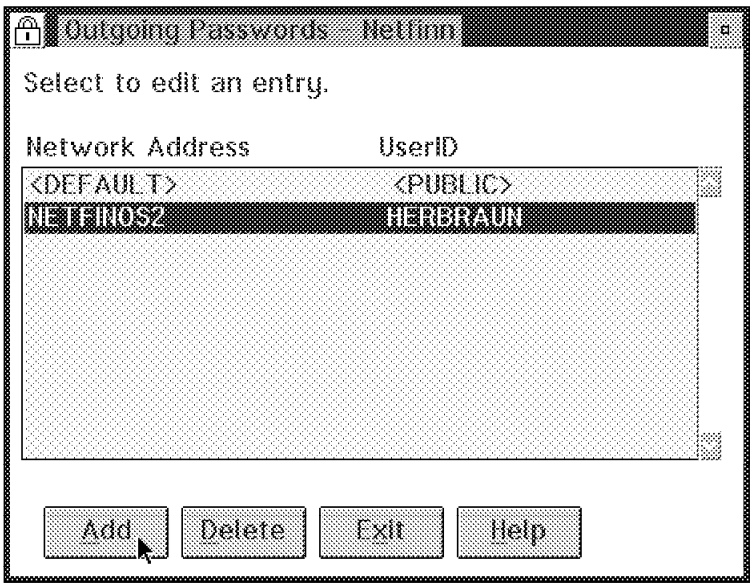


Figure 108. Outgoing Password Setup

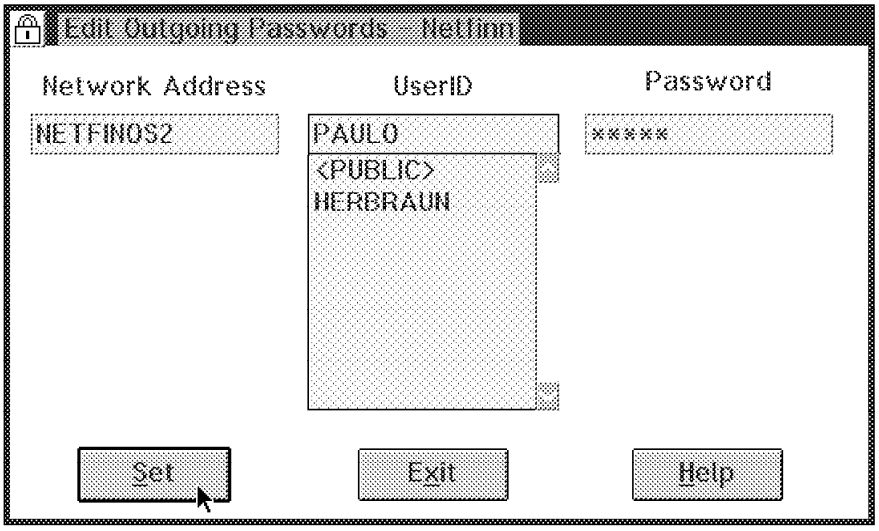


Figure 109. Editing Passwords for Remote System Connections

4.3 Screen View Service

Figure 110. Screen View Icon

Screen View enables you to view a snapshot of any NetFinity system that you have access to. This includes both remote access through the security manager

as well as your local system. When you use the Screen View function, the remote NetFinity system's video display is converted into a bit map and compressed. It is then transmitted to the local NetFinity manager system which displays a scalable window of the remote NetFinity system. This is particularly useful for remote system troubleshooting for a help desk.

The Screen View service has the following options:

- Scale screen shots to any size up to full screen.
- Save screen shots to a file for later reference.
- Load screen shot that were previously saved.
- Capture new screens on demand.

4.3.1 Screen View Service on Local NetFinity Systems

The Screen View service object is in the NetFinity Service Manager folder.

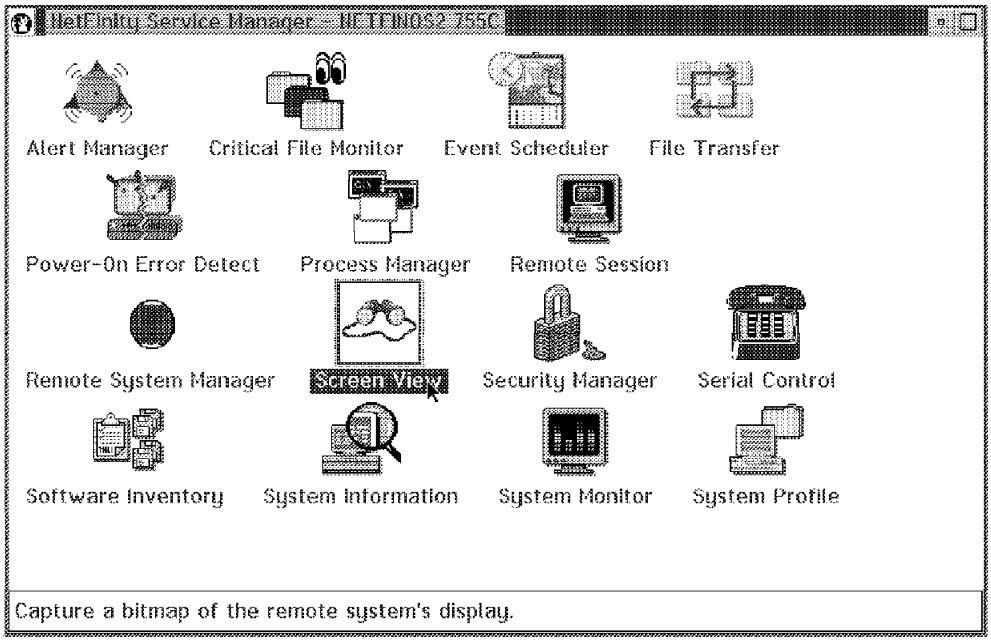


Figure 111. NetFinity Service Manager Folder with Screen View

- Double-click on the **Screen View** object in the NetFinity Service Manager folder and you get a screen snapshot of your own local NetFinity system as shown in Figure 112 on page 84.

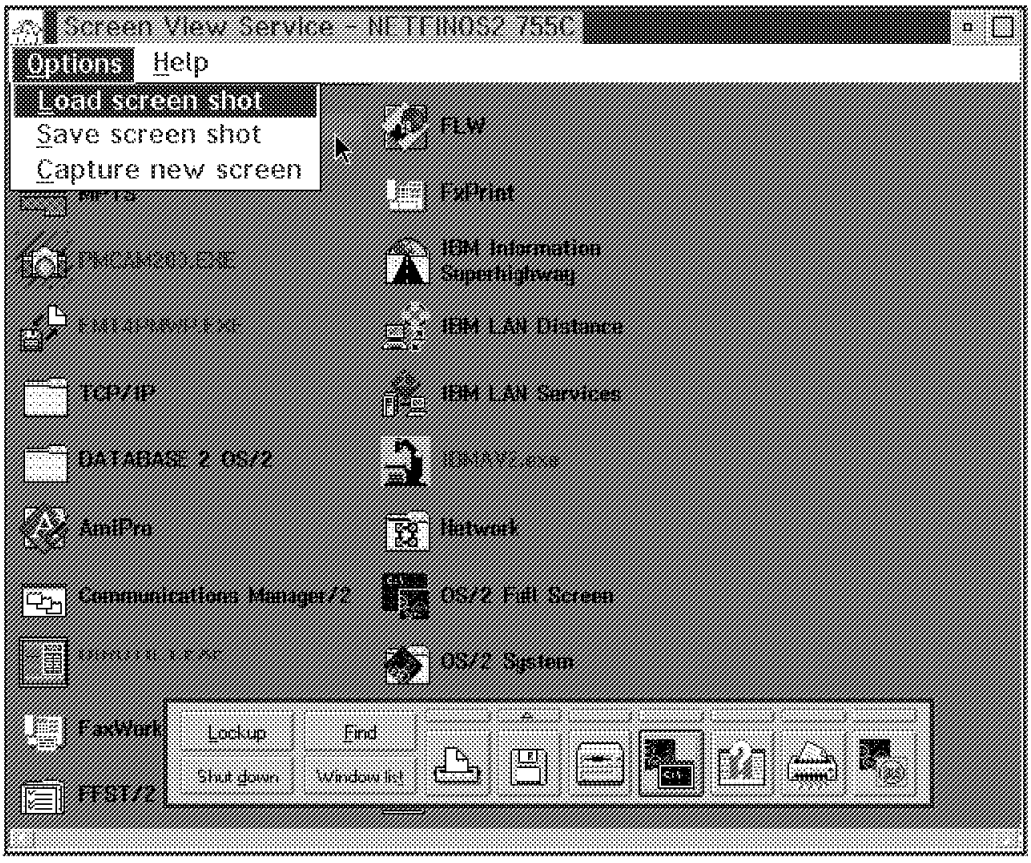


Figure 112. Screen View Service Window: Locally

- If you click on **Options** in the title bar you will get a pull-down menu with the following options:
  - Load screen shot
  - Save screen shot
  - Capture new screen
- Click on **Load screen shot**.

  The following Load Screen Shot window appears:

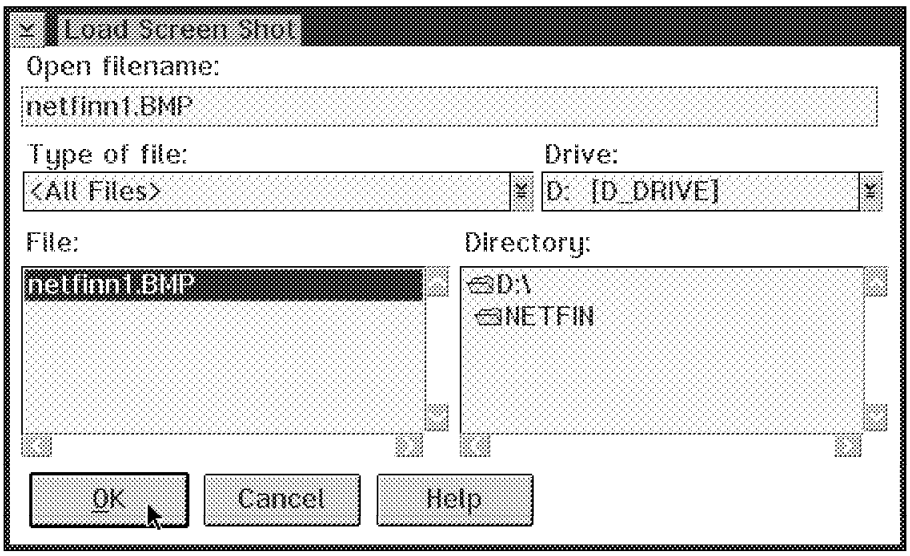


Figure 113. Load Screen Shot

- Enter the name of the screen snapshot you want to look at.
- Select the drive. In this case it is the D drive.
- Double-click on the directory where you want to put the screen capture.
- When you click on the filename, it appears in the Open filename field.
- Click on **OK** and the selected snapshot will be loaded.

  If you want to save a screen shot:
- Click on **Save screen shot** in the options pull-down menu in Figure 112 on page 84.

  The following screen capture appears:

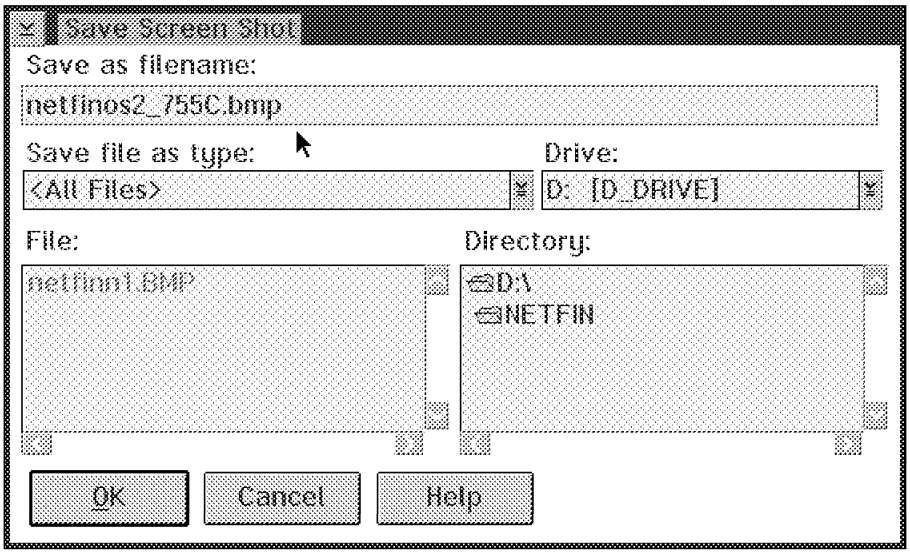


Figure 114. Save Screen Shot

- Enter the name of the screen capture you want to save.
- Select the drive to save it in.

- Double-click on the directory under which you want to save the snapshot.
- Click on the filename in the appropriate drive and directory you want to overwrite.
- Click on **OK** and the screen capture will be saved.

  If you want capture a new screen:

- Click on **Capture new screen** in the options pull-down menu in Figure 112 on page 84.

  The new screen will be captured.

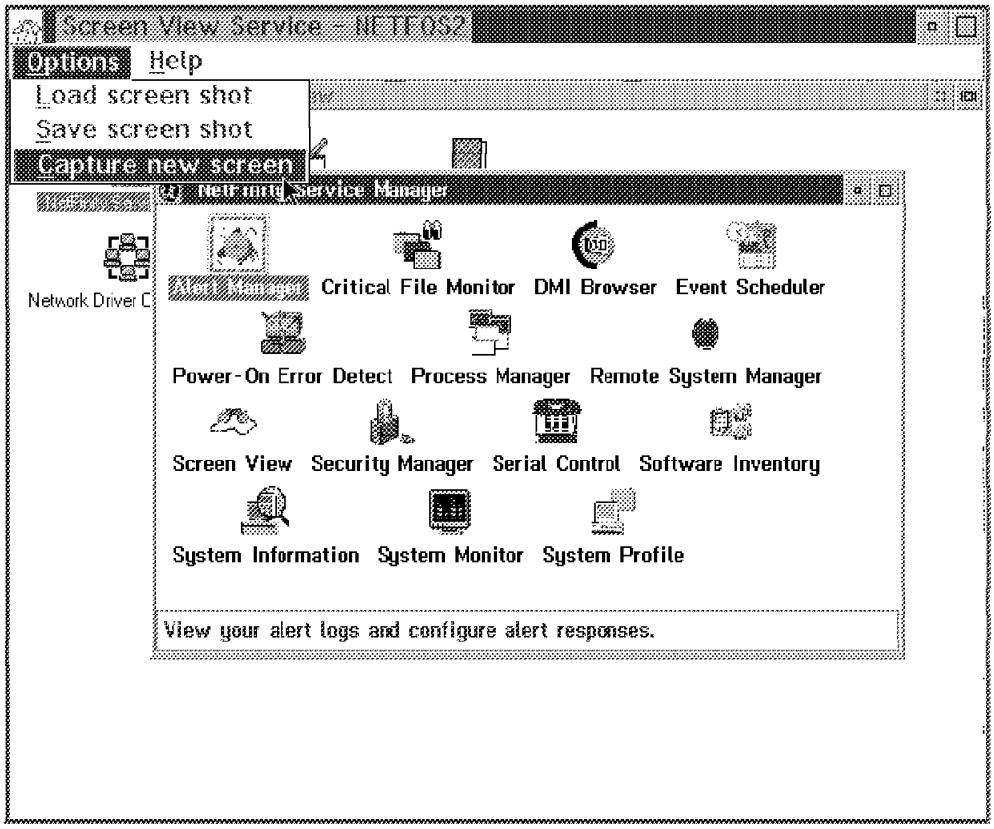


Figure 115. Capture New Screen Option

4.3.2 Screen View Service on Remote Monitored NetFinity Systems

A screen snapshot can also be taken of any remote NetFinity system. You must first select the desired remote NetFinity system using the Remote System Manager service before you can take a screen snapshot. This assumes that the NetFinity Manager has access to the remote systems. They will either have to know the current password or have accessed the system in the past and saved the password in their profile.

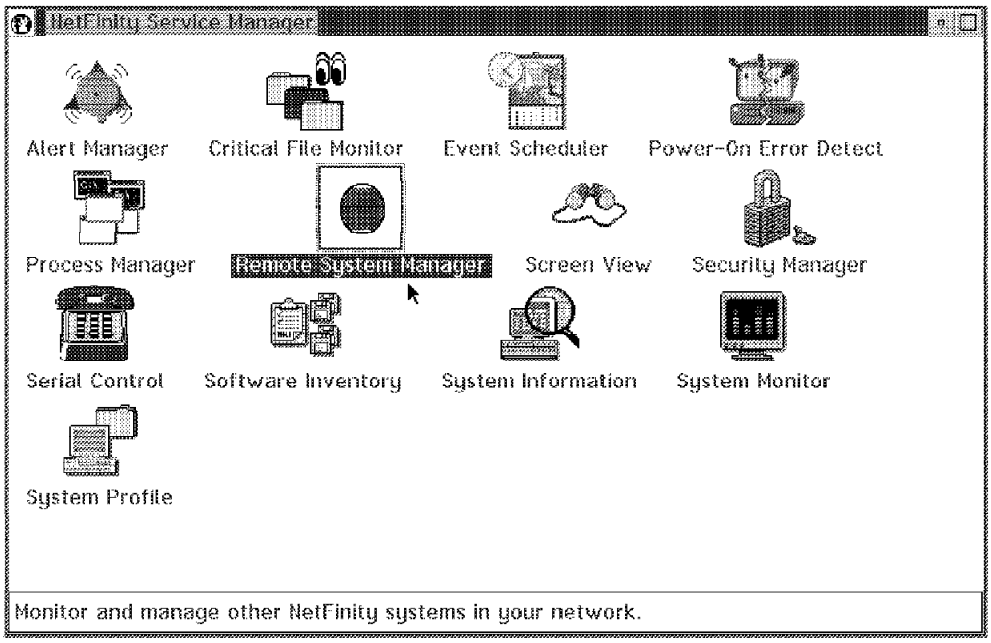


Figure 116. NetFinity Service Manager

- Double-click on the **Remote System Manager** object in the NetFinity Service Manager folder.

  We had already defined a few groups on this system, so you see four icons representing groups of systems that have NetFinity Managers and clients. You can see the systems that are in the Raleigh ITSO folder if you double-click on the **Raleigh ITSO** icon. The results are shown in Figure 118 on page 88.

  The System Group Management window with the predefined groups is shown in Figure 117.

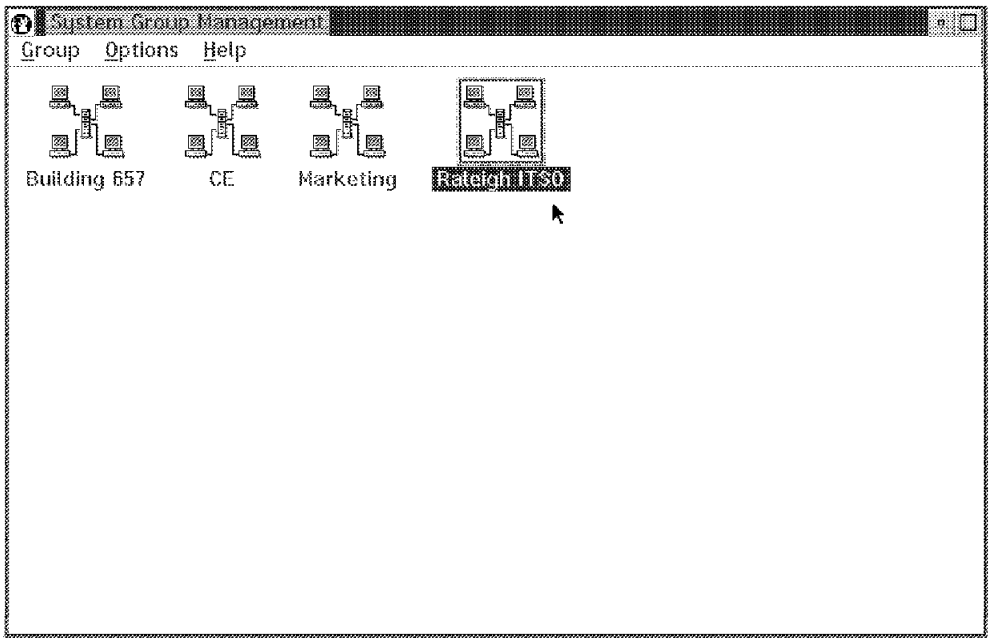


Figure 117. System Group Management

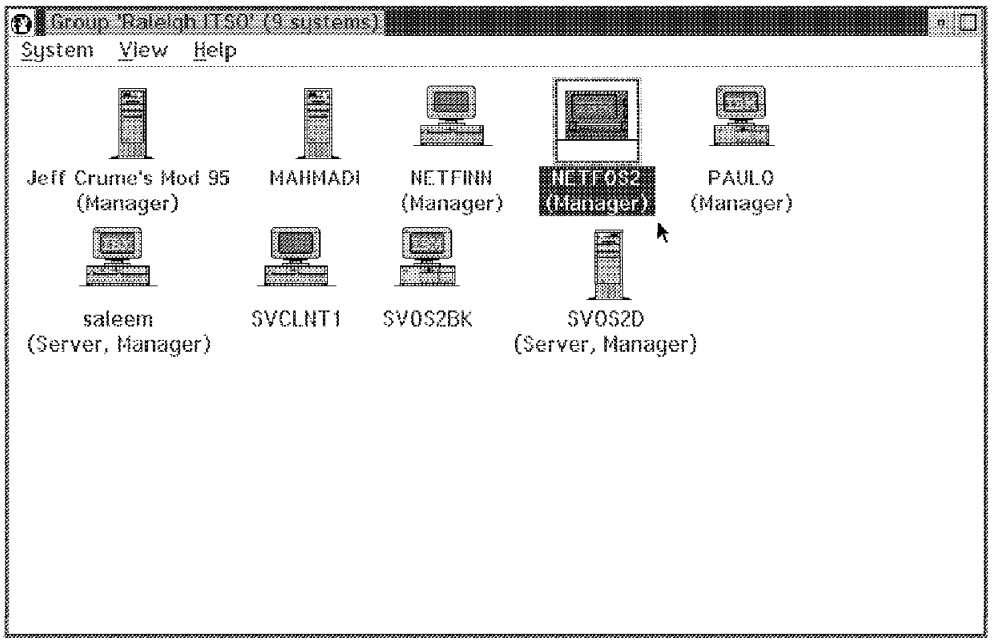


Figure 118. Group Raleigh ITSO

- In this example the system with the system name NETFOS2 was selected.
- Double-click on the system NETFOS2 and the NetFinity Service Manager from NETFOS2 window will appear. The title bar of the NetFinity Service Manager window shows which system the NetFinity Service Manager window is monitoring. Here the system name NETFOS2 is next to the text NetFinity Service Manager. If the window that you are looking at doesn't have a system name in it, then you are looking the services for the local NetFinity manager.

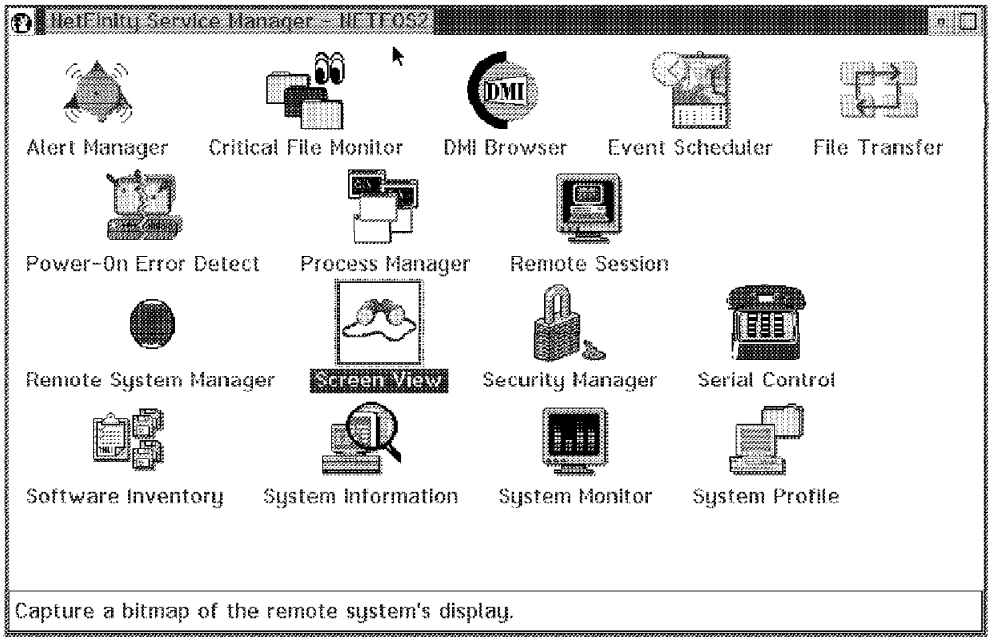


Figure 119. NetFinity Service Manager Window from NETFOS2

- Double-click on the **Screen View** manager object in the NetFinity manager folder representing system NETFINN. The following NetFinity Screen View Service window from the remote system NETFINN appears:

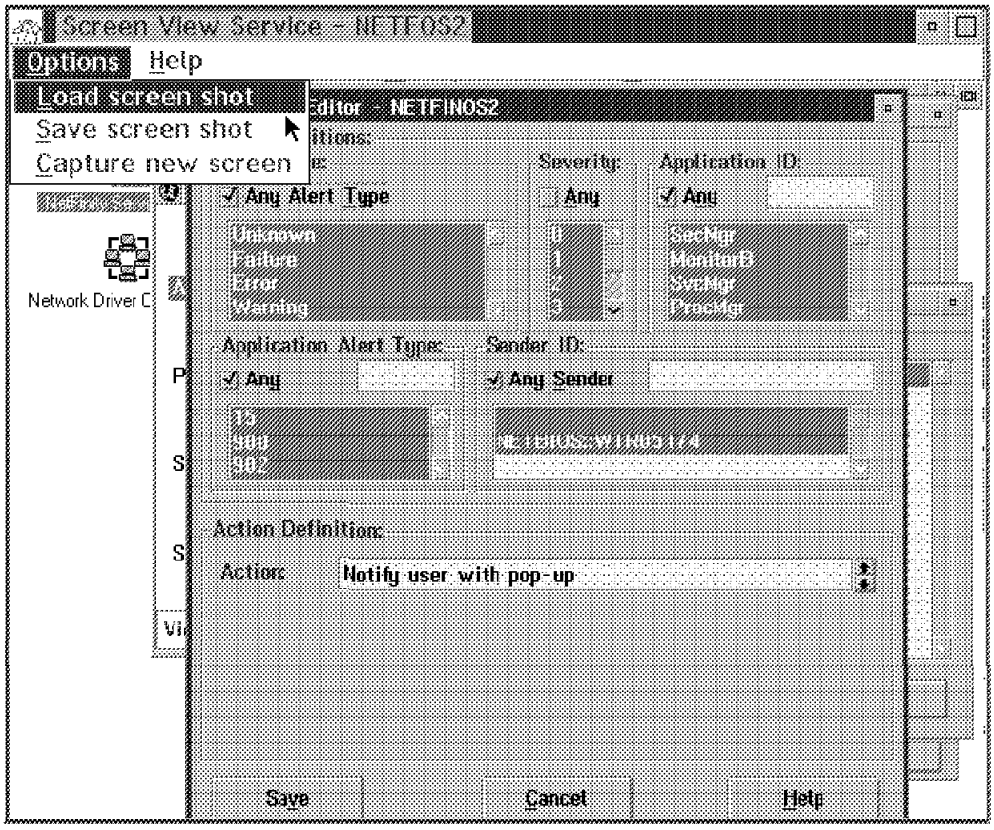


Figure 120. Screen View from NETFOS2

- Click on **Options** in the title bar and you get a pull-down menu with the following options:
  - Load screen shot
  - Save screen shot
  - Capture new screen
- Click on **Load Screen shot**

Note

You can load multiple screen shots from different NetFinity Systems. It is sometimes helpful to compare two screen shots from different systems for trouble shooting.

The following Load Screen Shot window appears:

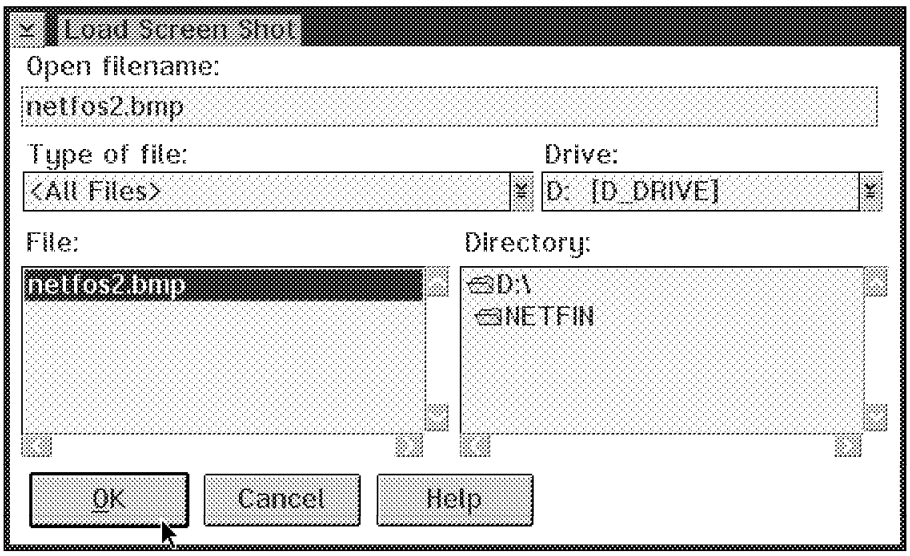


Figure 121. Load Screen Shot

- Enter the name of the screen snapshot you want to look at.
- Select the drive that the screen shot is on.
- Double-click on the directory where you want to save the image.
- Click on the filename.
- Click on **OK** and the selected snapshot will be loaded.

  If you want to save the Screen Shot:
- Click on **Save screen shot** in the options pull-down menu in Figure 112 on page 84.

  The following window appears:

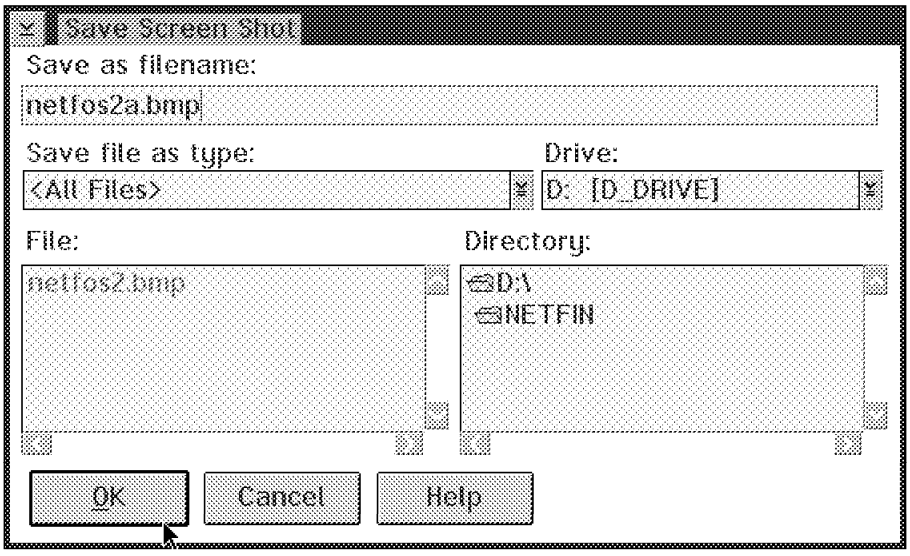


Figure 122. Save Screen Shot

Chapter 5. Hardware Manager Functions

This chapter describes the following management functions that can be performed from the NetFinity Manager using NetFinity V3.0 that relate to hardware functions:

- Power-On Error Detect
- ECC Memory Setup
- RAID Manager

5.1 Power-On Error Detection

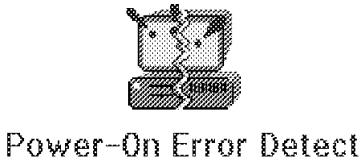


Figure 123. Power-On Error Detect Icon

When IBM Micro Channel systems are powered-on, they perform a series of system hardware and configuration tests called the power-on self test or POST. If an error is detected, the system records the error and takes some appropriate action, such as loading its configuration utility program from the System Partition.

In the case, if no one is present when the utilities are loaded, or if the system's user is unfamiliar with POST errors, the problem could go uncorrected for some time, leaving the system offline and unproductive.

If the Power-On Error Detect drivers are installed on an IBM Micro Channel system and an error is detected during POST, the system broadcasts a request for help message to the LAN. This message contains valuable information about the system that generated the POST error and about the POST error itself. Systems that have these drivers installed will also send a similar message out onto the LAN when their System Partitions are accessed during system startup (for example, when the user pressed Control-Alt-Insert during startup).

The Power-On Error Detect service receives these messages from the LAN and enables you to quickly determine:

- What system generated the POST error or System Partition access message.
- What POST error (if any) was reported.
- What caused the POST error.

The message also contains hardware configuration information that enables you to determine the possible cause of the problem. This can minimize system down time and the loss of productivity that would result without quick problem determination and resolution.

The Power-On Error Detect service is started from the NetFinity Service Manager folder.

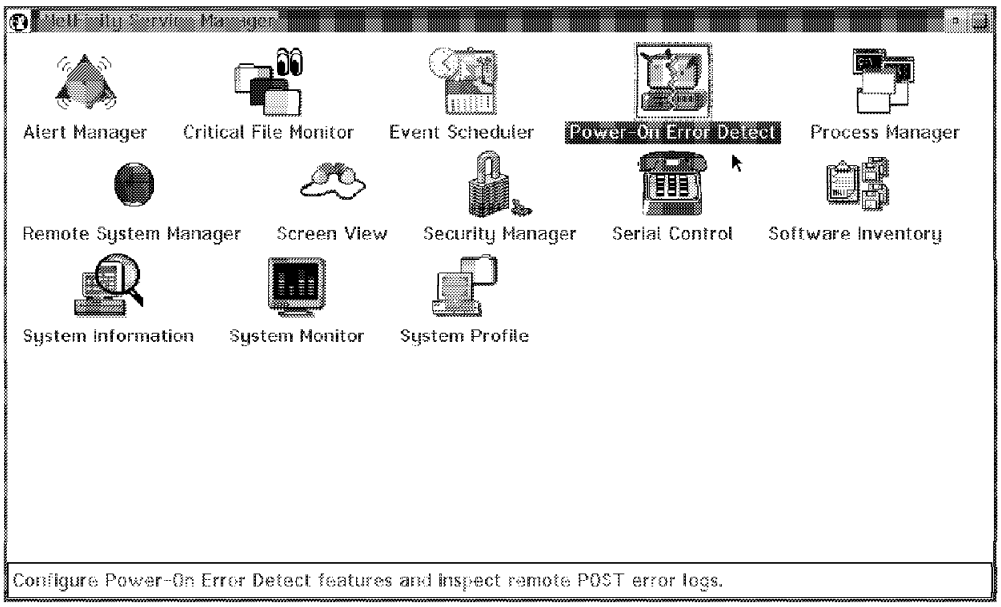


Figure 124. NetFinity Service Manager Window

- To start the Power-On Error Detect service, double-click on the **Power-On Error Detect** object in the **NetFinity Service Manager** folder. The following window appears.

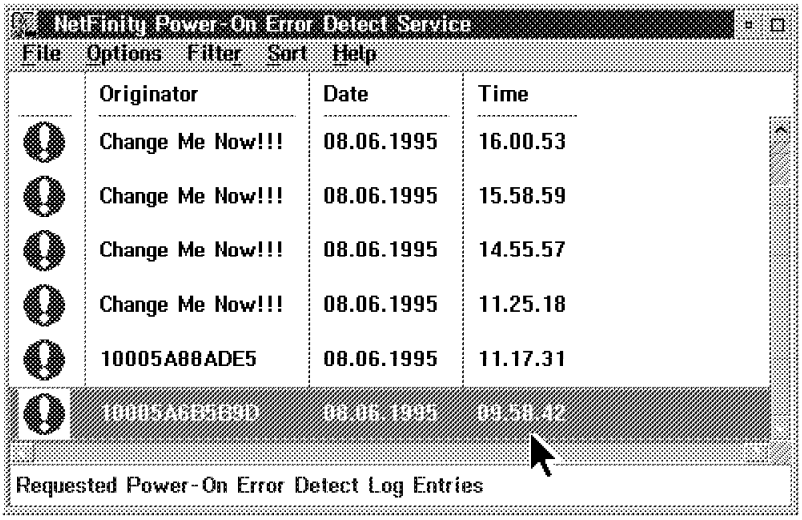


Figure 125. NetFinity Power-On Error Detect Service Window

The Power-On Error Detect log contains a list of all remote POST Errors that it has received.

The POED alerts that are generated due to a POST error have an exclamation point in a red circle in column 1. The Power-On Error Detect log entries that are displayed and the order in which they are displayed can be altered to suit your needs by selecting the Filter or Sort options from the pull-down menu.

Note

The Power-On Error Detect service is always included in the NetFinity Manager Services. To get a Power-On Error Detect Alert you must install a driver in the NetFinity system that has Micro Channel, a System Partition and NetBIOS running.

To install the support:

- Reboot from the POED Driver Installation Diskette.

  It is included in the NetFinity Package. Type 1 to install or type 2 to uninstall the driver.

- Press Enter.
- Remove the diskette from the diskette drive.
- Reboot the NetFinity system.

In order to send POED you do not need NetFinity. If you want to see the POED alerts, you will need NetFinity.

Each entry in the Power-On Error Detect log consists of a date, time, and originator value. To view more detailed information about an entry:

- Double-click on the entry from the Power-On Error Detect log.

  This will open the Power on Error Detect Entry Contents window.

  In the following window, the Power-On Error Detect log entry came from 10005A6B5B9D.

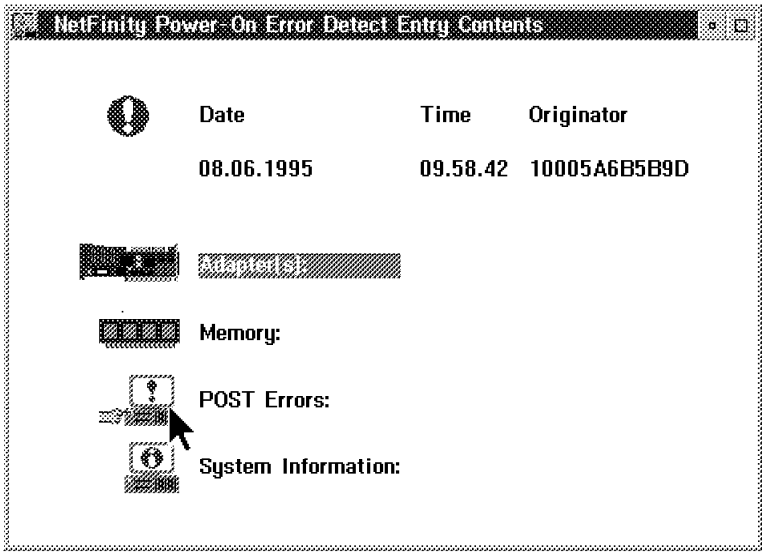


Figure 126. NetFinity Power-On Error Detect Entry Window

- You can then select from a variety of sub-entries to get additional information:
  - Adapters
  - Memory
  - POST Errors
  - System Information

These all provide additional detailed information.

- To get detailed information, double-click on the **POST Errors:** icon.

  The following window appears:

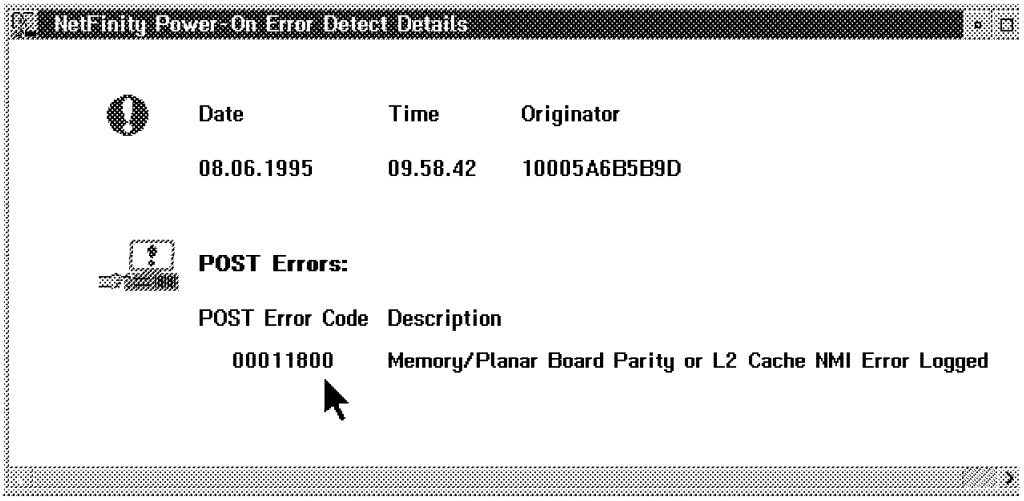


Figure 127. NetFinity Power-On Error Detect Details Window

- You can see the POST Error Code and a short description.

  This topic will not appear if the hardware error log is empty or if the POST error was produced as a result of changing memory or removing an adapter.

  To get more information about the adapters installed in this system close the current window, and go back to the Contents window.

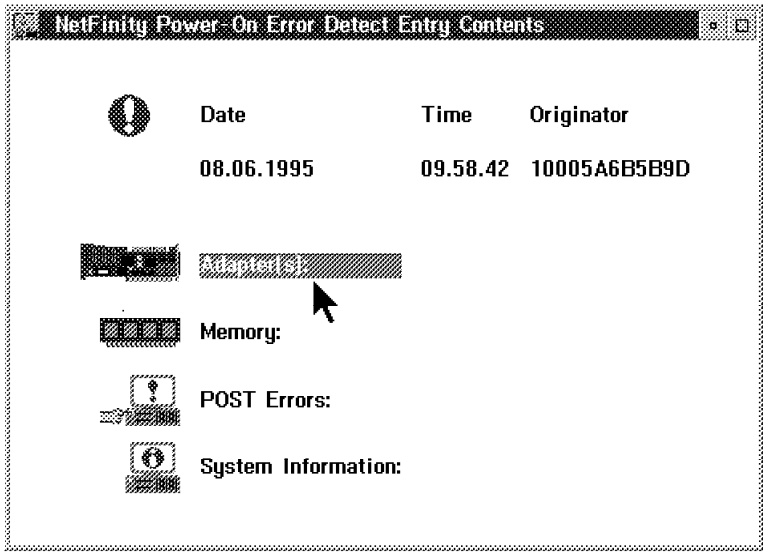


Figure 128. NetFinity Power-On Error Detect Entry Window

- Double-click on the **Adapter(s)** icon.

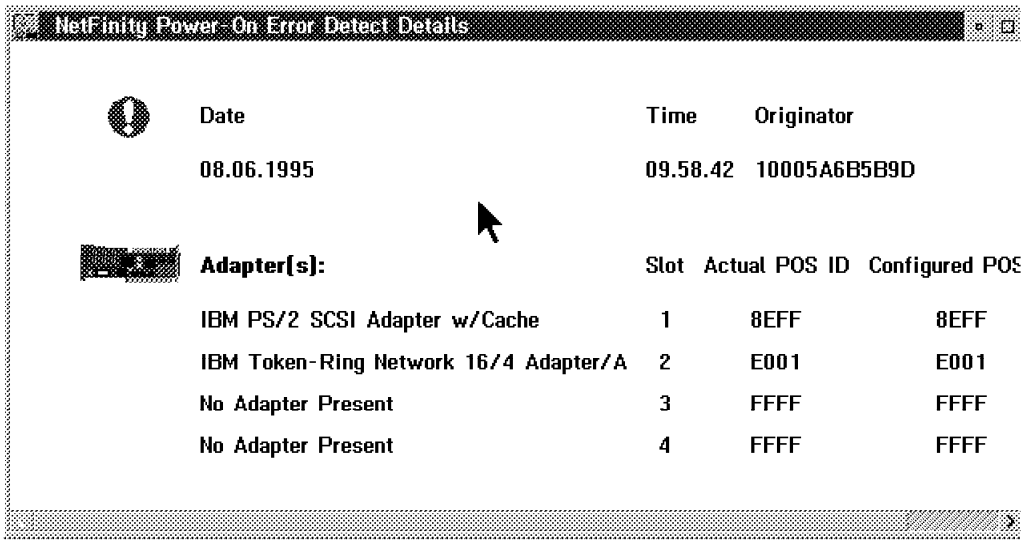


Figure 129. NetFinity Power-On Error Detect Details Window

- All adapter information, including adapter name, slot location, actual and configured POS ID are listed. If an adapter POS ID changes or an adapter is removed, the next reboot will cause a POED alert to flow and there will be an arrow next to the adapter icon. If you double-click on the Adapter icon you will see what it was configured for and what is actually there.

  The Power-On Error Detect drivers have been tested for the following adapters:

  - IBM Token-Ring adapter
  - IBM Ethernet adapter
  - 3Com EtherLink/MC adapter
  - SMC Ethernet Elite Plus/A adapter
  - Madge Smart 16/4 Ringnode adapter
  - Ether Streamer adapter
  - LAN Streamer 32 adapter
  - LAN Streamer 16 adapter

  This list is not all inclusive and it can change at any time.

- If you double-click on **Memory** icon in the window in Figure 126 on page 93 you get the following window:

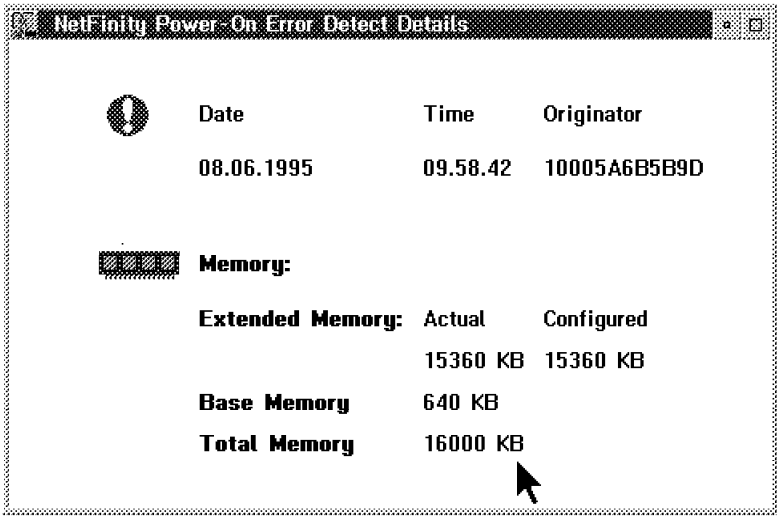


Figure 130. NetFinity Power-On Error Detect Details Window

- You should see information about the memory that is on that machine. It will show actual memory and configured memory.

  If the memory amount changed, you get a POST Error at the next reboot. If you have installed the POED driver, the NetFinity Manager gets an alert. Next to the Memory icon an arrow will appear. This means that something relating to the memory in this system produced this POED error and if you click on the Memory icon, you will see that the configured and the actual memory is different.

- If you double-click on the System Information icon on the window in Figure 126 on page 93 you get the following:

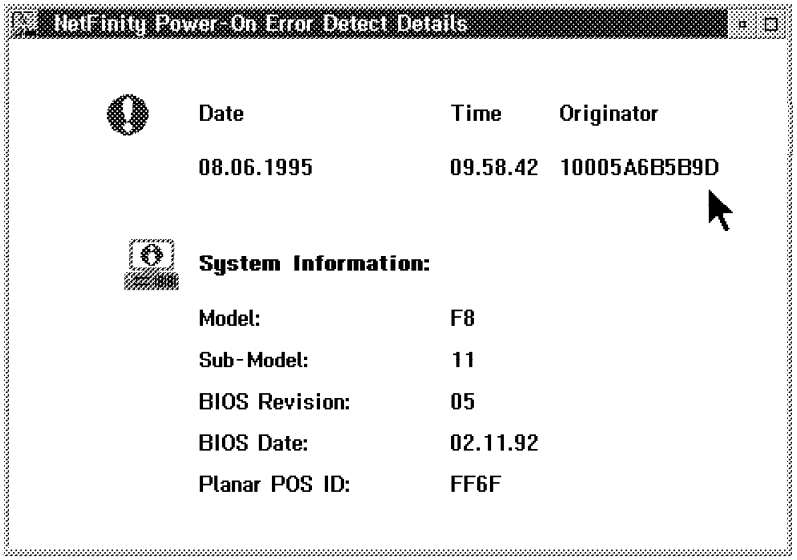


Figure 131. NetFinity Power-On Error Detect Details Window

- You can see System Information, including model, submodel, system board POS ID, and BIOS revision number and date. If Vital Product Data is provided, there will be an additional icon in the window.

In the next figure you will see a POED alert that was from a keyboard error. This can happen if you plugged the keyboard cable into the location for the mouse on the system unit.

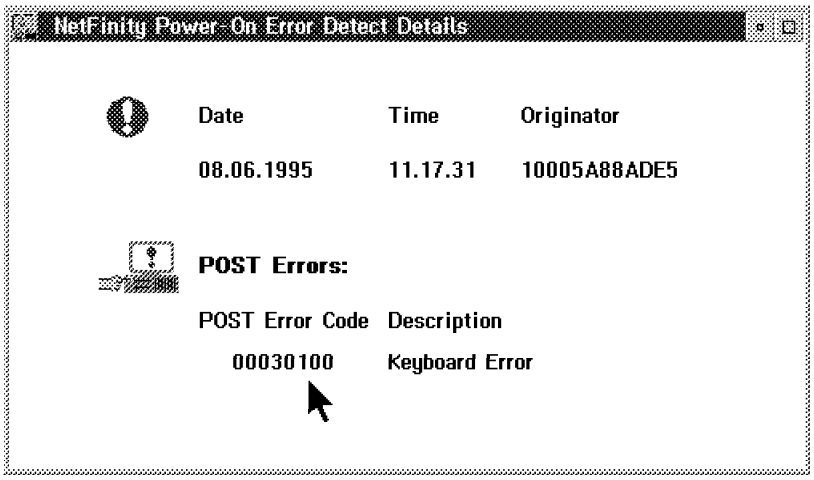


Figure 132. NetFinity Power-On Error Detect Details Window

You can use the information that is provided in the POST records to help in the problem determination and problem resolution process. This is true for the adapters, memory, and other hardware components.

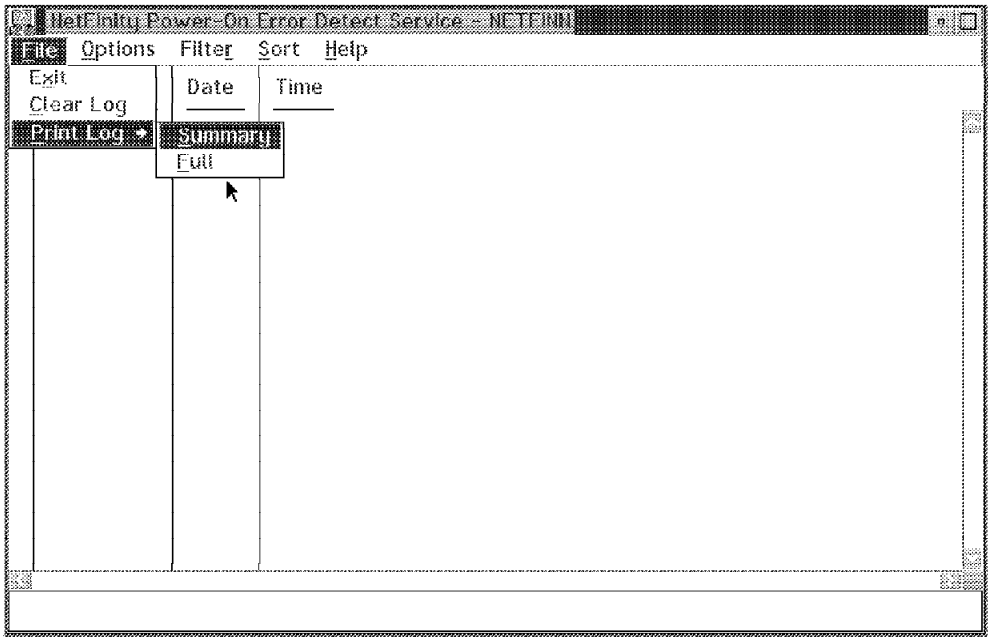


Figure 133. NetFinity Power-On Error Detect Service Window

If you select the **File** pull-down from the Power-on Error Detect Service window as shown in Figure 133 you will have a choice of:

- Exit the Power-On Error Detect Service
- Clear the Power-On Error Detect Log
- Print a report on the entries contained in the log

The option to print a report will let you:

- Select **Summary** to print a short report containing the following information on each entry in the Power-On Error Detect Log: date, time, originator and POST error.
- Select **Full** to print a detailed report on all entries in the Power-On Error Detect Log. This report will contain the following information on each entry in the Power-On Error Detect Log: date, time, originator, POST error and extensive system information. The fields for system information are:
  - Adapters
  - Memory
  - Hardware Error Log
  - Vital Product Data (VPD) if available

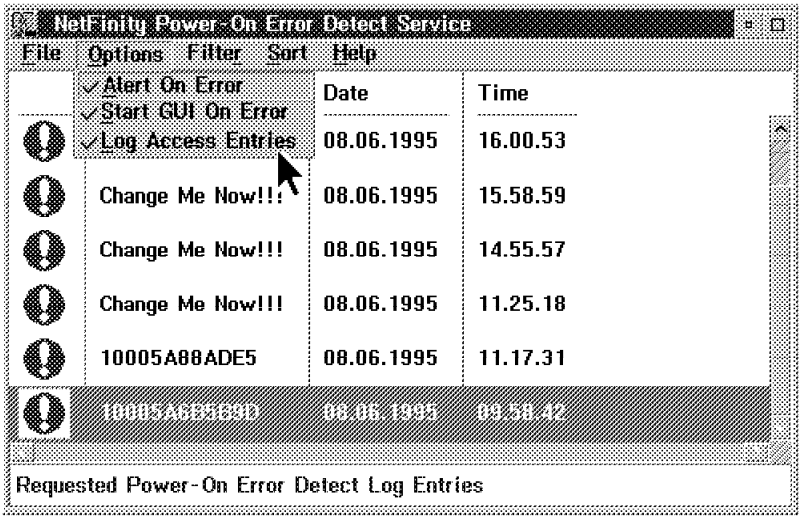


Figure 134. NetFinity Power-On Error Detect Service Window

- If you click on **Options** at the top of the Power-On Error Detect Service window you get a pull-down menu with the following options:
  - Alert on Error
  - Start GUI On Error
  - Log Access Entries
- Select the **Alert on Error** option to generate a NetFinity alert when a remote POST Error is received. The generated alert will be received by the NetFinity Alert Manager, and will contain the following alert information:
  - Alert Text: NetFinity Power-On Error Detect Alert
  - Type of Alert: Application Failure
  - Severity: 4
  - Application ID: Power-On Error Detect
  - Application Alert Type: 0201
  - Time and Date Received
- Select **Start GUI On Error** to automatically start the Power-On Error Detect Service's graphical user's interface (GUI) when a remote POST Error is received.
- If Log Access Entries is selected, the Power-On Error Detect service will log any messages generated by remote systems if the system's user has

accessed its System Partition during startup (pressed Control-Alt-Insert during startup). If log access entries are not selected, then these access messages are ignored. The following is an example of the Log Access Entries.

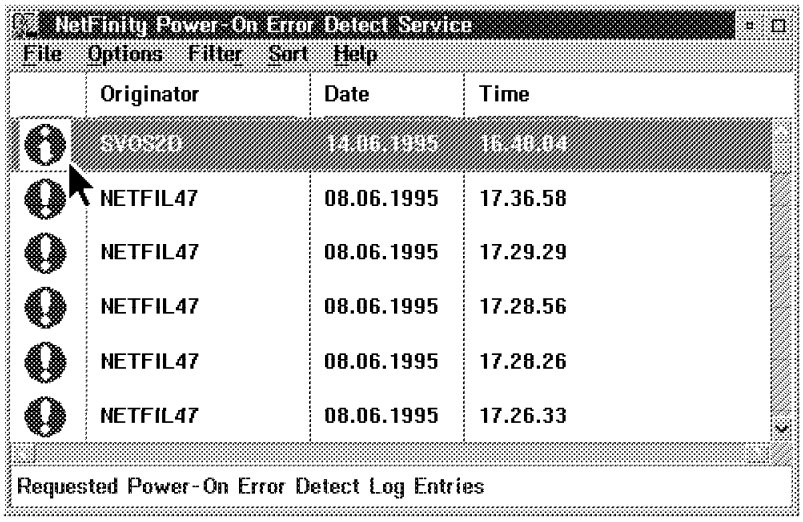


Figure 135. NetFinity Power-On Error Detect Service Window

- Double-click on the entry from the Power-On Error Detect Log.

  This will open the Power-On Error Detect Entry Contents window. Following the Power-On Error Detect Log entry will be the machine that sent the error (SVOS2D).

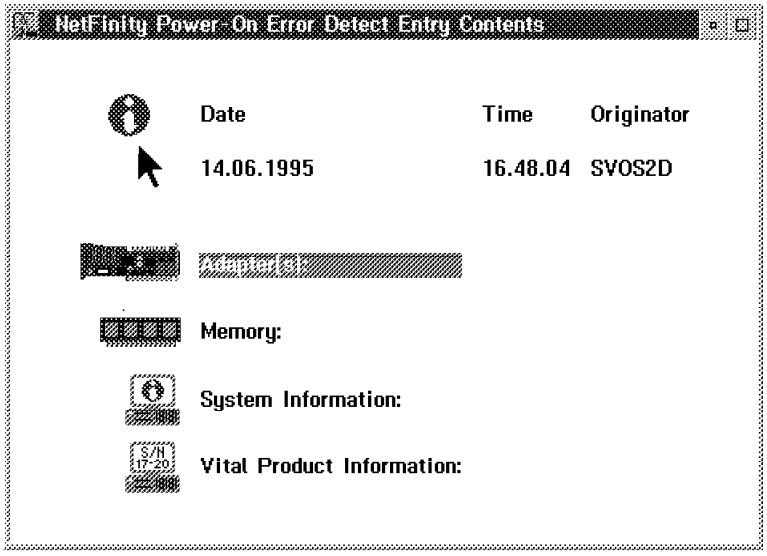


Figure 136. NetFinity Power-On Error Detect Detail Window

- Double-click on the **Vital Product Information** icon.

  This will open the Power-On Error Detect Detail Contents window. In this window you will see the VPD for SVOS2D.

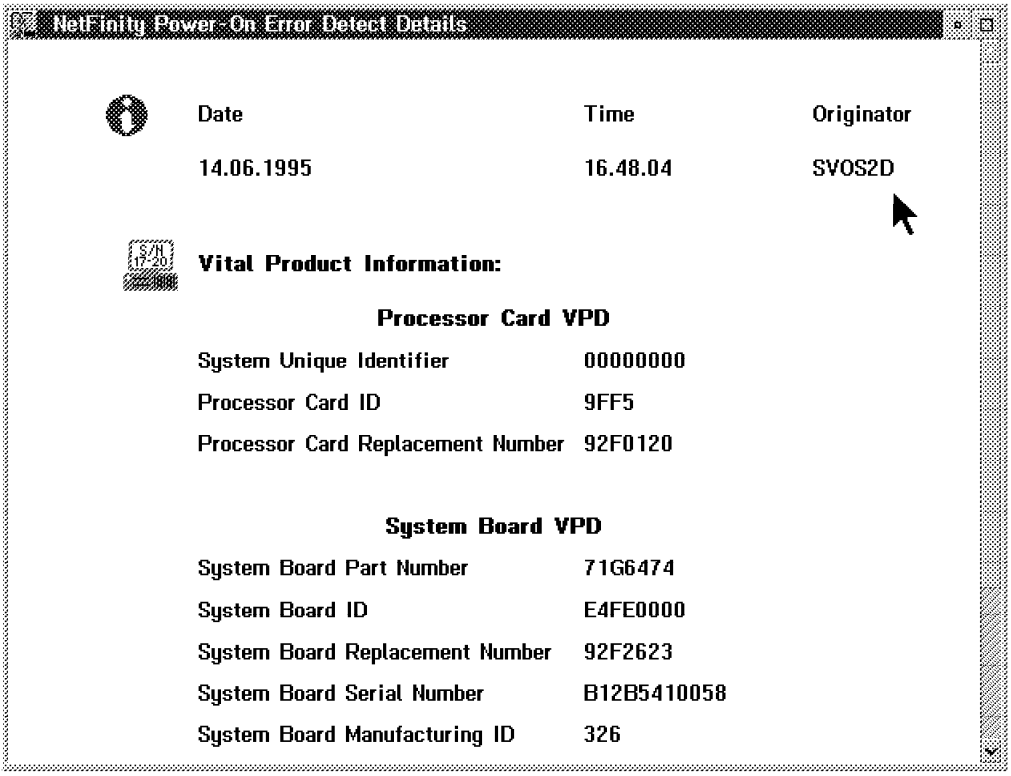


Figure 137. NetFinity Power-On Error Detect Service Window

5.2 ECC Memory Setup Code Service

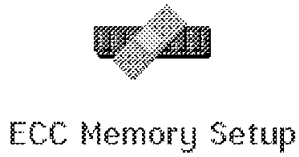


Figure 138. ECC Memory Setup Icon

The NetFinity Error Correction Code (ECC) memory setup enables you to monitor and manage ECC memory. If ECC memory is not installed before the installation of NetFinity no ECC Memory Setup object will appear in the NetFinity manager folder. NetFinity checks for the presence of ECC memory during the Netbase startup.

When you use the Remote System Manager service for a system that has ECC memory, you will see the ECC object in the remote folder even if there is no ECC memory object for your local system. This will permit you to remotely configure ECC settings from the manager. If there was a time that you had a machine with NetFinity installed before the ECC memory, and you were unable to re-install the NetFinity code, you could always install the manager code on another machine and make the original machine a client for ECC setup purposes.

The options that you can customize are shown in Figure 140 on page 101.

- Single-bit Error Scrubbing

- Single-bit Error Counting
- Single-bit Error Threshold Non-Maskable Interrupt (NMI)

You can also set the single-bit error threshold value that will trigger the Non-Maskable Interrupt (NMI) if the Single-bit Error Threshold option is selected. The ECC Memory Setup object is in the NetFinity Service Manager folder.

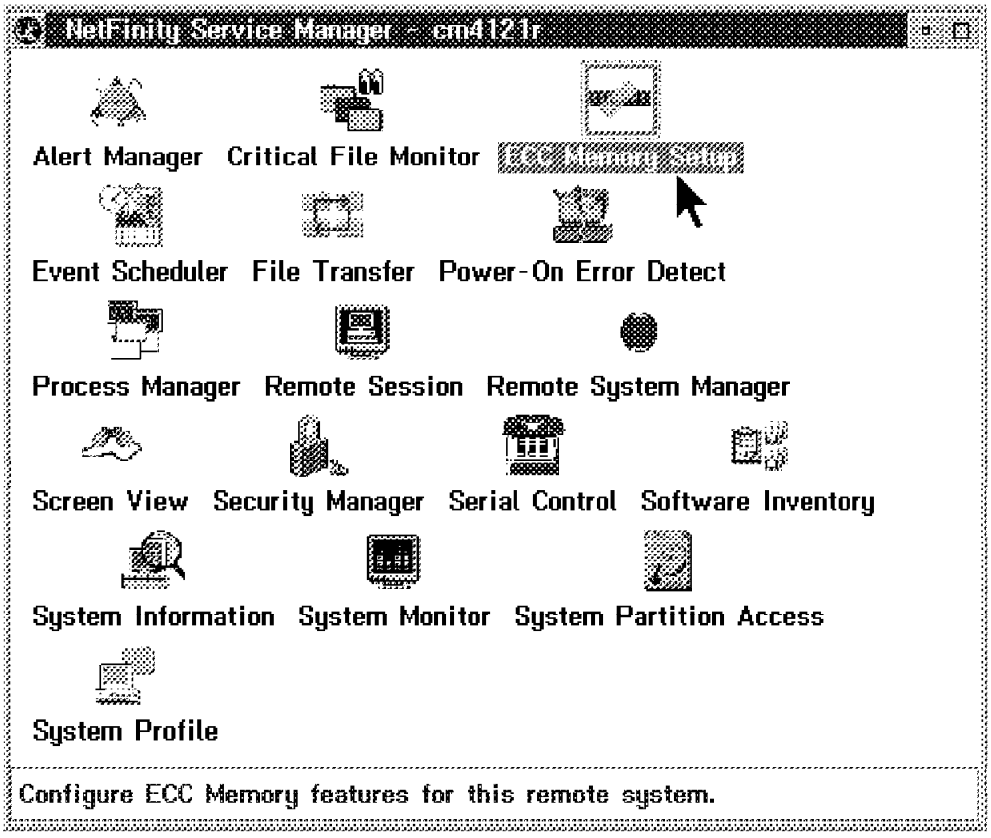


Figure 139. NetFinity Service Manager Folder

- If you double-click on the ECC Memory Setup object you get the following window:

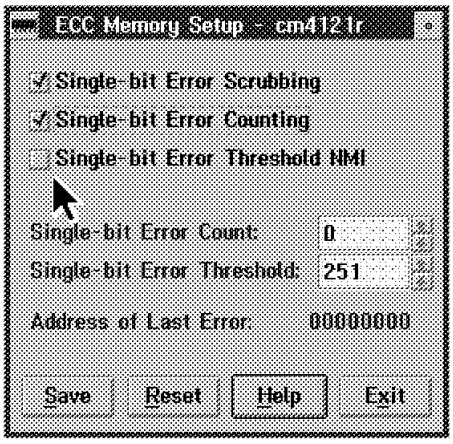


Figure 140. NetFinity ECC Memory Setup Window

To configure ECC memory, whether it is local or remote:

- You need to determine which of the ECC memory functions you wish to enable. The options are:
  - Single-bit error scrubbing

    Activating the single-bit error scrubbing option instructs ECC memory setup to activate the automatic error correction features of the ECC memory in the system. This will immediately correct any single-bit errors that occur. Selecting this option may negatively effect performance on some systems, but it ensures greater data integrity.

    Note

    The default option has none of the options enabled. You must configure one or more for it to take effect.

  - Single-bit Error Counting

    Activating the single-bit error counting option instructs ECC memory setup to keep a running count of all single-bit errors that occur in the ECC memory.

  - Single-bit error threshold NMI

    Activating the single-bit error threshold NMI option instructs ECC memory setup to cause a Non-Maskable Interrupt (NMI) if the number of single-bit errors exceeds the user-specified threshold. An NMI will often cause the system to immediately shutdown, so this feature should only be enabled if the system contains special NMI handling hardware or software.
- Change the single-bit error count if desired.

  Attention

  ECC memory setup does not generate NetFinity alerts.

- If you have chosen the single-bit error threshold NMI option, remember to set a single-bit error threshold value.

  The Single-bit Error Threshold field displays the user-specified number of ECC single-bit errors that will be allowed before ECC Memory Setup will trigger a non-maskable interrupt (NMI). If the NMI feature is not active, the single-bit error count will be reset to zero when the threshold is reached. An NMI only occurs if you activate the single-bit threshold NMI option.

  When you are finished click on the **Save** button. The Save and Reset button, are greyed until you change one or more of the settings.

  After you save the settings, the following window will appear:

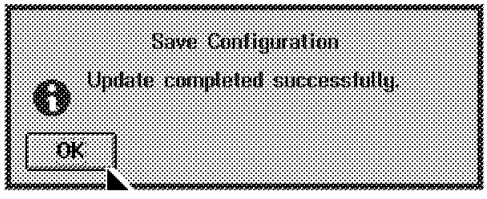


Figure 141. Save Configuration Update Window

- Click on **OK** and you are back to the ECC Memory Setup window.

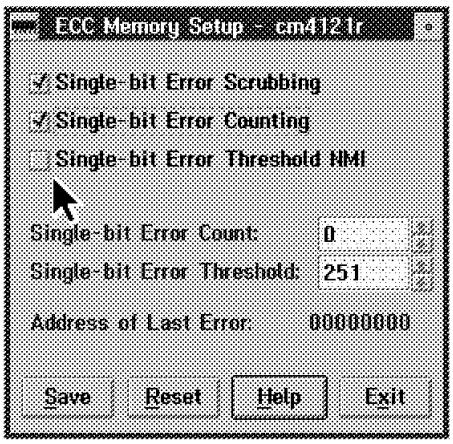


Figure 142. ECC Memory Setup Window

- Select **EXIT** to go back to the NetFinity Service window.

  All of the functions of ECC Memory Setup may also be accessed from the OS/2 command line, and thus can be used in a REXX routine. The command line format for ECCMEM.EXE is:

```
ECCMEM < /INIT > < /SCRUB:<ON OFF> > <
/THRESH:<ON OFF> > < /COUNT:<ON OFF> > < /QUIET
> < /COUNTVAL:num > < /THRESHVAL:num >

where:
/INIT     - Causes the ECC memory to be initialized to
            the saved settings

/QUIET    - Causes ECCMEM to generate no textual
            output

*/SCRUB:<ON OFF> - Enables or disables single-bit
            error scrubbing

*/COUNT:<ON OFF> - Enables or disables single-bit
            error counting

*/THRESH:<ON OFF> - Enables or disables single-bit
            error threshold NMI

/COUNTVAL:num - Sets the single-bit error count to a
            given value

*/THRESHVAL:num - Sets the single-bit error
            threshold to a given value

* = This option updates the saved settings to the
value provided.  Upon restarting the system, the
saved settings can be used to configure the ECC
memory through the /INIT option.
```

Figure 143. Command Line Interface for ECC Memory

5.3 RAID Manager

Redundant Array of Independent Drives (RAID) monitoring is available using NetFinity. Like all of the other NetFinity services, you can start up the RAID displays from the main NetFinity folder by double-clicking on the service icon. If you don't have RAID on your local system, you can still manage remote systems that have RAID using the Remote Systems Manager.

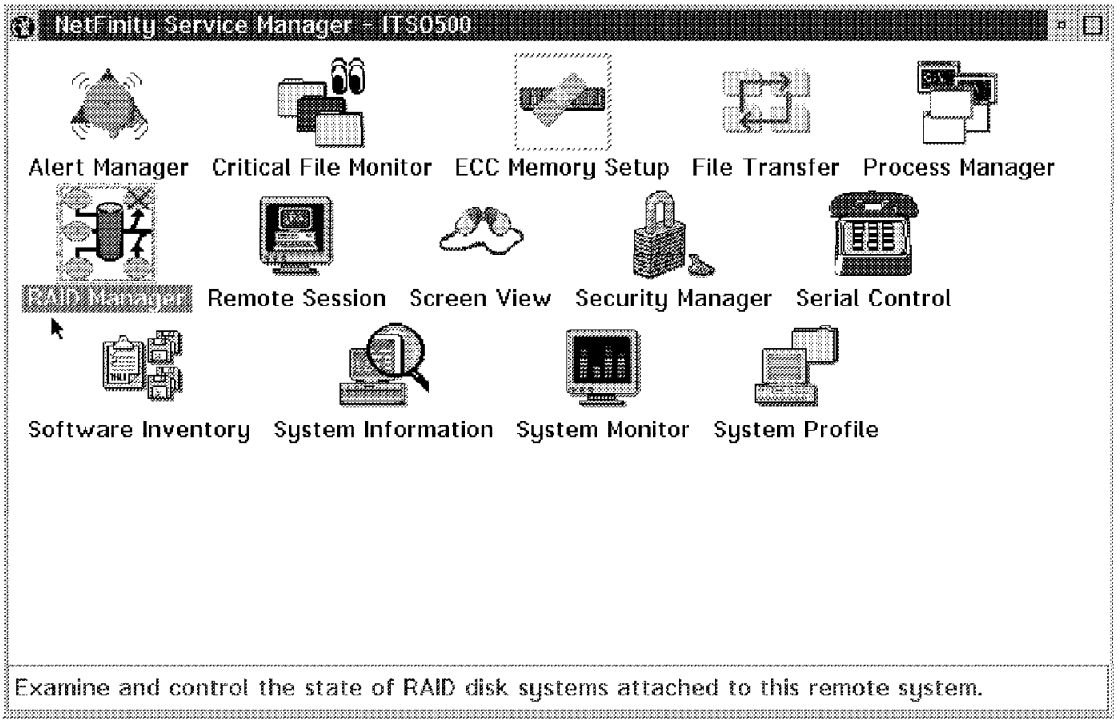


Figure 144. RAID in the Service Folder

After double-clicking, Figure 145 appears on your display while it is gathering information about the RAID device.

Figure 145. RAID Manager Icon

After NetFinity gathers the information about the RAID environment you will see an icon that represents the system and its components. If you use the left

mouse button and click on one of the modules in the bank (for example, Bank C), you will see which set of virtual drives are associated with it, as shown in Figure 146 on page 105.

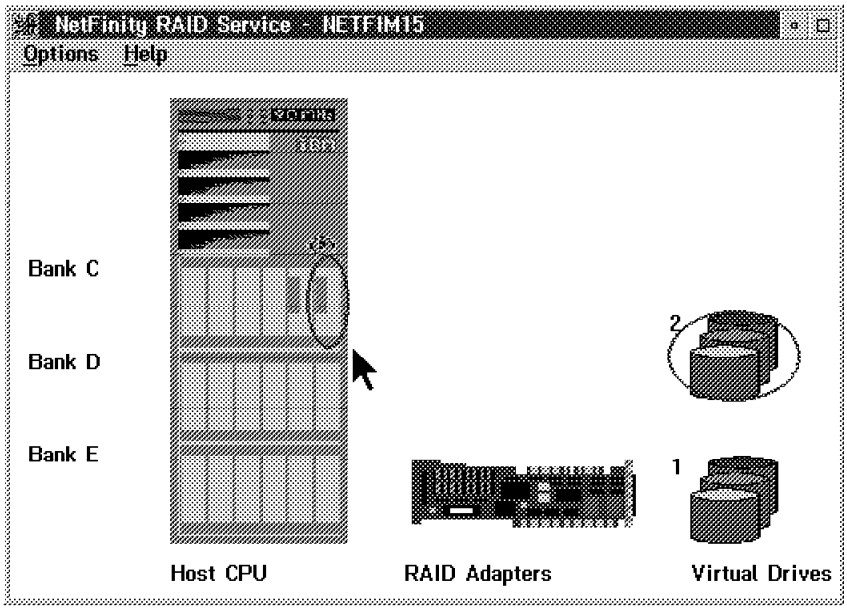


Figure 146. Graphical Display of the RAID Subsystem

For ease of use, you can re-size the window using the pull-down option Viewing Scale as shown in Figure 147, or you can change the Virtual Drive Columns, as shown in Figure 148 on page 106 to fit many RAID views on your display.

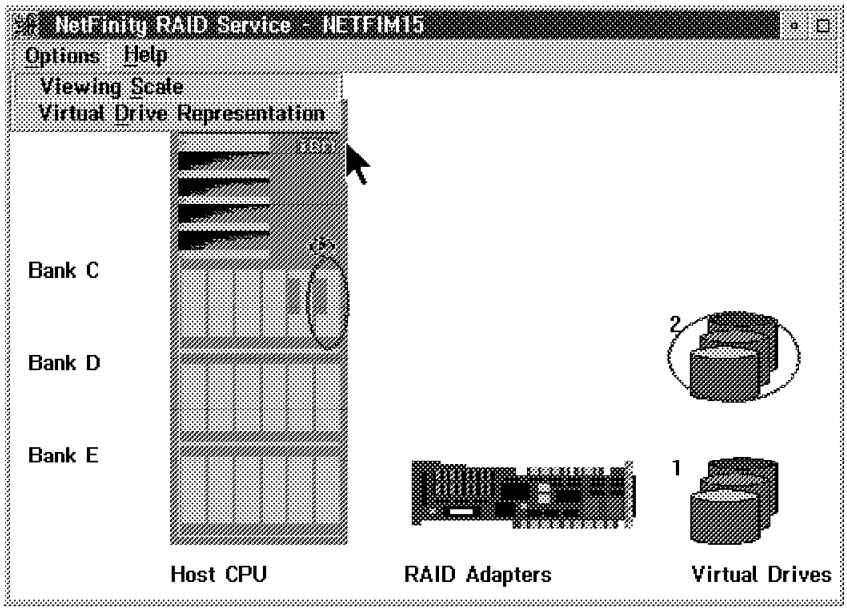


Figure 147. Re-scale RAID Window

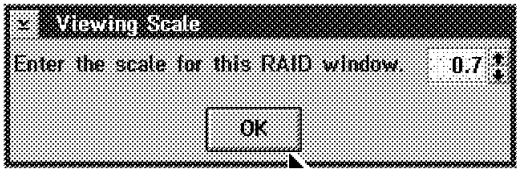


Figure 148. Virtual Drive Columns

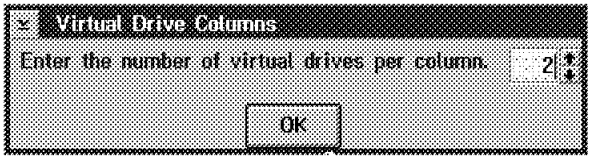


Figure 149. Views and Changes of RAID Subsystems

In addition to being able to view your devices and some statistics, you can make some configuration changes from your NetFinity RAID manager.

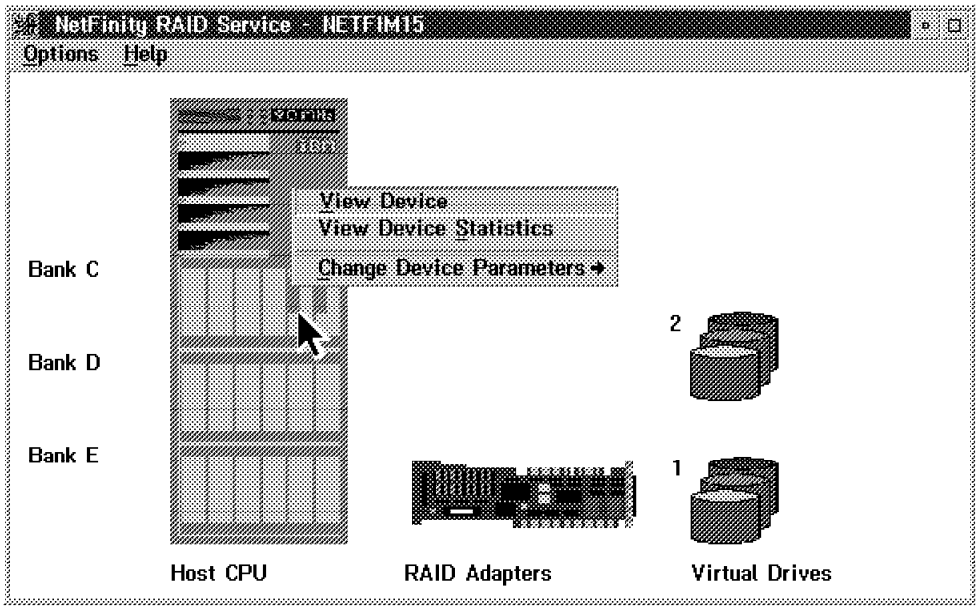


Figure 150. Device Information

Figure 151 on page 107 shows the status of the device we selected as well as characteristics about this device.

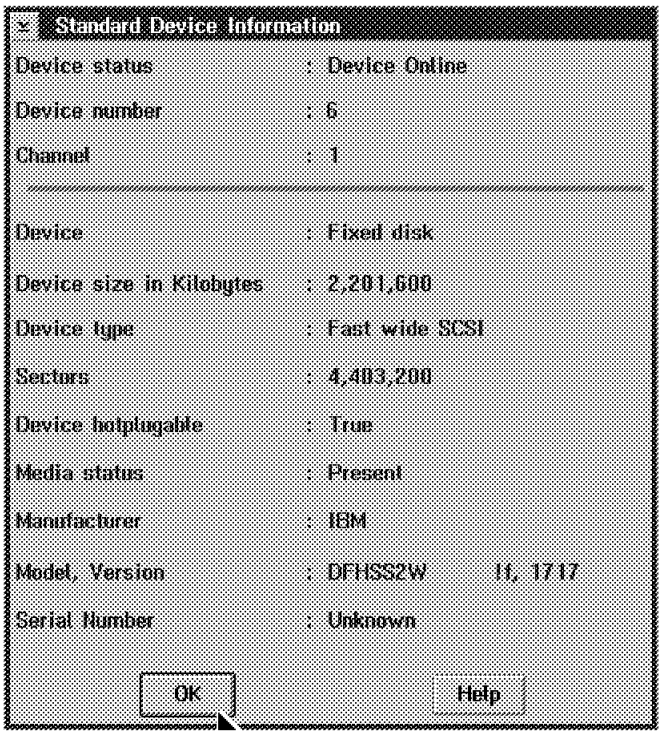


Figure 151. RAID Statistics

You can also monitor some statistics for the device.

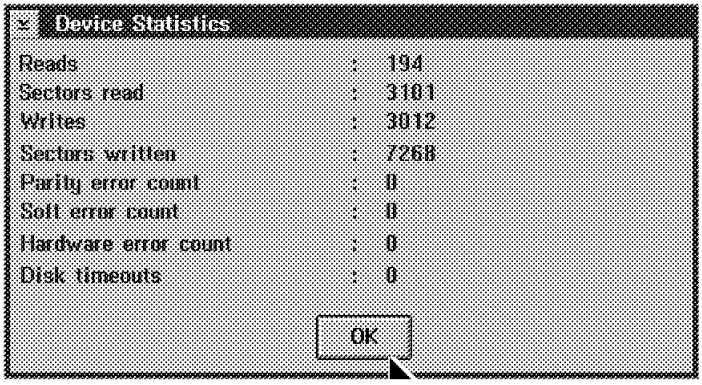


Figure 152. Changing Device Parameters

We were not set up in our environment to make any changes to the RAID subsystem, but as you can see in Figure 153 on page 108, you can take the following actions:

- Add a device
- Remove a device
- Format a device
- Rebuild the device
- Start the device
- Stop the device
- Set up a hot spare

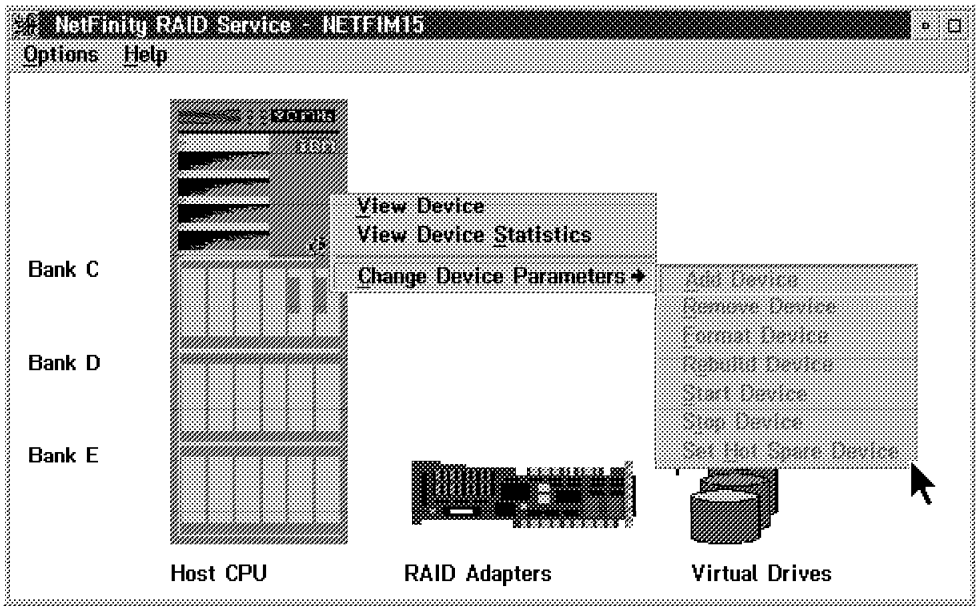


Figure 153. Configure RAID Adapter

If you click on the RAID adapter, you can view details about it locally or remotely, and you can also configure the adapter.

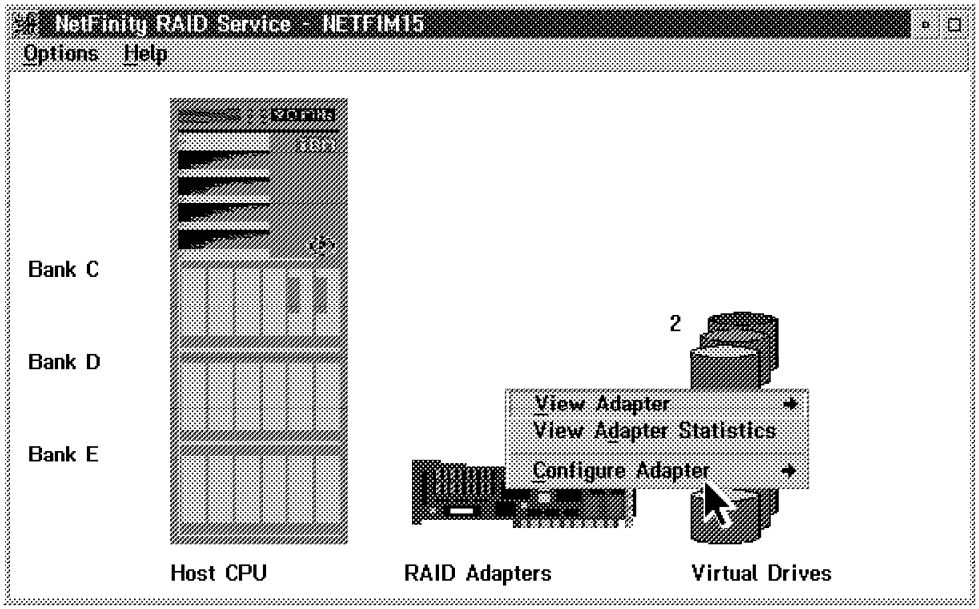


Figure 154. Information on the Adapter

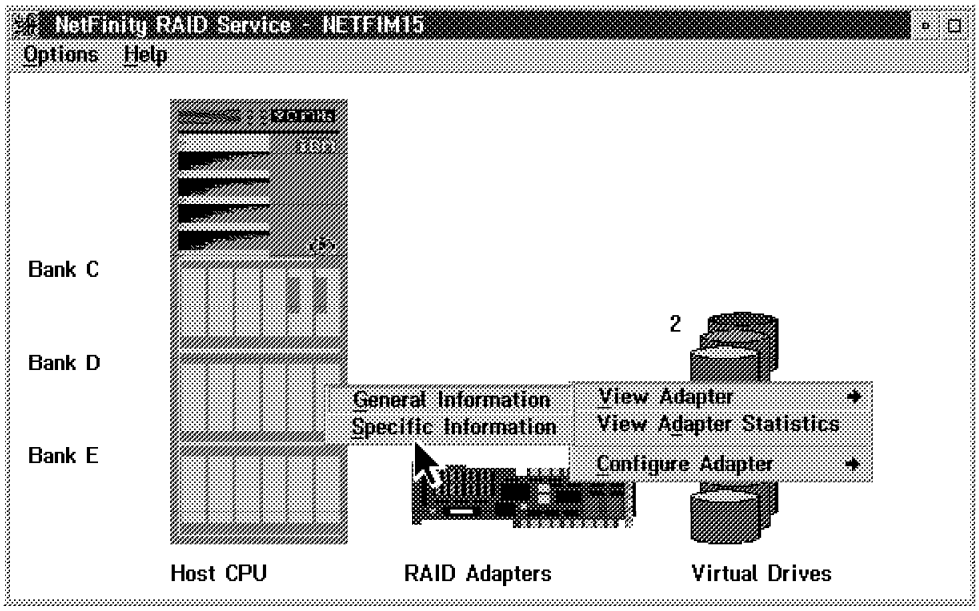


Figure 155. General and Specific Information on the Adapter

Detailed information on the adapter is shown below:

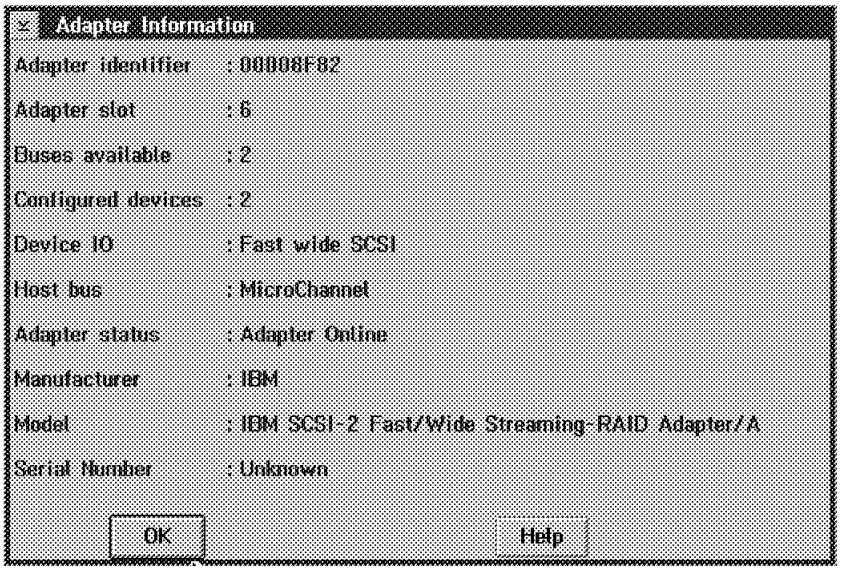


Figure 156. Adapter Information

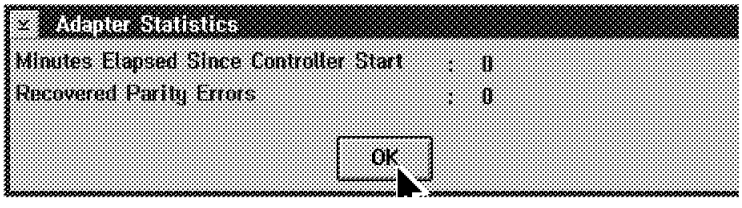


Figure 157. Adapter Statistics

5.3.1 RAID Alerts

There are three states that the RAID system drive can be in:

- Online
- Critical
- Offline

There are three states that the RAID physical drive can be in:

- Online
- Standby
- Dead

You will only receive a RAID alert when the device changes state. The RAID adapters that are supported are:

- IBM RAID Adapter
- IBM SCSI-2 Fast/Wide-Streaming RAID Adapter/A
- IBM SCSI-2 Fast PCI-Bus RAID Adapter

All of the application IDs for the alerts from the RAID subsystem are MonitorB. The application alert types are 130 for physical disks and 131 for system disks.

Chapter 6. NetFinity and NetView for AIX

This chapter will take a look at two different scenarios that are related to exchanging information with NetView for AIX. We will be using NetView for AIX V4.1 running on AIX V4.1.3. In these scenarios we will send traps from our NetFinity managers to our SNMP manager, and we will also have the SNMP manager issue remote commands to start a process on the NetFinity Manager.

6.1 NetFinity and NetView for AIX

Many of the services within NetFinity can be started automatically on either your local machine, or on a remote machine. This chapter will show how to start those services based upon alerts that were sent to a NetFinity manager and an SNMP manager, NetView for AIX.

If you have the NetFinity Software Developer's Kit (SDK), you will find an application that can read the service managers INI file. To extract the contents of the file, you need to execute: `\netfin\bdsvcmgr.exe\netfin\svcmgr.ini`

That will produce a window that will show you the name of the NetFinity service along with other details. Clicking on the next key will step you through all the services. An example of the window is shown in Figure 158 on page 112.

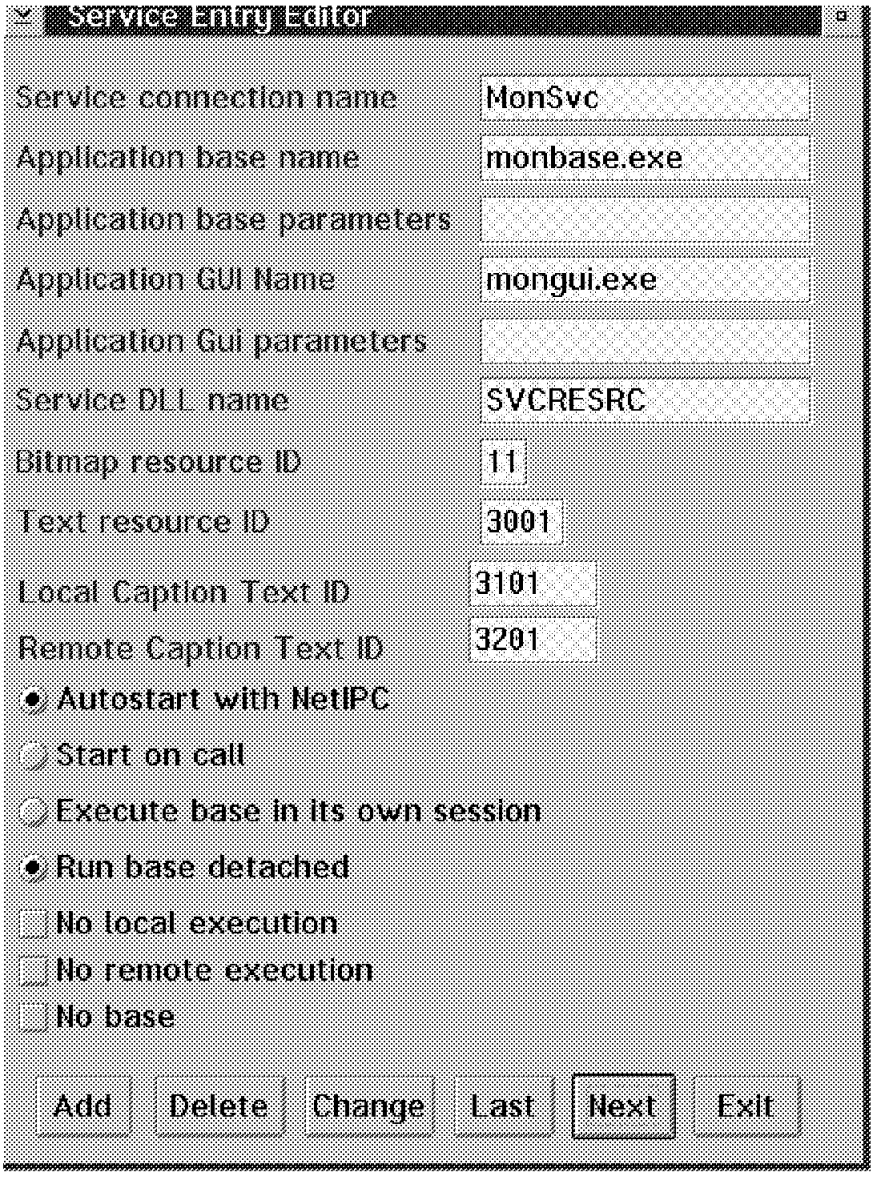


Figure 158. NetFinity SDK Tool Output

A list of all of the services and their executables follows:

```
Service Name          Appl Base Name   Appl GUI Name

ProfileBase           profileb.exe     porfileg.exe
SCH_BASE_NODE         schbase.exe      schgui.exe
RAID_BASE             raidsvcb.exe     raidserv.exe
SecMgr                netfbase.exe     secgui.exe
DMIBrowserBase        dmibrbas.exe     dmibrgui.exe
MonSvc                monbase.exe      mongui.exe
ScreenID              saveb.exe        saveg.exe
ECCMemory             eccmem.exe       eccgui.exe
NetMgr                netfbase.exe     nfsysmgr.exe
ShrieKerServiceBase   shrbase.exe      shrgui.exe
ProcMgr               procbase.exe     procgui.exe
CFMBase               cfmbase.exe      cfmgui.exe
Gatherer3.0           sinfb30.exe      sinfg30.exe
PFAServiceBase        pfab.exe         pfag.exe
Gatherer              sigather.exe     sysinfo.exe
AlertMgr              alertmgr.exe     nfalert.exe
PartionBase           partb.exe        partg.exe
FileBase              ftbase.exe       ftgui.exe
SerialBase            serbase.exe      sergui.exe
SoftInvB              sinvbase.exe     sinvgui.exe
RCSHD                 rcshd.exe        rcsh.exe
```

Figure 159. NetFinity Automation Services

In order to start the graphical application, the application base component must be started. Typically, if you have started NetFinity all of the components will be running. If you are either trying to save resources, or have a problem with a component, it is possible that NetFinity will be stopped; therefore, using TCP/IP RSH or REXEC you can start the components up remotely.

6.2 NetView for AIX Event Configuration

In this scenario, we will set up an alert on the NetFinity workstation manager, and forward it as an SNMP trap to NetView for AIX, when a NetFinity system comes online, or goes offline. When it gets to NetView for AIX, we will display it in the events window, as well as show how to automatically issue a remote command to start a process back on the NetFinity manager.

Since we wish to be notified if any systems′ status changes, we will need to use the Remote Systems Manager. After double-clicking on the Remote Systems Manager, we selected one of our logical groupings of systems. In this case, we will look at all_sys, as shown in Figure 160 on page 114.

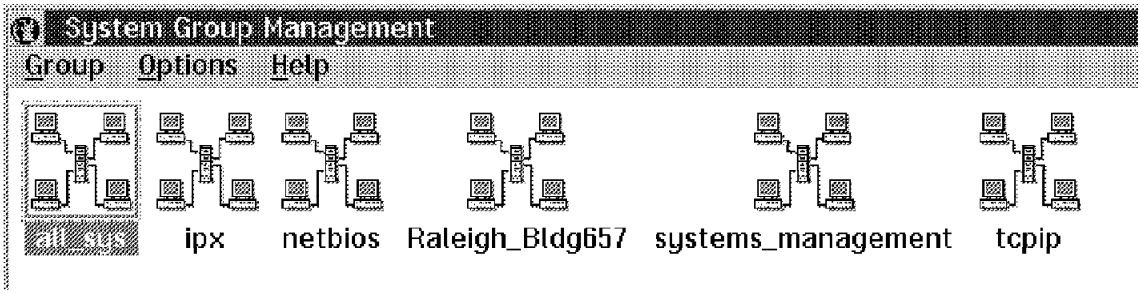


Figure 160. Remote Systems Manager all_sys Group

Using the right mouse button on the all_sys group, we see that there are several options to choose. We are going to set up the notifications for all of the systems in the group.

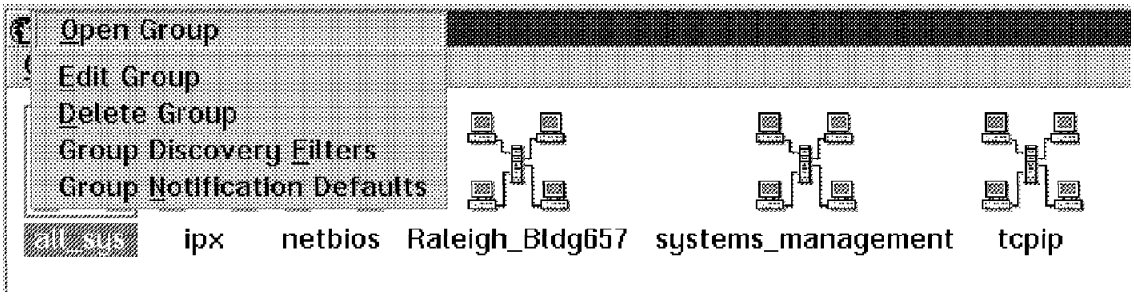


Figure 161. Group Editing Options

The default severity for systems coming online, or going offline is 0. This is important to remember when you configure the alert in the Alert Manager component. Figure 162 shows the defaults when you select Group Notification Defaults in Figure 161.

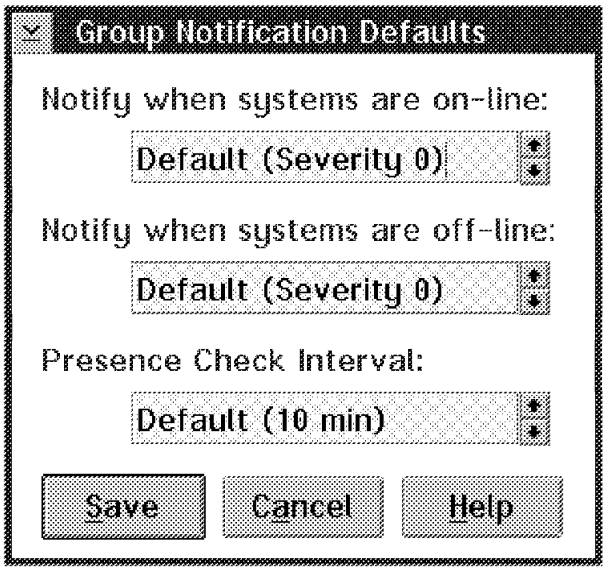


Figure 162. Default Group Notifications

When a system goes offline or is unreachable, based upon the Presence Check Interval that you set in the group notifications, an alert will flow to the Alert Manager. Figure 163 on page 115 shows several alerts. The first one that is high-lighted, also shows up in the detail section on the top part of the window. In this case, SVMGR02 went offline, and was using the IPX transport.

To configure the alert click on **Actions**.

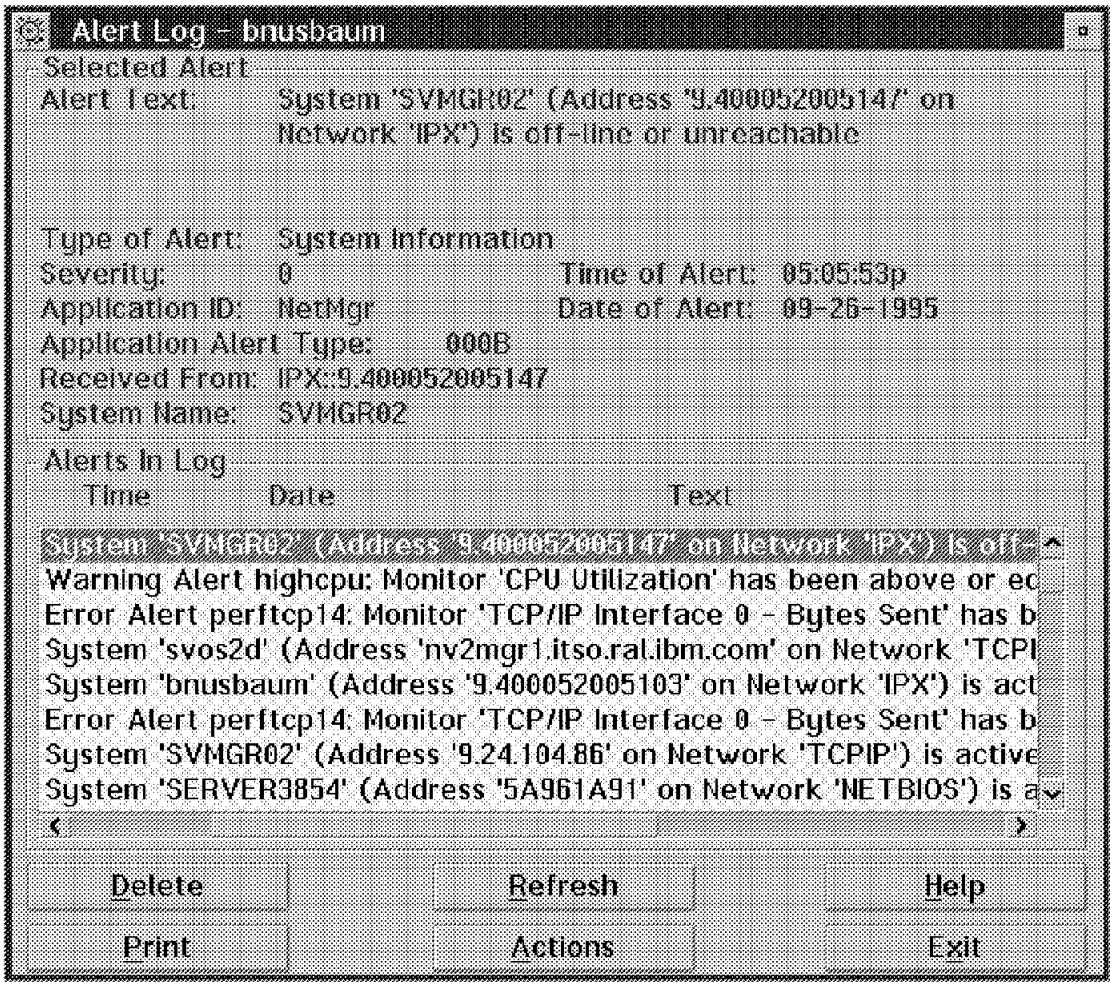


Figure 163. Alert Manager Alert Log

Figure 164 on page 116 shows a list of all of the actions that have already been configured. You can't tell any of the details about the actions without editing them and seeing which values have been set for the alerts. This means that you will have to be very specific when you customize your alerts, so you don't use several actions for one particular alert.

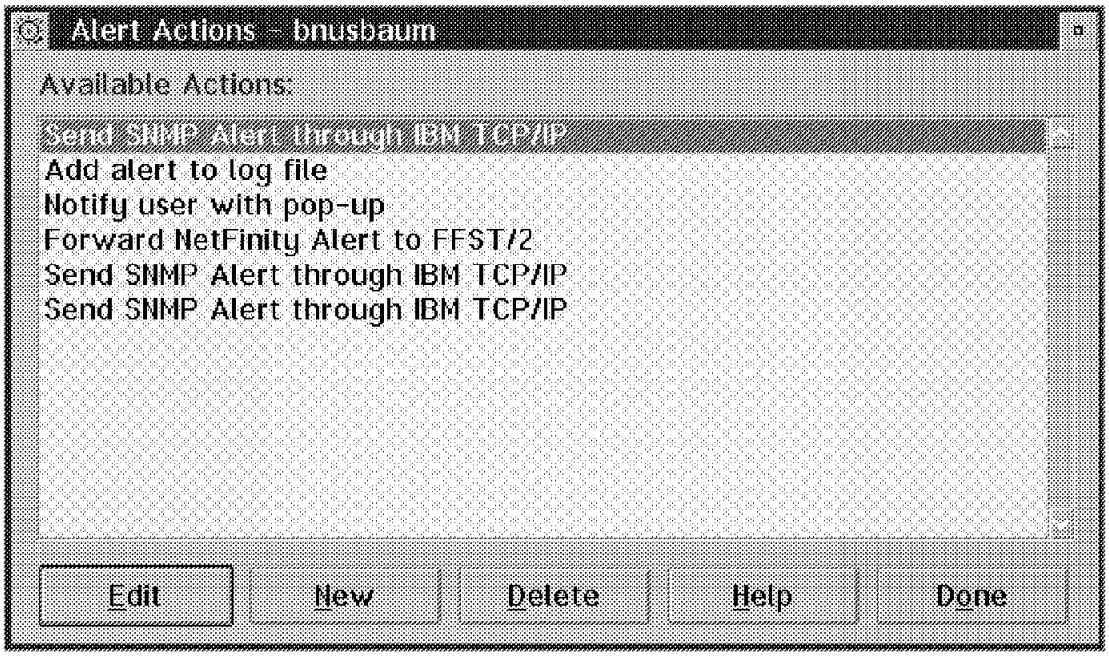


Figure 164. Configured Alert Manager Actions

If you compare the alert fields in Figure 165 on page 117 with the Alert Log entry in Figure 164, you will see that we specified that any system that comes online will cause a trap to get sent to our SNMP manager. The list of managers is customized in OS/2 TCP/IP in snmptrap.dst. In OS/2 TCP/IP V2.0 you will find that in a file. In V3.0 of OS/2 TCP/IP it is stored in an INI file. In both cases, you customize it when you customize TCP/IP. It is very important that you make sure you have the correct community name.

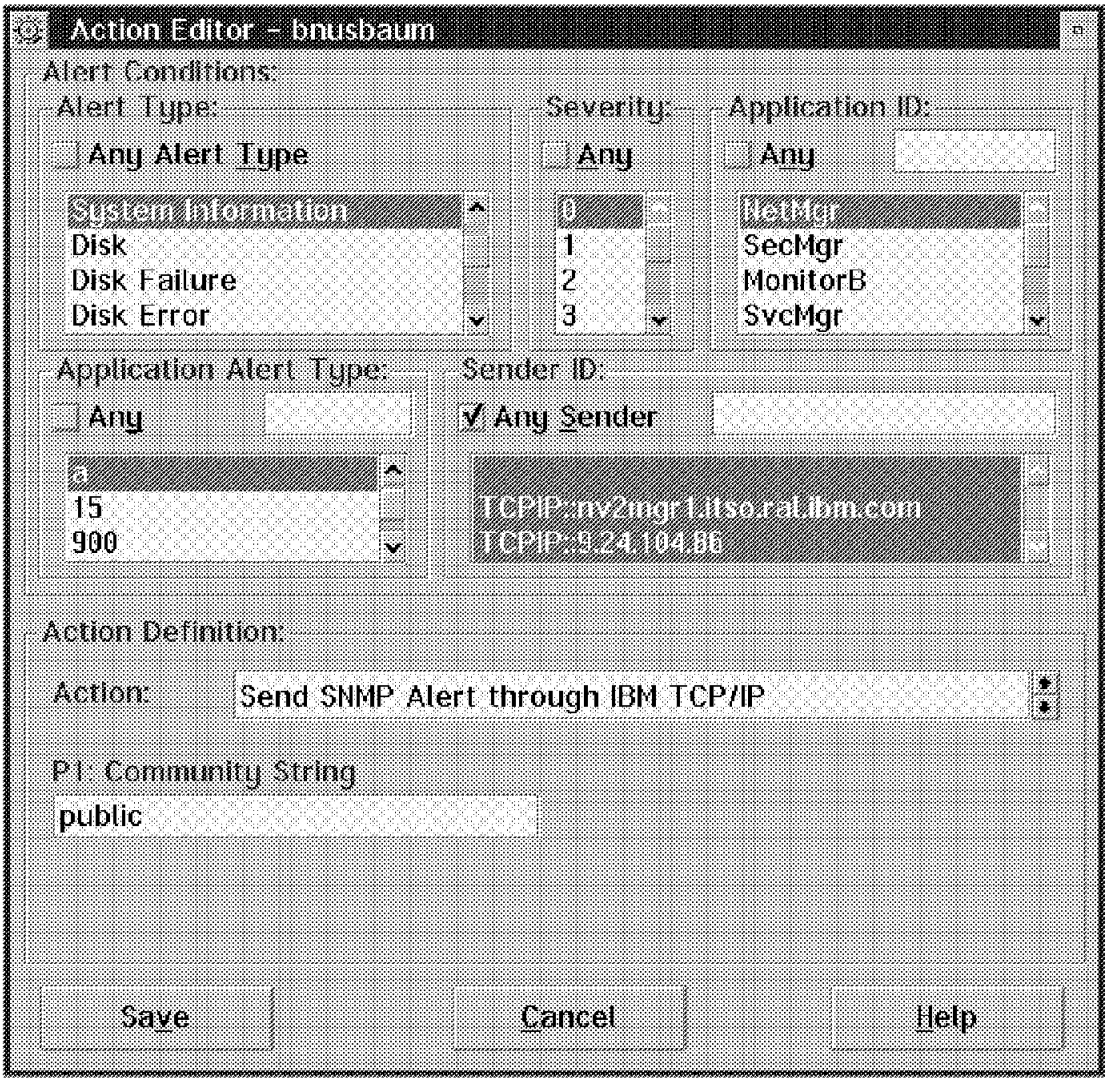


Figure 165. Action Editor Customization for Sending SNMP Traps

Figure 166 on page 118 is an example of an alert for when the system svos2d came online. The transport protocol that NetFinity discovered it on was TCP/IP. Note the Application Alert Type field has a value of 000A. This is important for the Action Editor.

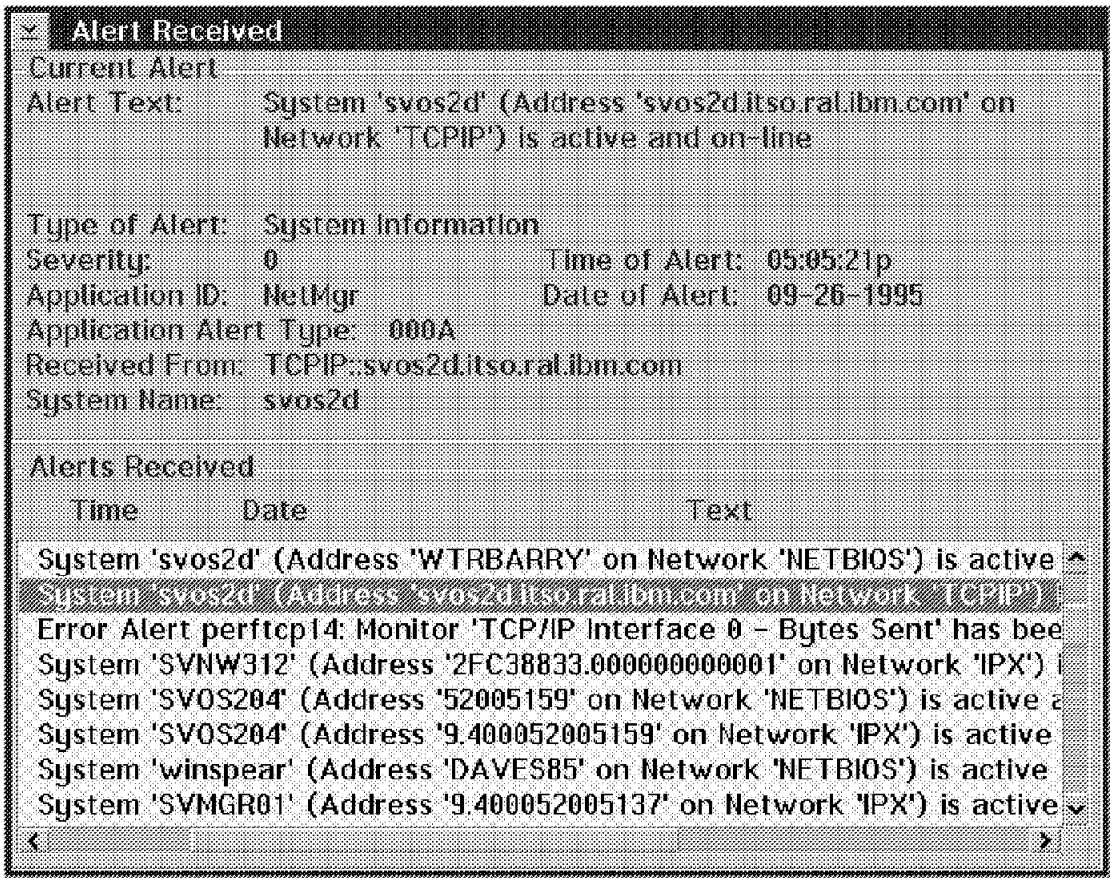


Figure 166. System Information Alert for a System Coming Online

Using the Dynamic Workspace feature of NetView for AIX, we set a filter to list only the events that were related to NetFinity. Figure 167 shows the events that came from our NetFinity managers.

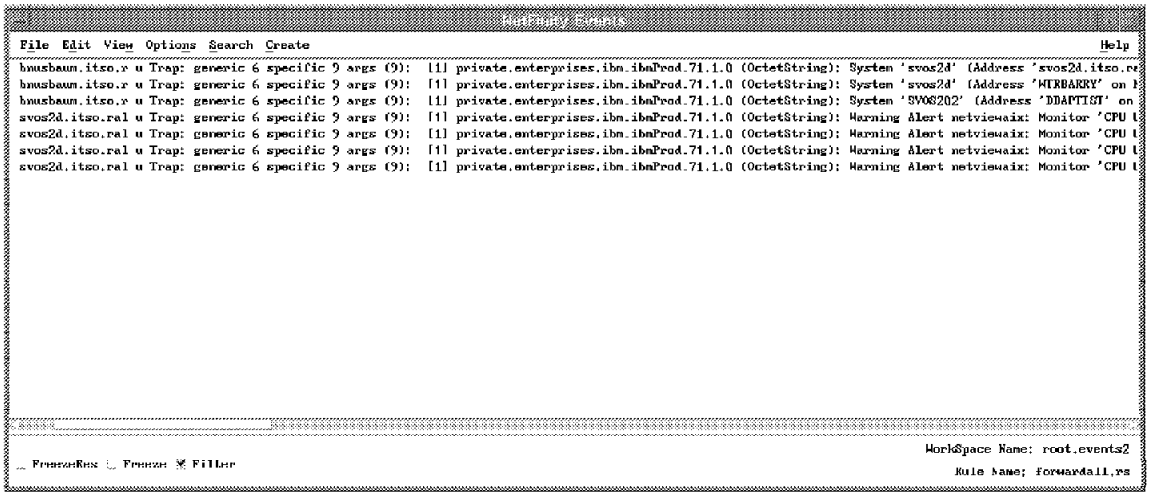


Figure 167. Nvevents for NetFinity Events in a Dynamic Workspace

If we wanted to see more detail in a card format, we would use the right mouse button anywhere in the NetView for AIX Events window and change it. It is often helpful to view it in card format so you can configure the event.

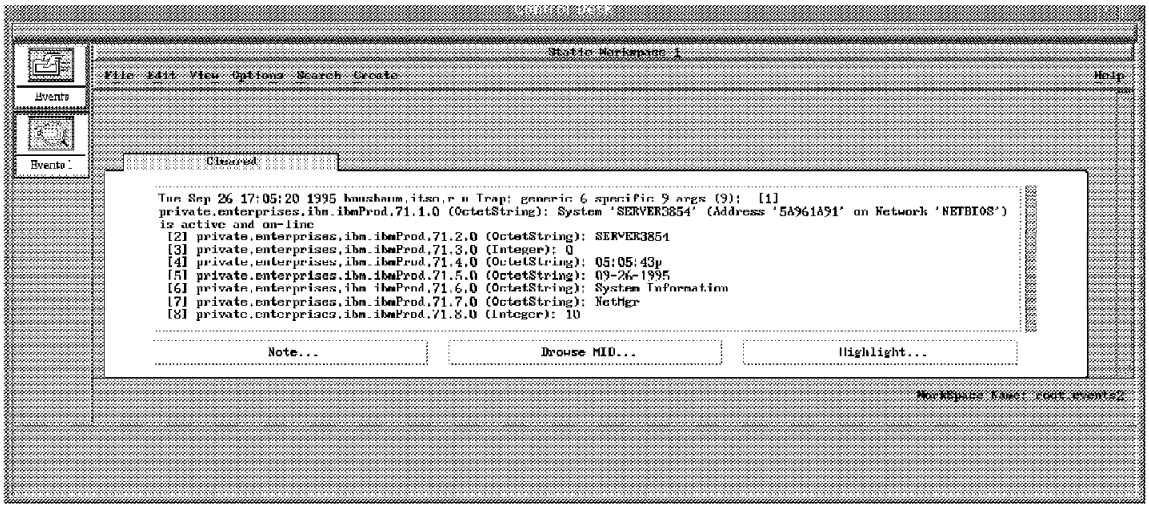


Figure 168. Nvevents Card Format

In order to set up the filter to find NetFinity traps, you can use the pull-down window in Figure 168 for the options. Select **Search**, then **By Filter**, then **Select Events** on WS to produce the window in Figure 169.

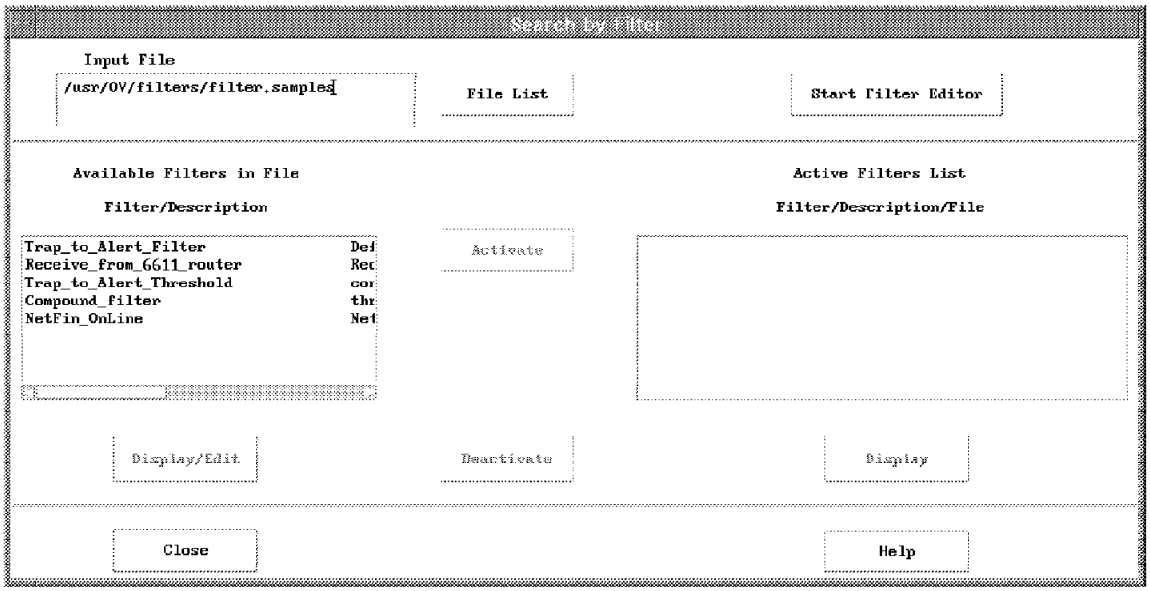


Figure 169. Search Events With a Filter

There are many filters that have already been provided by NetView for AIX, and one that we already customized for NetFinity. If you click on **Start Filter Editor** you will get Figure 170 on page 120.

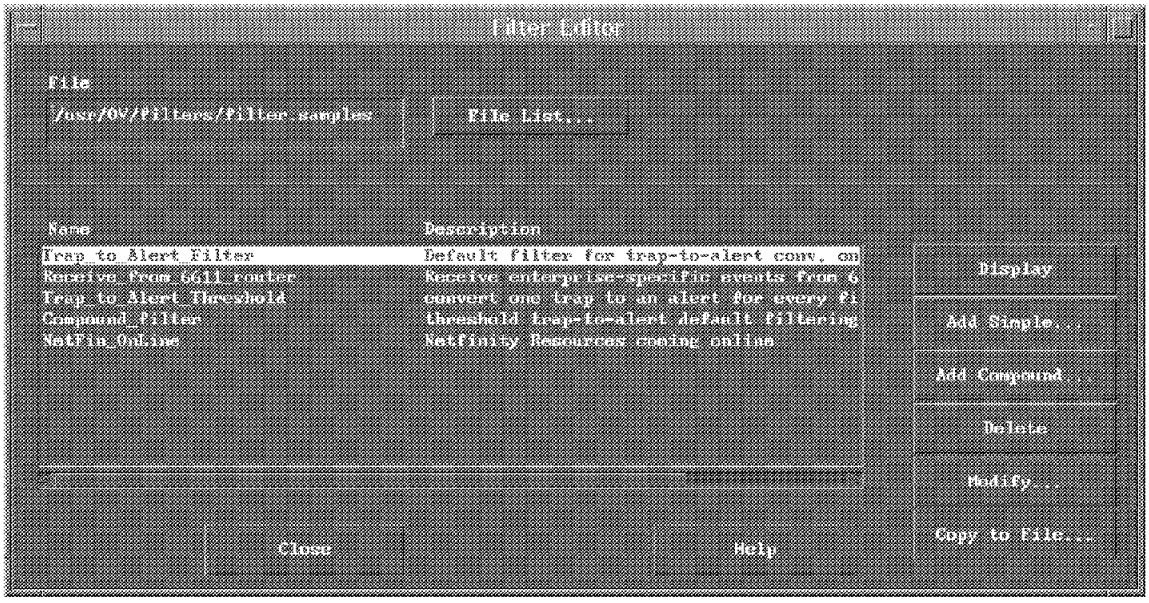


Figure 170. Filter Editor

To begin customizing for our specific event, you click on **Add Simple**. Then, in the new window click on **Events Equal to Selected**. You then need to click on **Add/Modify**. This will give you a list of all of the Enterprise Specific traps, as shown in Figure 171 on page 121.

Since NetFinity only sends one trap type, in this case specific trap number 9, we add that to the Selected Trap Types field after clicking on the NetFinity Enterprise Name in Figure 171 on page 121.

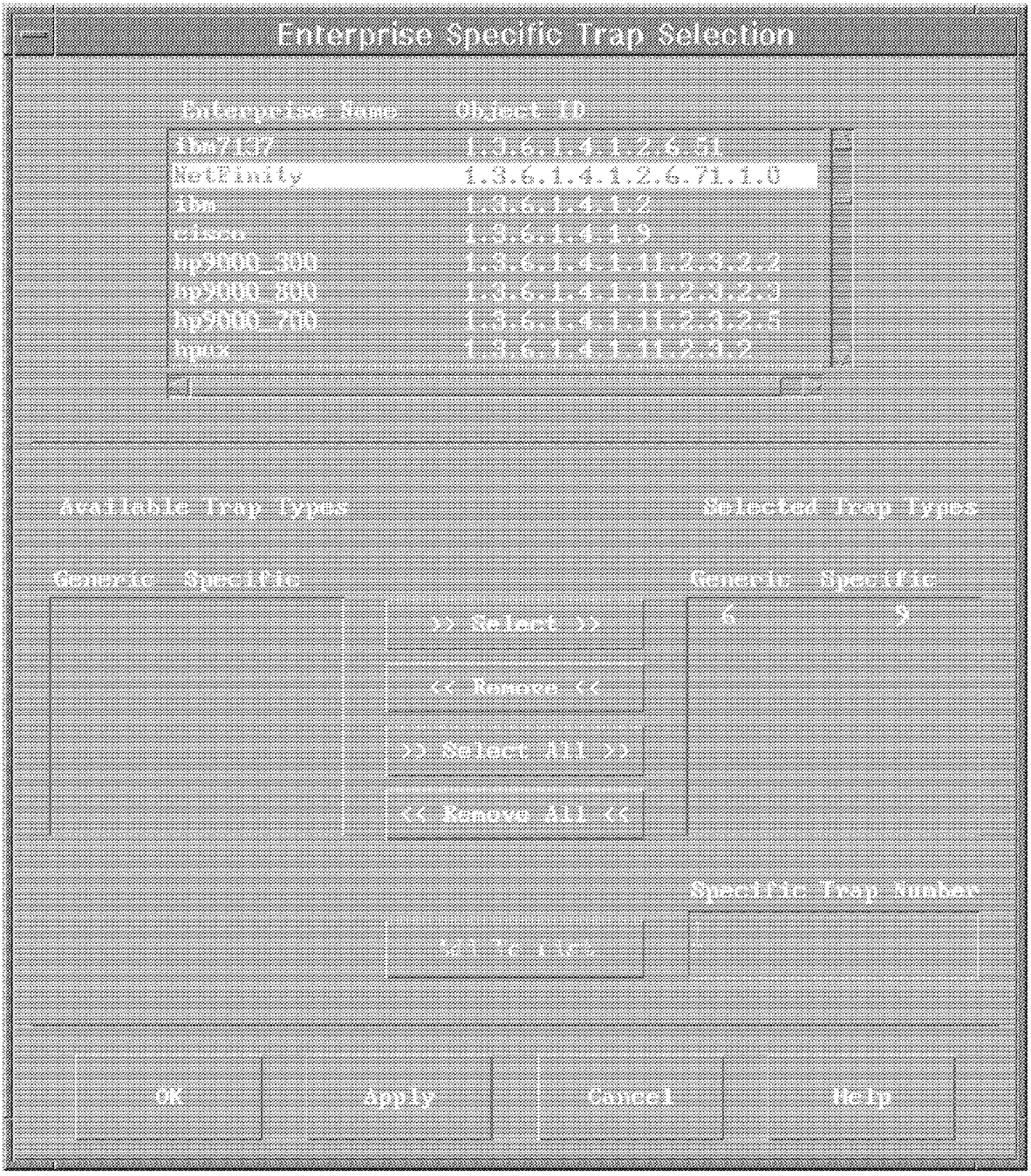


Figure 171. Enterprise Specific Trap

If you are not going to select a specific object ID, you just need to specify a filter name and optionally give it a description. Then click on **Save as** or **OK**.

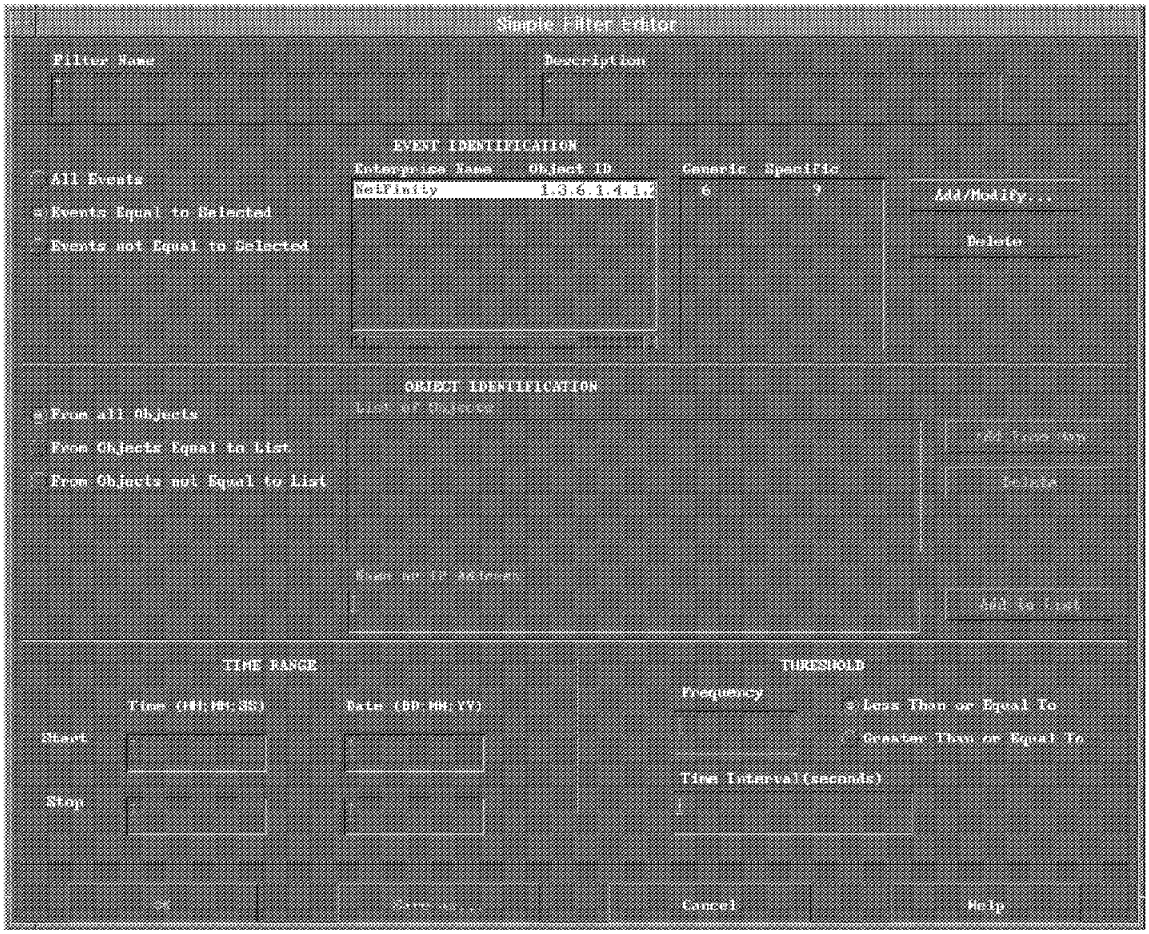


Figure 172. Simple Filter Editor for NetFinity Events

This brings you back to the Filter Editor. Simply click on **Close** if you have no more changes to make.

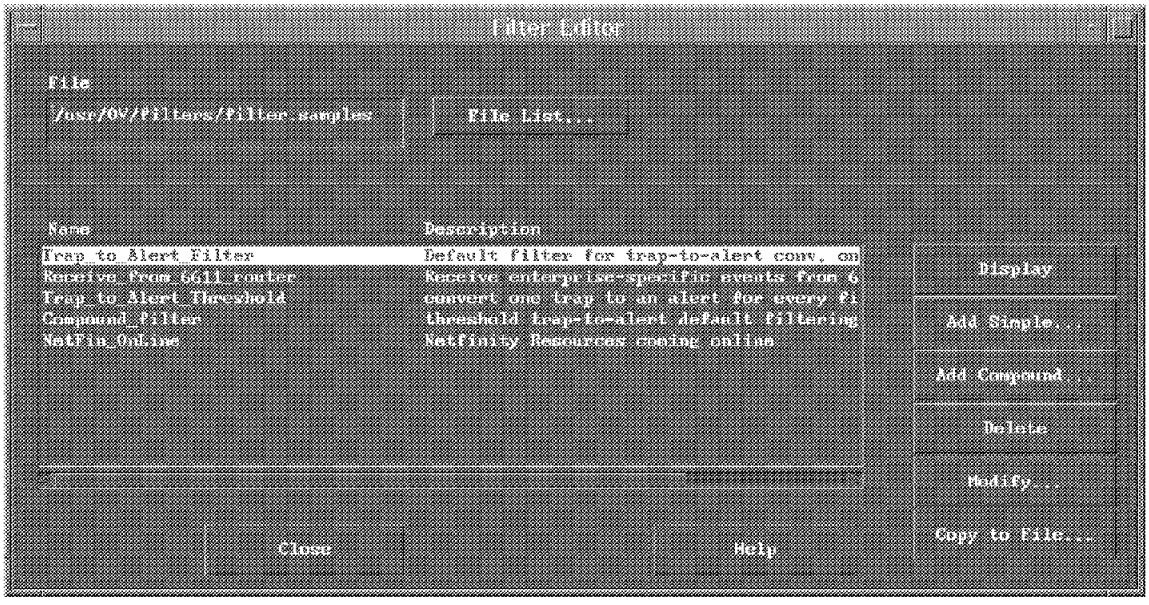


Figure 173. Filter Editor Changes Complete

You will be brought back to the Search by Filter window that is shown in Figure 169 on page 119. To specify the specific filter you wish to now use, click on **File List** and select the filter you created as shown in Figure 174 on page 123.

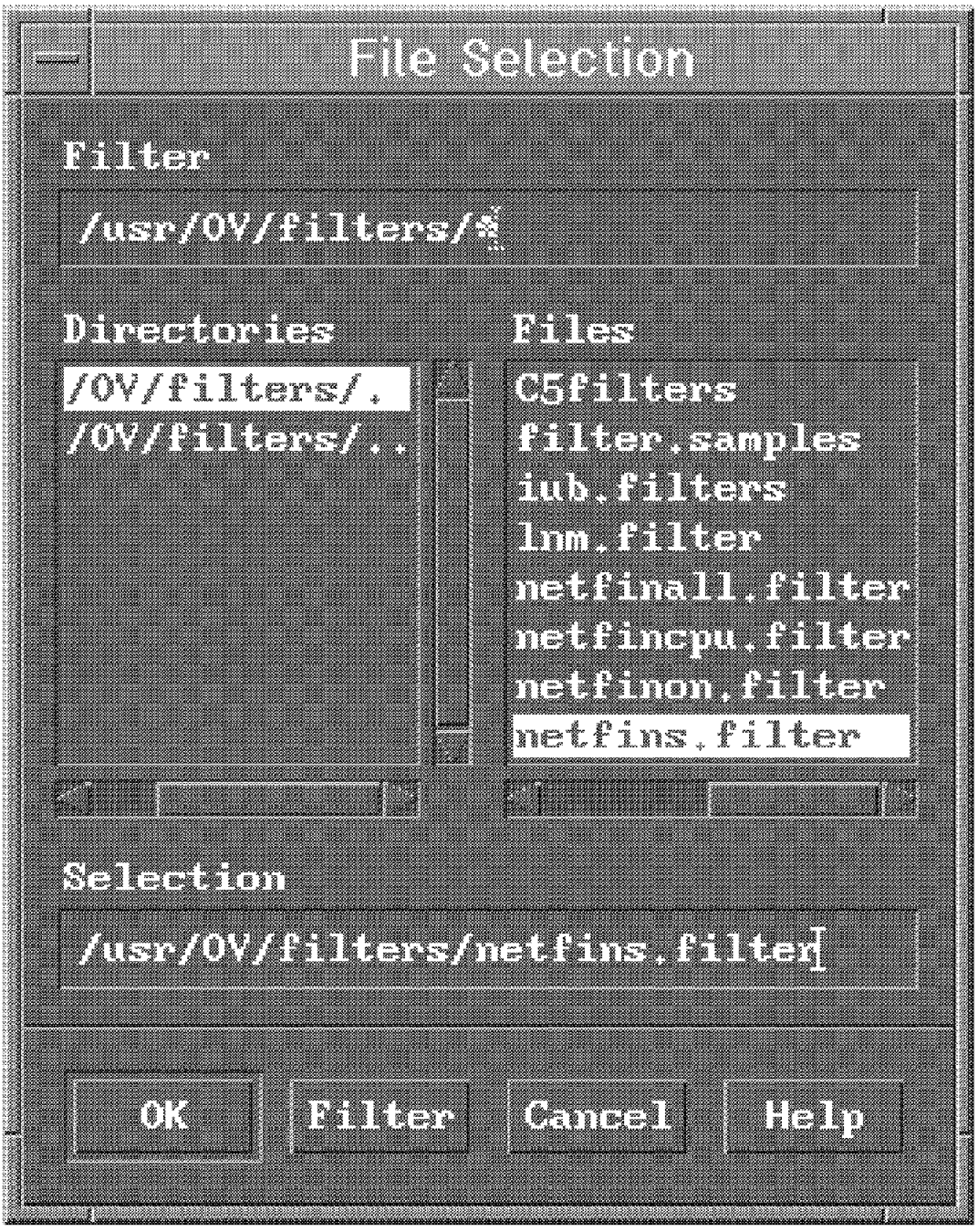


Figure 174. Select the Filter You Created

This will place the filter in the box under Filter/Description, as shown in Figure 175 on page 124. Click on the filter, then on **Activate**.

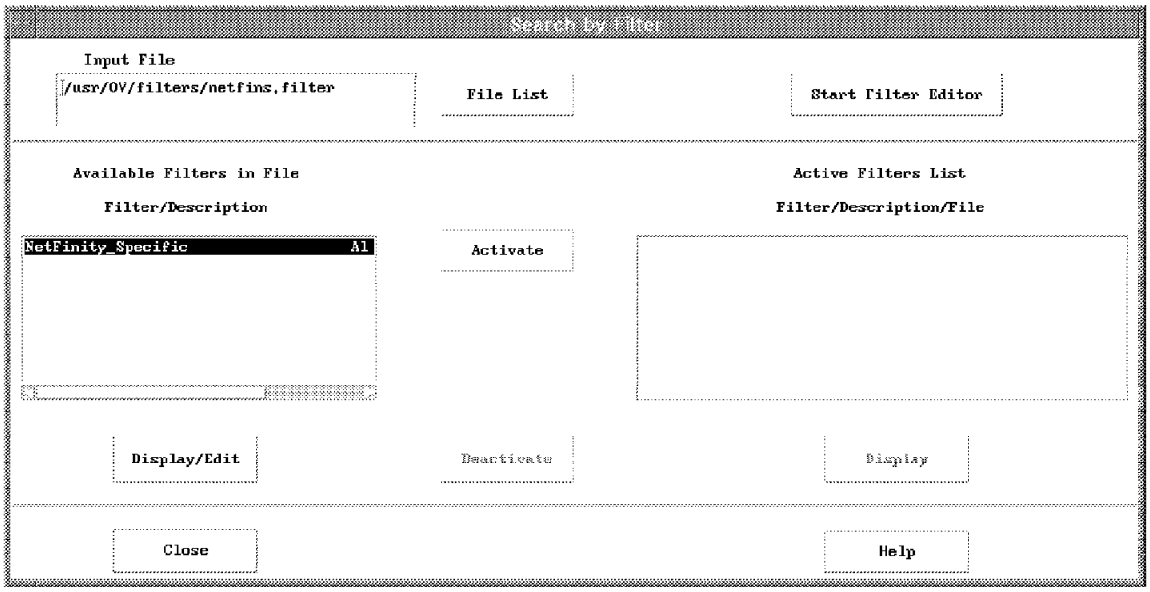


Figure 175. Activate Filter

This should find the next available event in the event window that matches the filter criteria.

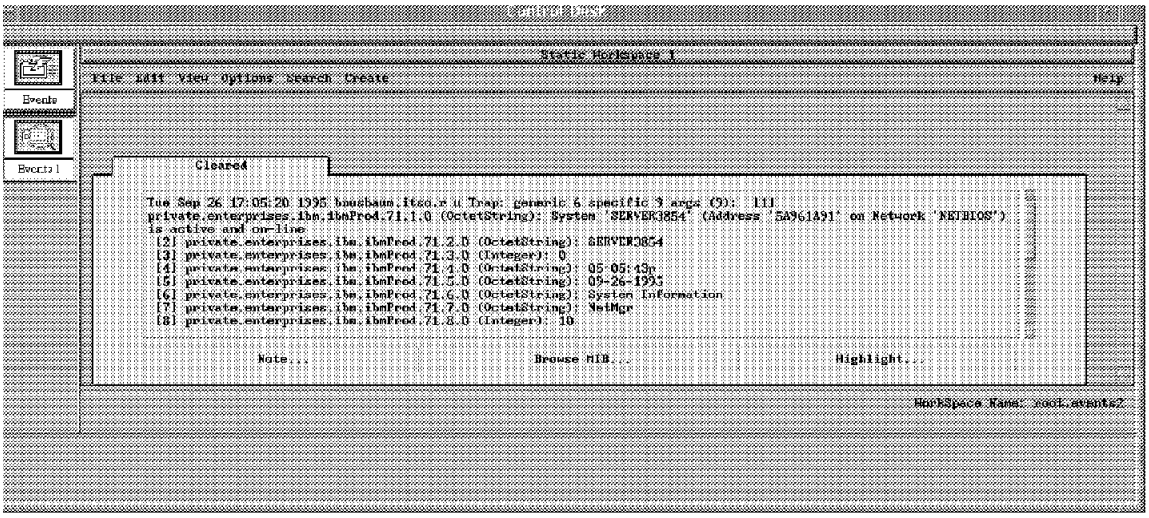


Figure 176. Search for Event Card

If you selected the pull-down options in Figure 176 Create->Static Workspace->Selected->Trap type, you would get a static window of all NetFinity traps that have occurred, as shown in Figure 177 on page 125.

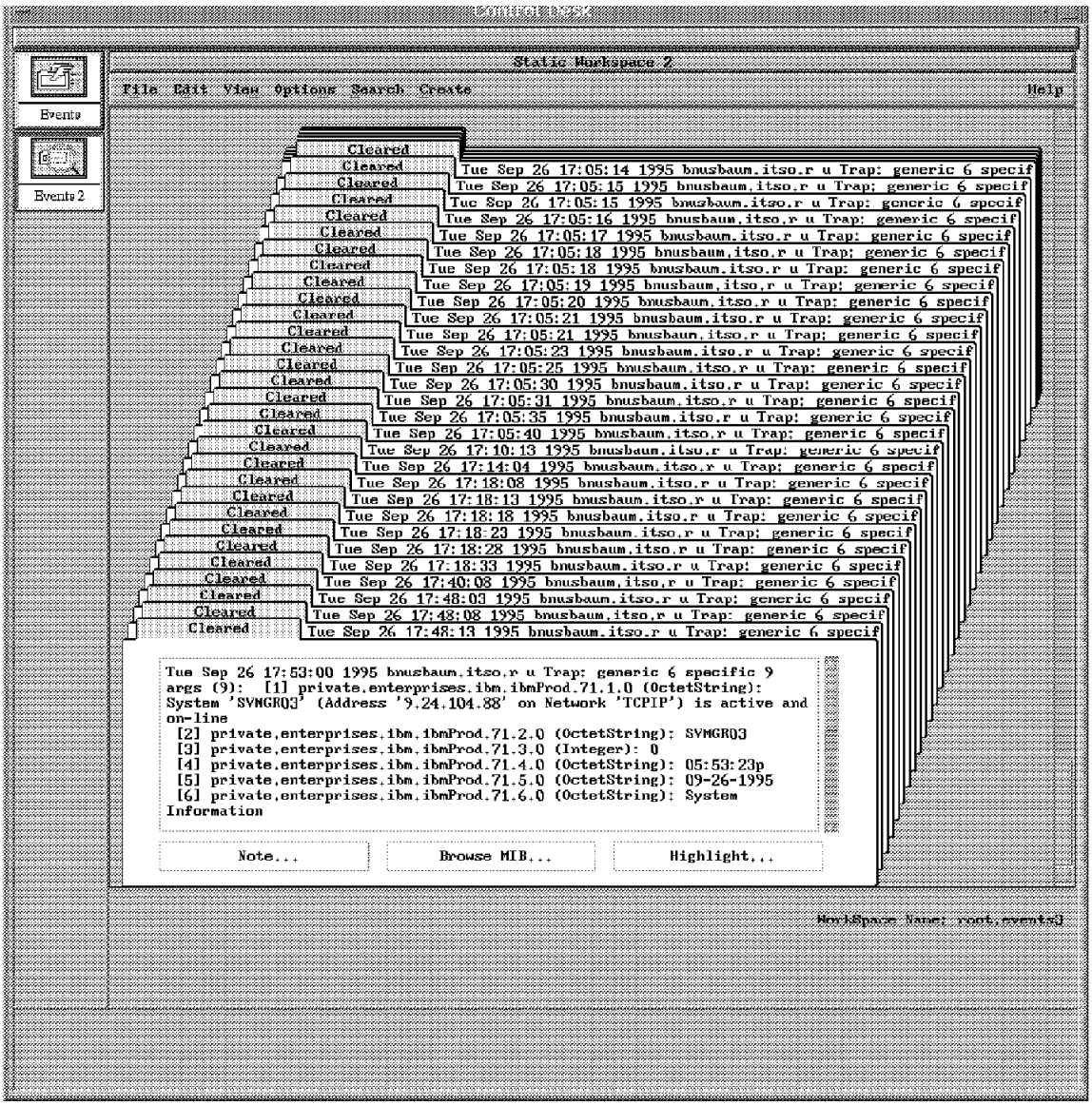


Figure 177. Static Workspace for NetFinity Events

Another alternative is to click on **Dynamic Workspace** in Figure 176 on page 124 to get the following window:

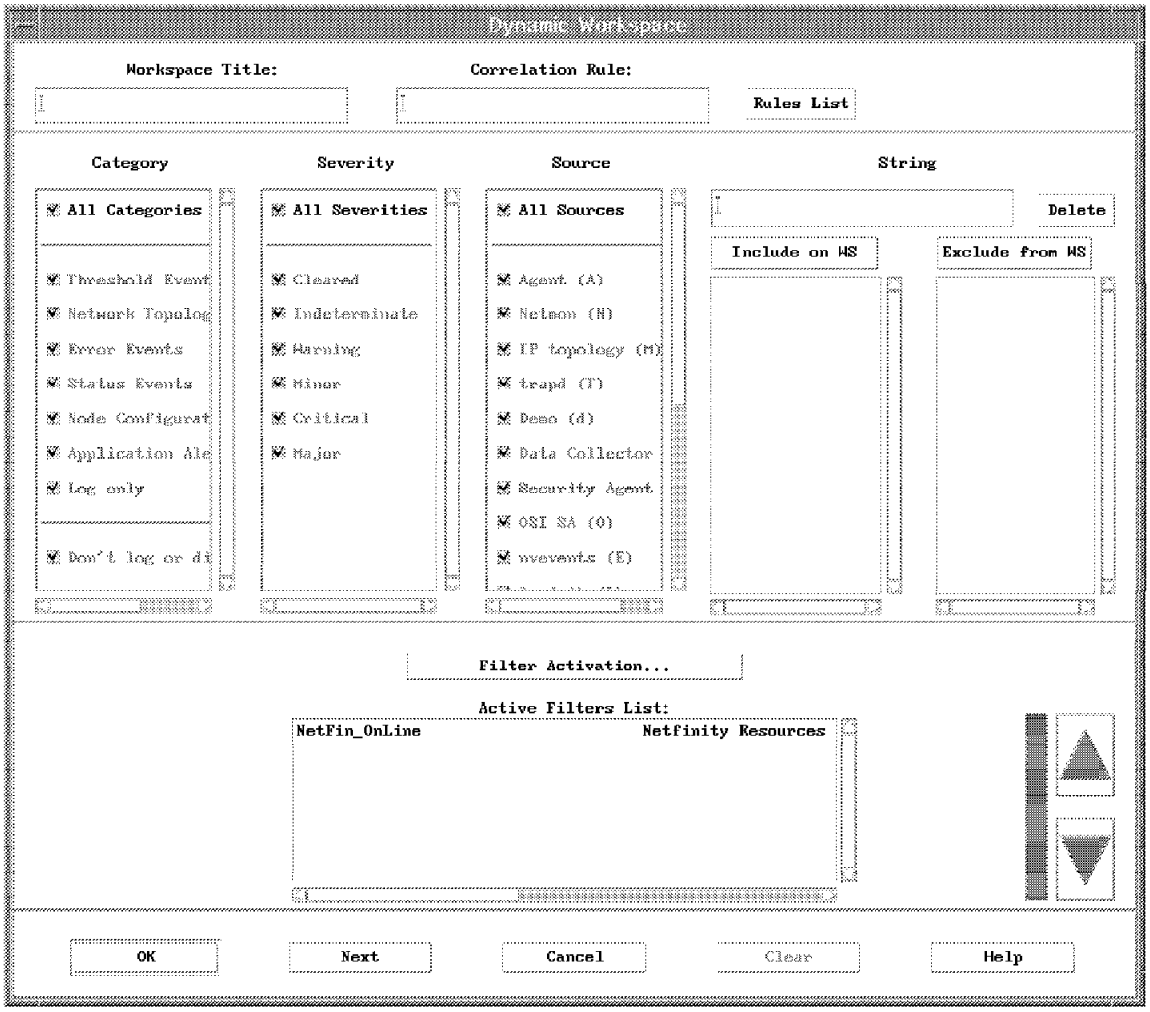


Figure 178. Create Dynamic Workspace

Select the filter you want, and click on **OK** and you will get a dynamic workspace as shown in Figure 179 on page 127. Whenever new events for this trap type flow to NetView for AIX, the dynamic workspace, and the regular Events window will get updated.

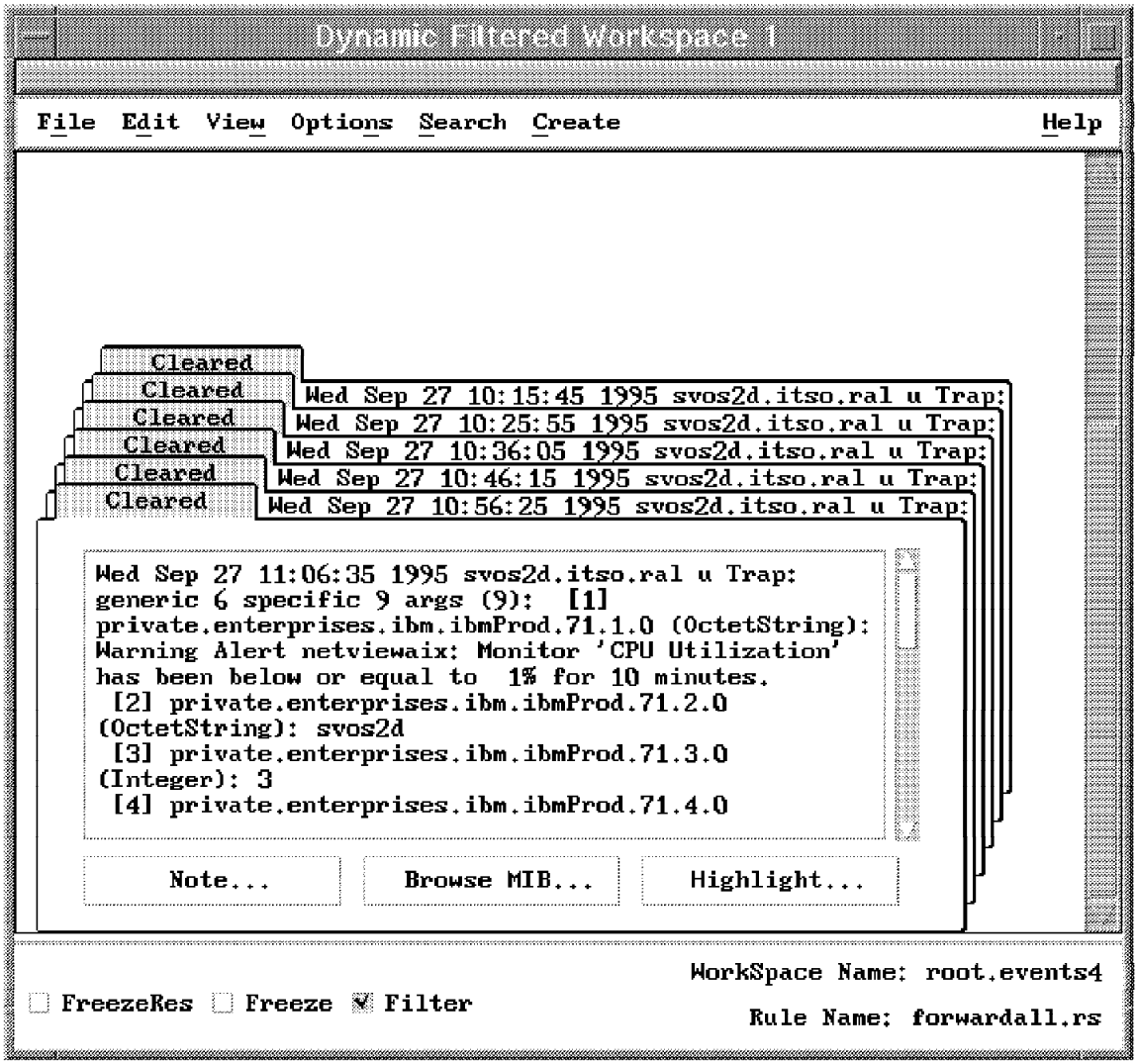


Figure 179. Dynamic Filtered Workspace

6.2.1 Remote Commands

If we wanted to have automation start a remote command back on the NetFinity workstation manager, we could use the facilities of NetView for AIX and TCP/IP. In Figure 180 on page 128 we show the pull-down windows that you need to start trap customization.

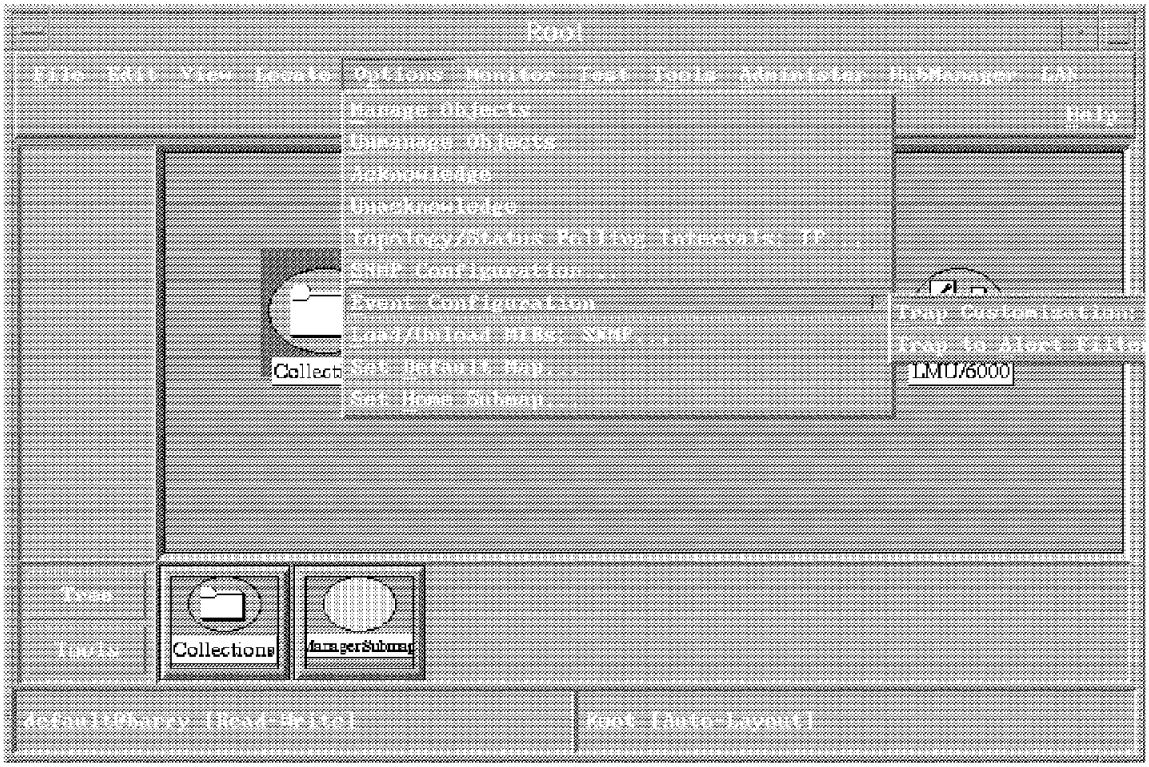


Figure 180. Trap Customization

The resulting window will be Figure 181. Select NetFinity, its Enterprise Specific trap and either Add or Modify.

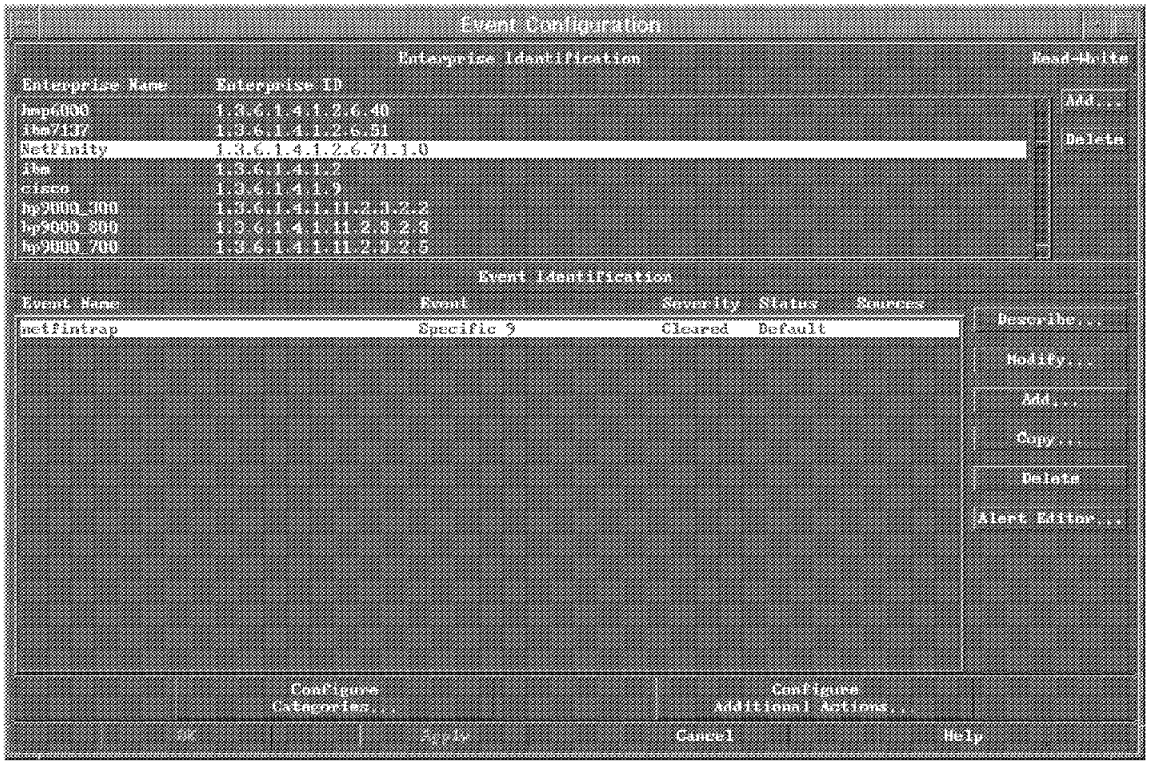


Figure 181. Event Customization

In Figure 182 on page 129 you can enter a rexec command to start the system's monitor facility on the NetFinity manager when you get a trap for high CPU utilization. The command that you need to use for that facility is `mongui`. If you look back at Figure 159 on page 113, you will see a list of all the NetFinity services you can start remotely.

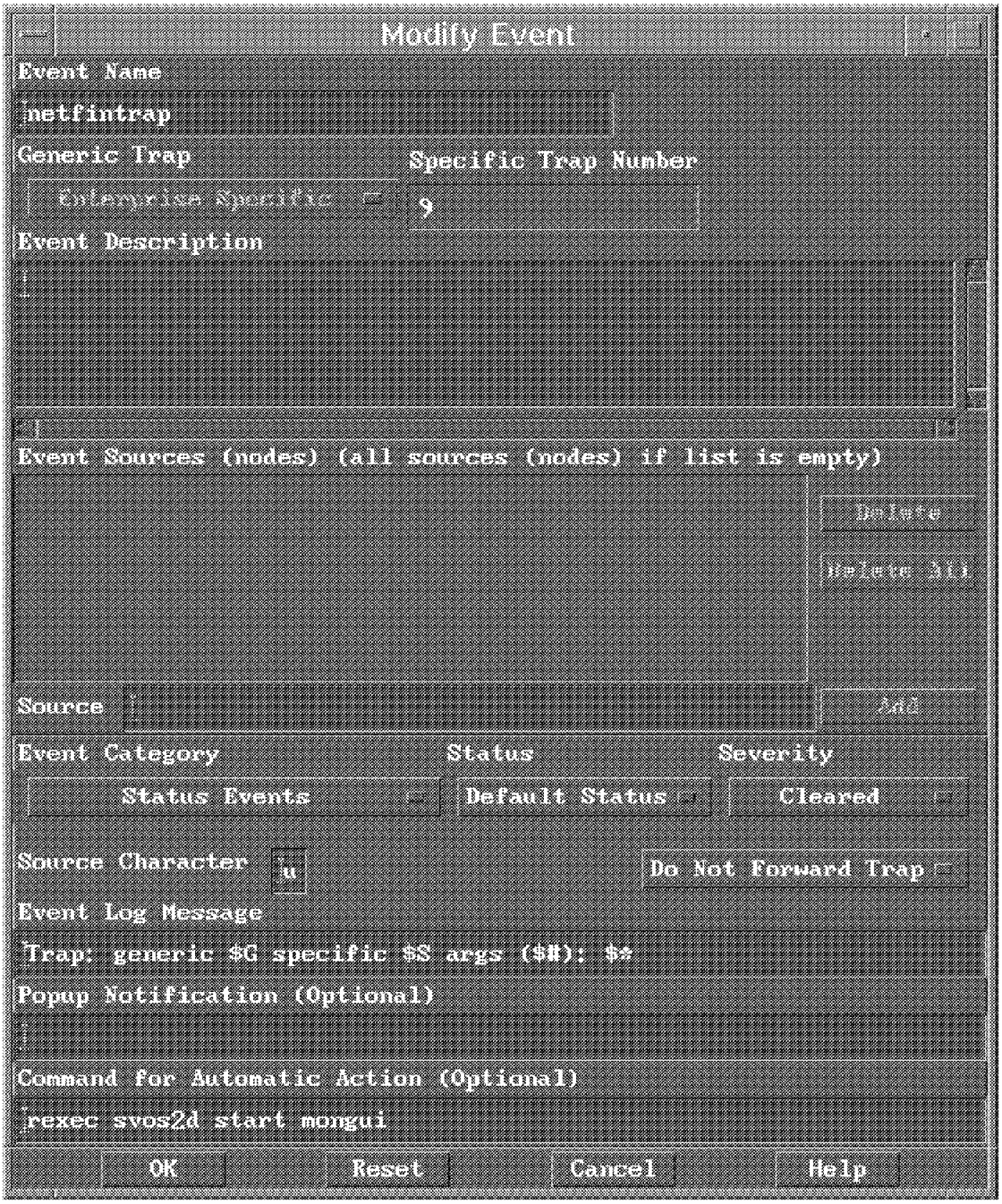


Figure 182. Command for Automatic Action

6.3 NetFinity and NetView for AIX Ruleset Editor

NetView for AIX V4.1, which runs on either AIX V3.2.5 or AIX V4.1.3 introduced a new function called Event Stream Enhancements. Along with ESE, there was a new tool called a Ruleset Editor that was introduced. These two functions help you set up your environment so that you only see and act on the events that you care about. All the others can be discarded. The creation of the rules is done using a graphical interface which looks like a flowchart of the process you wish the events to flow through. There are decision points in this stream as well as action points.

An event continues along a given route in the ruleset until it reaches a decision point that it can′t pass or until it reaches the end of the route. The way the rules are created, you can have several branches, or decision points, where different actions can happen. The daemon, nvcordd, will attempt to send every event that it receives along each path. To help reduce path length for processing purposes, it is best to place the most restrictive decision node at the beginning of each route through the ruleset.

Each ruleset is stored as a single file containing definitions for the nodes and the connections between them. However, you do not need to understand the format of these files. ESE includes a powerful graphical ruleset editor which allows you to draw the ruleset as a simple map and then save it in the ruleset file.

An application that wishes to use ruleset processing has to do two things:

- Register itself and the ruleset it wants to be processed
- Wait for events to be forwarded to it

ESE has an API which provides these functions, however, in the current release of NetView for AIX the API is not published. The only applications that currently use ESE are:

- nvevents - The event display application. In fact it is the server component, nvserverd, that opens the interface. nvevents allows you to create dynamic event workspaces with rulesets applied to them.
- actionsvr - This daemon executes automatic commands when they are invoked within a ruleset by an action or pager node. In fact, actionsvr performs this function for any application, so if you activate a dynamic event workspace and the ruleset includes an action node, it will be executed by actionsvr. You can also register rulesets that *only* perform automated actions by updating a configuration file.

6.4 Understanding the Ruleset Editor

The Ruleset Editor is available by selecting **Tools** and then **Ruleset Editor** from the NetView for AIX menu bar, or by dragging the Ruleset Editor icon from the tool bar and releasing it anywhere on the screen. Two windows will appear on the screen: The Template window and the Ruleset Work Area as shown in Figure 183 on page 131 and Figure 184 on page 131. The Template window contains all the possible templates of nodes that can be added to the Ruleset Work Area. To add a node to the Ruleset area, simply drag a template from the Template window into the work area.

A brief description of each type of template is listed in Table 1 on page 131.

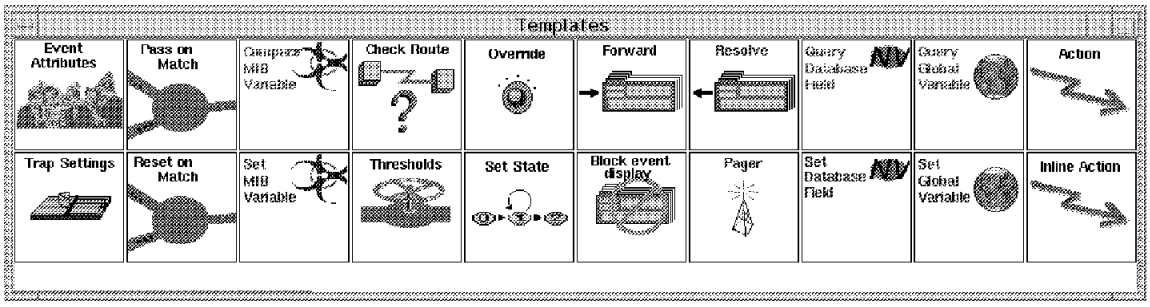


Figure 183. Ruleset Template

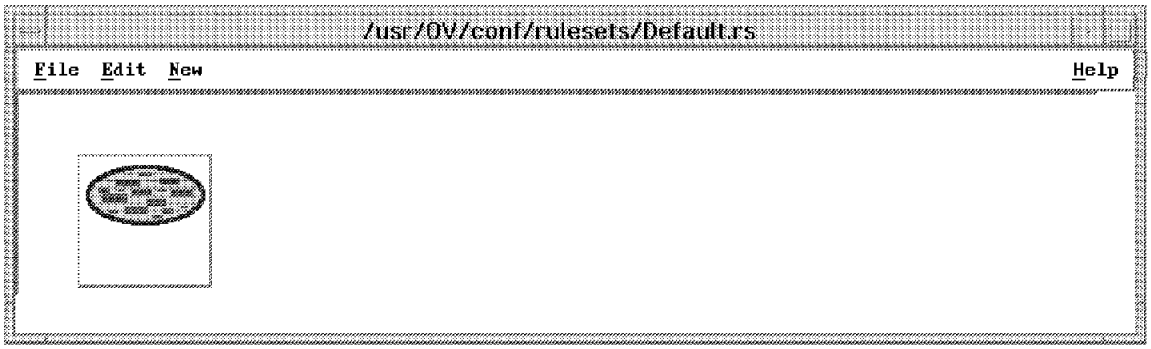


Figure 184. Ruleset Work Area

Table 1 (Page 1 of 3). Ruleset Editor Templates. Decision nodes control whether an event proceeds further into the ruleset. Action nodes invoke some shell or synchronous action.

Template	Node Type	Description
Action	Action	Specifies the action to be performed when an event is forwarded to this node. For example, you could use this node to execute the /usr/OV/bin/ovxecho command to display a dialog window. The action defined is performed by the actionsvr daemon.
Block Event Display	Action	Causes the event not to be forwarded (if the default action is to forward it).
Check Route	Action	Checks for communication between two network nodes and forwards the event based on the availability of this communication. For example, you can use this node to check the path from the Manager to a device before forwarding a node down trap.
Event Attributes	Decision	Compares any attribute of the incoming event to a literal value. For example, you can use this node to check for events generated by a particular device.
Forward	Action	Forwards the event to applications that have registered to receive the output of the ruleset. For example, when the registered application is nvevents, you must use the Forward node if you want to display the event.

Table 1 (Page 2 of 3). Ruleset Editor Templates. Decision nodes control whether an event proceeds further into the ruleset. Action nodes invoke some shell or synchronous action.

Template	Node Type	Description
Inline Action	Action	Specifies an action to be performed. Unlike the Action node, which always executes the action under the actionsvr daemon, the Inline Action executes under the main ruleset processing daemon, nvcorrd. Subsequent ruleset nodes wait for the action to complete (or for a timeout to expire).
Override	Action	Overrides the object status or severity assigned to a specific event and updates the Events Display application. For example, you can use this node to change the severity to Major when a node down event is received for a router. Use this node with the query database field node to override status or severity for specific device types.
Pager	Action	Issues a call to a pager that has been defined in a NetView for AIX user profile.
Pass on Match	Decision	Compares attributes between two events. You can use this node to check for two events that have something in common, for example, two events generated by the same node in the network.
Query Database Field	Decision	Compares a value from the NetView for AIX object database to a literal value or to a value contained in the incoming event. For example, you can use this node to check if the originating device is a router.
Query Global Variable	Decision	Queries the value of the global variable that has been previously set using the Set Global Variable node.
Reset on Match	Decision	Delays an event until either a timer has expired or an event with matching attributes occurs. You can use this node to check for two events that have something in common, for example, two events generated by the same node in the network.
Resolve	Action	Forwards a message to all registered applications indicating that a previous event has been resolved. You can use this node to delete an event card from the events display application when an subsequent event is received.
Set Database Field	Action	Sets the value of any NetView for AIX object database field.
Set Global Variable	Action	Sets a variable for use within the ruleset itself. For example, use this node to set a flag whose value will be checked later in the ruleset using the query global variable node.
Set MIB Variable	Action	Issues an SNMP SET command to set the value of a variable in the MIB representing any network resource. For example, you can use this node to dynamically change the configuration of a LAN hub device.

Table 1 (Page 3 of 3). Ruleset Editor Templates. Decision nodes control whether an event proceeds further into the ruleset. Action nodes invoke some shell or synchronous action.

Template	Node Type	Description
Set State	Action	Sets the correlation state of an object in the NetView for AIX object database. The current state is updated in the corrstat1 field in the object database, and the previous value in the corrstat1 field is moved to the corrstat2 field. This process continues until the current state and as many as four previous states are stored in the object database. You can view the correlation state by selecting the object and then selecting the Display Correlation Status option from the context menu.
Thresholds	Decision	Checks for repeated occurrences of the same trap or of traps with an attribute in common. You can use this node to forward an event after receiving the specific number of the same event received within a specific time period. Use this node with the Trap Settings node to identify a specific trap number.
Trap Settings	Decision	Specifies a specific trap to be processed and is identified by a pair of generic and specific trap numbers.

If you select **Tools** and then **Ruleset Editor** as shown in Figure 185 on page 134, you will get the ESE windows for the templates and its work area.

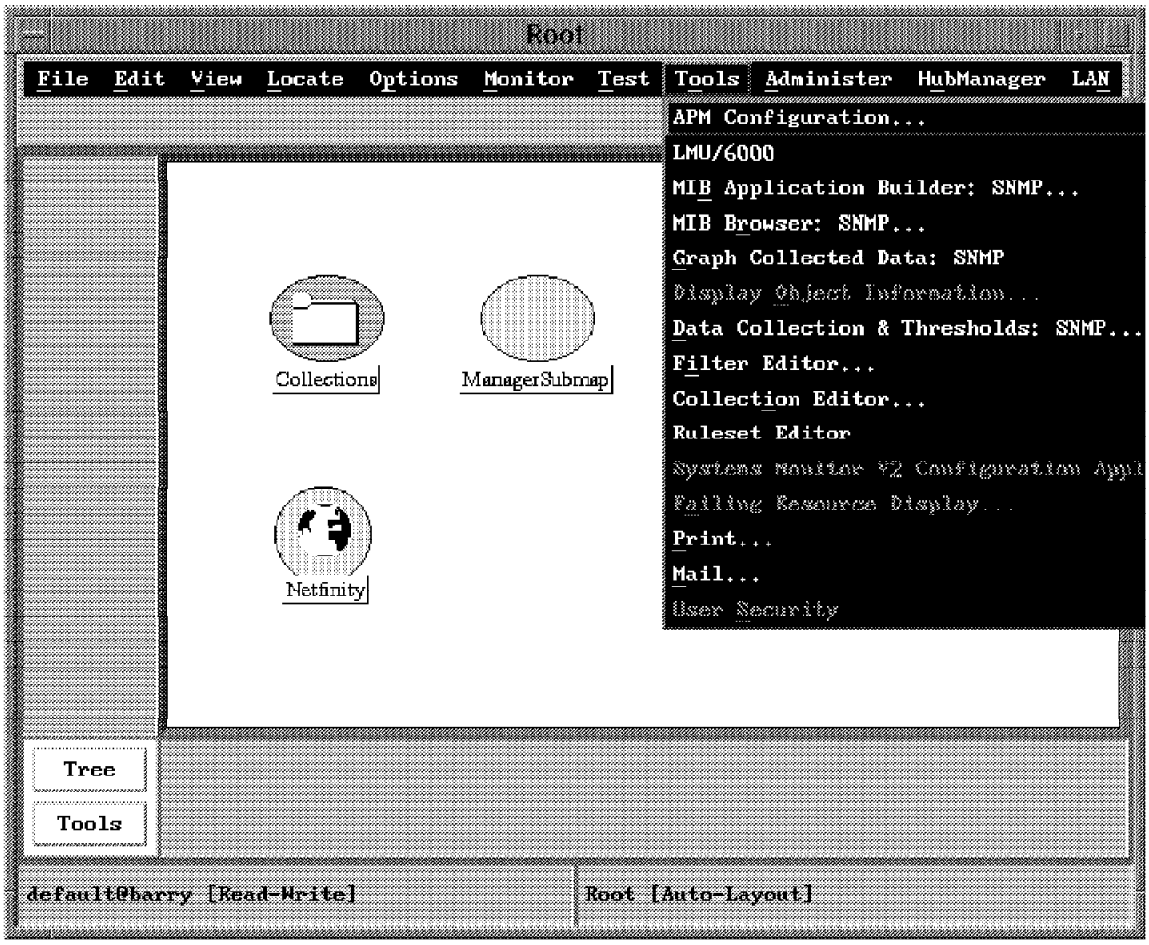


Figure 185. Invoking the Ruleset Editor

In Figure 186 on page 135 the ruleset has already been customized for extracting enterprise specific traps for NetFinity. This figure shows that all events should pass through the filter to check to see if it is from NetFinity's Enterprise ID and its Specific trap number. That logical pair is 1.3.6.1.4.1.2.6.71.1.0 and 9.

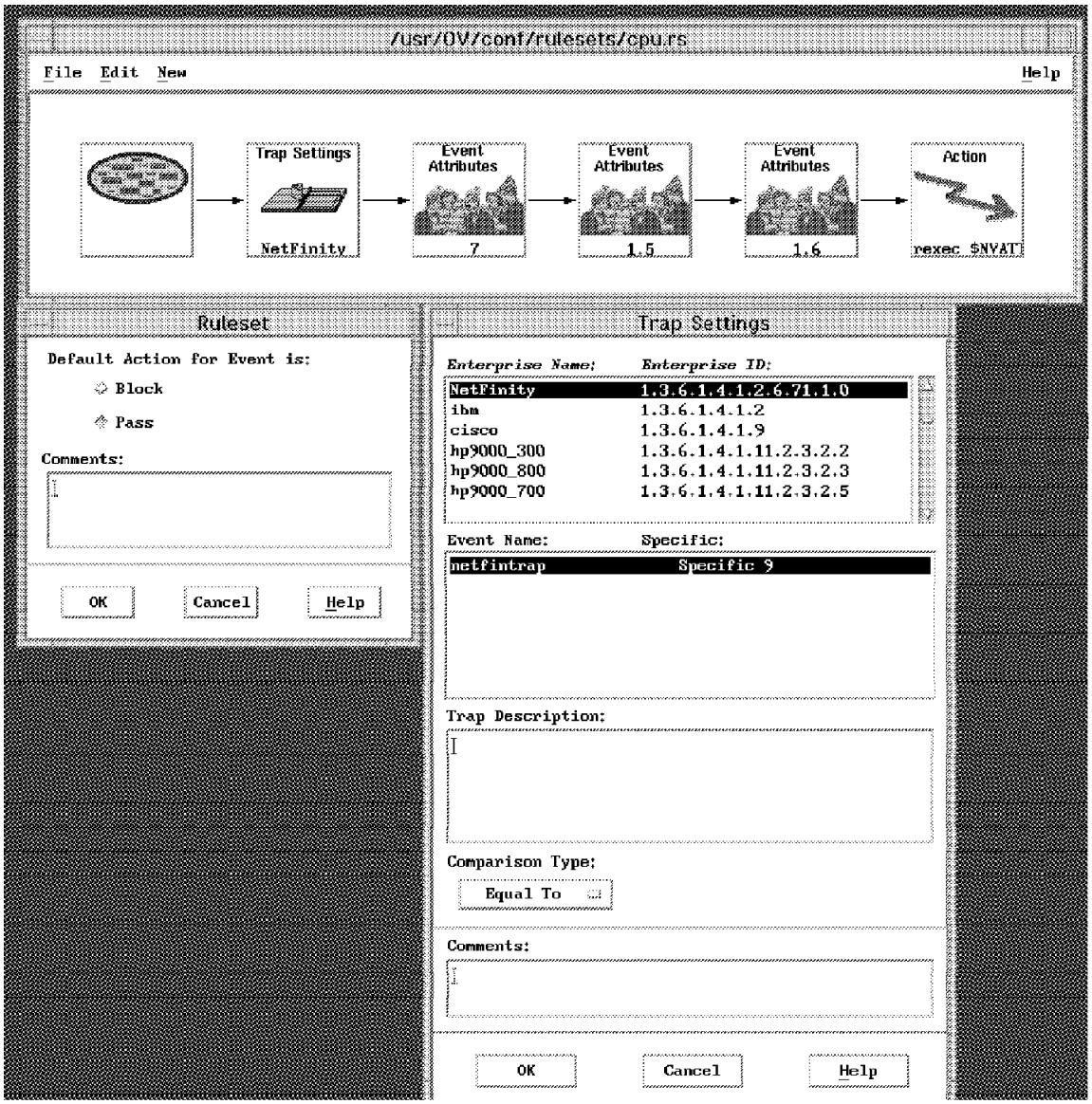


Figure 186. Ruleset Trap Settings

The event cards for NetView for AIX events, as shown in Figure 187 on page 136, provide all the details for the event. On this card you can see the top line of text refers to the CPU Utilization within its text. The keyword CPU is referred to as attribute 1.5 since it is the fifth word on attribute 1. Utilization is 1.6. Note that the single quote actually is used in the comparison, since it parses the string looking for blank characters as delimiters. The seventh attribute, trapApplicationID has the value MonitorB.

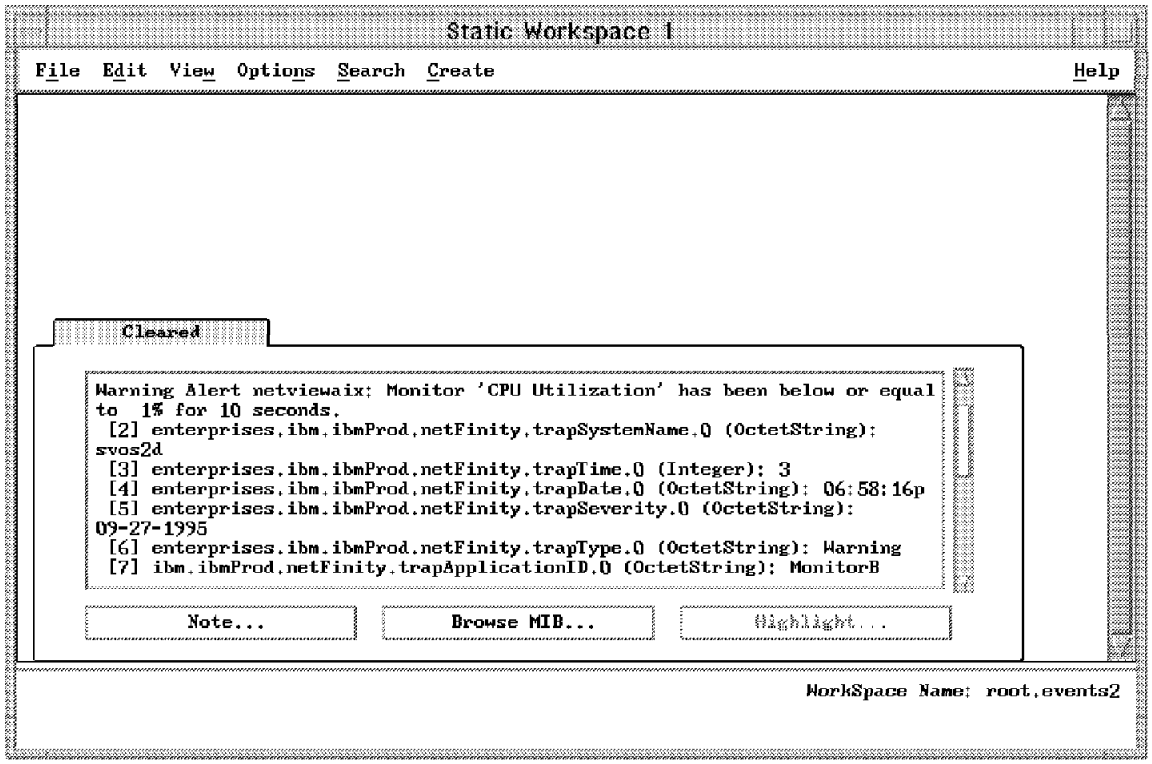


Figure 187. Event Attributes on the Card

All of the text from the card translates into ruleset language using the Ruleset Editor. If you select the Event Attributes symbol from the graphical editor, you can fill in the attribute numbers based upon the fields you would like to compare on. Figure 188 on page 137 translates to a search for a match on CPU Utilization and MonitorB in the trap.

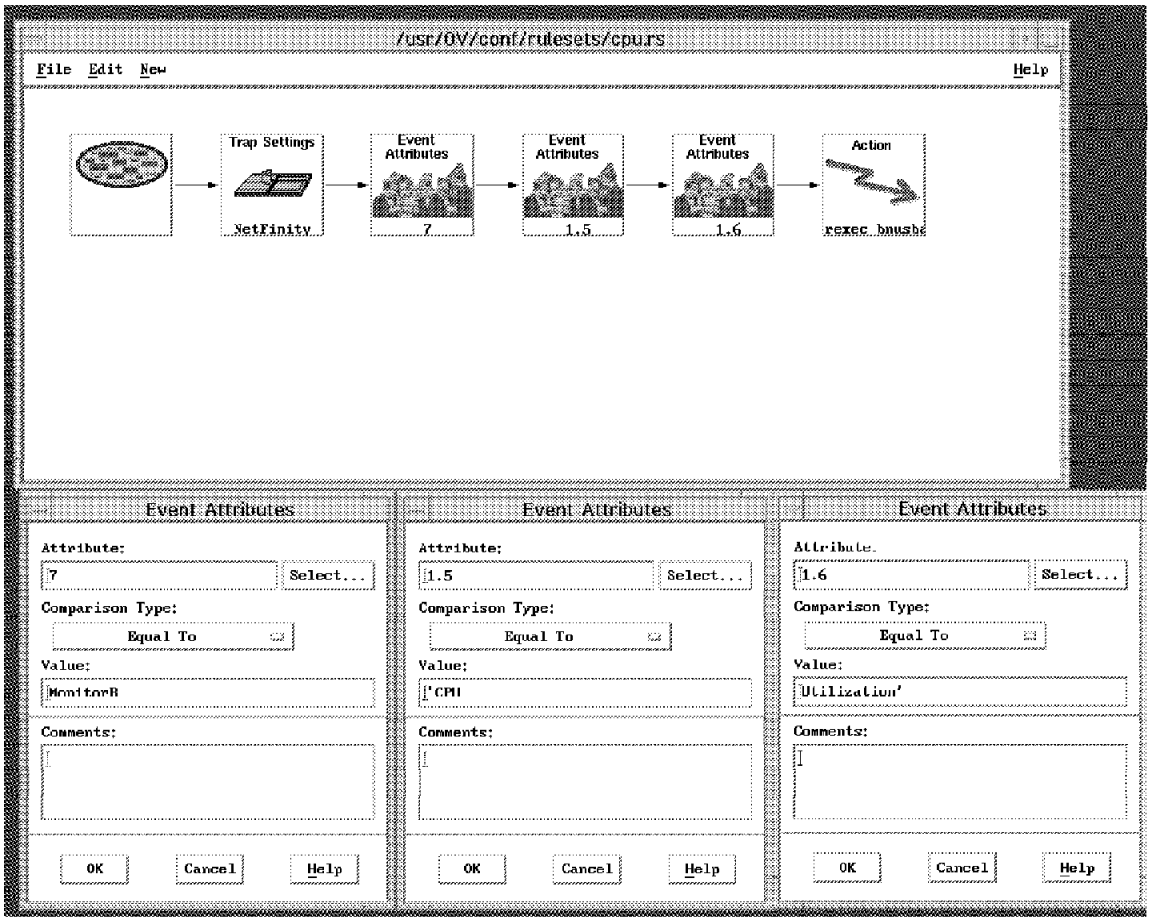


Figure 188. Event Attributes

The last piece of the scenario is based upon the Action symbol shown in Figure 189 on page 138. The action that we take is to issue a rexec command to a variable called $NVATTR_2. This translates into the trapSystemName from the event card in Figure 187 on page 136. If you are using TCP/IP rexec, you will need to make sure that the OS/2 TCP/IP system is enabled for rexec and that you either know the user ID and password for it, or you have .netrc updated on AIX so that you won't be prompted for the password.

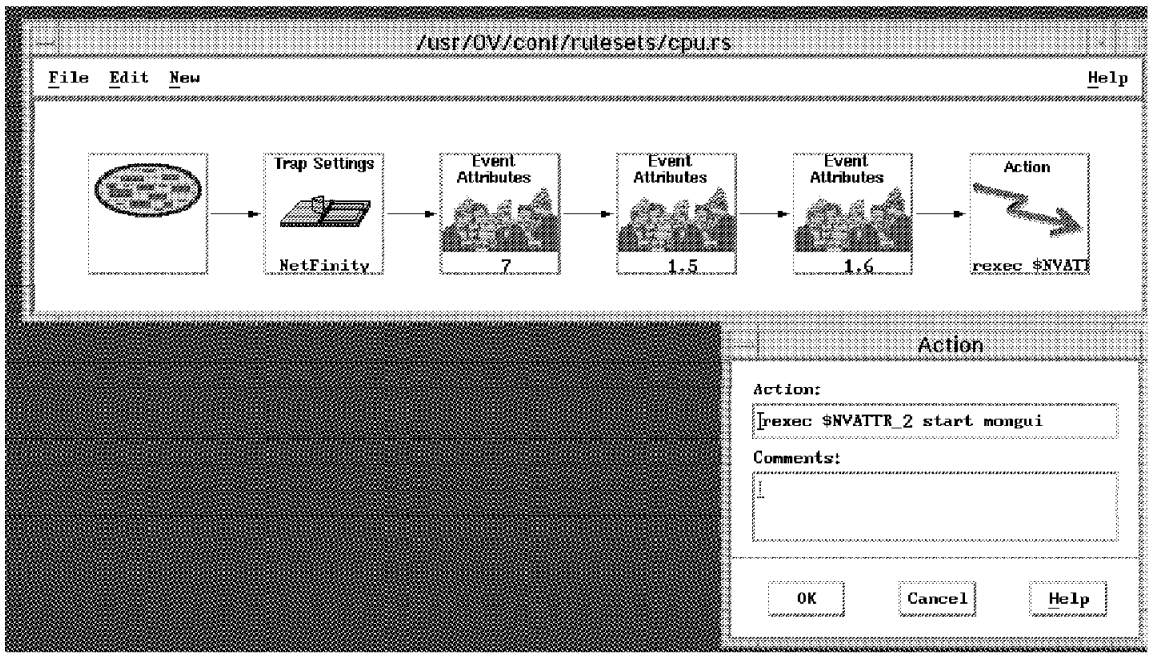


Figure 189. Automatic Command Executed with CPU Utilization Trap Flows

There are two other manual tasks that will need to be performed after you create the new ruleset. You will need to add the name of the new ruleset to /usr/OV/conf/ESE.automation as shown in Figure 190, and you will need to restart the actionsvr daemon as shown in Figure 191 on page 139.

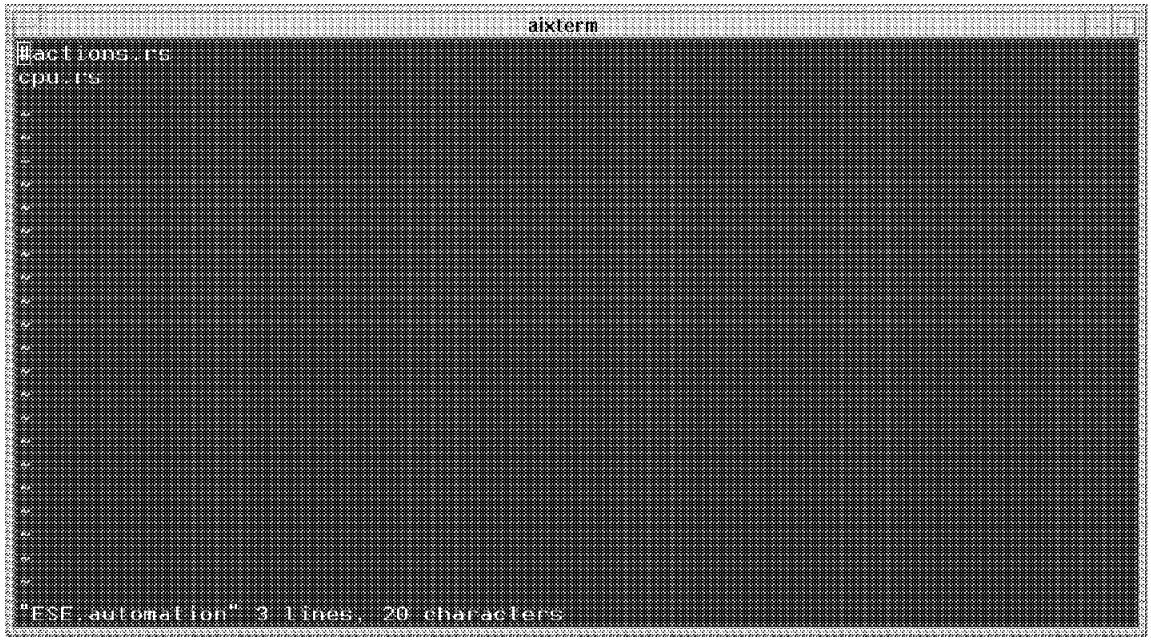


Figure 190. List of Rulesets

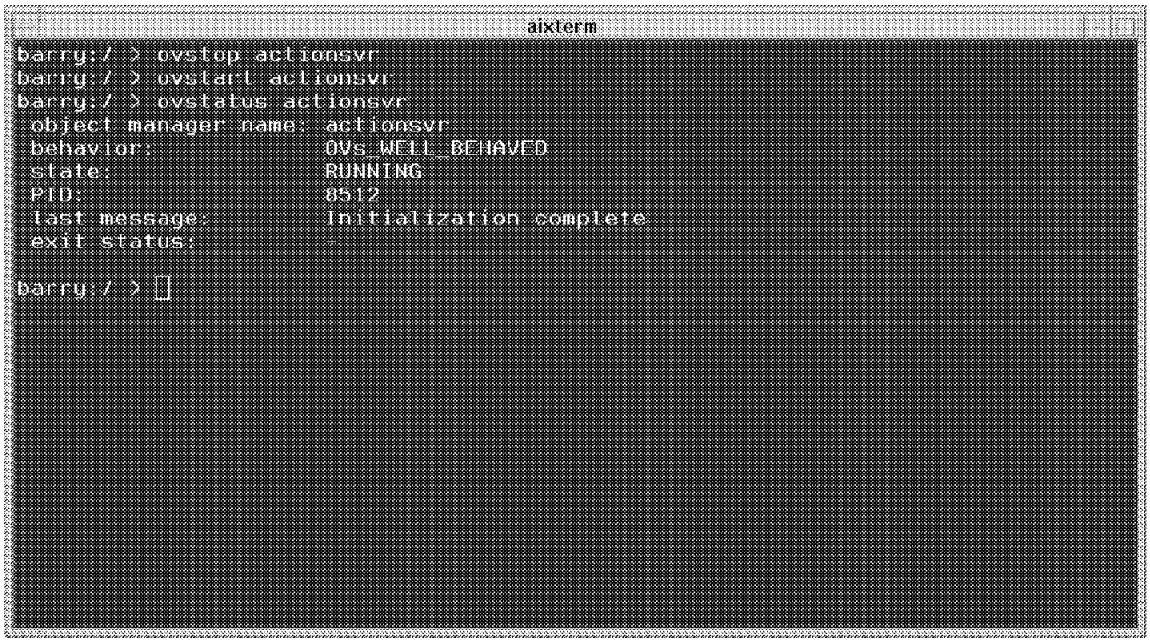


Figure 191. Stop and Start the actionsvr Daemon

Another example of a more complex command that can be issued is shown in Figure 192 on page 140. When this command is executed the following will occur.

Assuming the NetFinity manager is called bnusbaum and its client is represented by the IPX network address of 9.400088889999, TCP/IP on AIX will issue the rexec command to start up all the pre-defined monitors for that IPX connected client on the NetFinity manager bnusbaum.

At this point in time, there is no way to specify which of the individual monitor will get started. There are over a dozen default monitors that come with NetFinity, and you can add more using the Software Developer's Kit (SDK). The only ones that will start when you issue the REXEC command are the ones you have accepted as monitors in the Show Monitors window for NetFinity.

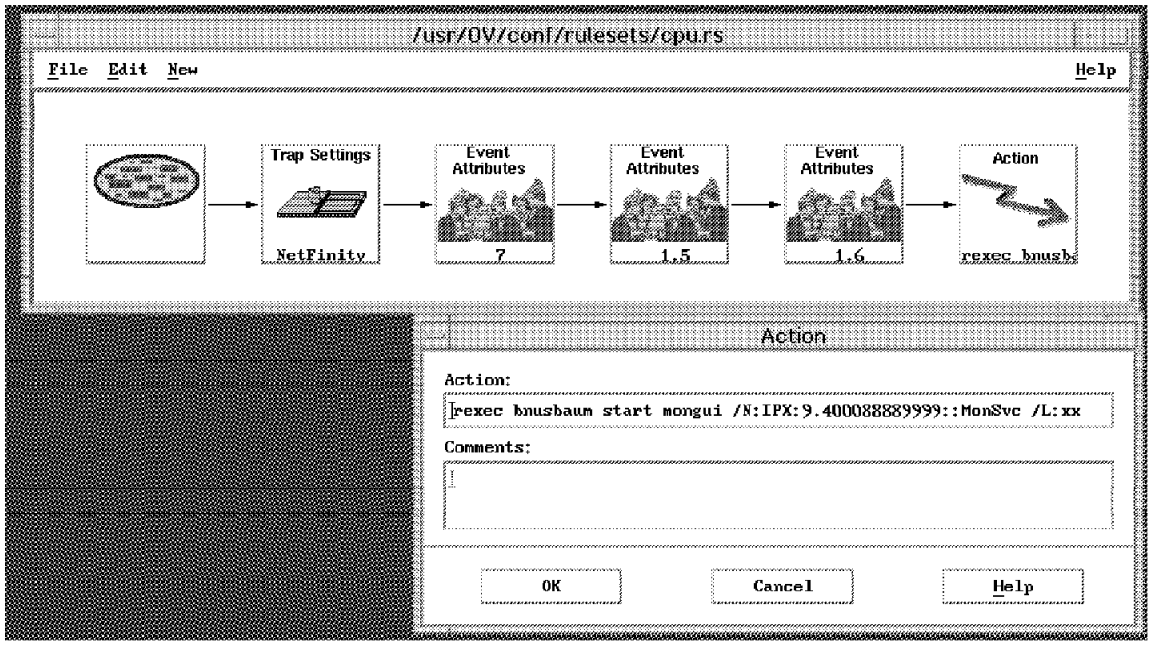


Figure 192. Remote Command Executed When Action Taken

If you use the dynamic workspace capability of nvevents, you can set up a correlation filter to only show NetFinity-related events. Figure 193 on page 141 shows the creation of the dynamic workspace. The Correlation File Selection window pops up when you click on the Rules List.

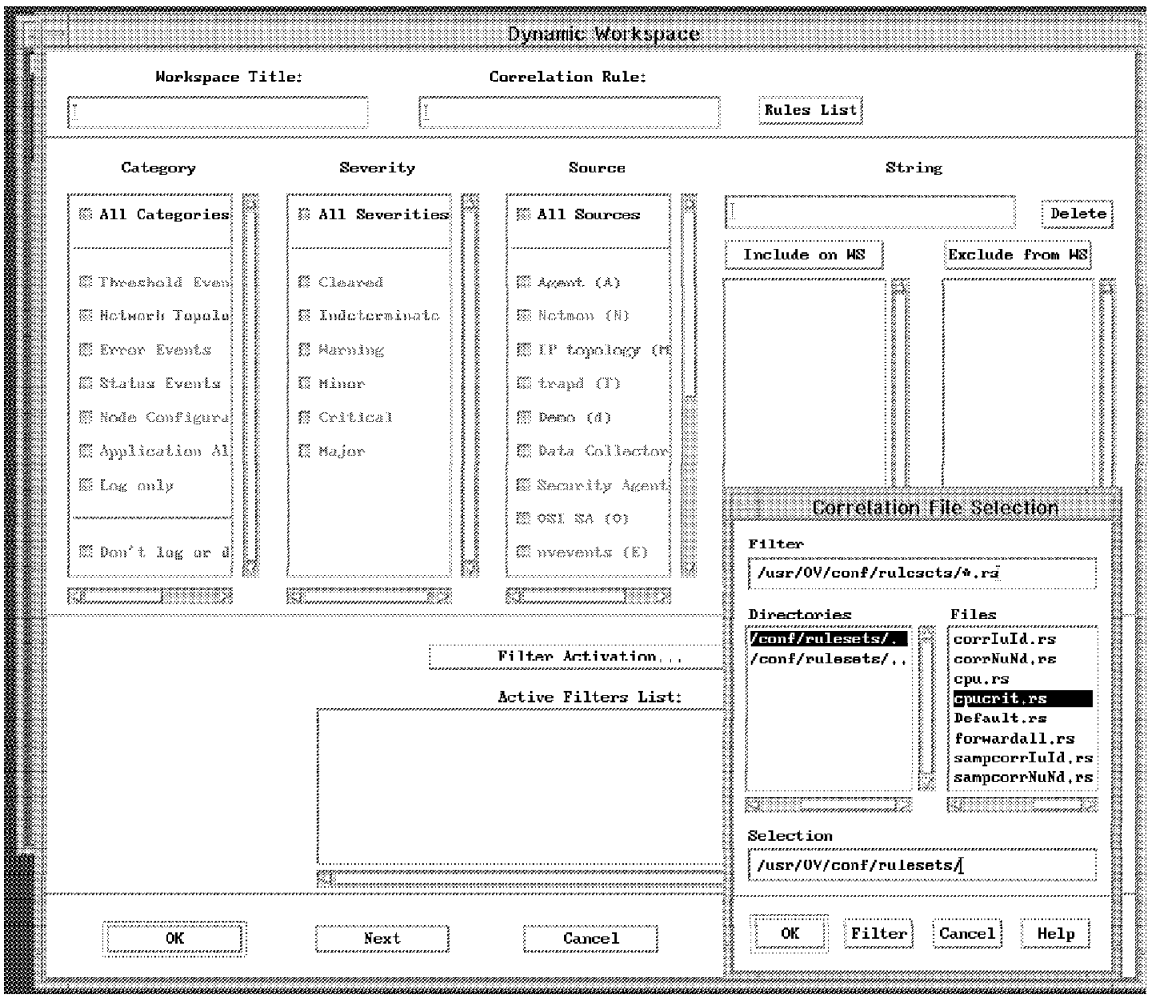


Figure 193. Dynamic Workspace

Chapter 7. NetFinity and NetView for MVS

This chapter looks at a scenario that has alerts flowing from NetFinity to the hardware monitor component of NetView for MVS. After the alert arrives at NetView for MVS, we can issue an action from either an automated operator, or manually enter commands. The setup of this environment will require some customization of Communications Manager/2. The commands will be issued using runcmds.

7.1 NetFinity, FFST and NetView for MVS

In this chapter we show how to convert NetFinity alerts into NetView for MVS alerts. This requires some setup work in Communications Manager/2 V1.11 (CM/2). There needs to be an LU 6.2 session between CM/2 and NetView for MVS. Before the alert gets to CM/2 it will first go to FFST/2.

If you double-click on the **Communications Manager/2** folder on the OS/2 desktop, you will see the icons for CM/2 as shown in Figure 194. To customize our system for an LU 6.2 session, double-click on the **Communications Manager Setup** icon, or type `cmsetup` in an OS/2 window.

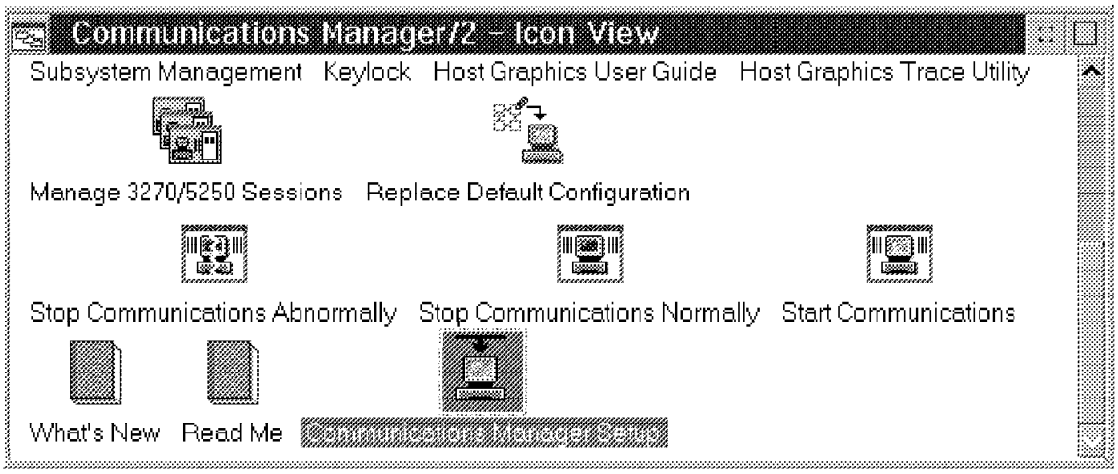


Figure 194. Communications Manager /2 Folder

For this scenario, in Figure 195 on page 144, we created a totally new configuration instead of modifying an old one. The configuration name is WTRNEW. At the end of the customization process there will be four files created in the CMLIB directory. You may want to make a backup of these files as you work on different configurations. The names of the files are:

- WTRNEW.CF2
- WTRNEW.CFG
- WTRNEW.NDF
- WTRNEW.SEC

The description field is just a comment.

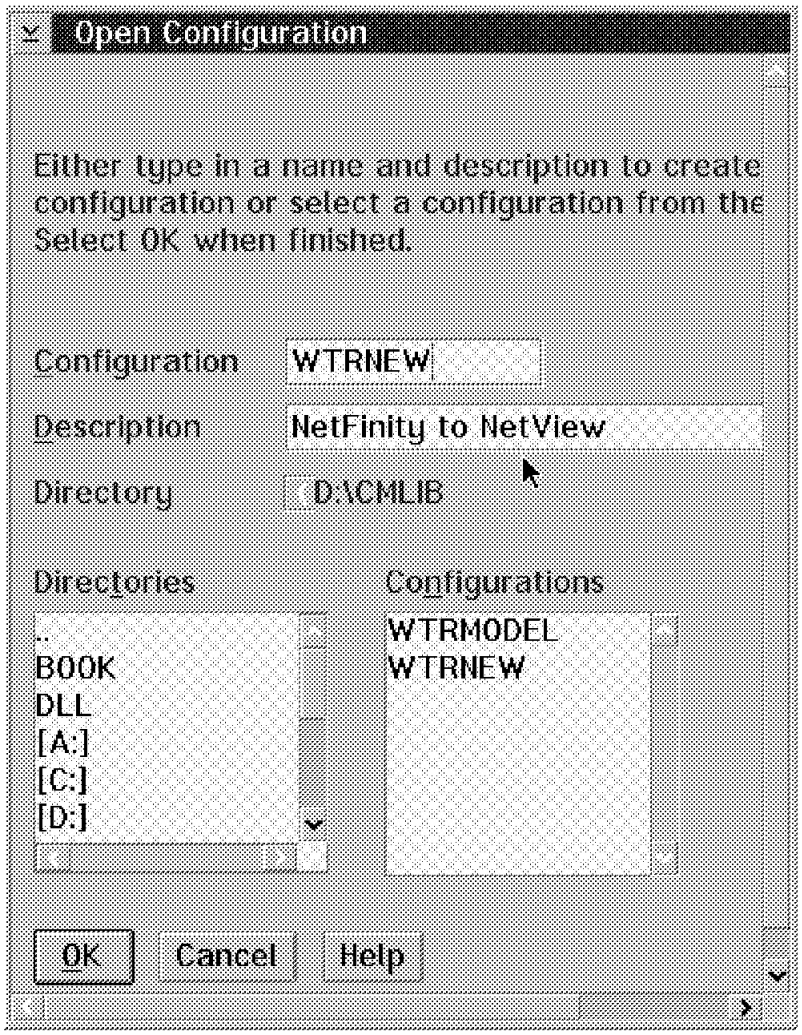


Figure 195. CMSETUP Configuration

After clicking on **OK**, a window will pop-up to check to see if this new configuration will be used on this workstation.

Figure 196. CM/2 Configuration Confirmation

To keep things simple, we selected the **Additional definitions** radio button and we were presented with the two scroll boxes shown in Figure 197 on page 145.

One was for **Workstation Connection Type**, and the other one was for **Feature or Application**.

Since we were using a token-ring, we clicked on the **Token-ring or other LAN types** as a workstation connection type, and on **3270 emulation** as a feature or application.

Note: If you already have 3270 emulation configured on your workstation, then you do *not* have to select it for configuration now.

To select more than one feature or application, such as the APPC APIs (which is mandatory for LU 6.2 communication to the host), press and hold the Ctrl key while clicking on the **APPC APIs** line item.

Next, click on the **Configure** button to configure each profile. You will be shown the Communications Manager/2 Profile List window as shown in Figure 198 on page 146.

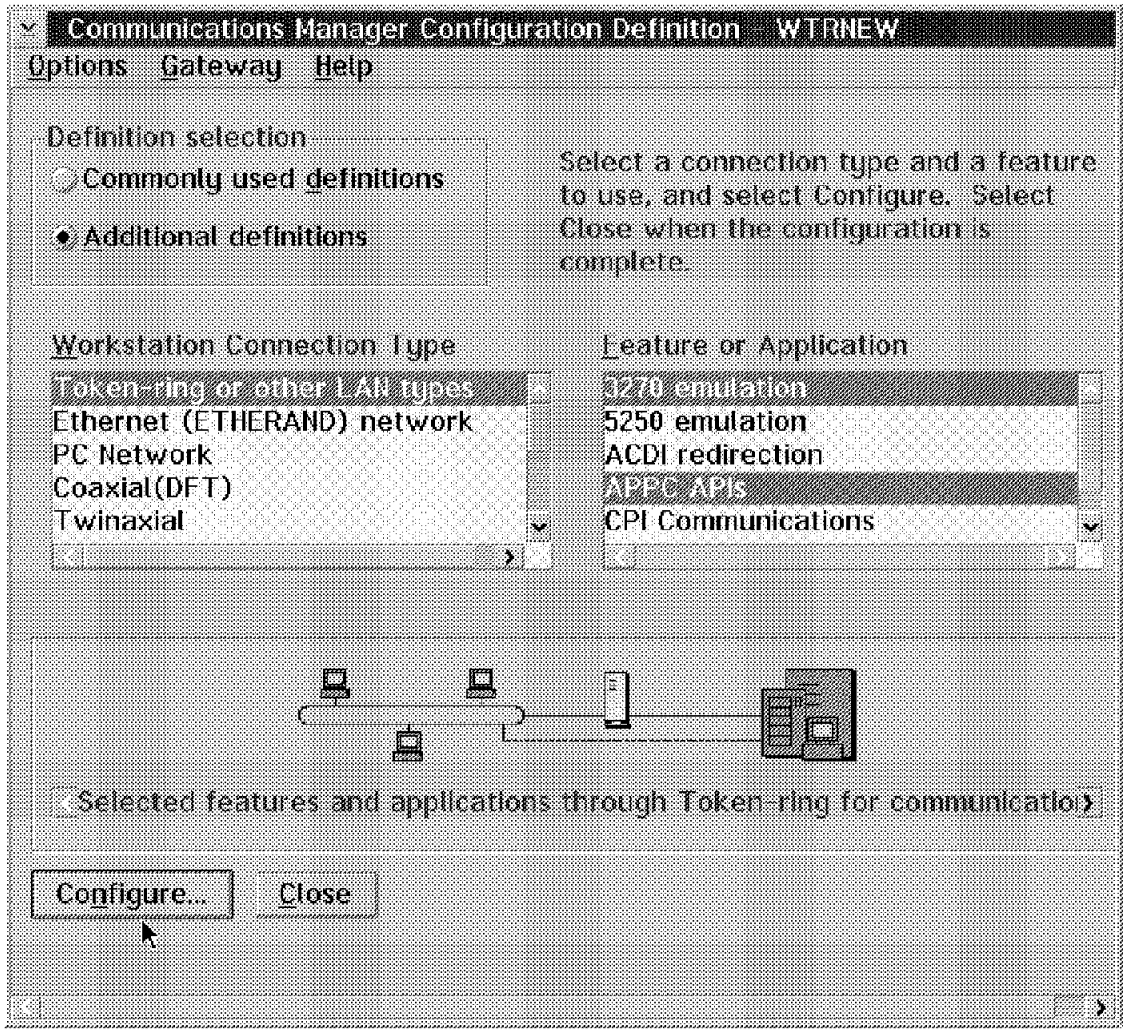


Figure 197. Token-Ring Configuration

The first thing that we will configure is the Data Link Control (DLC) parameters for token-ring. We click on the **DLC - Token-ring or other LAN types** line item as shown in Figure 198 on page 146.

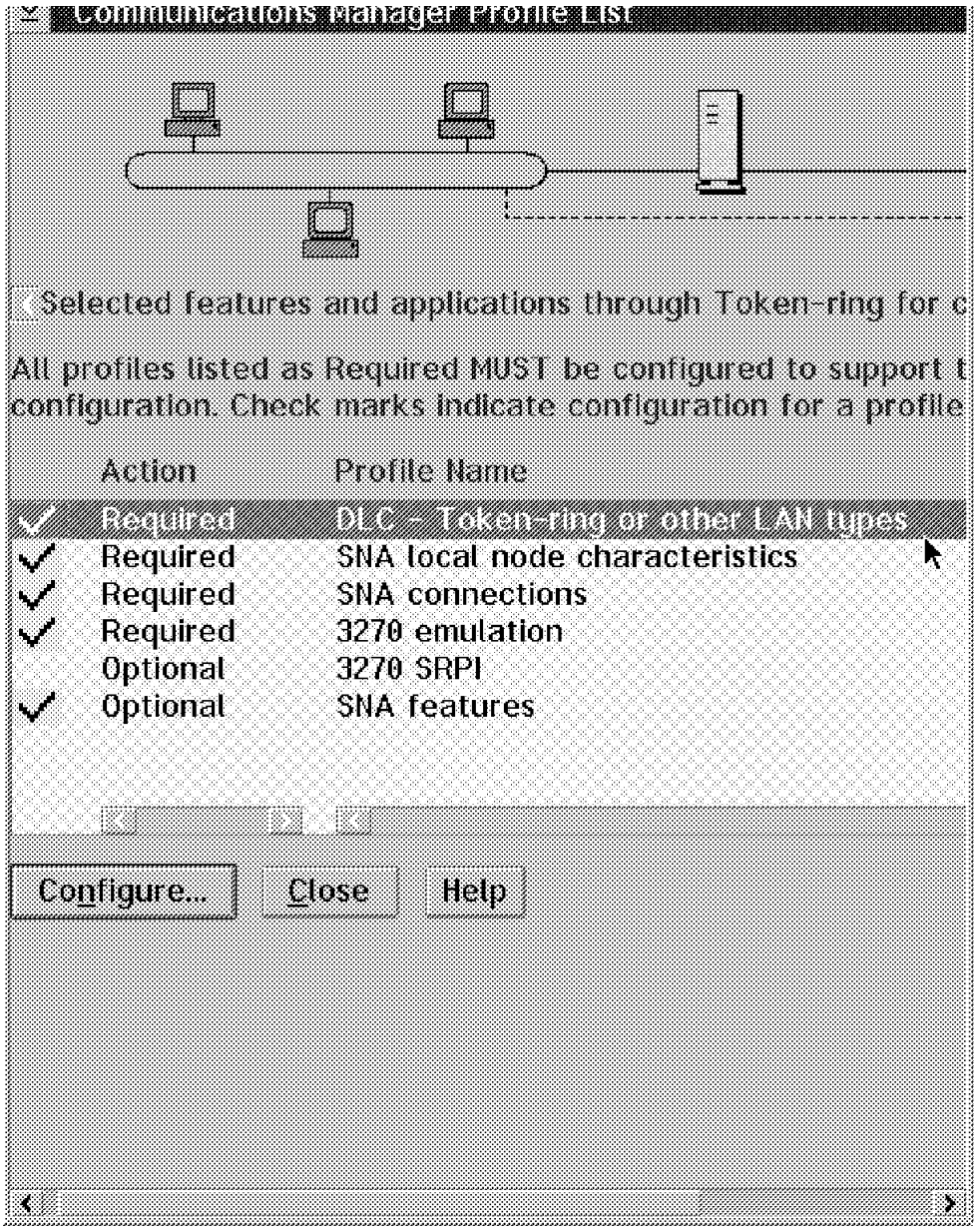


Figure 198. CM/2 Profile Listing

Click on the **Configure** button in Figure 198 and you will get the DLC adapter parameter entry window as shown in Figure 199 on page 147.

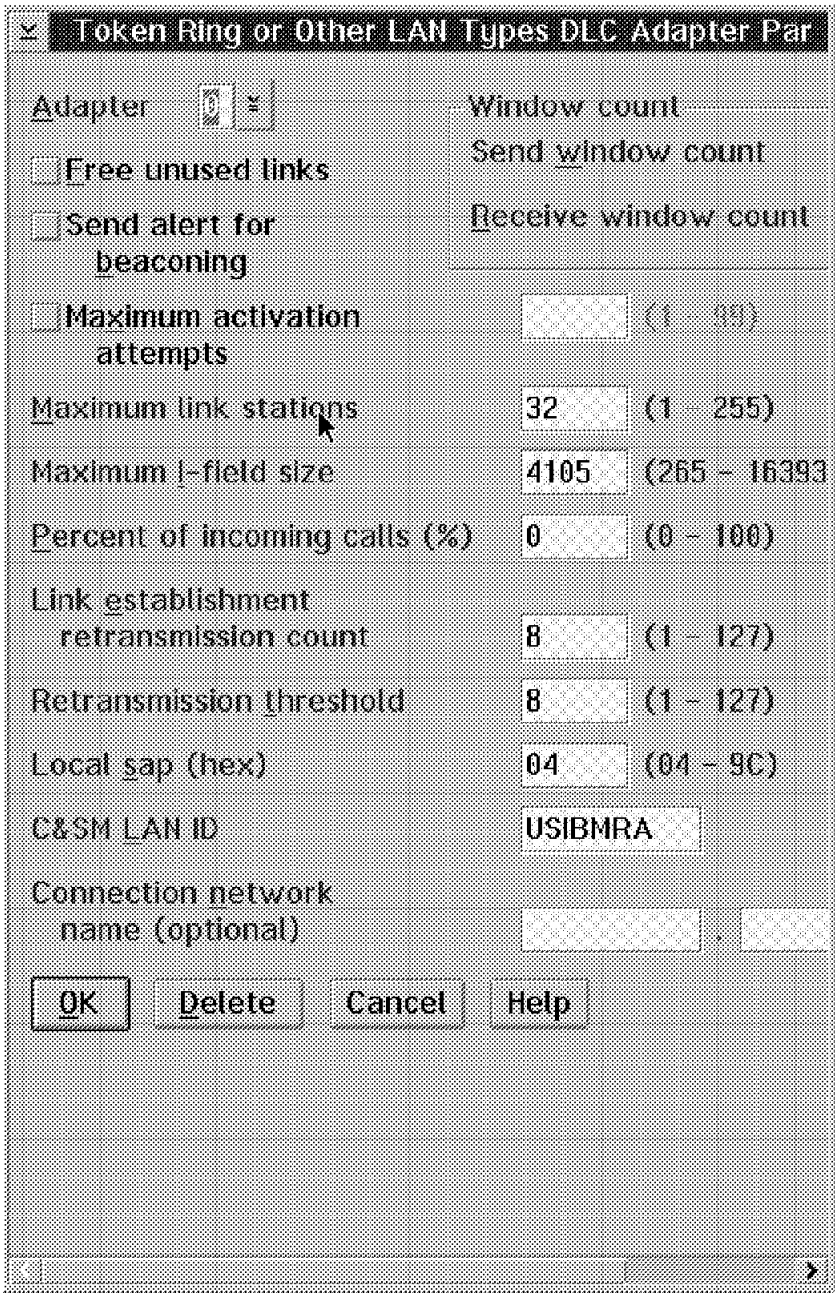


Figure 199. LAN DLC Adapter Parameter Values

We used all of the defaults for this window except the *Maximum link stations*. The default is 16 but we entered 32 because some of the other applications on this system require link stations for NetBIOS protocol support. You need one link station for every logical link that your system uses. We then entered USIBMRA as our C&SM LAN ID. This is the Communications and Systems Management LAN ID that identifies the LAN that our adapter is on. You will need to get this network ID parameter from your on-site LAN network administrator.

Note: In our case, it just happened to have the same name as our partner network ID for our host NetView. The two are independent of each other.

Once you have entered this parameter, click on the **OK** button which will take you back to the CM/2 Profile List window, as shown in Figure 200 on page 148.

We can now move to the next definition to be configured which is the SNA local node characteristic. Click on the **SNA local node characteristics** line item as shown in Figure 200.

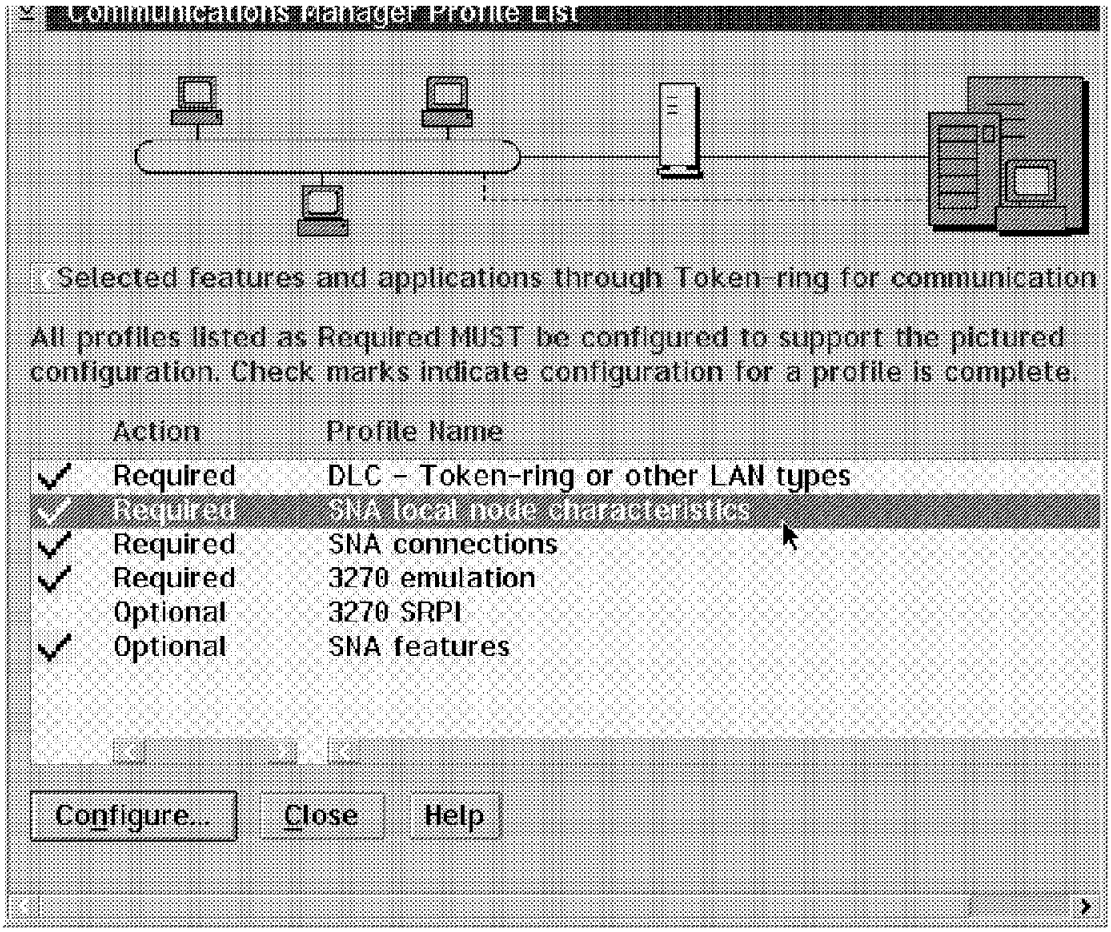


Figure 200. SNA Node Characteristics

Click on the **Configure** button and the next window will be the Local Node Characteristics window as show in Figure 201 on page 149.

In the Local Node Characteristics window, we entered the following parameters:

- USIBMMK in the Network ID field. This is the SNA NETID in which your node resides. When used with the local node name, it will become a fully qualified (FQ) Control Point (CP) name to uniquely identify your node in an interconnected network environment.

  You can get the value of this field by contacting your network administrator or by using the NetView for MVS/ESA LISTVAR command.

- Enter MK333720 in the Local node name field. This is your CP name that was set up by your VTAM administrator. It will define a Logical Unit (LU name) that will be used for your APPC communication.

- Click on the **End Node - no network node server** radio button.
- Enter 05D 33372 in the Local node ID field. You will have to obtain these values from the SNA VTAM administrator for your installation.

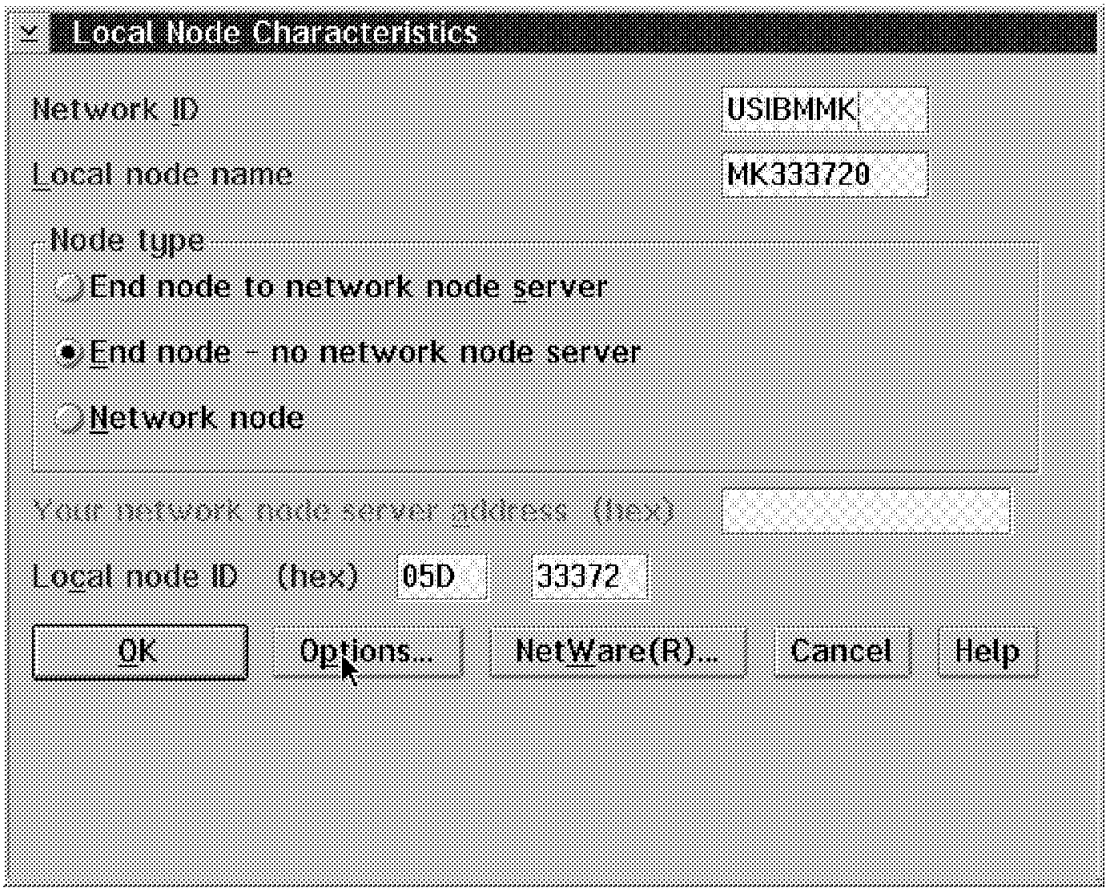


Figure 201. SNA Local Node Characteristics

We wanted to have an alias name for our local node, so we clicked on the **Options** button and got the Local Node Options window, as shown in Figure 201.

Our Local alias name is WTR33372. Click on the box for **Activate Attach Manager at start up**, and then **OK**. The next piece to configure is the SNA Connections.

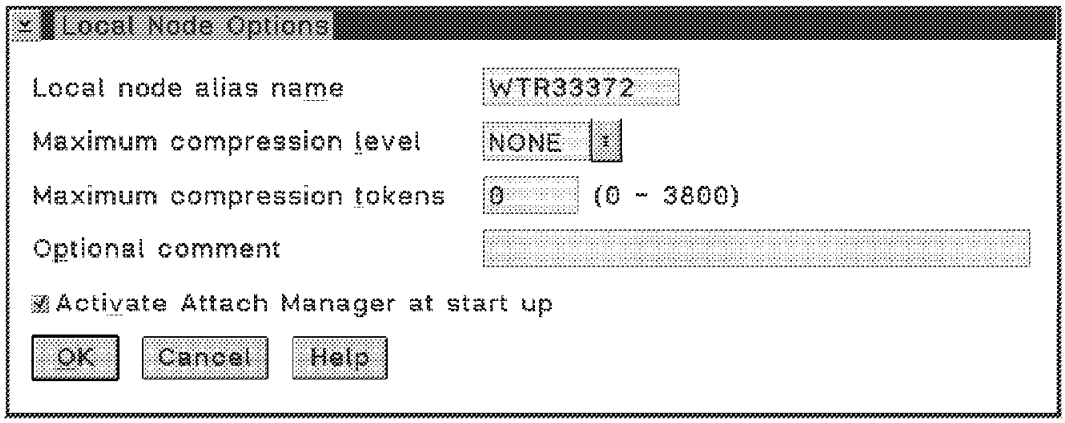


Figure 202. SNA Connections

Click on the SNA connections line, then the **Configure** button. This will bring you to the Connections List as shown in Figure 204 on page 151.

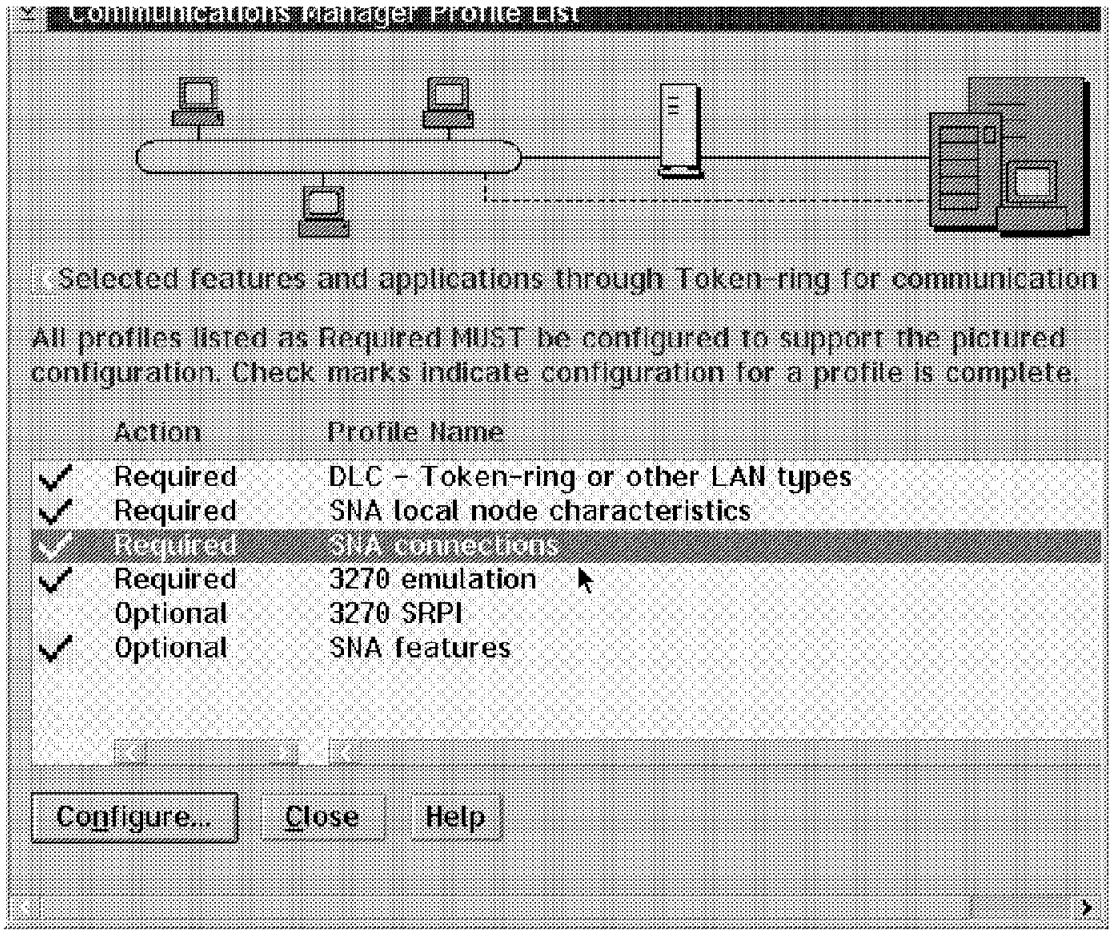


Figure 203. CM Profile List

Note: There is a line item for HOST$1 already in the window because we had previously created this link. If you are setting this up for the first time, then

there would be no Link Names defined and you would click on **Create** to set up a new one. Also note that the To host button was selected.

We chose the Change button to show you what parameters we entered to set up this host link. The first thing you see will be the Adapter List window as shown in Figure 205 on page 152.

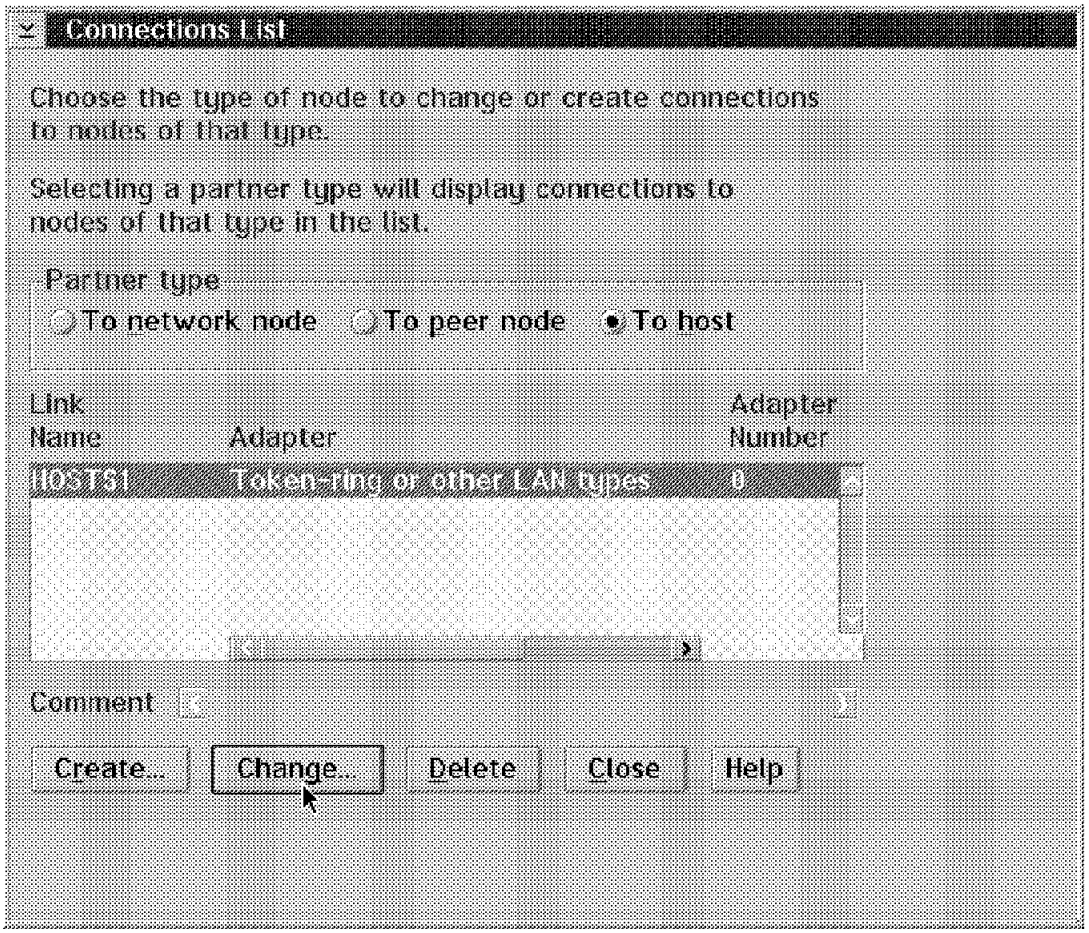


Figure 204. Connections List

In the Adapter List window, we selected the line item for **Token-ring or other LAN types** and then clicked on the **Continue** button. This presented us with the Connection to a Host window as shown in Figure 205 on page 152.

In the Connection to a Host window, we set up the following fields:

- Enter HOST$1 in the Link name field. You can enter any link name that you like in this field.
- Make sure that the Node ID (hex) field has the same values that were entered in the SNA Local Node Characteristics panel as shown in Figure 201 on page 149.
- Make sure that the LAN destination address field contains the MAC address or Locally Administered Address (LAA) of the IBM 3745 Communications Controller that is token-ring connected to your backbone LAN and provides the gateway to your host machine. Our Address format is token-ring and the Remote SAP should be 04.

- Enter USIBMMK in the Partner network ID field. This link will get to the machine where we normally log on. From there, the network will resolve the connection to the USIBMRA machine that we will set up as the true APPC partner in Figure 206 on page 153.
- Enter MK34 in the Partner node name field. The concatenation of partner network ID and partner node name will give you USIBMMK.MK34.

  This name will be referenced by the DEFINE_PARTNER_LU_LOCATION statement (when we create a partner LU) to indicate to CM/2 that our partner LU (USIBMRA.RAPAN) is located somewhere on the link that we defined.
- Click on the check box **Use this host connection as your focal point support**.
- Click on the **Define Partner LUs** button to get the Partner LUs window as shown in Figure 207 on page 154.

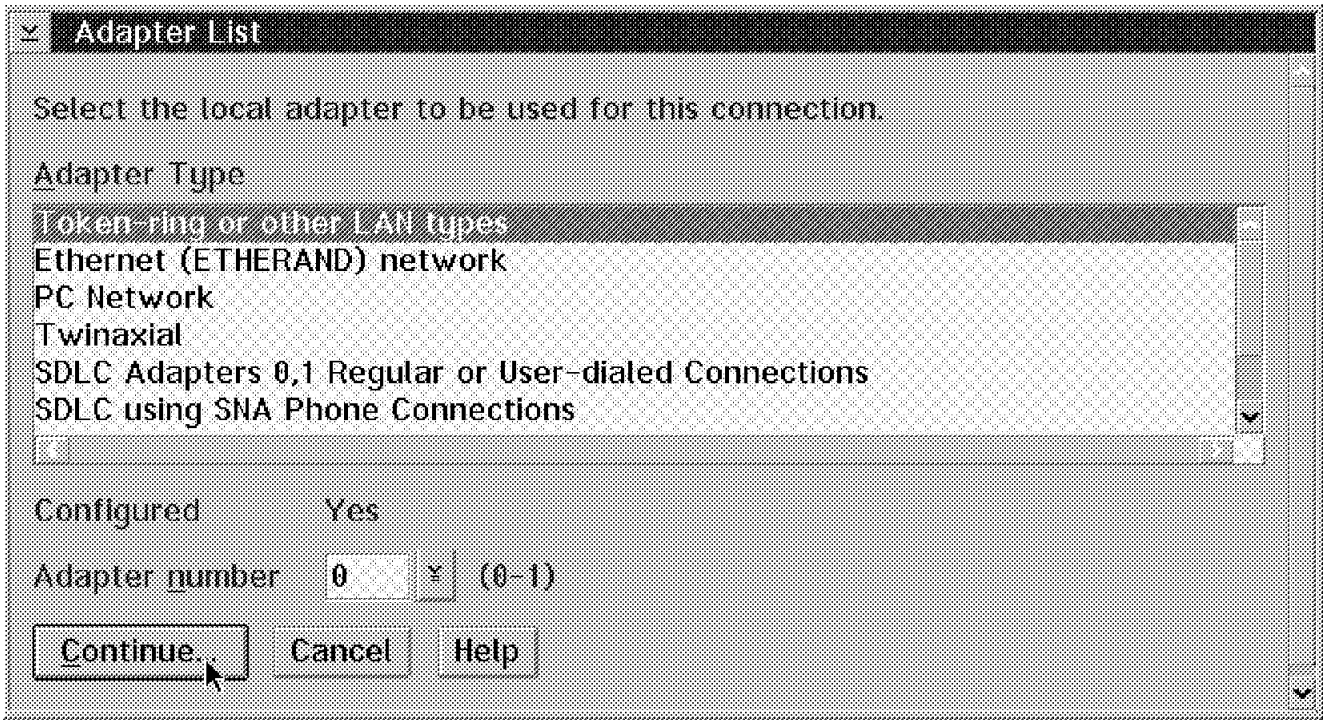


Figure 205. Adapter List

In Figure 207 on page 154, you can see that the definitions have already been set up. To define the host NetView application as our partner LU, we typed in the following:

- USIBMRA as the Network ID.
- RAPAN as the LU name.

  The DEFINE_PARTNER_LU_LOCATION parameter shows that USIBMMK.MK34 is our local owning CP name and that USIBMRA.RAPAN is the actual APPC partner. This will direct CM/2 to send a BIND for the requested partner LU on the link referenced in the DEFINE_PARTNER_LU_LOCATION statement.
- NETVIEW as the Alias. You can enter anything that you want for an alias name.

Once you click on **OK**, you are finished setting up your SNA connections and you can go back to the Communications Manager/2 Profile List window as shown in Figure 203 on page 150.

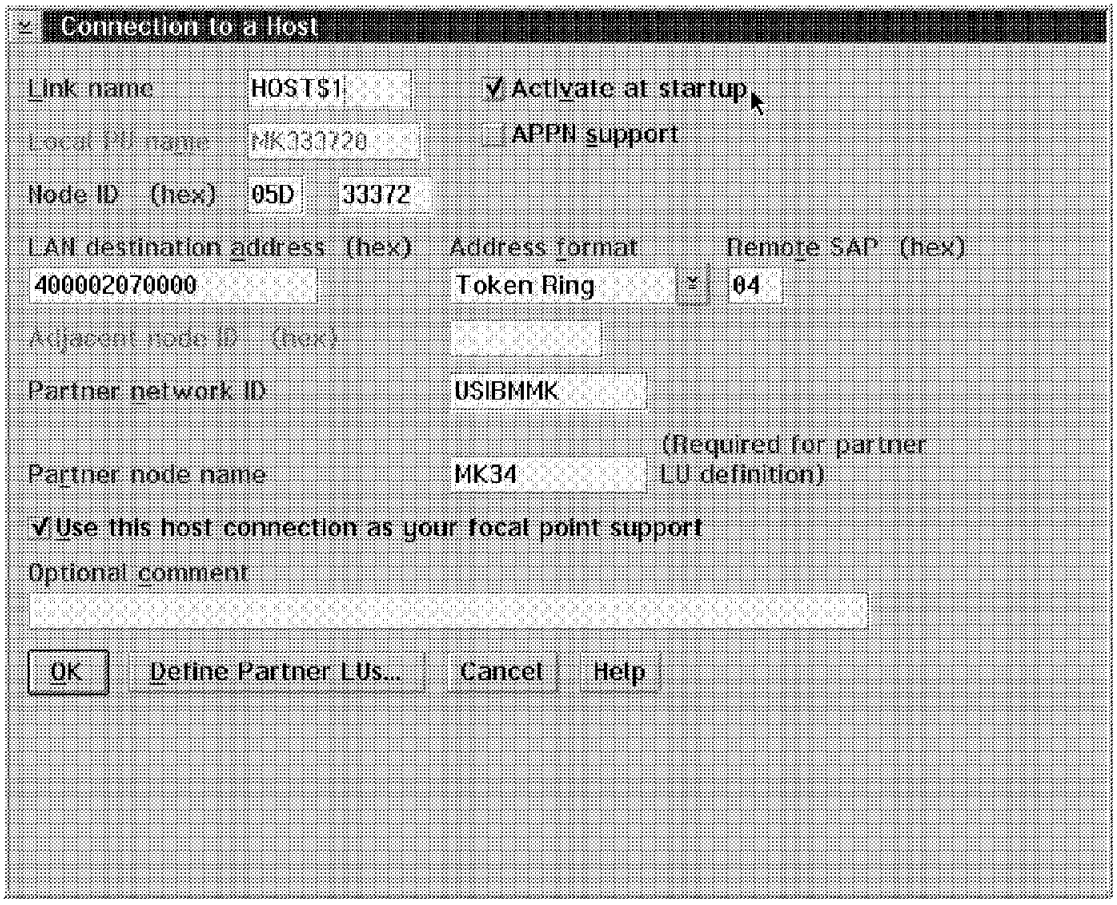


Figure 206. Define Link Names and Destination Address

From the Profile List window, select SNA Features, and click on **Configure**. From the SNA Features list, we selected Partner LUs. Figure 207 on page 154 shows the Partner LU window with the LU name of USIBMRA.RAPAN and the Alias of NETVIEW already configured.

Note that the Local LUs line item has been selected for you and that nothing appears in the Definition scroll box. You do not need to create a local LU here because it would be the second LU on your node. You can simply use the Control Point LU (USIBMMK.MK333720) that you set up earlier. When you start up Communications Manager/2, you will be initiating an implicit focal point relationship with the host NetView application by establishing an LU 6.2 session between your Control Point LU and the NetView Partner LU (USIBMRA.RAPAN).

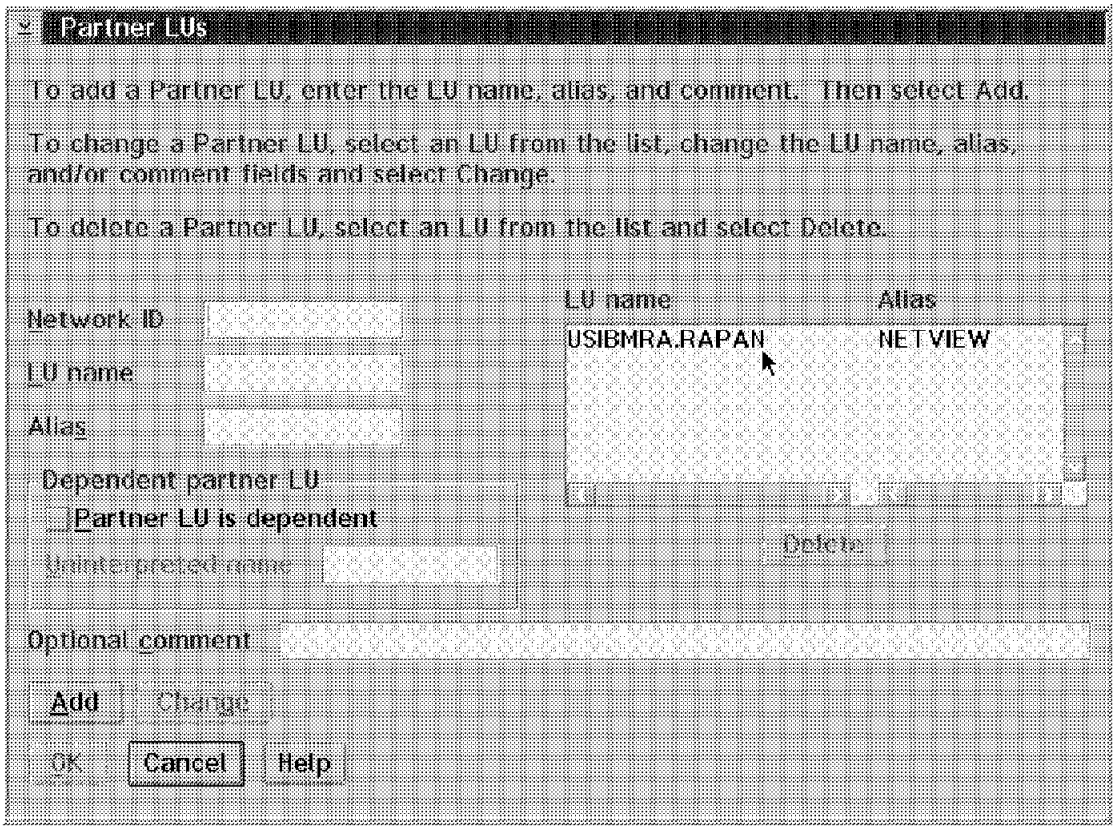


Figure 207. Partner LUs

The remote focal point name was not automatically generated for us, so we had to manually insert it into the NDF definition just before the Attach_Manager was started. Figure 208 on page 155 shows what syntax is needed for the remote focal point. A full copy of the NDF file that was created is shown in Figure 215 on page 160.

```
E.EXE - wtrnew.ndf
File  Edit  Options  Help

DEFINE_PARTNER_LU_LOCATION  FQ_PARTNER_LU_NAME(USIBMRA.RAPAN    )
                  WILDCARD_ENTRY(NO)
                  FQ_OWNING_CP_NAME(USIBMMK.MK34    )
                  LOCAL_NODE_NN_SERVER(NO);

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);

DEFINE_REMOTE_FOCAL_POINT  SNA_DEFINED_MS_CATEGORY(X'23',031)
                  DESCRIPTION(ALERT CATEGORY)
                  FQ_PRIMARY_FP_NAME(USIBMRA.RAPAN    );

START_ATTACH_MANAGER;
```

Figure 208. Remote Focal Point Definitions

Once all the definitions are set up and have been verified, you can restart CM/2 to test out the alert flow. Open the CM/2 folder again and double-click on **Start Communications** as shown in Figure 209.

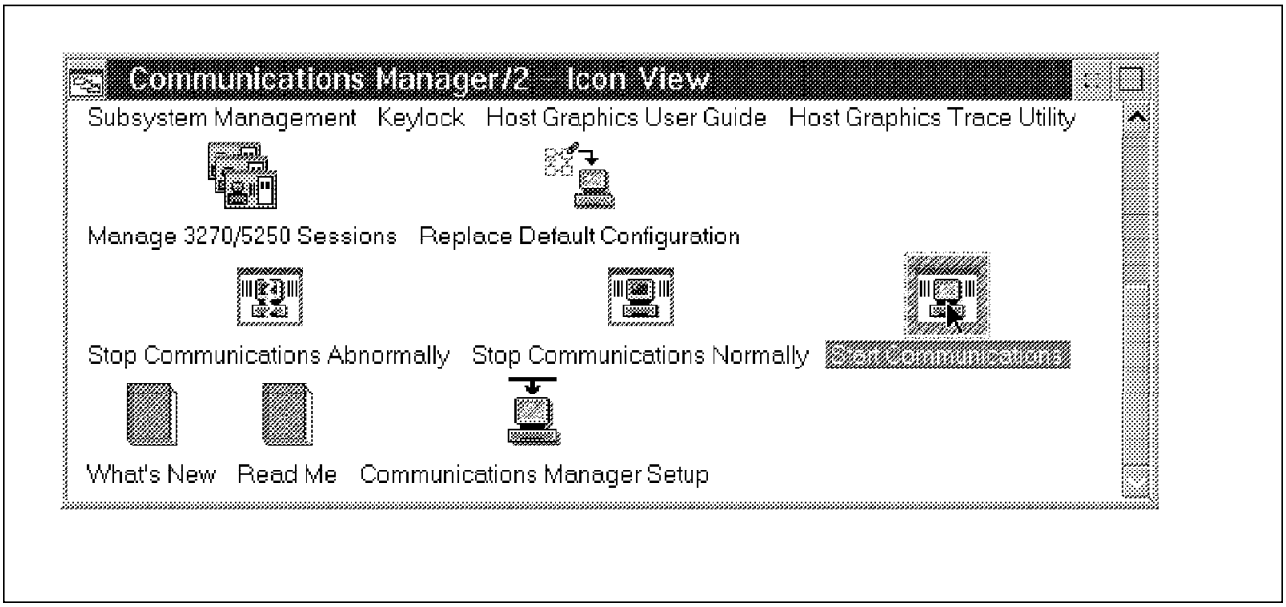


Figure 209. Start Communications

To test out the alert flow, you can set up the CPU monitor to monitor the CPU utilization for dropping below 5 percent and only leave the machine idle for the time period you specify in the threshold setup. Once you hear the beep for the alert, and see the Alert Received window pop-up you should have the entry in the FFST/2 log. To view the log, open the FFST/2 folder from the desktop. Figure 210 on page 156 shows the FFST/2 folder and the **System Error Log** icon highlighted. Double-click on it.

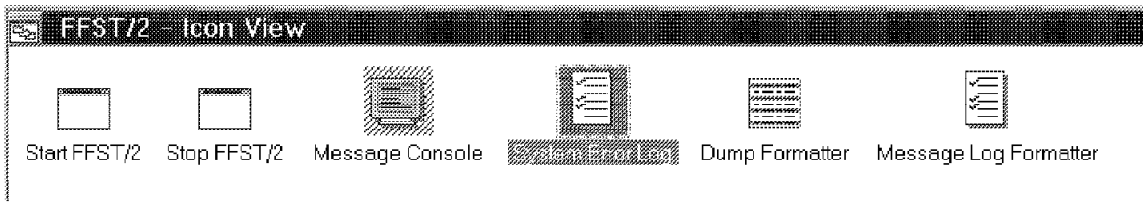


Figure 210. FFST/2 Folder

Click on the **Prev Rec** button until you see the Process name NETFIN\ALERTMGR.EXE in one of the records. You should see component information for NetFinity that should look familiar. In the Probe Description field, should be the Alert Text.

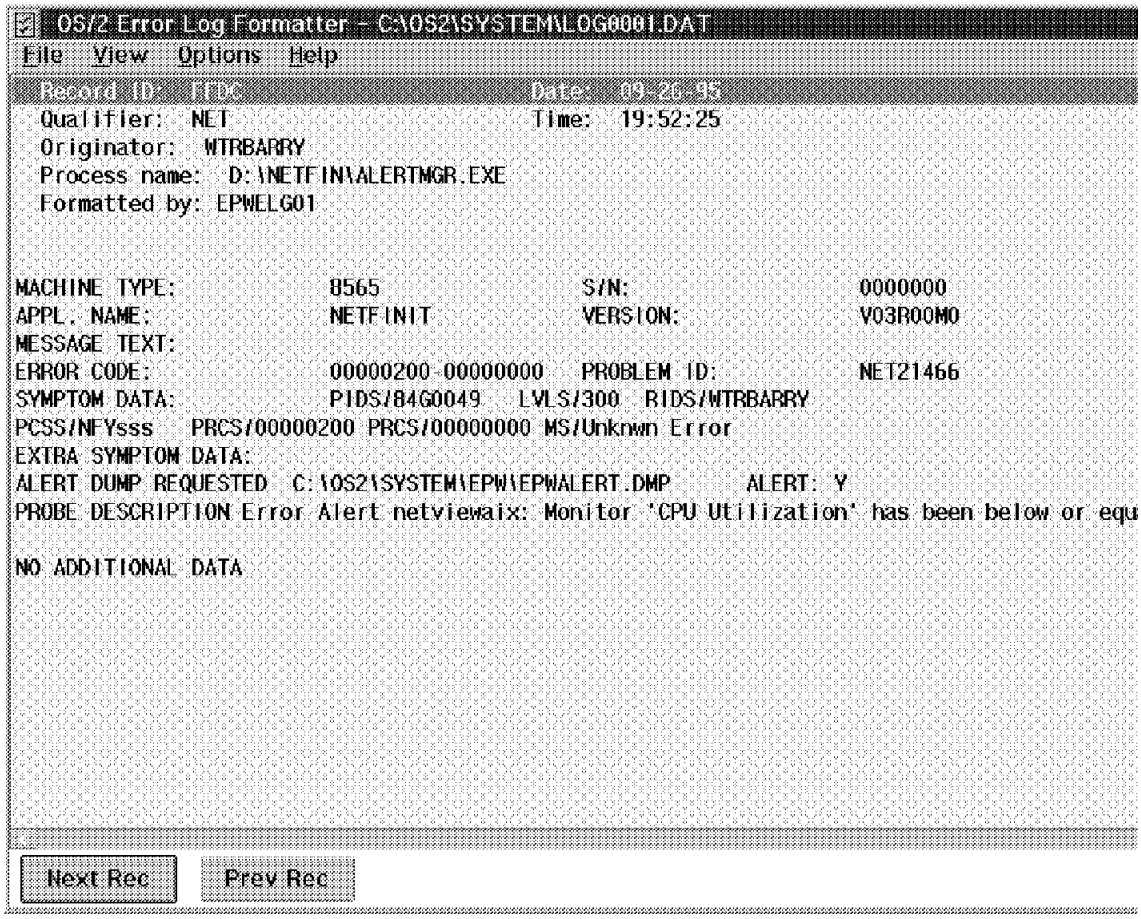


Figure 211. FFST/2 Alert Information

To verify that the alert made it to MVS, we need to log on to NetView for MVS, and check the Hardware Monitor log.

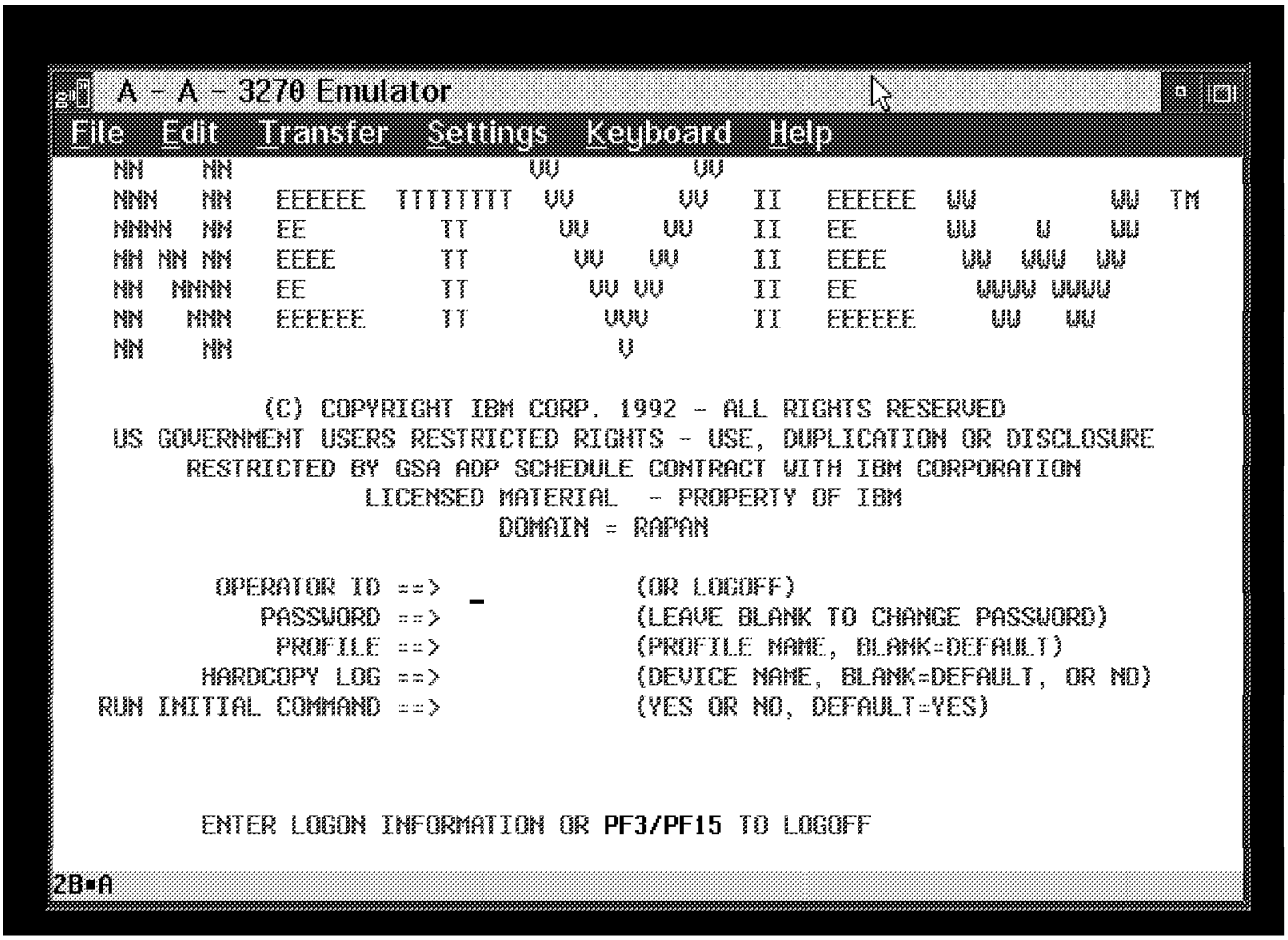


Figure 212. Host NetView Logon Screen

The first menu you see when you log on to NetView for MVS, is the main menu displayed in Figure 213 on page 158. To get to the alert, you can go to the Hardware Monitor alerts dynamic window by entering the command `npda ald`.

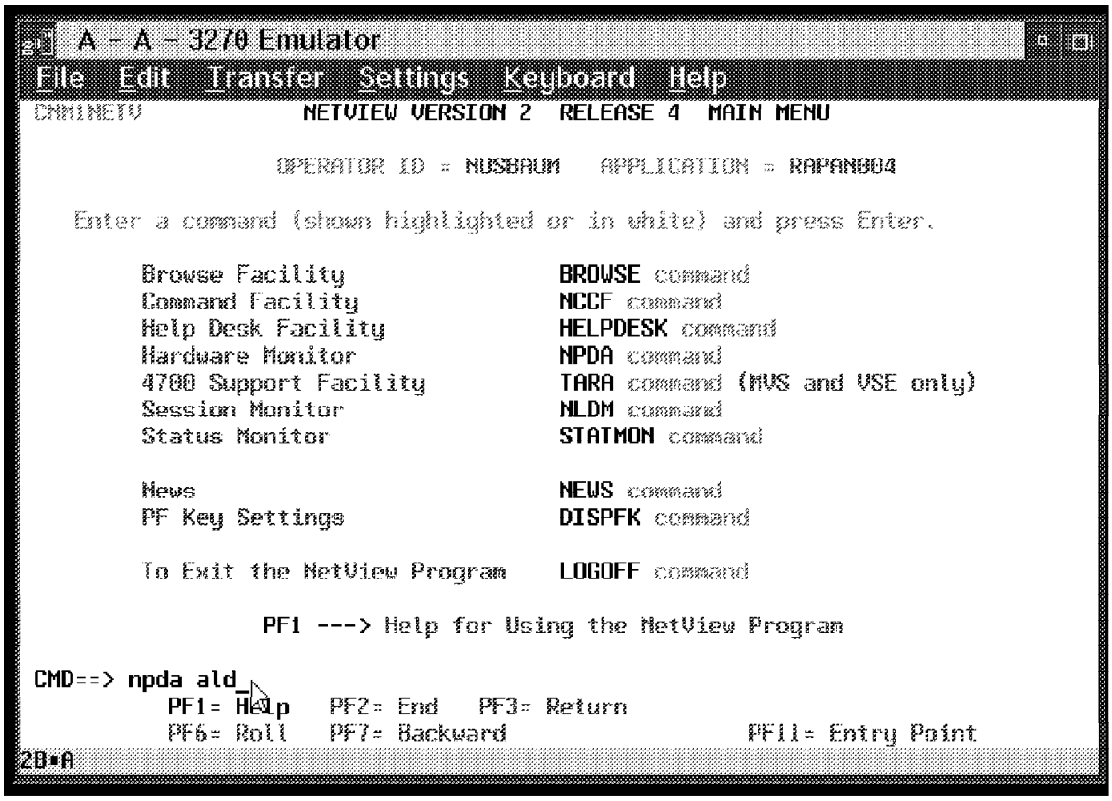


Figure 213. Host NetView Main Menu with NPDA ALD Command

In Figure 214 on page 159 the first several entries have a resource name of NETFINIT. If you are familiar with the hardware monitor, you can press Enter to go to the static display and then view details about the entry. More customization will need to be done to view the exact details of the alert text.

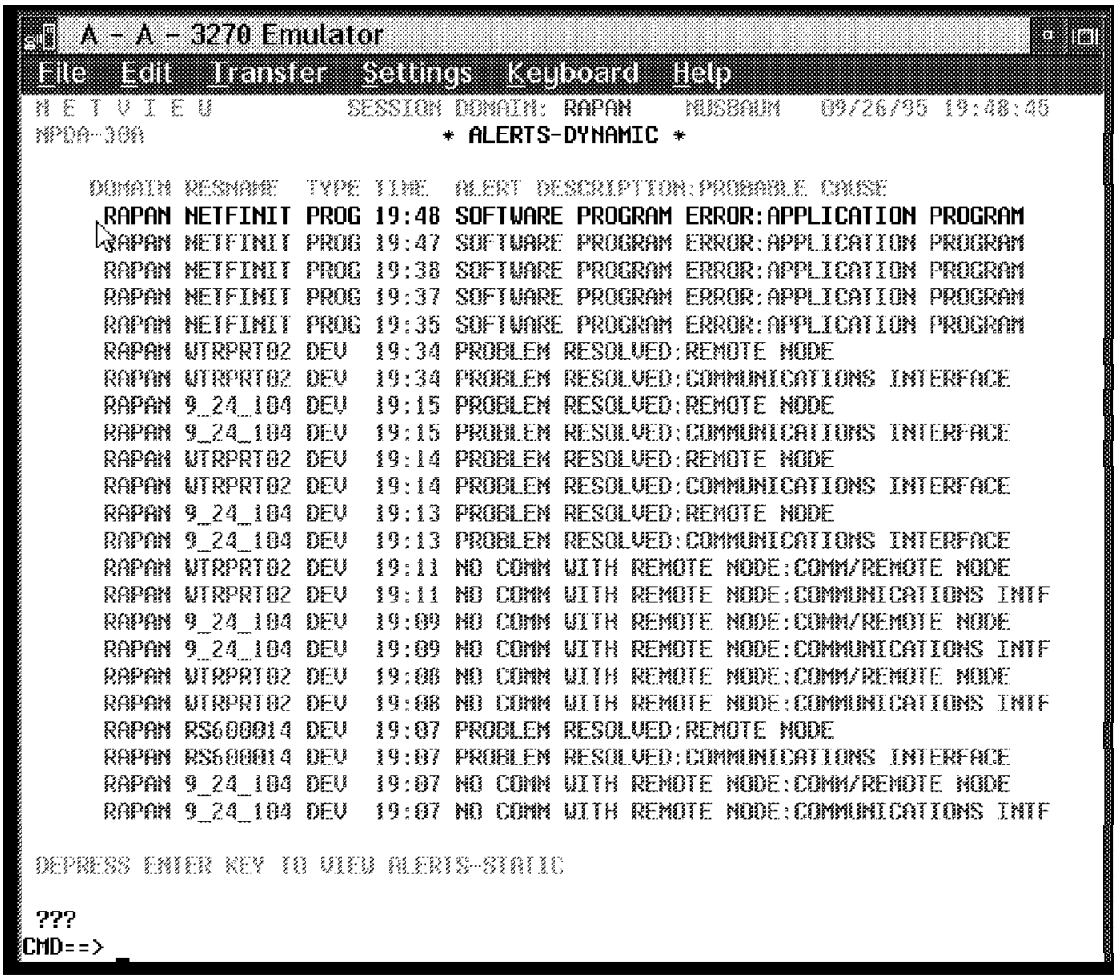


Figure 214. Hardware Monitor Alerts from FFST

```
DEFINE_LOCAL_CP  FQ_CP_NAME(USIBMMK.MK333720 )
                 CP_ALIAS(WTR33372)
                 NAU_ADDRESS(INDEPENDENT_LU)
                 NODE_TYPE(EN)
                 NODE_ID(X'05D33372')
                 NW_FP_SUPPORT(NONE)
                 HOST_FP_SUPPORT(YES)
                 HOST_FP_LINK_NAME(HOST$1  )
                 MAX_COMP_LEVEL(NONE)
                 MAX_COMP_TOKENS(0);

DEFINE_LOGICAL_LINK  LINK_NAME(HOST$1  )
                     FQ_ADJACENT_CP_NAME(USIBMMK.MK34     )
                     ADJACENT_NODE_TYPE(LEN)
                     DLC_NAME(IBMTRNET)
                     ADAPTER_NUMBER(0)
                     DESTINATION_ADDRESS(X'40000207000004')
                     ETHERNET_FORMAT(NO)
                     CP_CP_SESSION_SUPPORT(NO)
                     SOLICIT_SSCP_SESSION(YES)
                     NODE_ID(X'05D33372')
                     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);

DEFINE_PARTNER_LU  FQ_PARTNER_LU_NAME(USIBMRA.RAPAN    )
                   PARTNER_LU_ALIAS(NETVIEW)
                   PARTNER_LU_UNINTERPRETED_NAME(RAPAN   )
                   MAX_MC_LL_SEND_SIZE(32767)
                   CONV_SECURITY_VERIFICATION(NO)
                   PARALLEL_SESSION_SUPPORT(YES);

DEFINE_PARTNER_LU_LOCATION  FQ_PARTNER_LU_NAME(USIBMRA.RAPAN    )
                            WILDCARD_ENTRY(NO)
                            FQ_OWNING_CP_NAME(USIBMMK.MK34     )
                            LOCAL_NODE_NN_SERVER(NO);

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);

DEFINE_REMOTE_FOCAL_POINT  SNA_DEFINED_MS_CATEGORY(X'23',031)
                           DESCRIPTION(ALERT CATEGORY)
                           FQ_PRIMARY_FP_NAME(USIBMRA.RAPAN    );

START_ATTACH_MANAGER;
```

Figure 215. WTRNEW.NDF

7.2 Sending Runcmds From MVS to OS/2

Now that we have managed to get alerts to flow from NetFinity on OS/2, we can turn the communications flow around and take some actions based upon those the alerts. The simplest procedure is for an operator to be able to enter a command from NetView for MVS and have it sent to NetFinity using the CM/2 LU 6.2 interface. Eventually, NetView's automation table will be used to take specific actions based upon the alerts.

In order to send commands to NetFinity there is some additional setup that needs to happen on the OS/2 workstation. Two additional CM/2 components will need to be installed. If you didn't install *Service Point Application Router* (SPAR) and *Remote Operations Service* (ROPS), now is the time to do so. Assuming that they are already installed, you can either use the CM/2 GUI to start them, or you can place them in a command file for automatic startup. A typical place to place it would be in C:\STARTUP.CMD. If you are going to start it manually, the first component to be started needs to be SPAR. Double-click on the **SPAR** icon in the CM/2 folder, as show in Figure 216.

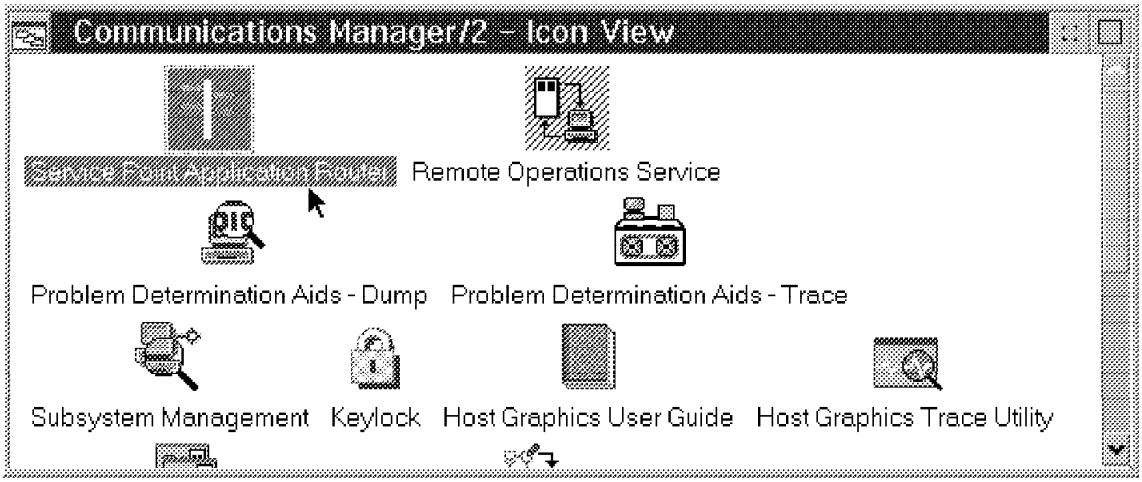


Figure 216. Communications Manager/2 Folder

This will cause a pop-up window for SPAR to appear, as shown in Figure 217 on page 162. You can also start SPAR by issuing the command `start \cmlib\rtr.exe` from the command line or in a REXX EXEC.

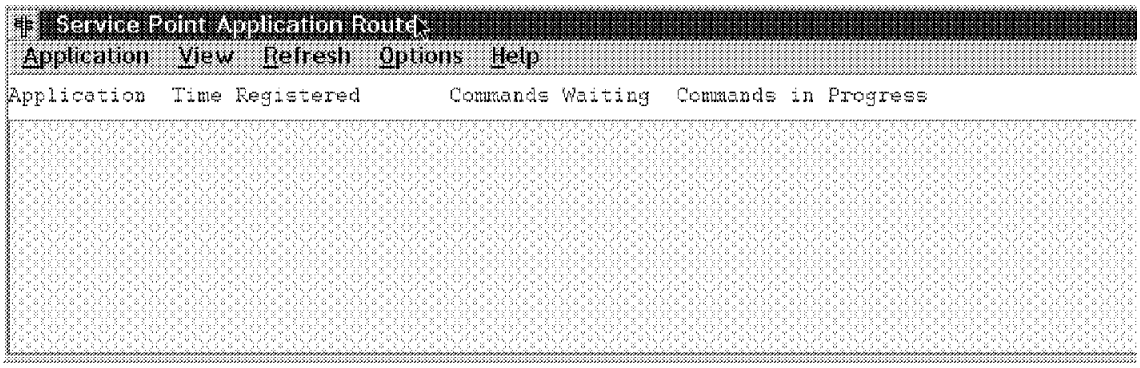


Figure 217. Service Point Application Router

Once SPAR is started, the next component to start is ROPS. You can start ROPS by either double-clicking on the icon in the CM/2 folder as shown in Figure 218, or by the command: `\cmlib\roppm.exe`.

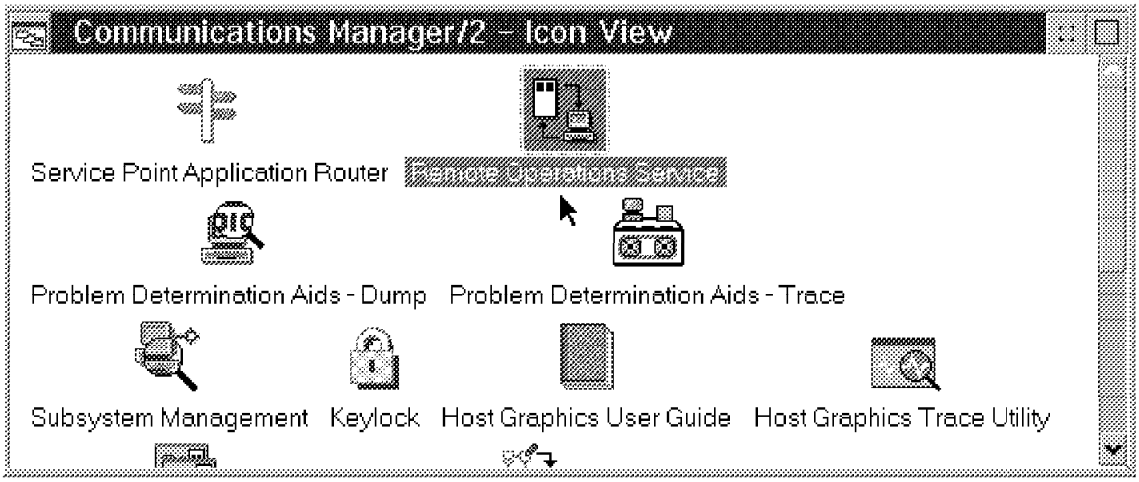


Figure 218. CM/2 Folder for Remote Operations

You will get a warning window as ROPS is starting up.

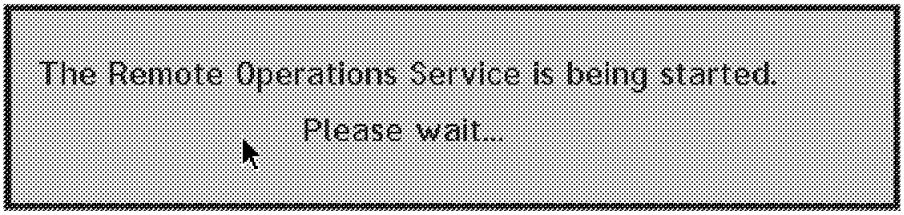


Figure 219. ROPS Starting

Once ROPS starts a new window pops up. You may need to change the default timeout values for ROPS Using the left mouse button on the **Options** pull-down menu, select **Program options**. We changed the timeout values to 600 seconds as shown in Figure 221 on page 163.

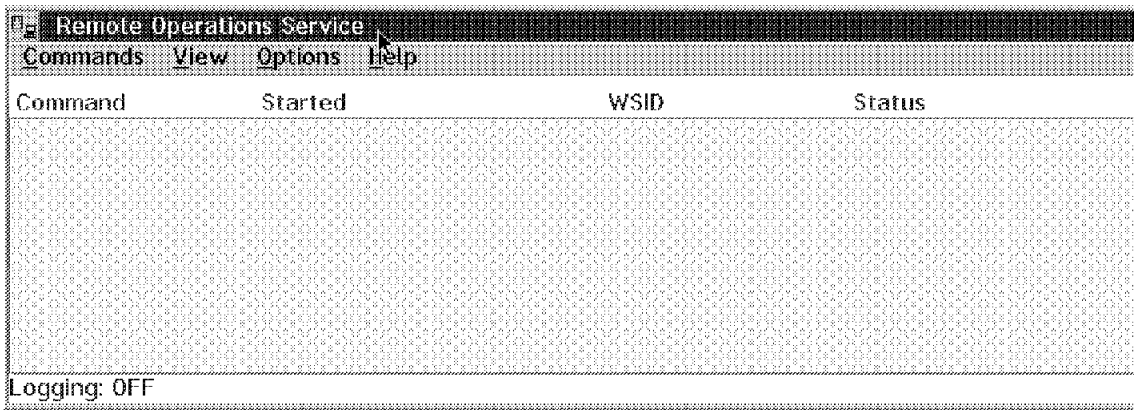


Figure 220. Remote Operations Service

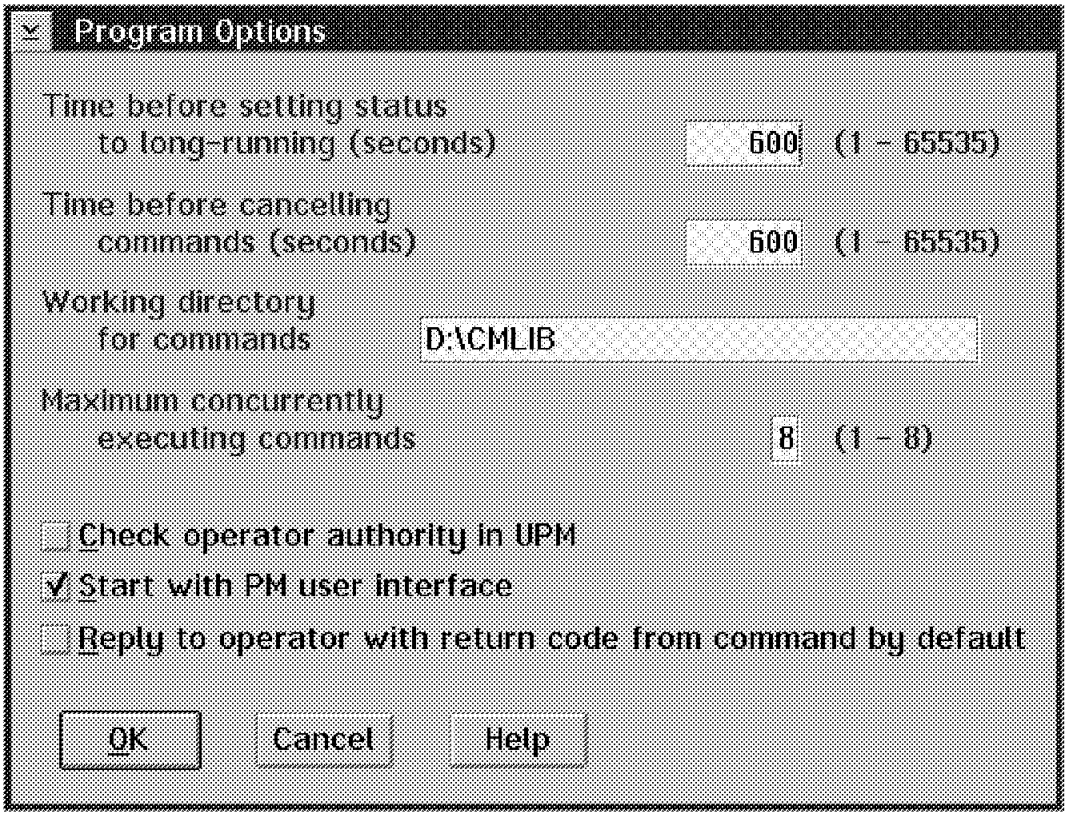


Figure 221. Program Options

Once ROPS is initialized, an entry for the REMOTEOP will appear in the SPAR window, as shown in Figure 222 on page 164.

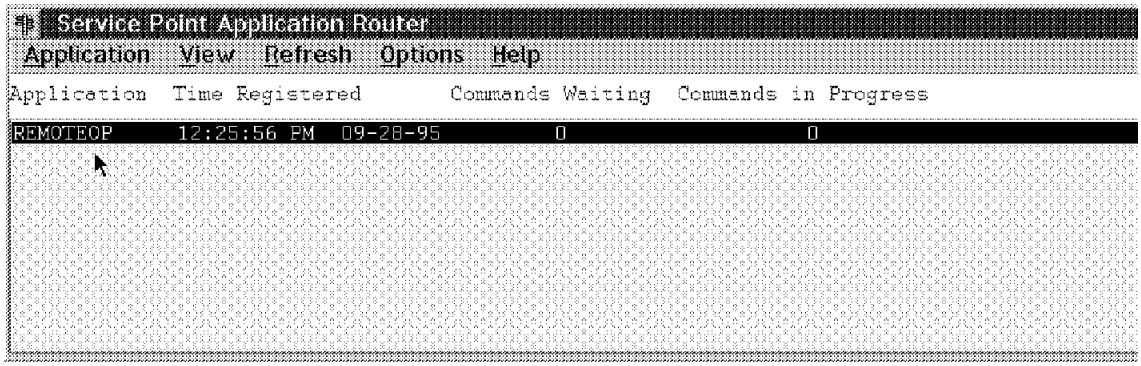


Figure 222. Service Point Application Started

From the NetView for MVS console, if you issue the command:

```
runcmd sp=mk333728 netid=usibmmk appl=remoteop op=; start mongui
```

you should see the systems monitors start up on your display. You can issue any NetFinity or OS/2 commands this way. You need to make sure that the values are correct.

- sp = service point applications lu 6.2 name
- netid = vtam network ID
- appl = service point application, in this case cm/2 application
- op = an operator ID

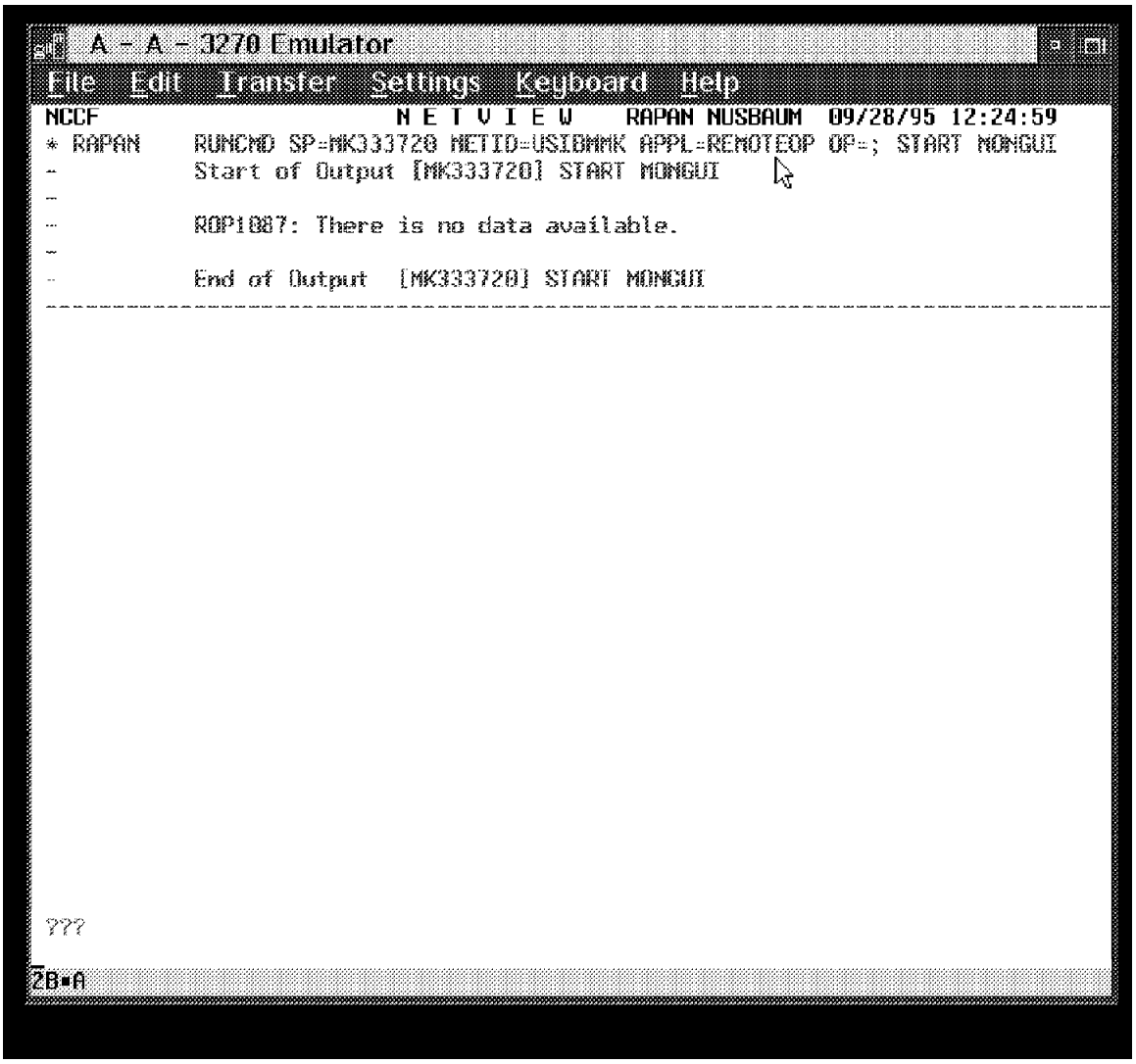


Figure 223. Sample Command Issued from NetView for MVS to NetFinity

If you want to see the status of your LU 6.2 connection you can use some other features of CM/2. If you look in the CM/2 folder there is an icon called **Subsystem Management**. You can either double-click on that, as shown in Figure 224 on page 166, or you can start it using the command `\cmlib\acssbmgt.exe`.

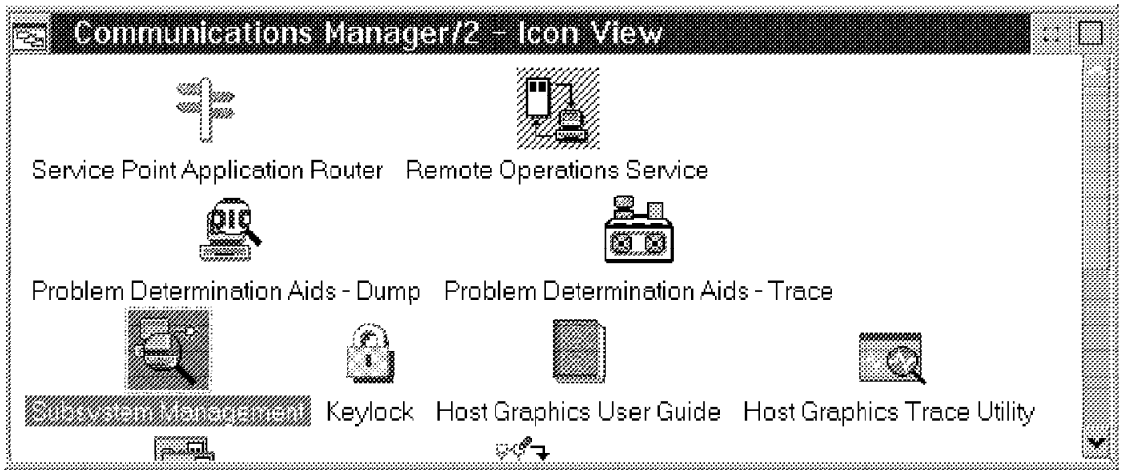


Figure 224. Subsystem Management

The Subsystem Management window in Figure 225 shows you the status of the CM/2 components. In addition you can see further details about the individual components.

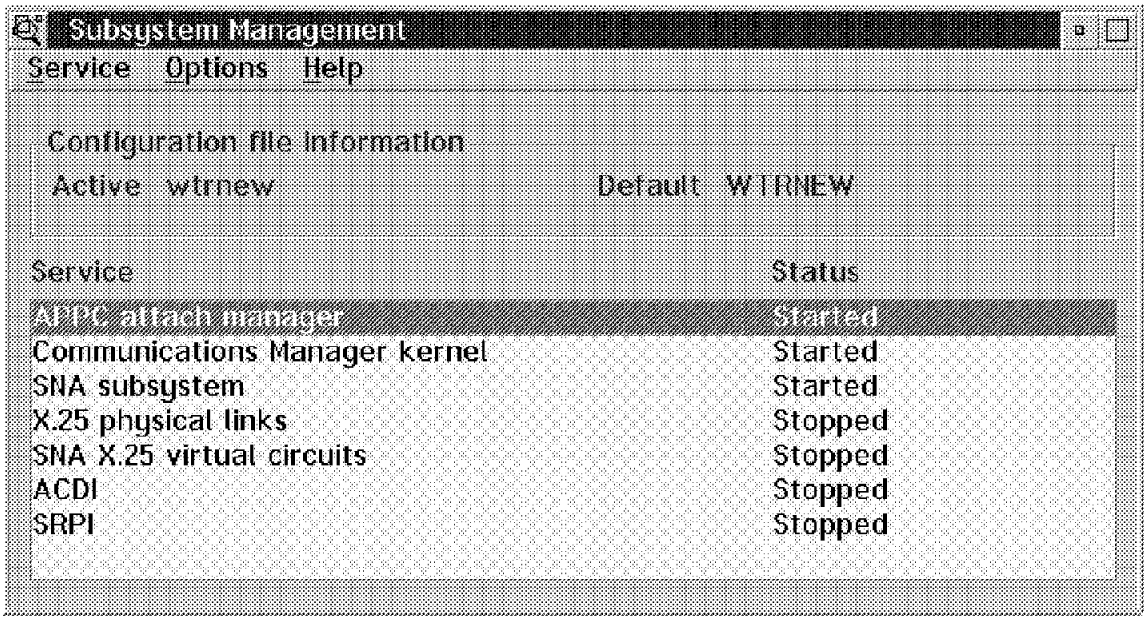


Figure 225. Status of Subsystem Components

If you double-click on the SNA Subsystem entry you will see a list of items that you can obtain information on, as shown in Figure 226 on page 167. To find out more information on the LU 6.2 sessions, double-click on that entry.

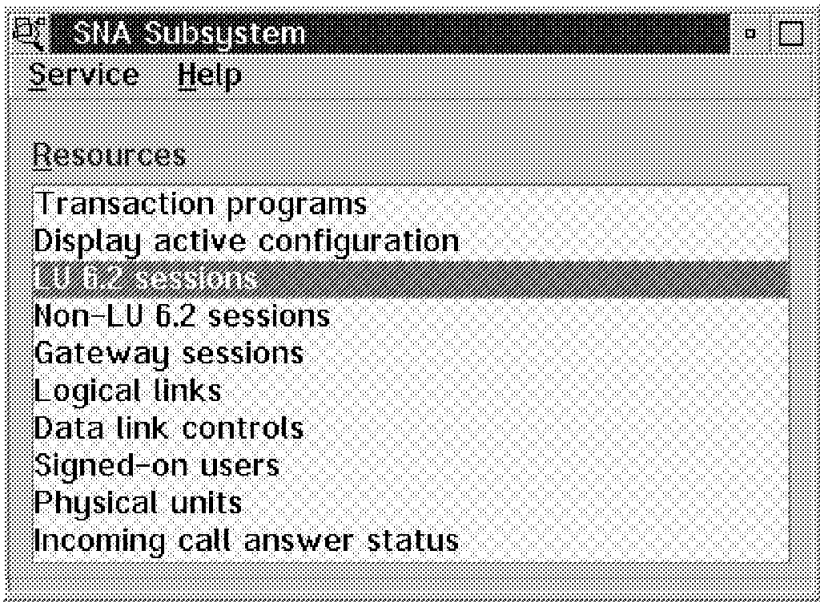


Figure 226. LU 6.2 Sessions

The LU 6.2 Sessions window shows you the partners involved in the LU 6.2 session as well as the alias name. This should match all the configuration information from your original setup of the LU 6.2 connection in CM/2.

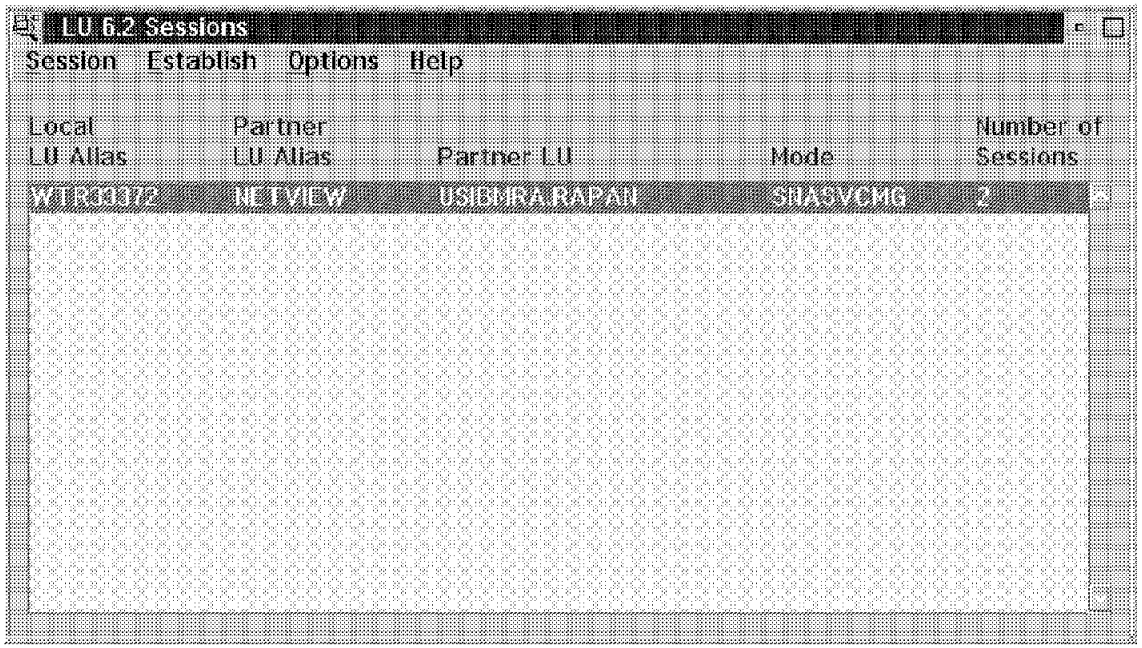


Figure 227. LU 6.2 Session Information

Double-clicking on that Local LU Alias entry will give you session details, as shown in Figure 228 on page 168.

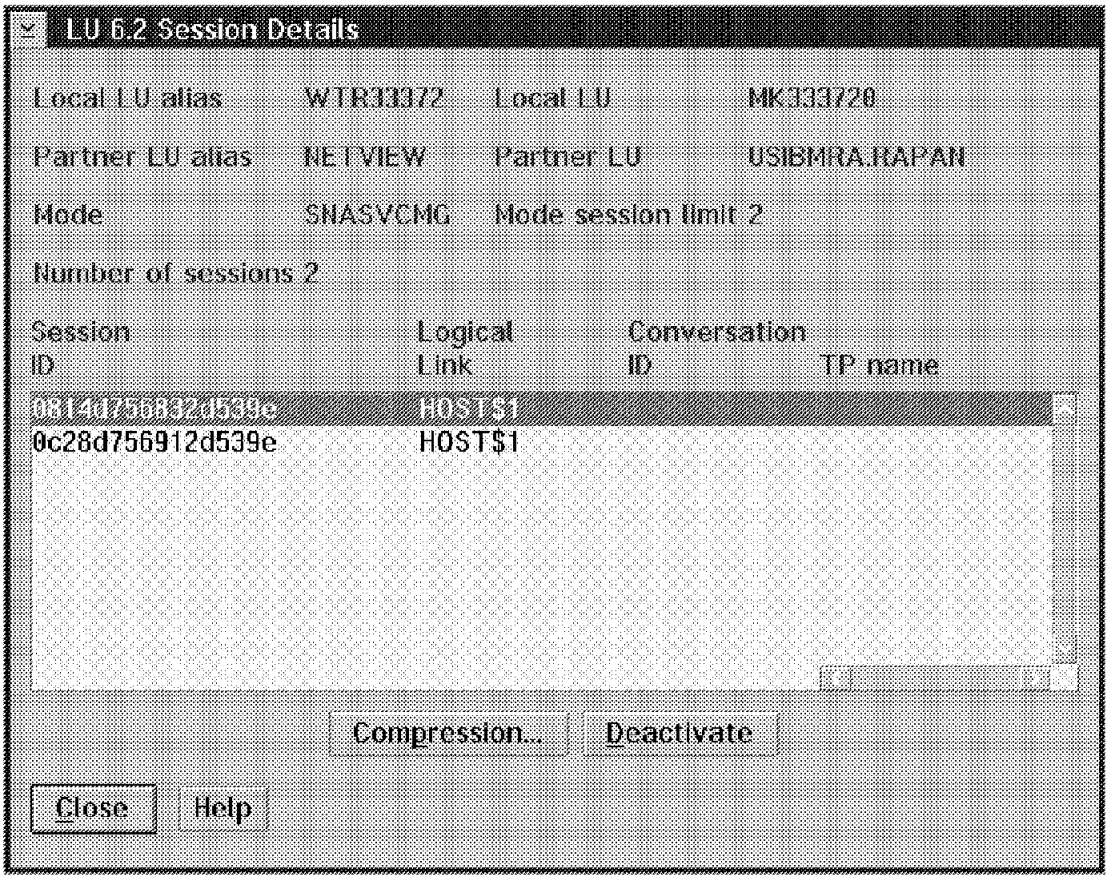


Figure 228. Session Details

If you wanted to see additional details about the active sessions, double-click on the **Display active configuration** entry in the SNA Subsystem window. Then using the pull-down window, select **Display->General SNA->Management Services**. The results are shown in Figure 229 on page 169.

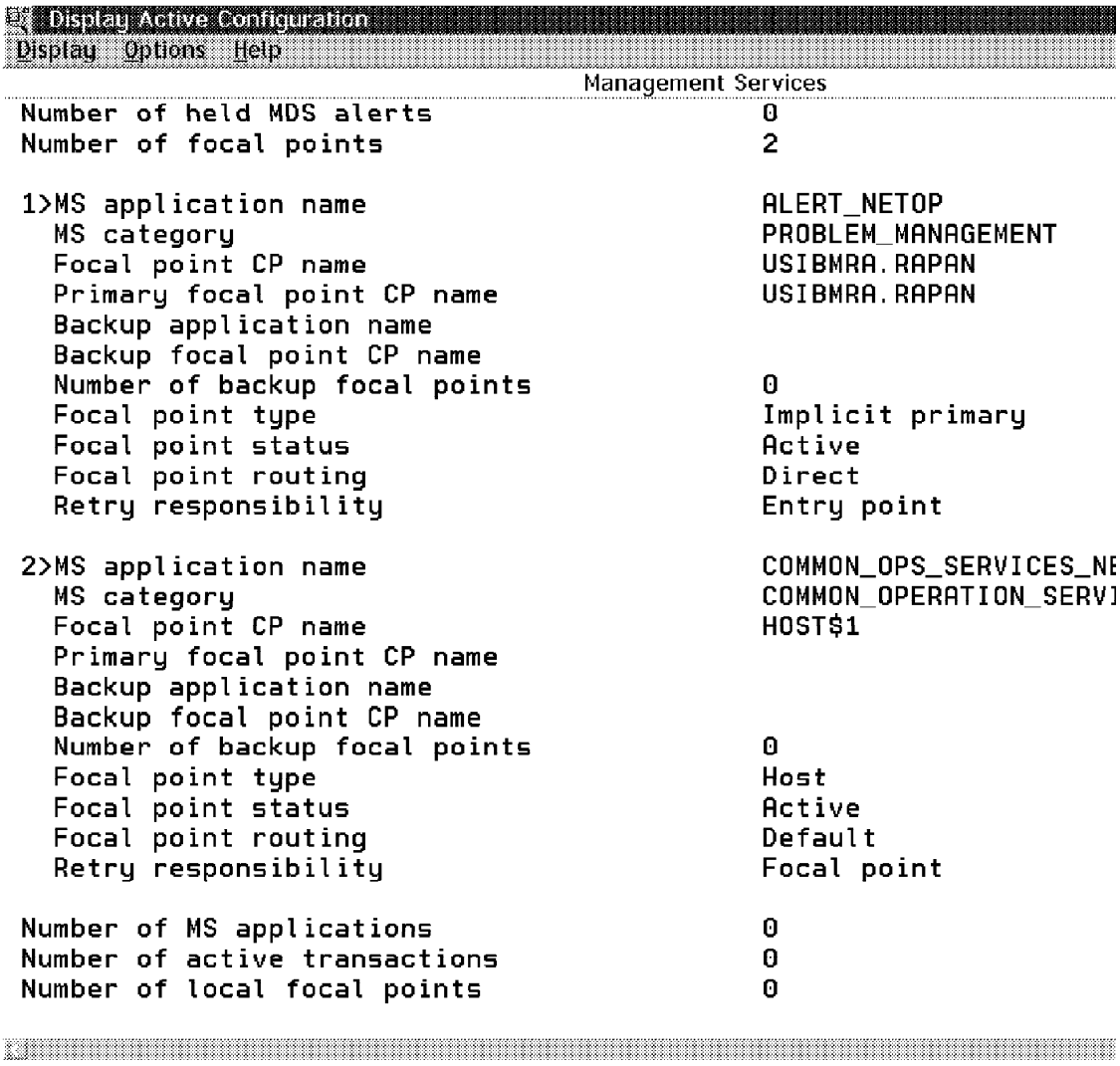


Figure 229. Active Configuration Information

Index

O

P

R

S

T

ITSO Technical Bulletin Evaluation RED000

International Technical Support Organization
LAN Management Processes (Alerts/Monitoring)
Using NetFinity
December 1995

Publication No. SG24-4517-00

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!)

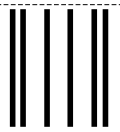
_____ _____
Name Address

_____ _____
Company or Organization

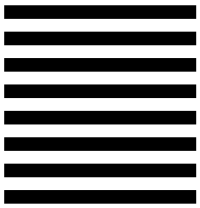
_____ _____
Phone No.

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 HZ8, Building 678
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.