Netfinity Manager

User’s Guide

Netfinity Manager

User's Guide

Note

Before using this information and the product it supports, be sure to read the general information under Appendix L, “Notices” on page 537.

First Edition (June 1998)

Contents

About This Book

This book provides detailed information on how to use each of the services included with Netfinity Manager. For information on how to install and configure Netfinity Manager, see *Netfinity Manager Quick Beginnings*. For information on Netfinity Manager command line interfaces, see the *Netfinity Command Reference*.

Who Should Read This Book

This book is for anyone who will be using the Netfinity Manager and Services for local or remote hardware systems management. It can also be used for quick reference by users of individual services. However, detailed online helps are available for all Netfinity services.

You should have general knowledge of your operating system, network operations, and database functions.

Chapter 1. Starting Netfinity

To start Netfinity:

1. Open the Netfinity folder or program group.

   During installation of Netfinity Manager, a Netfinity folder (OS/2, Windows 95, or Windows NT 4.0 only) or a Netfinity program group (Windows NT 3.51 only) was added to your Desktop. The Netfinity folder or program group contains the Netfinity Service Manager object.

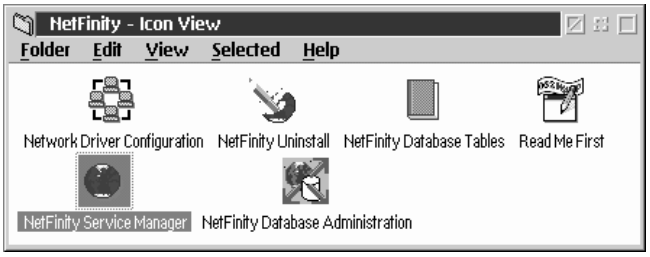

Figure 1. The Netfinity Folder

Notes:

a. In your Netfinity folder or program group is a document titled *Read Me First*, which contains information about Netfinity that might not be covered in your documentation.

b. The Netfinity folder also contains the Network Driver Configuration object, which allows you to reconfigure your network protocols and system keywords, and the Netfinity Database Tables object, which contains a handy online reference for all of the data tables in the Netfinity database. For more information on Netfinity's database support see and Appendix I, "Netfinity Relational Database Tables" on page 480 and "Netfinity Database Support" in *Netfinity Manager Quick Beginnings.*

c. The Netfinity folder also contains a Netfinity Database Administration object. You can use Netfinity Database Administration to configure Netfinity database support. For more information on Database Administration, see "ODBC Database Support" in *Netfinity Manager Quick Beginnings*

2. Start the Netfinity Service Manager.

   To start the Netfinity Service Manager, use mouse button 1 to double-click on the Netfinity Service Manager object.

Netfinity Service Manager

All Netfinity services that are supported by your system can be started from the Netfinity Service Manager window. The services that are available for use depend on the installation configuration you selected during installation.

Figure 2. Netfinity Service Manager

To start any Netfinity service that appears in your Service Manager window, double-click on the icon for that service. To start a Netfinity service on a remote system, you must use the Remote System Manager service. For more information on Remote System Manager, see Chapter 16, “Remote System Manager” on page 199.

Netfinity Service Descriptions

Each Netfinity service consists of a base program and a graphical user interface (GUI). The service base programs enable the individual services to be accessed remotely by the Netfinity Manager, but do not allow for local access. The service GUIs, when functioning along with their respective base program, enable you to access the service.

Some services are available only on systems with certain system configurations. These services are:

- DMI Browser (requires DMI Service Layer)
- ECC Memory Setup (requires ECC memory)
- Predictive Failure Analysis (requires a PFA-enabled hard disk drive)
- RAID Manager (requires a RAID hard disk drive subsystem)
- System Partition Access (requires a built-in System Partition)

Brief descriptions of each of the Netfinity services follow. Complete instructions on how to use each of these services can be found in the service-specific chapters of this book.

Alert Manager

The Alert Manager is an extendable facility that allows receiving and processing of application-generated alerts. A variety of actions can be taken in response to alerts, including logging alerts, notifying the user, forwarding the alert to another system, executing a program, playing a WAV file (available only on multimedia systems), generating an SNMP alert message, dialing out to a digital pager service (available only on systems that have a modem), or taking an application-defined action. Actions are user-definable, using a highly flexible action management interface.

Also, an extensive, detailed log is kept of all alerts received by the Alert Manager. Logged information available from the log includes date and time the alert was received, type and severity of the alert, the ID of the application that generated the alert, as well as any text that was generated and any action taken by the Alert Manager.

Individual or multiple alerts can be selected from the log and printed for later reference, or deleted once problems are corrected. This service is available for both stand-alone and network use.

Capacity Management

Capacity Management is an easy to use resource management and planning tool for network managers and administrators, allowing remote performance monitoring of every server on the network.

Cluster Manager

Cluster Manager is a powerful application designed to enhance the cluster management capabilities of the Microsoft Cluster Server (MSCS) administration console, included with Microsoft Windows NT version 4.0 Enterprise Edition. Cluster Manager builds on the power of MSCS, providing an integrated graphical interface that enables you to quickly and easily monitor and manage the clustered systems on your network. This service is available only on systems running Windows NT Workstation 4.0.

Critical File Monitor

Critical File Monitor enables you to be warned whenever critical system files on your system are deleted or altered. Critical File Monitor makes it simple for you to generate Netfinity alerts when an important System File (such as the CONFIG.SYS file) changes date, time, size, or when it is deleted or created. Critical File Monitor can also be used to monitor any other files that reside on a Netfinity system.

DMI Browser

DMI Browser enables you to examine information about the DMI-compliant hardware and software products installed in or attached to your system.

ECC Memory Setup

The ECC Memory Setup allows for monitoring of ECC memory single-bit errors, and can automatically “scrub,” or correct, the ECC memory when errors are detected. Also, you can keep a running count of single-bit errors, and can set a single-bit error threshold

that will cause a nonmaskable interrupt (NMI) if the ECC single-bit error threshold is exceeded. This service is available for both stand-alone and network use by any system that has ECC memory.

Event Scheduler

You can use Event Scheduler to automate many Netfinity services. With Event Scheduler, you can automatically gather and export System Information Tool, System Profile, and Software Inventory data, distribute or delete files, restart systems, execute commands, and access and manage System Partitions on all of the Netfinity systems on your network. Scheduled events can be performed one time only, or can be performed according to a user-defined schedule.

File Transfer

You can use the File Transfer service to easily send, receive, or delete files or entire directories to and from remote Netfinity systems on your network.

Power-On Error Detect

The Power-On Error Detect service immediately warns you when a remote Netfinity system has start-up problems, enabling you to react quickly to problems and minimize downtime.

Predictive Failure Analysis

The Predictive Failure Analysis (PFA) service enables you to continually monitor and manage PFA-enabled hard disk drives. A PFA-enable hard disk drive features hardware designed to help detect drive problems and predict drive failures before they occur, thus enabling you to avoid data loss and system downtime.

Process Manager

You can use Process Manager to view detailed information about all processes that are currently active on any system. You can also stop or start processes and generate Netfinity alerts if a process starts, stops, or fails to start within a specified amount of time after system startup.

RAID Manager

The RAID Manager service enables you to monitor, manage, and configure an assortment of Redundant Arrays of Independent Disk (**RAID**) adapters and arrays without requiring you to take the RAID system offline to perform maintenance. Use the RAID Manager to gather data about your system's RAID array and RAID adapter, rebuild failing drives, add (or remove) logical drives, perform data integrity tests, and many other RAID system tasks. This service is available for both stand alone and network use by any system that has a supported RAID adapter.

Remote Session

You can use Remote Session to establish a fully-active command session with any remote Netfinity system.

Remote System Manager

You can use Remote System Manager to access and manage any Netfinity service on any Netfinity system in your network. The Netfinity systems on your network are organized into easy-to-manage logical groups that can be updated automatically using the auto-discovery feature.

Remote Workstation Control

Remote Workstation Control enables you to monitor or control the screen display of a remote Netfinity system. Once you initiate a Remote Workstation Control session with another Netfinity system, you can passively monitor events that are occurring on the display of the remote system or actively control the remote system's desktop. When you initiate an active Remote Workstation Control session, all mouse clicks and keystroke entered on your system are automatically passed through to the remote system. With Remote Workstation Control, you can remotely start programs, open and close windows, enter commands, and much more.

Screen View

The Screen View service takes a "snapshot" of any remote Netfinity system's graphic display and displays it on your screen. These snapshots can then be saved as bitmaps and viewed later.

Security Manager

The Security Manager can prevent unauthorized access to some or all of your Netfinity services. It uses incoming user ID and password combinations, and is available for network use only.

Serial Connection Control

The Serial Connection Control service enables remote Netfinity Managers to access your system through a phone line and modem. With the Serial Connection Control service, you don't have to be attached to a network to benefit from Netfinity's outstanding remote system access, monitoring, and management capabilities.

Note: Your system *must* have a properly installed and configured modem that supports at least 9600 baud for the Serial Connection Control service to function.

Service Configuration Manager

Service Configuration Manager enables you to save the configuration of a Netfinity service from a selected system to a service configuration file (SCF). Once created, SCF files can be used by Event Scheduler to restore the configuration back to the same system, or it can be used (in conjunction with the Event Scheduler) to propagate that configuration on whatever other similar systems you choose.

Service Processor Manager

Service Processor Manager enables you to configure and monitor many features of your systemCluster Managers Advanced Systems Management Adapter. This service enables you to dialout and directly access and control a remote system's Advanced Systems Management Adapter. With Service Processor Manager you can configure Advanced Systems Management Adapter events (such as POST, loader, and O/S timeouts; critical temperature, voltage, and tamper alerts; redundant power supply failures).

Software Inventory

Enables you to create and manage software product dictionaries that can be used to easily maintain an inventory of all application programs installed on your system.

System Diagnostics Manager

System Diagnostics Manager enables you to initiate a variety of diagnostic tasks on systems that support ROM based diagnostics. The results of all previously run diagnostic sessions are stored on the system and can be examined using System Diagnostics Manager to help diagnose and resolve system problems.

System Information Tool

The System Information Tool enables you to quickly and conveniently access detailed information on the hardware and software configurations of your system. System Information Tool gathers information about almost any computer; however, the most detail is provided when this service is used with IBM computers. This service is available for both stand-alone and network use.

System Monitor

The System Monitor provides a convenient method of charting and monitoring the activity of a number of components in a system, including processor usage, disk space used, and ECC memory errors. These convenient monitors are detachable and scalable, enabling you to keep only the monitors you need available at all times. You can use System Monitor's Threshold Manager to set threshold levels for any of the monitored components. When exceeded, these thresholds will generate user-configured alerts.

Data is continually collected from the time the system starts. A sophisticated data-handling technique is used to weigh the individual values, average concurrent samples, and post single values that accurately reflect long-term system activity. This technique allows you to maintain system activity records without creating enormous data files. This service is available for both stand-alone and network use.

System Partition Access

The System Partition Access allows for greatly simplified System Partition file handling, both locally and remotely. Individual files and entire directories can be renamed or deleted from the System Partition. Individual files can be renamed, deleted, or copied into the System Partition. Also, the entire partition can be backed-up, restored, or deleted. This service is available for both stand alone and network use by any system that has a System Partition.

System Profile

The System Profile provides a convenient notebook of pertinent data about a particular user or system. It features many predefined fields for extensive user-specific data, including name, address, office number and location, and phone number. System Profile also includes many predefined fields for system-specific data that might not be available to System Information Tool, including model and serial numbers and date of purchase. Finally, there are many user-definable "miscellaneous" fields that can be used to hold any data the user or administrator requires.

Web Manager Configuration

You can use the Web Manager Configuration service to limit access to the Netfinity Manager for Web to user-specified TCP/IP host or ranges of TCP/IP host addresses. You can also enable or disable the Netfinity Manager for Web and specify the TCP/IP port number that the Netfinity web server functions on.

Delaying Netfinity Startup on OS/2 Systems

In some cases, it might be necessary for you to delay the automatic startup of the Netfinity Network Interface (NETFBASE.EXE) in order to allow other time-sensitive applications to start up correctly or to allow your system to fully configure itself prior to beginning network operations. NETFBASE.EXE includes a parameter (WAIT) that enables you to specify the number of seconds that NETFBASE.EXE will wait before starting.

During Netfinity installation, the Netfinity Network Interface object is placed in the Startup folder. To configure Netfinity to wait a specified number of seconds before starting:

1. Shut down the Netfinity Network Interface if it is running.
2. Open the Startup folder.
3. Using mouse button 2, click on the Netfinity Network Interface object. This will open the Netfinity Network Interface context menu.
4. Select **Settings** to open the Netfinity Network Interface **Settings** notebook.
5. Type in the **Parameters** field

   `WAIT:`*x*

   where *x* is the number of seconds that you want the Netfinity Network Interface to wait before starting.
6. Close the Netfinity Network Interface **Settings** notebook.

With the WAIT parameter set to *x*, whenever you start your system, the Netfinity Network Interface will wait *x* seconds before starting.

Note: This feature is available only on systems that are running OS/2.

Chapter 2. Alert Manager

Netfinity Alert Manager enables your system to receive and automatically respond to alerts generated by other Netfinity services. Using a variety of alert-specific information (including the severity of the alert, the name of the Netfinity service that generated the alert, the type of alert, and the network address of the system that generated the alert), Netfinity alerts are categorized into alert profiles. Profiles can be bound to one or more Alert Manager actions (such as logging the alert or executing a command). Once a profile is bound to an action, the action will be performed whenever an alert that fits the profile is received.

Netfinity Alert Manager includes actions that do the following:

- Log the alert to a file
- Display the alert in a pop-up window
- Forward the alert to another workstation
- Execute a command
- Execute a minimized command
- Send a *simple network management protocol* (SNMP) version of the alert (not available for local use on systems running Windows 3.1 or Windows 95.)
- Send a mapped SNMP version of the alert (similar to the standard SNMP version of the alert, but featuring specific Enterprise ID values for each of the various alert types; not available for local use on systems running Windows 3.1 or Windows 95)
- Play a waveform (WAV) sound file (requires multimedia support)
- Send a message to a digital pager through a modem (requires modem attached to system)
- Send the alert information to an alphanumeric pager through a modem (requires modem attached to system)
- Send the alert to another user using TCP/IP SENDMAIL (available only on systems running OS/2; requires TCP/IP for OS/2 2.0 or later)
- Send an email version of the alert using Vendor Independent Messaging (VIM) (requires VIM support)
- Send a *messaging application programming interface* (MAPI) version of the alert (requires MAPI support)
- Export the alert information to a Netfinity database

- Export the alert information to a Lotus Notes database
- Generate a Desktop Management Interface (DMI) event and send it to the DMI Service Layer (requires DMI support)
- Display the alert on PC Server 720 front panel (available only on IBM PC Server 720 systems)
- Add an error condition to the system (see “Error Conditions” on page 222)
- Remove the error condition from the system (see “Error Conditions” on page 222)
- Send the alert to mainframe applications such as NetView MVS using APPC
- Send the alert to a remote system using a serial connection
- Add the alert to the Windows NT Event Log (available only on systems running Windows NT)
- Send a TCP/IP Web mail version of the alert, including links to the Netfinity Web Manager interfaces, to another user using TCP/IP SENDMAIL (available only on systems running OS/2; requires TCP/IP for OS/2 2.0 or later)
- Send an alert to FFST/2

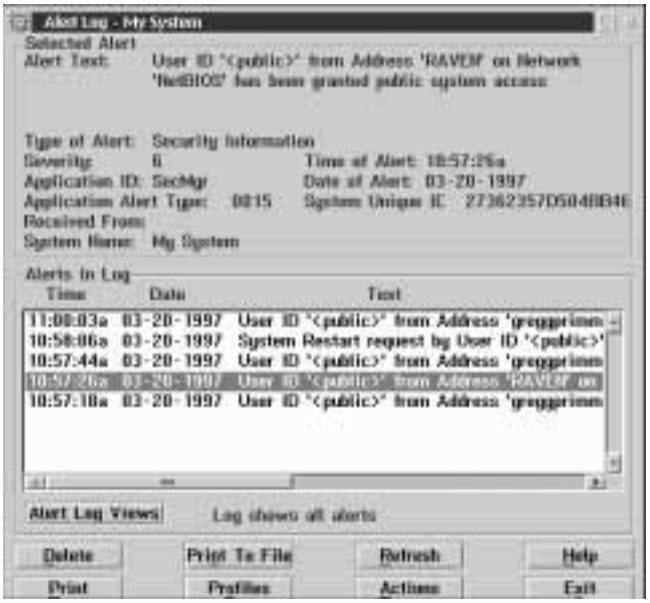

Figure 3. Alert Manager Service

Note: Netfinity can be used to remotely manage Netfinity Manager, Client Services for Netfinity Manager, or SystemView LAN clients. However, these systems management products do not support some of the features of the Netfinity Alert Manager, including alert profiles. If you will be remotely managing systems that are running any of these systems management products, see Appendix A, "Alert Manager on Downlevel Netfinity Systems" on page 445.

Alert Manager performs two essential systems management functions:

1. Maintains a log of all received and logged alerts that can be viewed with configurable filters.

   The Alert Log lists all alerts that are currently recorded in the Alert Log file. The Alert Log can be configured to display:

   - All logged alerts
   - Alerts that were received and logged within a specified time or date range
   - Alerts that were received and logged and that fit specified alert profiles
   - Alerts that were received within a specified time or date range *and* that fit specified alert profiles.

   Note: Only alerts that have been received and entered into the Alert Log using the **Add the alert to log file** alert action will appear in the **Alerts in Log** field. For information on this and other alert actions, see "Netfinity Alert Actions" on page 21.

   For information on configuring the Alert Log views, see "Alert Log Views" on page 17. For information on alert profiles, see "Alert Profiles" on page 32.

2. Automatically responds to the alerts it receives with user-specified actions.

   You can use Alert Manager manager to select one or more alert profiles and bind them to one of Alert Manager' alert actions. Once one or more profiles are bound to an alert action, this

action will automatically execute whenever an alert is received that fits a profile to which it is bound. For information on alert profiles, see “Alert Profiles” on page 32. For information on binding alert profiles to alert actions, see “Binding Profiles to Actions” on page 41.

Note: Netfinity can also be used to remotely manage Netfinity Manager, client Services for Netfinity, or SystemView LAN clients. However, these systems management products do not support some of the features of the Netfinity Alert Manager, including alert profiles. If you will be remotely managing systems that are running any of these systems management products, see Appendix A, “Alert Manager on Downlevel Netfinity Systems” on page 445.

The Alert Log

The Alert Log window is the first window that you see when you start the Alert Manager service. Any alerts that have been logged using the **Add alert to log file** action, appear in the **Alerts in Log** field in the bottom half of the Alert Log window.

Select an alert from the **Alerts in Log** to display information about the alert in the upper half of the Alert Log window.

Note: You can select multiple alerts for the purposes of deleting multiple files or printing reports, but only the currently highlighted alert in the log will have its alert-specific information displayed at the top of the screen.

Information displayed about the selected alert includes:

- Alert Text
- Type of Alert
- Severity
- Application ID
- Application Alert Type
- System Received From
- System Name
- Time of Alert
- Date of Alert
- System Unique ID

Alert Text

The Alert Text includes the name of the alert, as well as any textual commentary included by the application that generated the alert.

Type of Alert

This is the application-specified alert type. A Type of Alert consists of an alert sender ID followed by an alert type value. The alert sender ID describes the nature of the device that generated the alert, and the alert type value describes the content of the alert itself.

The possible alert sender IDs are:

- System
- DASD
- Network
- Operating System
- Application
- Device
- Security

An alert sender might also be unspecified, in which case an alert sender ID will not be displayed.

The possible alert type values are:

- Failure
- Error
- Warning
- Information

An alert type can also be unspecified, in which case an alert type value will not be displayed.

Severity

The alert Severity is a value from 0 to 7, with 0 being the most severe. For example, an alert Severity of 0 could be assigned to a disk failure, while a value of 7 could simply represent a system going offline at the end of a day. Alert Severity is determined by the application that generates the alert.

Application ID

The Application ID is the name of the application that sent the specified alert to the log.

Application Alert Type

The Application Alert Type is a numeric value assigned to an individual alert by the application that generated it. This value is often used by the application that generated the alert.

Received From

The Received From value is the network address of the system that generated the alert. The Received From value could be the local system or a remote system that has been instructed to relay alerts to the local error log.

System Name

The System Name value is the name of the system that generated the alert. This name is specified by the user during Netfinity installation.

Time of Alert

The Time of Alert is the time of day when the alert was generated and logged.

Date of Alert

The Date of Alert is the calendar date on which the alert was generated.

System Unique ID

The System Unique ID is a random 16 character identification string that is assigned to the system when Netfinity is installed. It is stored in the NFUNIQUE.ID file in the Netfinity directory of the system that generated the alert. The System Unique ID is primarily used for the identification and management of systems that frequently change network addresses (such as when DHCP is used).

Alert Log Views

You can configure Alert Manager to filter the alerts that will be visible in the **Alerts in Log** field. The current Alert Log View is shown beside the **Alert Log Views** button. The available Alert Log Views are:

- Log shows all alerts

  All alerts contained in the Alert Log are shown in the **Alerts in Log** field.

- Log is currently viewed by time

  The alerts shown in the **Alerts in Log** field have occurred within a specified time frame.

- Log is currently viewed by profile

  The alerts shown in the **Alerts in Log** field fit selected alert profiles.

- Log is currently viewed by time and profile

  The alerts shown in the **Alerts in Log** fit selected alert profiles *and* have occurred within a specified time frame.

Note: Only alerts that have been received and entered into the Alert Log using the *Add the alert to log file* alert action will appear in the **Alerts in Log** field. For information on this and other alert actions, see "Netfinity Alert Actions" on page 21.

To change the Alert Log view:

1. Select **Alert Log Views**.

   This opens the View Alert Log window (see Figure 4 on page 18).

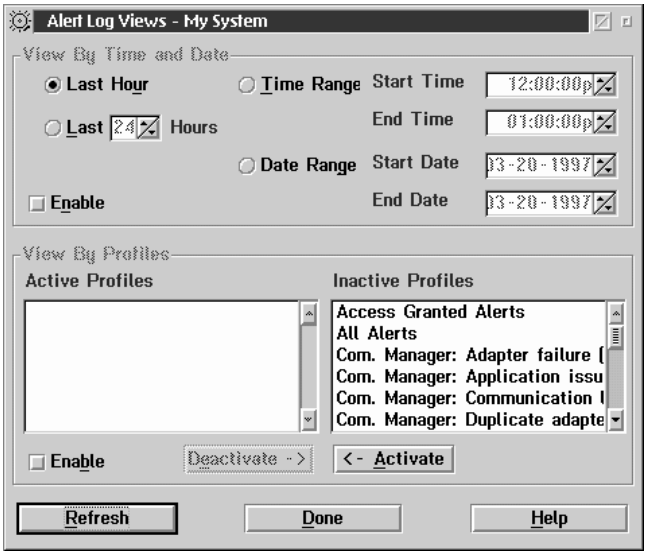

Figure 4. The View Alert Log window.

2. Enable (or disable) Alert Log view filters.

   There are two Alert Log view filters:

   - View by Time and Date
   - View by Profiles

   To enable the View by Time and Date filter:

   a. Select the radio button that describes the time and date range for alerts that will appear in the **Alerts in Log** field. The available selections are:

      - Last Hour

        Only alerts logged in the last hour will appear in the **Alerts in Log** field.

      - Last (1—48) Hours

        Only alerts logged within the number of hours that you specify will appear in the **Alerts in Log** field.

- Time Range

  Only alerts logged within the time range specified in the **Start Time** and **End Time** fields, on the date specified in the **Start Date** field, will appear in the **Alerts in Log** field.

- Date Range

  Only alerts logged within the date range specified in the **Start Date** and **End Date** fields will appear in the **Alerts in Log** field.

b. Select **Enable**.

To enable the View by Profiles filter:

a. Select one or more alert profiles from the **Inactive Profiles** field.

   Select only the alert profiles that correspond to the alerts that you want to appear in the **Alerts in Log** field.

b. Select **Activate**.

   Selected alert profiles are removed from the **Inactive Profiles** field and appear in the **Active Profiles** field.

c. Select and remove any unwanted alert profiles from the **Active Profiles** field.

   If there are any alert profiles contained in the **Active Profiles** field, select them and then select **Deactivate** to remove them from the **Active Profiles** field. They then appear in the **Inactive Profiles** filed.

d. Select **Enable**.

Alert log entries that correspond to one or more of the selected profiles will appear in the **Alerts in Log** field.

3. Select **OK** to save these changes and close the View Alert Log window.

To close this window without saving any changes, select **Cancel**.

To disable the View by Time and Date filter or the View by Profiles filter, deselect **Enable** in the filter's button group.

Alert Manager Functions

Alert Manager functions are activated from push buttons in the Alert Manager window. These buttons are:

- Delete
- Print
- Print to File
- Profiles
- Refresh
- Actions
- Help
- Exit

Information on each of the Alert Manager functions follows.

Delete

Select **Delete** to delete any selected alerts from the Alert Log. To use this function, select the alerts that you want to discard from the Alert Log and select **Delete**.

Print

Select **Print** to print a hardcopy of all selected alerts (and all specific alert information for the selected alerts) within the Alert Log.

Print to File

Select **Print to File** to save all selected alerts to a user-specified file.

Profiles

Select **Profiles** to configure, edit, or delete alert profiles. For detailed instructions on how to create, edit, or delete profiles, see “Alert Profiles” on page 32.

Refresh

Select **Refresh** to add any alerts that have been generated since the Alert Log window was displayed.

Actions

Select **Actions** to bind alert actions to any configured alert profiles. Alert actions can also be configured to respond to individual alerts that are not included in a Alert Manager alert profile. For instructions on how to bind alert actions to alert profiles, see "Binding Profiles to Actions" on page 41. For instructions on how to configure an alert action to respond to an alert that is not part of an alert profile, see "Binding Actions to Individual Alerts" on page 43. For information on alert actions, see "Netfinity Alert Actions."

Help

Select **Help** to access the online help for Alert Manager. Detailed information is available for all of Alert Manager's functions.

Exit

Select **Exit** to exit Alert Manager.

Netfinity Alert Actions

Alert Manager includes alert actions that do the following:

- Add the alert to log file

  Puts the alert into the Alert Log. This alert action does not require that you provide additional information.

- Display the alert in a pop-up window

  Displays a small window with all alert-specific information. This alert action does not require that you provide additional information.

- Forward the alert to another workstation

  Sends the alert to another user over a specified network. Once received, the alert is treated as though it were generated locally. When configuring this action, you must specify the following parameters:

Parameter Description

<P1>: Network Type

The network type that will be used to forward the alert. The network type **must** be entered as NETBIOS, TCPIP, IPX, SNA, or SERIPC (for serial connections).

Note: To forward an alert to a remote system using SERIPC (a serial connection), the serial connection must be active. This alert action will forward the alert to a remote system using SERIPC only if a serial connection to the remote system exists. To forward alerts to remote systems using a serial connection that is not currently active, use the "Send alert to remote system through serial connection" alert action.

<P2>: Network Address

The network type-specific address used by the remote system to which the alert will be forwarded.

If you are unsure of the workstation's network type or network address, you can use Remote System Manager's Edit System action (see "Edit System" on page 219) or system group Detail View (see "Detail View" on page 216) to check this information.

- Execute a command

  Executes a single command. When configuring this action, you must specify the following parameter:

  Parameter Description

  <P1>: Command Line

  The command that will be executed on the system.

  This action includes special command strings (or *macros*) that enable you to imbed alert-specific data in the command. This data can then be used by the application that is started by the command line. These macros are:

Macro	Imbedded Information
%TXT	Alert text
%TIM	Alert time
%DAT	Alert date
%SEV	Alert severity
%SND	Alert sender (for example, “NETBIOS::USER1”)
%TYP	Alert type
%APP	Alert application ID
%AT	Alert application-specific type
%SYS	System Name
%P1–%P9	Alert-specific text strings that are imbedded in the Alert Text. The content of these parameters is dependent on the alert itself. For more information, see Appendix J, “Netfinity Alerts” on page 503.

- Execute a minimized command

  Executes a single, minimized command. When configuring this action, you must specify the following parameter:

  Parameter Description

  <P1>: Command Line
  The command that will be executed on the system.

  This action includes special command strings (or *macros*) that enable you to imbed alert-specific data in the command. This data can then be used by the application that is started by the command line. These macros are:

Macro	Imbedded Information
%TXT	Alert text
%TIM	Alert time
%DAT	Alert date
%SEV	Alert severity

%SND	Alert sender (for example, "NETBIOS::USER1")
%TYP	Alert type
%APP	Alert application ID
%AT	Alert application-specific type
%SYS	System Name
%P1–%P9	Alert-specific text strings that are imbedded in the Alert Text. The content of these parameters is dependent on the alert itself. For more information, see Appendix J, "Netfinity Alerts" on page 503.

- Send SNMP Alert through TCP/IP

  Uses an SNMP agent to generate an SNMP version of the alert. When configuring this action, you must specify the following parameter:

  Parameter Description

  <P1>: Community String
  The community string name used by SNMP applications in your network.

  Notes:

  1. This action requires IBM TCP/IP for OS/2 version 2.0 or later in an OS/2 environment.
  2. This action is not available for local use on systems running Windows 3.1 or Windows 95.
  3. Netfinity's management information base (MIB) file for use with SNMP management applications is found on the Netfinity CD in the SNMP_MIB directory. It is named NETFIN.MIB. For information on how to use NETFIN.MIB with your SNMP-based systems management software, see the documentation that was supplied with your SNMP agent or with your systems management product.
  4. Netfinity's management information base (MIB) file for use with OS/2 SNMP management applications is found on the Netfinity CD in the SNMP_MIB directory. It is named

MIB2.TBL. You can append this file to your existing MIB2.TBL file, or replace your MIB2.TBL with this file.

- Map Alert to SNMP Trap

  Uses an SNMP agent to generate an SNMP trap featuring an Enterprise OID value for use by SNMP-based management applications. When configuring this action, you must specify the following parameter:

  Parameter Description

  <P1>: Community String
  The community string name used by SNMP applications in your network.

  Notes:

  1. This action requires IBM TCP/IP for OS/2 version 2.0 or later.
  2. This action is not available for local use on systems running Windows 3.1 or Windows 95.
  3. Netfinity's management information base (MIB) file for use with SNMP management applications is found on the Netfinity CD in the SNMP_MIB directory. It is named NETFIN.MIB. For information on how to use NETFIN.MIB with your SNMP-based systems management software, see the documentation that was supplied with your SNMP agent or with your systems management product.
  4. Netfinity's management information base (MIB) file for use with OS/2 SNMP management applications is found on the Netfinity CD in the SNMP_MIB directory. It is named MIB2.TBL. You can append this file to your existing MIB2.TBL file, or replace your MIB2.TBL with this file.

- Play a WAV file (requires multimedia support)

  Plays a specified waveform (WAV) audio file in response to the alert. When configuring this action, you must specify the following parameter:

Parameter Description

<P1>: Waveform file name
The fully-qualified filename of the waveform that will be played in response to the alert.

- Activate a numeric pager using a modem (requires a 100% Hayes-compatible modem attached to the system)

  Uses a modem attached to the system to dial out to a digital pager service. After the modem connects to the pager service, it will send all numeric data entered in the **Digital Pager Display** field. If your digital pager service requires that you press the pound sign (#) to send a page, be sure to type the # in the **Digital Pager Display** field after the numeric data. When configuring this action, you must specify the following parameters:

  Parameter Description

  <P1>: Modem COM port
  The COM port that the modem is configured to use. The COM port **must** be entered as COM*x*, where *x* is the number of the COM port.

  <P2>: Pager number
  The telephone number that will be dialed by the modem to transmit the information to the pager.

  <P3>: Digital pager display
  The numeric data that will be displayed on the pager.

  Note: Depending on your paging service, you might need to increase the amount of time that this alert action waits after dialing the telephone number in filed **<P2>** before it transmits the numeric data in field **<P3>**. To increase the amount of time that will pass before the numeric data is transmitted, add one or more commas (“,”) to the end of the telephone number in field **<P2>**. Each comma will cause the modem to wait two seconds before transmitting the numeric data.

- Send alert to alphanumeric pager through TAP using a modem (requires a 100% Hayes-compatible modem attached to the system)

  Uses a modem attached to the system to dial out to an alphanumeric pager service. After the modem connects to the alphanumeric pager service, it will send all alert information.

  Parameter Description

  <P1>: Modem COM port
  The COM port that the modem is configured to use. The COM port **must** be entered as COM*x*, where *x* is the number of the COM port.

  <P2>: TAP access number
  The telephone number that will be dialed by the modem to transmit the information to the pager.

  <P3>: Pager ID
  The identification number of the pager to which the data will be sent.

  <P4>: Additional text to send
  Any additional text that you want to send along with the alert data. This parameter is optional.

  Notes:

  1. This action will work only with pager services that use the telocator alphanumeric protocol (TAP).
  2. You must provide your pager's Pager ID.

- Send alert as TCP/IP mail (available only on systems running OS/2; requires TCP/IP for OS/2 2.0 or later)

  Uses the TCP/IP SENDMAIL program to send the Netfinity alert as a note to a specified e-mail address. When configuring this action, you must specify the following parameters:

  Parameter Description

  <P1>: Target user ID
  The TCP/IP ID of the system to which the alert will be sent.

<P2>: Target host address
The TCP/IP host address of the target user's system.

- Send alert as TCP/IP Web mail (available only on systems running OS/2; requires TCP/IP for OS/2 2.0 or later)

  Uses the TCP/IP SENDMAIL program to send the Netfinity alert as a note to a specified e-mail address. The alert text will be in HTML format. When configuring this action, you must specify the following parameters:

  Parameter Description

  <P1>: Target user ID
  The TCP/IP ID of the system to which the alert will be sent.

  <P2>: Target host address
  The TCP/IP host address of the target user's system.

- Send to E-Mail via VIM interface (requires VIM support)

  Uses the Vendor Independent Messaging (VIM) interface to generate a VIM-version of the alert that can be sent to any properly configured system that is 32-bit VIM-compliant, such as Lotus Notes.

  The requirements for a system running Lotus Notes are identical to the requirements for a system to export data to a Lotus Notes database. For more information, see see "Lotus Notes Database Support" in *Netfinity Manager Quick Beginnings*.

  When configuring this action, you must specify the following parameters:

  Parameter Description

  <P1>: Mail System Password
  The password that must be used to enable access to the VIM mail system.

  <P2>: E-Mail Address
  The email address of the system to which the alert information will be sent.

- Send to E-Mail via MAPI interface (requires MAPI support)

Uses the MAPI interface to generate a MAPI-version of the alert that can be sent to any system that is MAPI-compliant. When configuring this action, you must specify the following parameters:

Parameter Description

<P1>: Mail System Password
The password that must be used to enable access to the VIM mail system.

<P2>: E-Mail Address
The email address of the system to which the alert information will be sent.

<P3>: Profile Name
Some MAPI-compliant applications require a Profile Name to properly process MAPI data. If the MAPI-compliant application to which this alert will be sent requires a Profile Name, type it in this field. If your MAPI-compliant application does not require a Profile Name, leave this field blank.

- Export to a Netfinity database

  Exports the alert information to a selected Netfinity DB2 or ODBC database. When configuring this action, you must specify the following parameters:

  Parameter Description

  <P1>: Database Name
  The name of the Netfinity database to which the data will be exported.

  <P2>: User ID
  The ID that, when combined with a password, will enable access to the specified database.

  <P3>: Password
  The password that, when combined with a user ID, will enable access to the specified database.

- Export to a Lotus Notes database

Exports the alert information to a selected Lotus Notes database. When configuring this action, you must specify the following parameters:

Parameter Description

<P1>: Lotus Notes Password
The password that will give you access to the Lotus Notes database server.

<P2>: Lotus Notes Server Name
The name of the Lotus Notes database server to which the data will be exported.

- Send DMI Event through DMI Service Layer (requires DMI support)

  Converts the alert into a DMI event, which is then forwarded to the DMI Service Layer. Once it is received by the DMI Service Layer, it can be used by other DMI-compliant management applications. This alert action does not require that you provide additional information.

- Display on PC Server 720 Front Panel (available only on IBM PC Server 720 systems)

  Displays the alert-specific information on the PC Server 720's front panel LED screen. This alert action does not require that you provide additional information.

- Set error condition for sending system

  Adds an Error Condition to the system's Error Condition log. When configuring this action, you must specify the following parameter:

  Parameter Description

  <P1>: Error Condition
  The name that will be used to identify this error condition in the Error Condition log.

  A system's Error Condition log is accessed with the Remote System Manager. For more information on Error Conditions, see "Error Conditions" on page 222.

- Clear error condition for sending system

Removes a previously generated Error Condition from the system's Error Condition log. When configuring this action, you must specify the following parameter:

Parameter Description

<P1>: Error Condition
The name of the error condition that will be removed from the Error Condition log.

A system's Error Condition log is accessed with the Remote System Manager. For more information on Error Conditions, see "Error Conditions" on page 222.

- Send alert to remote system through serial connection

  Uses a previously defined serial connection to send the alert to a Netfinity system that can be accessed using Netfinity's Serial Connection Control service (see Chapter 20, "Serial Connection Control" on page 253). When configuring this action, you must specify the following parameter:

  Parameter Description

  <P1>: Connection Name
  The name of serial connection as defined in Serial Connection Control.

- Send alert to host via APPC

  Converts the Netfinity alert to a network management vector transport (NMVT) alert for use by host-based management applications (such as NetView for MVS). This alert action does not require that you provide additional information.

  Notes:

  The NMVT.INI file, found in the Netfinity directory, contains alert descriptions that map standard Netfinity alerts to NMVT-style alerts that can then be properly passed to a host system using APPC and the "Send alert to host via APPC" alert action. If you define new Netfinity alerts (using, for example, Netfinity's GENALERT command), you must make changes to this file for the alerts to be converted properly. For more information, see "Adding GENALERT Alert Descriptions to the NMVT.INI File" on page 467.

- Add event to Windows NT Event Log (available only on systems running Windows NT)

  This action adds information about the alert to the Windows NT Event Log. This alert action does not require that you provide additional information.

- Forward alert to FFST/2 (available only on systems running OS/2)

  This action sends a version of the Netfinity alert to FFST/2. This alert action does not require that you provide additional information.

Alert Profiles

Alert profiles are simple filters that enable you to better manage alerts received by your system. Using alert-specific information a profile describes a class, or set of classes, of alerts. With alert profiles you can classify alerts by service or application, by responsible person, or simply by urgency. Alert profiles can be bound to Alert Manager actions, enabling you to react automatically to alerts generated by Netfinity systems in your network. Alert profiles can also be used to filter the type of alerts that are shown in the Alert Log (see "Alert Log Views" on page 17).

Netfinity Alert Manager comes with many predefined alert profiles that will meet the needs of most users. Using these predefined alert profiles, you will be able to quickly and easily configure Alert Manager to respond and react to received alerts automatically. See "Predefined Alert Profiles" on page 37 for more information on Netfinity's predefined alert profiles.

Select **Profiles** from the Alert Log window to open the Alert Profiles window (see Figure 5 on page 33). The Alert Profiles window displays a list of all available profiles. You can select individual profiles for editing or deleting, or create completely new profiles.

- To create a new alert profile, see "Creating New Alert Profiles" on page 33.
- To edit an alert profile, see "Editing Alert Profiles" on page 37.

- To delete an alert profile, see “Deleting Alert Profiles” on page 37.

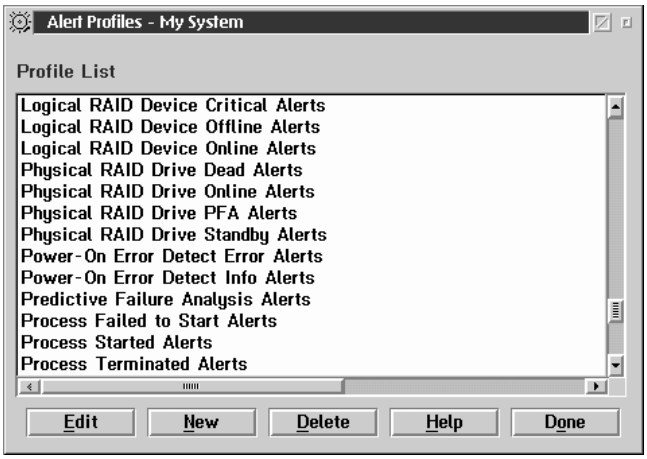

Figure 5. The Alert Profiles window.

Creating New Alert Profiles

To create a new alert profile:

1. Select **New**.

   This opens the Profile Editor window (see Figure 6 on page 34). Use the Profile Editor to specify the alert-specific information (called *alert conditions*) that will determine whether a received alert fits the alert profile.

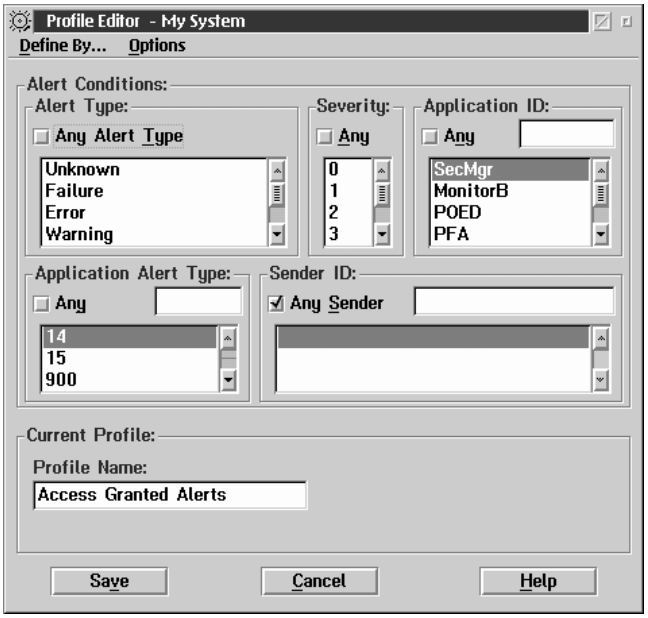

Figure 6. The Profile Editor window.

2. Set the **Alert Conditions**

   When creating an alert profile action, you must first specify the alert conditions that must be met for the received alert to fit a specific alert profile. As alerts are received, the Alert Manager checks each of these conditions to see if they meet the specifications for a defined alert profile. If *all* alert conditions are met, the alert fits the alert profile. If an alert fits an alert profile, any actions that are bound to that profile will be executed. For instructions on how to bind alert actions to alert profiles, see "Binding Profiles to Actions" on page 41.

   There are five alert conditions that are used by the Alert Manager to determine whether an alert fits an alert profile. For an alert to fit an alert profile, it must meet all of the alert conditions for the action. These five alert conditions are:

   - Alert Type
   - Severity
   - Application ID

- Application Alert Type
- Sender ID

To specify the alert conditions for this alert profile:

a. Select an Alert Type.

   The Alert Type is a brief description of the generated alert. It describes the nature of the alert (unknown, failure, error, warning, information), and can also contain a general description of the source of the alert (system, disk, network, operating system, application, device, or security).

   To check incoming alerts for specific Alert Types, select one or more Alert Types from the selection list. If you do not want to check for specific Alert Types, select the **Any** check box above the selection list.

b. Select a Severity.

   The Severity is a number from 0 through 7 that indicates how serious a generated alert is. A severity of 0 represents a very serious alert, while a severity of 7 is relatively minor.

   To check incoming alerts for specific Severity values, select one or more Severity values from the selection list. If you do not want to screen for specific Severity values, select the **Any** check box above the selection list.

c. Select an Application ID.

   The Application ID is the alphanumeric identifier of the application that generated the alert.

   To check incoming alerts for specific Application IDs, you can choose one or more from the Application ID selection list. If an Application ID that you require is not available from the list, you can add it to the list by typing the ID in the entry field above the selection list and pressing **Enter**. If you do not want to check for specific Application IDs, select the **Any** check box above the selection list.

d. Select an Application Alert Type.

   The Application Alert Type is a numeric value assigned to an individual alert by the application that generated it. This value is often used by the application itself.

   To check incoming alerts for specific Application Alert Types, you can 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 can add it to the list by typing it in the entry field above the selection list and pressing **Enter**. If you do not want to check for specific Application Alert Types, select the **Any** check box above the selection list.

e. Select a Sender ID.

   The Sender ID is the network address of the system that generated the alert.

   To check incoming alerts for specific Sender IDs, you can choose one or more from the Sender ID selection list. If a Sender ID that you require is not available from the list, you can add it to the list by typing it in the entry field above the selection list and pressing **Enter**. If you do not want to check for specific Sender IDs, select the **Any** check box above the selection list.

3. Name the alert profile.

   This is the name that will appear in the Alert Profile window **Profile List** field. Type in the **Profile Name** field a name for the Alert Profile. This name can be up to 64 characters long.

4. Save the Alert Profile.

   Select **Save** to save the Alert Profile. This Alert Profile will now appear in the Alert Profile window **Profile List** field.

Select **Cancel** to close this window without saving any alert profile information.

Editing Alert Profiles

To edit a previously defined alert profile:

1. Select from the **Profile List** the name of the alert profile you want to edit.
2. Select **Edit**.

   This opens the Profile Editor window (see Figure 6 on page 34).
3. Change alert conditions, if necessary.

   If you are editing this alert profile to alter the alert conditions that must be met for the received alert to fit the alert profile, select the appropriate new Alert Type, Severity, Application ID, Application Alert Type, or Sender ID values as necessary.
4. Change the profile name, if necessary.

   If you want to rename this alert profile, type in the **Profile Name** field the new profile name.
5. Save this alert profile.

   Select **Save** to save the changes you've made to this alert profile.

Select **Cancel** to close this window without changing any alert profile information.

Deleting Alert Profiles

To delete an alert profile, select an alert profile from the **Profile List** field, and then select **Delete**.

Predefined Alert Profiles

Alert Manager includes many predefined alert profiles. A list of predefined alert profiles that will be installed on *all* Netfinity systems, and a brief description nature of the alert-specific information that fits the profile, follows:

Profile Name	Alert Description
Power-On Error Detect Error Alerts	
	POST error detected by Power-On Error Detect on a Netfinity system.

Power-On Error Detect Information Alerts
System Partition access during startup detected by Power-On Error Detect on a Netfinity system.

Predictive Failure Analysis Alerts
Imminent failure of a PFA-enabled hard disk drive reported by Predictive Failure Analysis.

File Changed Alerts
Critical File Monitor detected that a monitored file has been changed.

File Deleted Alerts Critical File Monitor detected that a monitored file has been deleted.

File Created Alerts Critical File Monitor detected that a monitored file has been created.

Process Terminated Alerts
Process Manager detected that a monitored process has ended.

Process Started Alerts
Process Manager detected that a monitored process has started.

Process Failed to Start Alerts
Process Manager detected that a monitored process has failed to start.

System Online Alerts
Remote System Manager has reported that a specific remote system is online and functional.

System Offline Alerts
Remote System Manager has reported that a specific remote system is offline or unreachable.

Access Granted Alerts
Security Manager allowed a remote user that provided a User ID/Password combination access to the system.

Public Access Granted Alerts
Security Manager has allowed a remote user Public access to the system.

System Access Denied Alerts
Security Manager has denied a remote user access to the system.

System Restart Initiated Alerts
Security Manager has detected and permitted a system restart request by a remote user.

System Restart Rejected Alerts
Security Manager has detected and rejected a system restart request by a remote user.

Service Start Request Alerts
Service Manager has allowed use of a Netfinity service by a remote user.

Service Start Rejected Alerts
Service Manager has denied use of a Netfinity service by a remote user.

Threshold Error Alerts
A System Monitor error threshold condition has been met.

Threshold Warning Alerts
A System Monitor warning threshold condition has been met.

Threshold Return to Normal Alerts
A previously registered System Monitor warning or error threshold condition has returned to normal.

Physical RAID Device Online Alerts
A physical RAID device attached to the system has changed state to **Online**.

Physical RAID Device Standby Alerts
A physical RAID device attached to the system has changed state to **Standby**.

Physical RAID Device Dead Alerts
A physical RAID device attached to the system has changed state to **Dead**.

Logical RAID Device Online Alerts
A logical RAID device attached to the system has changed state to **Online**.

Logical RAID Device Critical Alerts
A logical RAID device attached to the system has changed state to **Critical**.

Logical RAID Device Offline Alerts
A logical RAID device attached to the system has changed state to **Offline**.

Physical RAID Drive PFA Alerts
A physical RAID device attached to the system has reported the imminent failure of a PFA-enabled hard disk drive in the RAID array.

Severity 0 Alerts A severity 0 alert has been received.

Severity 1 Alerts A severity 1 alert has been received.

Severity 2 Alerts A severity 2 alert has been received.

Severity 3 Alerts A severity 3 alert has been received.

Severity 4 Alerts A severity 4 alert has been received.

Severity 5 Alerts A severity 5 alert has been received.

Severity 6 Alerts A severity 6 alert has been received.

Severity 7 Alerts A severity 7 alert has been received.

All Alerts An alert has been received.

Many additional alert profiles will be installed if your system uses specific software or communications products (such as Communications Manager or LAN Server).

To create new alert profiles, see “Creating New Alert Profiles” on page 33. To edit an existing alert profile, see “Editing Alert Profiles” on page 37.

Binding Profiles to Actions

To enable Alert Manager to automatically respond to received alerts, you must bind alert profiles to alert actions. Once an alert profile is bound to an alert action, the alert action will be performed automatically whenever Alert Manager receives an alert that fits the profile. Multiple profiles can be bound to individual alert actions, and an individual alert profile can be bound to multiple alert actions.

To bind an alert profile to an alert action:

1. Select **Actions** from the Alert Log window.

   This opens the Alert Action window (see Figure 7). This window contains a list of all currently configured alert actions.

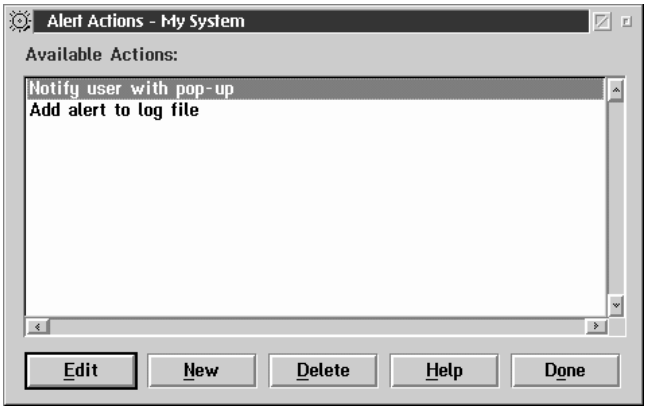

Figure 7. The Alert Actions window.

2. Select **New**.

   This opens the **Action Editor** window (see Figure 8 on page 42).

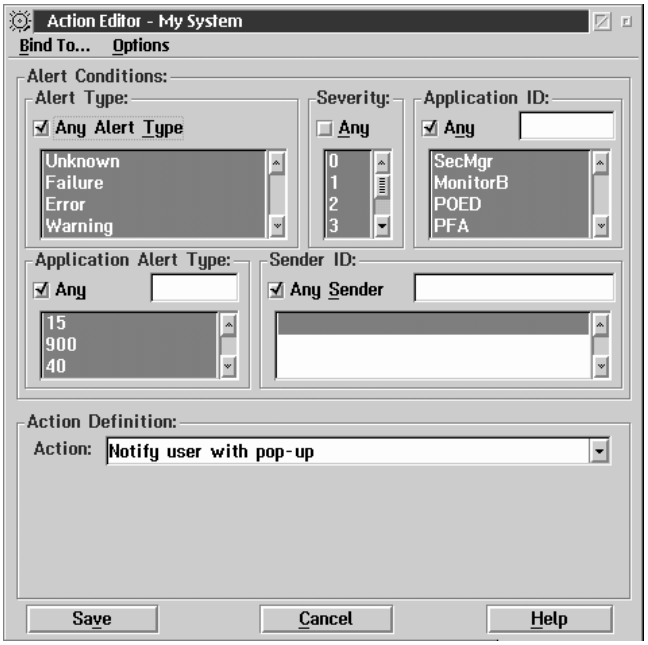

Figure 8. The Action Editor window.

3. Select **Profiles** from the **Bind To...** pull-down menu. This switches the Action Editor window to the Profiles view.
4. Bind one or more alert profiles to an alert action.

   To bind alert profiles to an alert action, you must first select the profiles that will trigger the action, and then select the alert action and provide any necessary defining information.

   a. Select one or more alert profiles to bind to an action.

      All currently available and unused alert profiles are listed in the **Other Profiles** field. Select one or more alert profiles from this list, and then select **Trigger By**. All selected profiles will then appear in the **Triggering Profiles** field. Received alerts that fit any of the profiles listed in the **Triggering Profiles** field will cause Alert Manager manager to perform an alert action.

      Note: To remove alert profiles from the **Triggering Profiles** field, select the profiles that you want to remove and

then select **Do Not Trigger By**. Selected profiles are then moved to the **Other Profiles** field.

b. Select an alert action.

   Use the spin buttons at the right of the **Action** field to see the available alert actions.

c. Enter additional information, if necessary.

   Some alert actions will require you to provide additional information (to whom alerts should be sent, what command to execute, and so on). If additional information is required, the parameter will be displayed in the Action field group as <P#>, where # is the number of the parameter. An Action Definition parameter field appears for each required parameter, along with a brief description of the information that is required. Enter the necessary information in each field.

5. Label this action.

   Type in the **Action Label** field a brief description of this alert profile and alert action combination. This description can be up to 32 characters. When you finish binding the alert profiles and the alert action, the Action Label will appear before the name alert action in the **Available Actions** field in the Alert Actions window.

6. Finish binding the alert profiles to the selected alert action.

   Select **Save** to finish binding the alert profiles to the selected action. The Action Editor window will close, and the Action Label, followed by the name of the alert action that you selected, appears in the **Available Actions** field in the Alert Actions window.

Select **Cancel** to close this window without saving any information.

Binding Actions to Individual Alerts

To enable Alert Manager to automatically respond to individual alerts that are not part of a defined Alert Profile, you must bind the desired action to specific specific alert conditions. Once an alert

profile is bound to specific alert conditions, the alert action will be performed automatically whenever Alert Manager receives an alert that contains **all** of the specified conditions.

Configuring an action is a two-step process. First, you must set the Alert Conditions that Alert Manager will look for. Then, you must set an Action Definition to define what action the Alert Manager will take in response to the received alert. Detailed descriptions of this process follow.

1. Select **Actions** from the Alert Log window.

   This opens the Alert Action window (see Figure 7 on page 41). This window contains a list of all currently configured alert actions.

2. Select **New** from the Alert Actions window.

   This opens the Action Editor window.

3. Select **Alert Conditions** from the **Bind To...** pull-down menu.

4. 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.

   There are five Alert Conditions that are used by the Alert Manager to determine appropriate action responses. For an alert to trigger an action, the alert must meet all of the alert conditions for the action. These five alert conditions are:

   - Alert Type
   - Severity
   - Application ID
   - Application Alert Type
   - Sender ID

   To specify the **Alert Conditions**:

   a. Select an Alert Type.

The Alert Type is a brief description of the generated alert. It describes the nature of the alert (unknown, failure, error, warning, information), and can also contain a general description of the source of the alert (system, disk, network, operating system, application, device, or security).

To screen incoming alerts for specific Alert Types, select one or more Alert Types from the selection list. If you do not want to screen for specific Alert Types, select the **Any** check box above the selection list.

b. Select a Severity.

The Severity is a number from 0 through 7 that indicates how serious a generated alert is. A severity of 0 represents a very serious alert, while a severity of 7 is relatively minor.

To screen incoming alerts for specific Severity values, select one or more Severity values from the selection list. If you do not want to screen for specific Severity values, select the **Any** check box above the selection list.

c. Select an Application ID.

The Application ID is the alphanumeric identifier of the application that generated the alert.

To screen incoming alerts for specific Application IDs, you can choose one or more from the Application ID selection list. If an Application ID that you require is not available from the list, you can add it to the list by entering the ID in the entry field above the selection list and pressing **Enter**. If you do not want to screen for specific Application IDs, select the **Any** check box above the selection list.

d. Select an Application Alert Type.

The Application Alert Type is a numeric value assigned to an individual alert by the application that generated it. This value is often used by the application itself.

To screen incoming alerts for specific Application Alert Types, you can 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 can add it to

the list by entering it in the entry field above the selection list and pressing **Enter**. If you do not want to screen for specific Application Alert Types, select the **Any** check box above the selection list.

e. Select a Sender ID.

The Sender ID is the network address of the system that generated the alert.

To screen incoming alerts for specific Sender IDs, you can choose one or more from the Sender ID selection list. If a Sender ID that you require is not available from the list, you can add it to the list by entering it in the entry field above the selection list and pressing **Enter**. If you do not want to screen for specific Sender IDs, select the **Any** check box above the selection list.

5. Set an Action Definition.

You must select a specific action, and supply any necessary information for the completion of the action.

a. Select an Action.

An action is a program that is executed in response to an alert that meets the Alert Conditions that you have specified. Use the spin buttons at the right of the **Action** field to see the available action handlers.

b. 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 appears for each required parameter, along with a brief description of the information that is required. Enter the appropriate information in each field.

6. Save the defined action.

Once all Alert Conditions and Action Definition information has been entered, select **Save** to save the configured action. This action will now appear in the Available Actions field of the Alert Actions window. After you select **Save**, the Action Editor window closes automatically.

Remotely Managing Downlevel Netfinity Systems

If you are using Netfinity Alert Manager to remotely manage systems that are using downlevel Netfinity Manager, Client Services for Netfinity Manager, or SystemView LAN clients, you will not be able to bind alert profiles to alert actions. If you will be remotely managing systems that are running any of these systems management products, you must configure each alert action to respond specifically to a specified alert conditions. For more information on how to remotely manage systems that are running these products, see Appendix A, "Alert Manager on Downlevel Netfinity Systems" on page 445.

Receiving Alerts from First Failure Support Technology (FFST)

If your system is running OS/2 Warp version 3.0 or later and you use Warp's built-in First Failure Support Technology (FFST) to track problems with other products, you can enable Netfinity to receive any FFST information and convert the FFST trap into a Netfinity alert. If FFST is enabled on your system you will be asked during installation whether you want FFST trap information to be forwarded to Netfinity Alert Manager. Select **Yes** to enable this feature. Once this feature is enabled, FFST trap information will be converted automatically into Netfinity alerts. Also, systems that have FFST installed will also have additional alert profiles available that are specifically designed to work with a variety of FFST-enabled products (such as IBM Communication Manager or LAN Server).

Chapter 3. Alert On LAN Configuration

Use the Alert on LAN configuration service to configure monitoring options of Alert on LAN-capable systems locally and remotely. Systems with Alert on LAN capability provide critical status information about system states. The data is reported by hardware or software (depending upon whether the systems in currently powered on or not) using TCP/IP. Some of the status information that is reported includes:

- missing processors
- chassis intrusion
- broken LAN connections

Figure 9. The Alert on LAN Configuration service.

For Alert on LAN to function properly, you must configure the following options:

Option **Description**

Alert on LAN enable status Use this option to enable or disable all Alert on LAN capabilities on the system you are configuring

Netfinity Manager IP Address Enter the IP address of a system running Netfinity Manager. All Alert on LAN data on the system you are configuring will report data to this IP address.

Netfinity Manager Port Number Enter the port number of the system running Netfinity Manager at the IP address you entered in the **Netfinity Manager IP Address** field. All Alert on LAN data on the system you are configuring will report data to this port number.

Heartbeat Timer Use the values available in this field to set the time interval at which Alert on LAN will send out a heartbeat message to the Netfinity Manager at the IP address specified in the **Netfinity Manager IP Address** field. If the message fails to be sent, the Netfinity Manager will send out an alert.

Note: This interval must be a multiple of 43 seconds.

Watchdog Timer Use the values available in this field to set the time interval at which Alert on LAN will send out an alert if the operating system experiences a crash.

Note: This interval must be a multiple of 86 seconds.

Retransmission Timer Use the values available in this field to set the time interval at which Alert on LAN will send message packets for each alert sent out.

Note: These alerts are sent out at multiples of 3 seconds.

Agent Polling Period Use the values available in this field to configure the time interval at which Alert on LAN software checks the status of hardware.

Monitor Events Enable/Disable individual events Alert on LAN is capable of monitoring.

Chapter 4. Capacity Management

Capacity Management is an easy-to-use resource-management and planning tool for network managers and administrators, allowing remote performance monitoring of every server on the network.

IBM Capacity Management identifies potential bottlenecks in a network, allowing for effective planning of future capacity needs, such as microprocessor, disk, or memory upgrades, thus preventing network slow downs and downtime. With Capacity Management you can intelligently plan for future hardware upgrades and how best to spend your resource dollars.

Capacity Management includes extensive online help, including online tours. The online tours are interactive helps that guide you through Capacity Management's functions, making it especially simple to learn and understand this service. To use an online tour, select **Tour the Generator**, **Tour the Scheduler**, or **Tour the Viewer** from the Capacity Management window (see Figure 10).

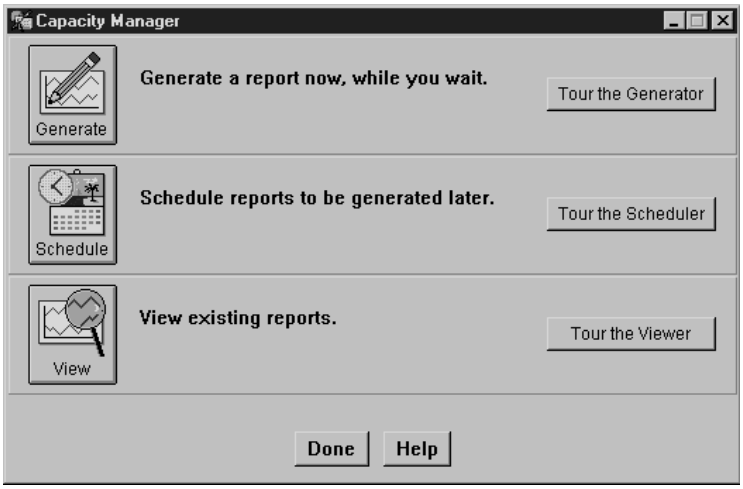

Figure 10. The Capacity Management window

Note: The Capacity Management interface is available for use only on systems running Windows NT. However, data can be collected from any remote systems running Client Services for Netfinity Manager for OS/2, Windows 95, Windows NT, or NetWare.

Generating Reports

To generate a new Capacity Management report:

1. Select **Generate** from the Capacity Management window.

   This opens the Generate Reports notebook. Initially, the notebook opens to the Overview page. This page provides brief step-by-step instructions on generating reports. When you are ready to begin generating a report, select **Next**. This will open the Generate Reports notebook to the Report Definition page (see Figure 11).

Figure 11. Report Generator notebook — Report Definitions page

2. Select a Report Definition.

   The Report Definitions page of the Generate Reports notebook contains all previously defined Report Definitions. Report Definitions specify the data that is collected for a Capacity Management report. You can:

   - Select a previously defined Report Definition

To select a previously defined Report Definition, select the Report Definition and then select **Next**. This opens the Generate Reports notebook to the Systems page. If you are using a previously created report, go to step 4 on page 53.

- Edit a previously defined Report Definition

  To edit a previously defined Report Definition, select the Report Definition and then select **Edit**. This opens the Report Definition window (see Figure 12).

- Create a new Report Definition

  To create a new Report Definition, select **New**. This opens the Report Definition window (see Figure 12).

Figure 12. Report Definition window

3. Create (or edit) the Report Definition.

   Use the selections available on the Report Definitions window to configure the Report Definition. You will need to specify:

   - The time period for which data will be collected (Duration)
   - The amount of data to collect (Global Sampling Frequency)

- The days on which the data will be collected (Days)
- The specific monitored data that will be included in the report (Monitors to include ub the report)

Select **Next** to continue.

4. Select systems to include in the report.

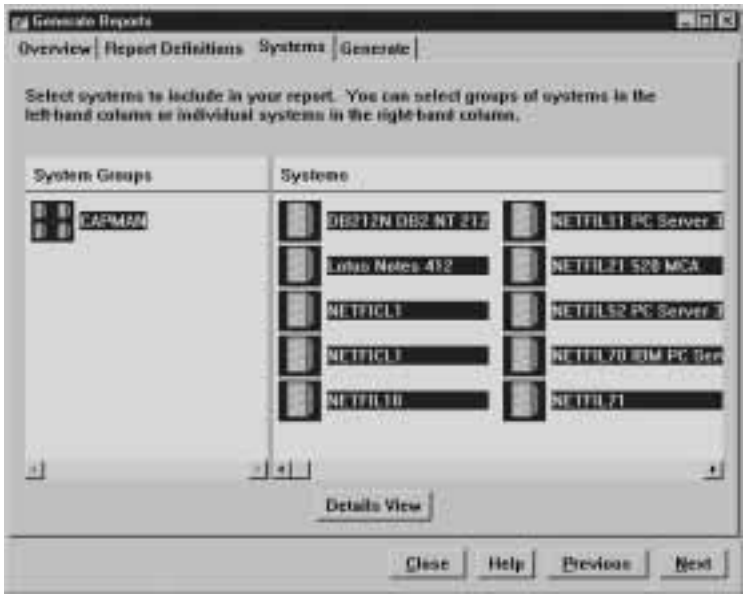

Figure 13. Report Generator notebook — Systems page

Select Netfinity groups or systems that will be included in the report. Then, select **Next** to open the Report Generator notebook to the Generate page (see Figure 14 on page 54).

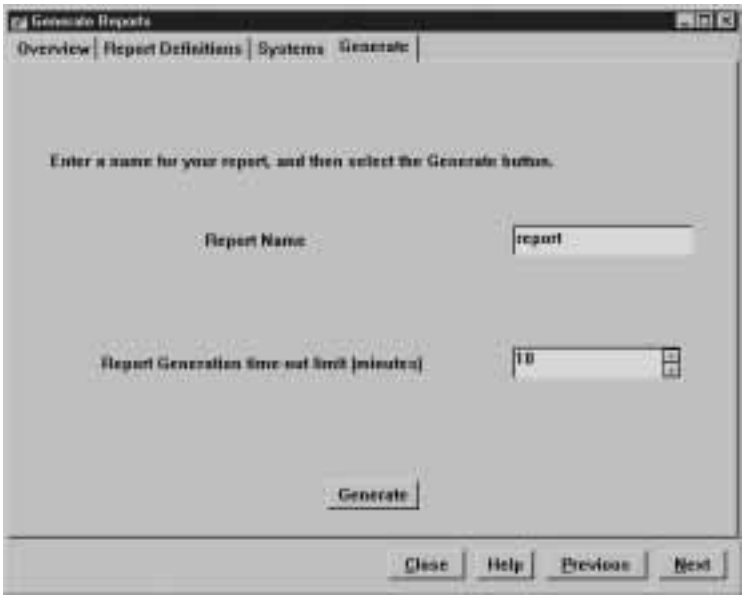

Figure 14. Report Generator notebook — Generate page

5. Name the report, and specify a Report Generation timeout interval.

   You must provide a name for your report. Report Generation timeout interval specifies the amount of time Capacity Management will attempt to collect data from any system you specified in your Report Definition. If the timeout interval is exceeded without Capacity Management having successfully collected any data from the system, Capacity Management will ignore the system and continue generating the report using the other selected systems.

6. Select **Generate** to generate the Capacity Management report.

   Capacity Management will immediately begin compiling the report based on your Report Definition. When the report is complete, it is displayed in the Report Viewer window.

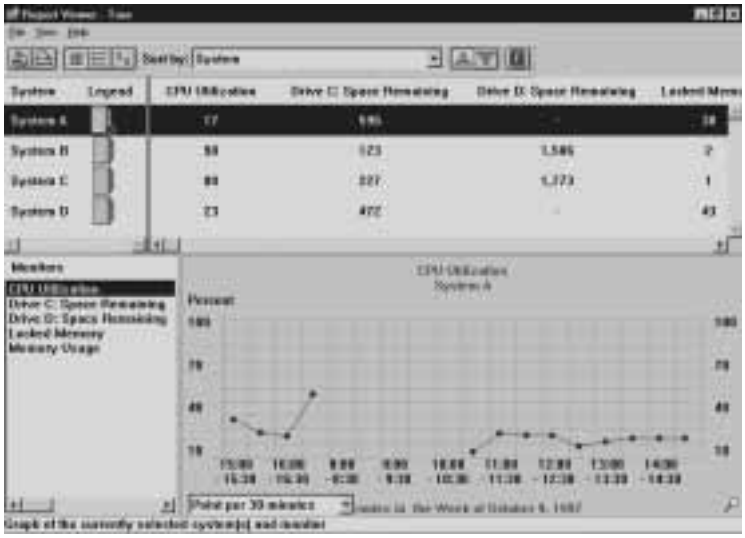

Figure 15. The Report Viewer window

Scheduling Reports

You can use Capacity Management to automatically gather data and create reports. Select **Schedule** from the Capacity Management window to open the Netfinity Event Scheduler service. Then Create a new scheduled event using the Capacity Management task. For more information, see "The Capacity Management Task Specific Window" on page 143.

Viewing Reports

After reports have been created, you can use the Capacity Management Report Viewer to examine the data that has been collected. The Report Viewer presents the collected data in an easy-to-understand and -manipulate interface. With this interface you can view collected data from one or more systems simultaneously.

To view a previously generated report:

1. Select **View** from the Capacity Management window.

This opens the Open window. Use this window to select the report file that you want to view.

2. Select **Open** to open the selected report file.
3. Once the report is loaded into the Report Viewer, select one or more systems whose data will be displayed in the Report Viewer.
4. Select a monitor from the Monitor pane.

   You can select one monitor at a time. Once you select a monitor, the data that was collected from the selected system (or systems) is plotted as a line graph in the Report Viewer window. If you select another monitor, the data will be plotted again.

Chapter 5. Cluster Manager

Cluster Manager is a powerful application designed to enhance the cluster management capabilities of the Microsoft Cluster Server (MSCS) administration console, included with Microsoft Windows NT Server version 4.0 Enterprise Edition. Cluster Manager builds on the power of MSCS, providing an integrated graphical interface that enables you to quickly and easily monitor and manage the clustered systems on your network. Clusters, the nodes that make up a cluster, and their associated groups, resources, and network information are presented in a tree view, making it simple to quickly find the cluster element you want to work with. As cluster elements are selected from the tree view, information about the selected element appears in the Group, Resource, and Node or Network information panels on the right side of the interface.

Note: The Node or Network Information panel displays information about nodes when a group, resource, node, or cluster is selected from the tree view. However, when network or network resource items are selected from the tree view, this panel displays network information.

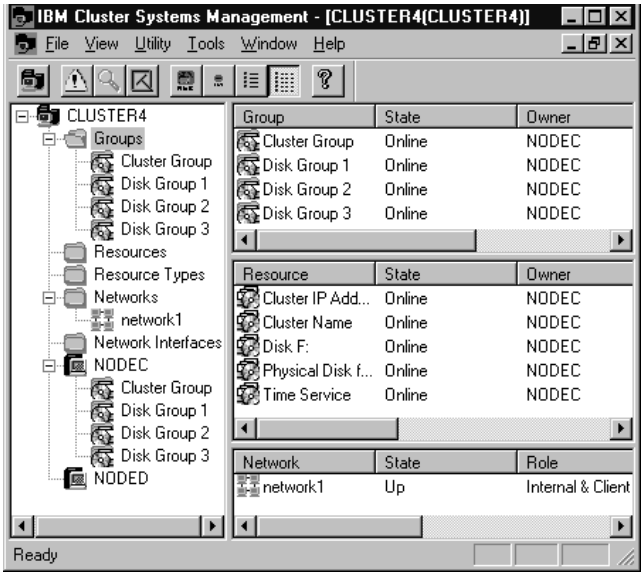

Figure 16. Cluster Manager

Cluster Manager also provides powerful additional function that greatly improves your ability to manage your clustered systems effectively. With Cluster Manager, you can:

- Manage all of your clusters from a single Microsoft NT Workstation console running Netfinity Manager.
- Manually allocate (or reallocate) dynamic resources and balance the resources and load on your clustered servers.
- Generate Netfinity alerts when cluster-related events (such as failovers or other cluster-element changes) occur. Alerts can be configured for individual clusters and cluster elements.
- Search for all clusters on your network using the Cluster Manager *Discovery* Function.
- Use the Cluster Manager *Cluster Expert Wizards* to simplify the creation of new file share, Internet Information Server, and print spooler resource groups.
- Simplify the management of the virtual IP addresses of the clustered systems.
- Use the Cluster Manager Scheduler to automatically perform certain cluster-management tasks (such as taking cluster groups offline, bring cluster groups online, or moving cluster groups between nodes) at specified times of day or on specified dates.

Notes:

1. Cluster Manager runs only on systems running Microsoft Windows NT Workstation version 4.0 with Service Pack 3 and the Microsoft Cluster Server administrator console (MSCS) installed. MSCS is included with Microsoft Windows NT Server version 4.0 Enterprise Edition. For information on how to install the MSCS Administrator Console, see the documentation that came with Windows NT Server Enterprise Edition.
2. Cluster Manager requires the TCP/IP communications protocol to communicate with clusters on your network.
3. Unlike other Netfinity services, Cluster Manager cannot be used remotely by a Netfinity Manager using the Remote System Manager service. Cluster Manager must be used locally, and

can only manage clusters that it can communicate with directly using TCP/IP.

The Cluster Systems Manager Interface

To start Cluster Manager, double-click on the Cluster Manager icon in the Netfinity Service Manager. After you start the Cluster Systems Manager, you must open a connection to a cluster on your network. To open a connection to a cluster:

1. Select **Connect to** from the **File** pull-down menu (or select the **Connect** button from the button bar).
2. Type in the **Cluster Name** field the name of the cluster you want to connect to and manage.

   If you do not know the name of the cluster, use the Cluster Manager Discovery function to find clusters on your network (see "Discovering Clusters" on page 77).
3. Select **OK** to open a view of the cluster.

Note: After you have established a connection with a cluster, the cluster's name will appear as a selection in the **View** pull-down menu. Once this selection is available, you can open a connection with this cluster by selecting its name from the **View** pull-down menu.

After you open a connection to a cluster, the Cluster Manager interface displays detailed information about the cluster (see Figure 16 on page 57). The Cluster Manager window is divided into four panels. The panel on the left side of the Cluster Manager window contains a tree view of all cluster elements. The tree view includes the names of all clusters to which your system is currently connected (for information on how to connect to a cluster, see "Managing Clusters" on page 65).

If you select the plus sign beside any cluster, the tree view of that cluster will expland to show folders and objects representing that cluster's groups, resources, resource types, networks, network interfaces, and nodes. Plus signs will appear beside some of these folders and objects; if you select these additional plus signs, the tree

view will further expand, revealing other cluster elements such as group names, network names, and cluster group owner names.

When you select a cluster element from the tree view, the three panels on the right side of the window immediately are updated and display information about the selected element. The three panels are:

- Group Panel

  The Group Panel contains the names of all groups that are associated with the selected cluster element, as well as detailed information about each cluster group including:

Group Item	Meaning
State	The current state of the cluster group (online or offline)
Owner	The node (within the cluster) that currently owns this group
Description	A user-defined description of the group

- Resource Panel

  The Resource Panel contains the names of all resources that are associate with the selected cluster element, as well as detailed information about each resource including:

Resource Item	Meaning
State	The current state of the cluster resource (online or offline)
Owner	The node (within the cluster) that currently owns this resource
Group	The group that currently owns the resource
Resource Type	The type of resource (for example, Shared File Resource)
Description	A user-defined description of the resource

- Node or Network Panel

  If you select a cluster, node, group, resource, or network resource from the tree view, the Node or Network Information Panel contains information about the node or nodes that are associated with the selected element including:

Node Item	Meaning
Network	The name of the network that owns the network node
State	The current state of the network connection (up or down)
Adapter	The name of the adapter that connects this node to the network
Address	The node's virtual TCP/IP address
Description	A user-defined description of the node

  If you select the networks element from the tree view, the Node or Network Information Panel contains information about the cluster's network connection and resources, including:

Network Item	Meaning
State	The current state of the network connection (up or down)
Role	The network's role
Mask	The subnet mask for this network
Description	A user-defined description of this network

The information that is displayed in the information panels is dependent upon the cluster element that you select from the cluster tree view. For example, if you select a cluster from the tree view, information on all groups and resources defined for use on the cluster will be displayed in the information panels on the right side of the window. However, if you select a node from the tree view, only information about the groups and resources that are currently owned by the selected node are displayed. Finally, if you select a

group from the tree view, only the selected group and its resources and the the node that currently owns the selected group will be displayed.

Pull-Down Menus

Once you have opened a connection with a cluster, the Cluster Manager window will feature five pull-down menus. These menus are:

- File

  Use the selections available from the File pull-down menu to open or close a connection with a cluster, create new groups or resources, and change the properties of currently defined groups and resources.

  Also, additional selections will appear in this pull-down menu when you select cluster elements from any of the Cluster Manager window panels. For example, if you select a resource from the Resource Panel, additional selections appear that you can use to change the group that owns this resource or to initiate a failure of the selected resource.

  All additional File pull-down menu selections are also available if you open the selected cluster element's context menu. To open a element's context menu, use the right mouse button to select the element.

- View

  Use the selections available from the View pull-down menu to change the appearance of certain elements of the Cluster Manager window, including the button bar and the size of the icons that appear in the panels. You can also use the View pull-down menu to see a list of all clusters to which your workstation is currently connected, and to refresh the information in the Cluster Manager window.

- Utility

  Use the selections available from the Utility pull-down menu to access Cluster Manager's powerful cluster-management utility programs. The following selections are available:

- Discover Cluster

  Select **Discover Cluster** to use the Cluster Manager *Discovery* function to search for and identify clusters that are accessible from your workstation. For more information, see "Discovering Clusters" on page 77.

- Alert Management

  Select **Alert Management** to configure Cluster Manager alert actions that will automatically be carried out when changes to specified cluster elements occur. For more information, see "Alert Service" on page 81.

- Scheduler

  Select **Scheduler** to automatically take cluster groups offline, bring cluster groups online, or move cluster groups between nodes at specified times of day or on specified dates. For more information, see "Scheduler" on page 79.

- Cluster Expert Wizard

  Select **Cluster Expert Wizard** to simplify the creation of new file-share resource groups, Internet Information Server groups, or print spooler groups. For more information, see "Cluster Expert Wizard" on page 91.

- Tools

  Use the selections available from the Tools pull-down menu to reset the virtual IP address range that is used by the Cluster Expert Wizard. For more information, see "Cluster Expert Wizard" on page 91.

- Window

  Use the selections available from the Window pull-down menu to rearrange the windows or icons currently displayed on your desktop. You can choose cascade, tile and split window views, and you can arrange the icons that are currently displayed.

- Help

  Use the selections available from the Help pull-down menu to access online help for this service.

The Button Bar

The Cluster Manager button bar features nine buttons that you can use to quickly access many of the Cluster Manager most frequently used functions. These functions are:

- Open Connection

  Opens the Open Connection window.

- Alerts

  Opens the Alert Service (for more information, see “Alert Service” on page 81).

- Discover

  Opens the Clusters Discovery window (for more information, see “Discovering Clusters” on page 77).

- Refresh

  Refreshes the contents of the Cluster Manager interface.

- Switch to Large Icon View

  Displays all cluster elements in the Cluster Manager information panels as large icons.

- Switch to Small Icon View

  Displays all cluster elements in the Cluster Manager information panels as small icons.

- Switch to List View

  Displays all cluster elements in the Cluster Manager information panels as a list.

- Switch to Details View

  Displays all cluster elements in the Cluster Manager information panels as a list with detailed information about each element.

- About

  Displays information about this version of Cluster Manager.

Managing Clusters

You can use Cluster Manager to manage a wide variety of cluster-specific functions on all your cluster elements. After you open a connection to a cluster, you are presented with a tree view of the cluster and its elements (including nodes, groups, resources, networks, and network resources). As you select individual elements from the tree view, the information that appears in the information panels on the right side of the window is updated automatically, providing you with information specifically related to the selected cluster element.

Before you can manage a cluster, you must first open a connection to the cluster. You can open a connection to a cluster in two ways:

- Select **Open Connection** from the File pull-down menu (or select the **Open Connection** button from the button bar).

  This opens the Open Connection window. To open the connection, type in the **Cluster Name** field the name of the cluster you want to manage and then select **Done**.

- Use the Discovery function.

  If you don't know the name of the cluster you want to manage, or if you want to select from a list of clusters that are available on your network, select **Discover Cluster** from the Utility pull-down menu (or select the **Discover** button from the button bar). This opens the Cluster Discovery window. For information on how to use the Discovery function, see “Discovering Clusters” on page 77.

When you've opened a connection to a cluster, all elements of the cluster are displayed in the Cluster Systems Manager window tree view. From this window you can easily:

- Move groups among nodes
- Move resources among groups
- Change cluster element properties
- Manage nodes
- Create, delete, and manage cluster groups

- Create, delete, and manage cluster resources
- Manage the cluster network and network resources

Moving Groups

A group is a collection of related resources. Groups are owned by a single node within the cluster, and can be configured to failover to other nodes within the cluster in the event of a node failure.

With Cluster Manager, you can manually reallocate groups to specific nodes. To move a group from one node to another node, drag the group icon and drop it onto the icon of the node that you want to own the group. Once the group icon is dropped, the group and all its resources will automatically be transferred to the node.

You can also move groups by selecting the group, and then selecting **Move Group** from the File pull-down menu.

Moving Resources

Resources are physical parts of the cluster (such as disk drives or IP addresses) that are shared by the applications that run on your cluster and that are associated with specific groups. You can use Cluster Manager to manually move resources among groups on your cluster.

To move a resource from one group to another group, drag the resource icon from the former group and drop it onto the icon of the new group that you want to own the resource. Once the resource icon is dropped, the resource and all its dependencies are automatically transferred to the group.

You can also move resources by selecting the resource, and then selecting **Move Resource** from the File pull-down menu.

Changing Cluster Element Properties

All cluster elements feature user-definable properties. To examine or change the properties of a cluster element, select the cluster element and then select **Properties** from the File pull-down menu. The cluster element Properties window opens.

Once the Properties window is open, you can make changes to the cluster element's properties. When you have finished making changes to these properties, select **OK** to save these changes and close the Properties window. To close the window without saving changes, select **Cancel**.

The contents of the Properties window depend on the cluster element that is selected, and some Properties windows include more than one page of properties. Also, some windows contain data fields that cannot be altered.

Cluster Properties

The Cluster Properties window contains the following items:

Name	The name of the cluster
Description	A description of the cluster (optional)
Quorum Resource	The quorum disk resources used by the cluster

Node Properties

The Node Properties window contains the following items:

Name	The name of the node
Description	A description of the node (optional)
State	The current state of the node

Group Properties

The Group Properties window contains the following items:

- General Page

Name	The name of the group
Description	A description of the group (optional)
Preferred Owners	The name of the node that is the preferred owner of the group
State	The current state of the group
Node	The name of the node that currently owns the group

- Failover Page

  Threshold — The number of times failover is permitted during a specified time period (the value in the **Period** field) before the group is taken offline

  Period — The time period used to determine whether a group must be taken offline after a specific number of failovers (the value in the **Threshold** field)

- Failback Page

  Prevent Failback radio button — Prevents this group from failing back to its preferred owner once a failover has occurred.

  Allow Failback radio button — Permits this group to fail back to its preferred owner once a failover has occurred. Use the **Immediately** and **Failback Between** radio buttons to specify the manner in which failback will occur.

Resource Properties

The Resource Properties window contains the following items:

- General Page

  Name — The name of the resource

  Description — A description of the resource (optional)

  Possible owners — The groups that have access to the resource. Select **Modify** to add or remove owners from the possible owners list.

Run this resource in a separate resource monitor check box
Select this check box to run this resource in a separate resource monitor.

Note: Use this option only if you anticipate a conflict with another resource or for debugging purposes.

Group The name of the group that currently owns the resource

State The current state of the resource

Node The node that currently owns the resource

- Dependencies Page

  Lists all other cluster resources that must be brought online before this resource can be brought online. Select **Modify** to add dependencies to or remove dependencies from this list.

- Advanced Page

  Do Not Restart radio button
  Prevents this resource from restarting if it fails.

  Restart radio button Permits this resource to restart after a failure. Select the **Affect the group** check box to enable the group that currently owns the resource to return to online after the resource restarts.

  "Look Alive" Poll Interval
  The amount of time between "Look Alive" polls

  "Is Alive" Poll Interval The amount of time between "Is Alive" polls

  Pending Timeout The amount of time allowed for resources to be in a pending state before they fail

- Parameters Page

  Contains a list of all cluster nodes that own or share this resource

Network Properties

The Network Properties window contains the following items:

Name The name of the network

Description A description of the network (optional)

Enable for cluster use check box
Enables the cluster to use this network. Use the **Use for all communications**, **Use only for internal communications**, and **Use only for client access** buttons to specify the manner in which the cluster will use this network.

State The current state of the network

Subnet mask The subnet mask used by the network

Managing Nodes

A node is a single system that is part of a cluster and that owns groups and their resources. The cluster server runs on each node and enables each node to communicate and work with the other nodes in the cluster. You can use Cluster Manager to:

- Start a node

  Starts the cluster server on a node. To start a node, select the node from the tree view and then select **Start** from the File pull-down menu.

- Stop a node

  Stops the cluster server on a node. To stop a node, select the node from the tree view and then select **Stop** from the File pull-down menu.

- Evict a node

Removes the node from the cluster. To evict a node, select the node from the tree view, select **Stop** from the File pull-down menu, and then select **Evict** from the File pull-down menu.

- Pause a node

  Temporarily stops the node from functioning as part of the cluster. To pause a node, select the node from the tree view and then select **Pause** from the File pull-down menu.

- Resume a node

  Restarts a paused node. To resume a node, select the node from the tree view and then select **Resume** from the File pull-down menu.

- Change node properties

  For information on changing node properties, see "Changing Cluster Element Properties" on page 66.

Creating, Deleting, and Managing Groups

A group is a collection of shared resources that are used by applications running on the cluster. You can use Cluster Manager to:

- Create groups

  To create a new group:.

  1. Select **New** and then **Group** from the File pull-down menu.

     This opens the New Group window (see Figure 17 on page 72).

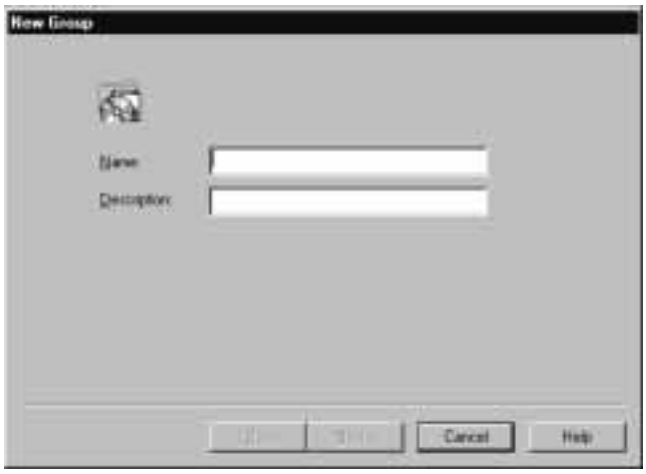

Figure 17. The New Group window

2. Type in the **Name** field the name of the new group.
3. Type in the **Description** field a description of the group (optional)
4. Select **Next**.

   This opens the Preferred Owners window (see Figure 18 on page 73).

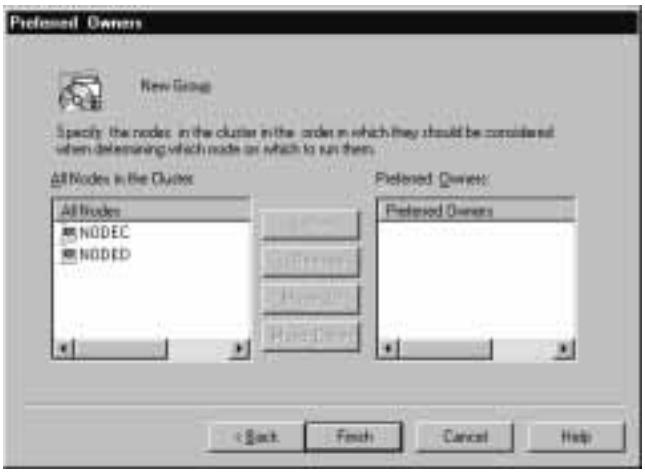

Figure 18. The Preferred Owners window

5. Select preferred owners for this group.
6. Select **Finish**.

You can also use the Cluster Expert Wizard to create resource groups. For more information, see "Cluster Expert Wizard" on page 91.

- Delete groups

  To delete a group, select the group from the tree view and then select **Delete** from the File pull-down menu.

- Bring groups online

  To bring a group online, select the group from the tree view and then select **Bring Online** from the File pull-down menu.

- Take groups offline

  To take a group offline, select the group from the tree view and then select **Take Offline** from the File pull-down menu.

- Change group properties

  Changing group properties enables you to rename the group, change the preferred owners of the group, and set failover and failback policies for the group. For information on changing

group properties, see “Changing Cluster Element Properties” on page 66.

- Moving groups to other nodes

  For information on moving groups, see “Moving Groups” on page 66.

Creating, Deleting, and Managing Resources

Resources are physical parts of the cluster (such as disk drives or IP addresses) that are shared by the applications that run on your cluster and that are associated with specific groups. You can use Cluster Manager to:

- Create resources

  To create a resource in a cluster:

  1. Select **New** and then **Resource** from the File pull-down menu.

     This opens the New Resource window (see Figure 19).

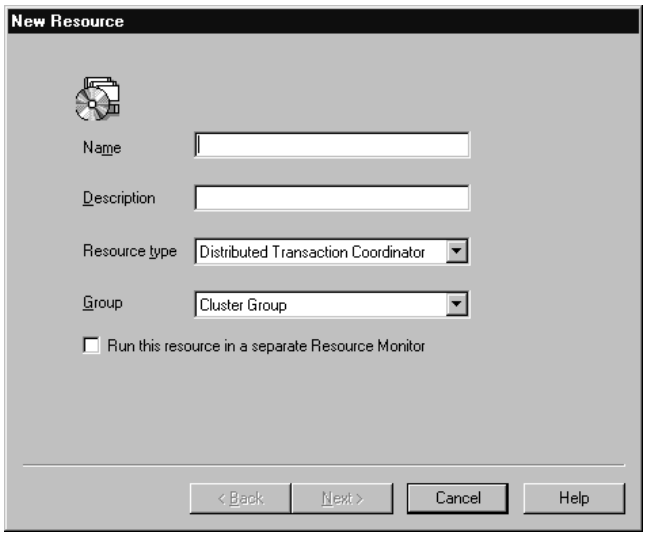

Figure 19. The New Resource window

  2. Type in the **Name** field the name of the resource.

3. Type in the **Description** field a description of the resource (optional).
4. Select from the **Resource type** selection list the type of resource you want to create.
5. Select from the **Group** selection list the name of the group that the resource will be created in.
6. Select the **Run the resource in a separate Resource Monitor** check box if needed.

   Note: Use this option only if you anticipate a conflict with another resource or for debugging purposes.

7. Select **Next**. This opens the Properties window for this resource (see Figure 20).

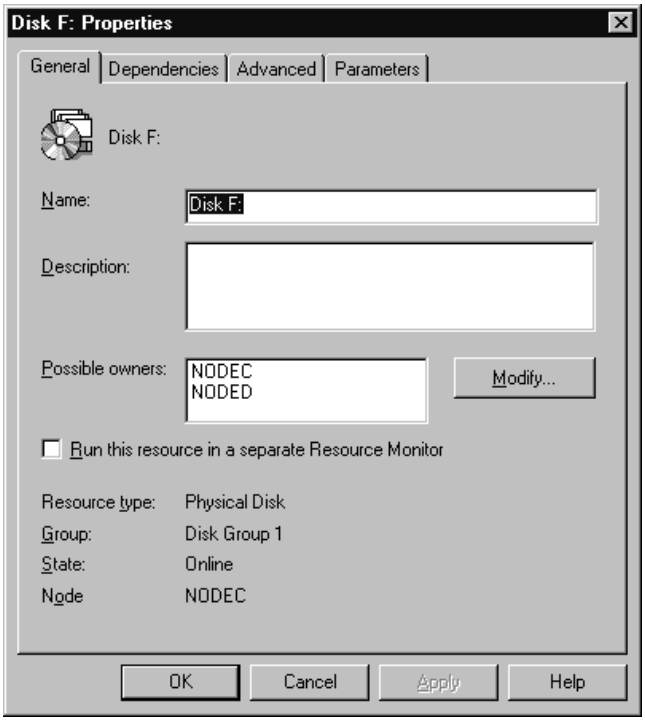

Figure 20. The Resource Properties window

8. Specify possible owners for this resource. To add or remove possible owners from the list of owners displayed in the **Possible owners** field, select **Modify**.
9. Select **OK**. This opens the Dependencies window (see Figure 21).

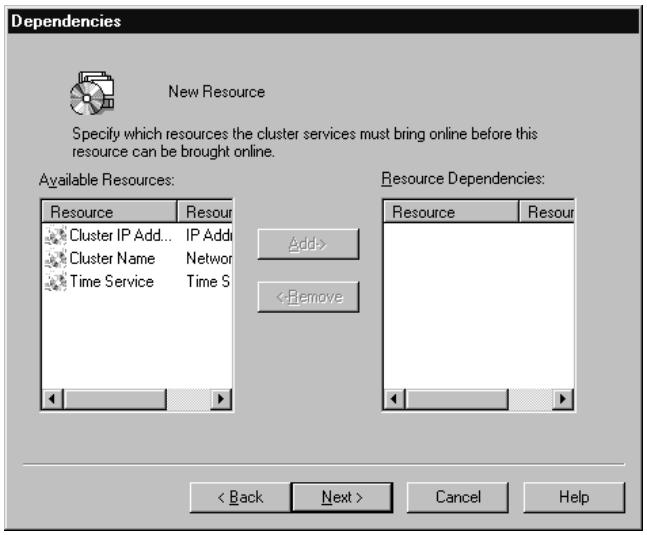

Figure 21. The Dependencies window

10. Select dependencies (if any) for this resource from the **Available Resources** selection list and then select **Add** to add them.
11. Select **Next** and then **Finish** to create the new resource.

- Delete resources

  To delete a resource, select the resource from the tree view and then select **Delete** from the File pull-down menu.

- Bring resources online

  To bring a resource online, select the resource from the tree view and then select **Bring Online** from the File pull-down menu.

- Take resources offline

To take a resource offline, select the resource from the tree view and then select **Bring Online** from the File pull-down menu.

- Initiate resource failures

  You can initiate resource failures to test failover and failback functions. To initiate a resource failure, select the resource from the tree view and then select **Initiate Failure** from the File pull-down menu.

- Change resource properties

  Changing resource properties enables you to rename, add or remove possible owners, add or remove dependencies, set restart policies, specify polling intervals, and set pending timeout values for the resource. For information on changing resource properties, see "Changing Cluster Element Properties" on page 66.

- Move resources to other groups

  For information on moving resources, see "Moving Resources" on page 66.

Managing the Cluster Network and Network Resources

The cluster network and network resources are very similar to other cluster resources. All management of the cluster network resources is performed using the Network Properties window. Using this window, you can rename the network, enable or disable the network for use by the cluster, and specify the manner in which the network will be used by the cluster. For more information on changing network properties, see "Changing Cluster Element Properties" on page 66.

Discovering Clusters

You can use the Cluster Manager *Discovery* function to easily search your TCP/IP network for all clusters that are accessible from your workstation. Once remote clusters are discovered, you can open a connection to any discovered cluster and begin managing it immediately. Discovery can search for clusters on all domains in your network, or you can specify that only specified domains be searched.

To use the Cluster Manager Discovery function:

1. Select **Discover Clusters** from the Utility pull-down menu, or select the **Discover Clusters** button from the Cluster Manager window button bar. The Discover Clusters window opens (see Figure 20 on page 75).

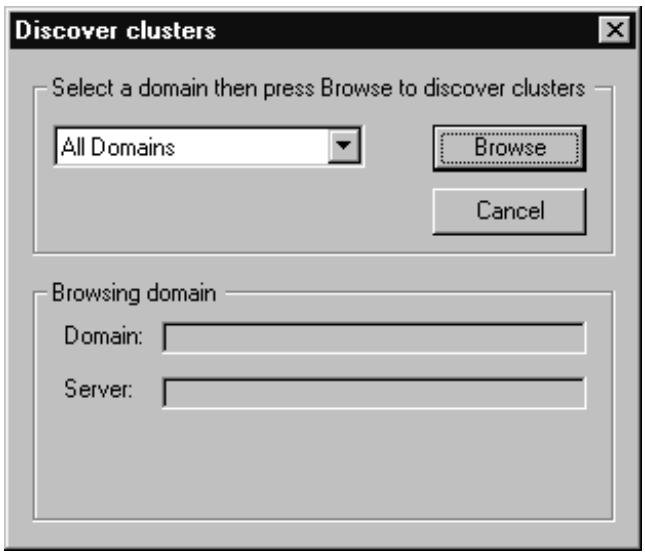

Figure 22. The Discover Clusters window

2. Specify TCP/IP domains to be searched for clusters (optional).

   By default, the Discovery function will search for clusters on *all* TCP/IP domains on your network. To limit Discovery searches to a specific TCP/IP domain, select a domain from the **Domain** selection list.

3. Select **Browse** to initiate the cluster search.

A list of all clusters that are found on your TCP/IP network (or, if you limited the search to a specific domain, a list of all clusters found in the specified TCP/IP domain) appears in the **Discovered Cluster Process** window (see Figure 23 on page 79). From this window you can open a view of the cluster in the Cluster Systems Manager window or define alerts for the discovered clusters (for

more information on alerts see “Alert Service” on page 81). To open a view of a discovered cluster in the Cluster Systems Manager window, double-click on the discovered cluster.

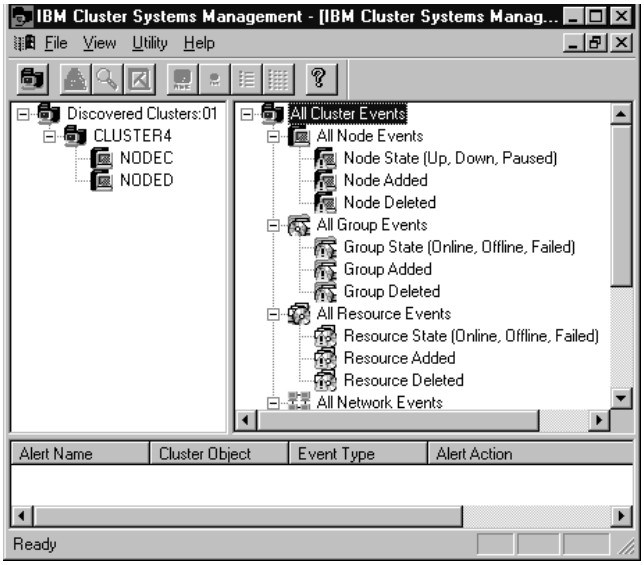

Figure 23. The Discovered Clusters Process window

Note: You can also define alerts from the Cluster Discovery window. The process for defining alerts from this window is identical to the process for defining alerts using the Cluster Manager Alert Service. However, only cluster events that affect *all* of a type of cluster element (for example, all groups in a cluster or all nodes in a cluster) can be defined from the Cluster Discovery Service. For more information, see “Alert Service” on page 81.

Scheduler

You can use the Cluster Manager Scheduler to perform cluster-specific tasks automatically at a user-specified time. With the Cluster Manager Scheduler, you can automatically:

- Bring groups online
- Take groups offline

- Move groups to other nodes

When the Scheduler performs these tasks, results are reported using the Cluster Manager Alert Service. The Cluster Manager Scheduler runs independent of Cluster Manager, so Cluster Manager does not need to be running for scheduled tasks to be performed.

Note: Scheduled tasks will be performed once and once only. To perform scheduled cluster-management tasks repeatedly over a specified time interval (once a week, for example) you must assign multiple scheduled tasks.

To start the Cluster Manager Scheduler, select **Scheduler** from the Utility pull-down menu. This opens the Scheduler window (see Figure 24).

Figure 24. The Cluster Manager Scheduler window

The Scheduler window is divided into three panels. The view on the top left side of the window shows the schedule time tree (hierarchically organized by year, month, day, hour, and five-minute intervals). The view on the top right side of the window shows a list of tasks that can be scheduled. Finally, the view on the bottom shows the currently scheduled tasks.

To update the information that is presented in the Scheduler window, select **Update** from the View pull-down menu or select the **Update** button on the button bar.

Scheduling a Cluster Task

To schedule a Cluster Manager task:

1. Start the Cluster Manager Scheduler.
2. Select a task from the top right panel of the Scheduler window.
3. Drag the selected task to the schedule time tree view and drop it on the time period at which the task will be performed.

After you finish scheduling the task, it will appear in the currently defined tasks panel at the bottom of the Scheduler window. The task will be performed automatically when scheduled time period arrives.

Deleting a Scheduled Cluster Task

To delete a previously scheduled task, use the right mouse button to select the scheduled task from the Scheduler window (this opens the task context menu) and then select **Delete** from the context menu **or** select the scheduled task from the Scheduler window and then select **Delete** from the File pull-down menu.

Alert Service

Cluster Manager can be configured to monitor the clusters on your network for cluster-related changes (such as cluster elements being added, being deleted, or changing state). If any of these events occurs, Cluster Manager can be configured to automatically generate a Netfinity alert and perform one of a variety of alert actions in response to the alert.

Alerts can be configured in one of two ways:

- Using the Alert Service

  The Alert Service is used to configure alerts after you have opened a connection with a cluster (either by connection to the cluster using the **Connect to** button or by double-clicking on a

cluster that you have discovered using the Discovery function). When you use the Alert Service window, you can assign events and alerts for any cluster element, including individual groups and resources.

- Using the Cluster Discovery window

  After clusters are discovered, they are displayed in a tree view in the Cluster Discovery window (see Figure 23 on page 79), a window that closely resembles the Alert Service window. Alerts can be configured using this window. However, only events that affect *all* cluster elements on a cluster (all resources, nodes, or groups for example) can be assigned to generate alerts when you define alerts using the Cluster Discovery window. Though you cannot assign events and alerts to individual cluster elements, you can use the Cluster Discovery window to easily assign alerts to multiple clusters on your network simultaneously.

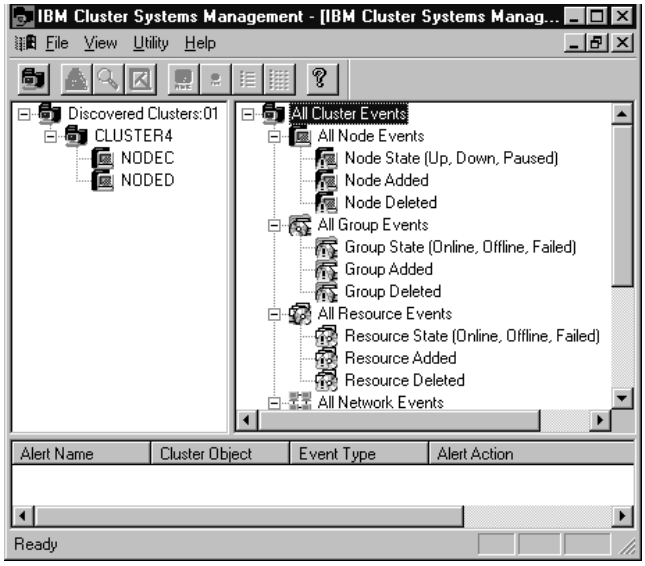

Figure 25. The Alert Service window

Whether you us the Alert Service of the Cluster Discovery function, you use the same process to select a cluster element event, assign it

to a cluster or cluster element, and configure the alert and response that will be generated in response to the event.

1. Open a connection to a cluster.

   To open a connection to a cluster:

   a. Select **Connect to** from the File pull-down menu (or select the **Connect** button from the button bar).

   b. Type in the **Cluster Name** field the name of the cluster you want to connect to and manage.

   c. Select **OK** to open a view of the cluster.

   If you do not know the name of the cluster, use the Cluster Manager Discovery function to find clusters on your network and then double-click on a discovered cluster. For more information on the Discovery function, see "Discovering Clusters" on page 77.

2. Select **Alerts** from the Utilities pull-down menu (or select the **Alerts** button from the button bar).

For information on how to open the Discovery Clusters window, see "Discovering Clusters" on page 77.

Defining Cluster Alerts

To define a cluster event alert and alert action response:

1. Start the Alert Service (or open the Discover Clusters window. For information on how to open the Discovery Clusters window, see "Discovering Clusters" on page 77).

2. Select the event you want to monitor for from the Alert Service events panel (the upper right-hand panel of the window).

   For information about cluster events that can be monitored using the Cluster Manager Alert Service , see "Available Cluster Events" on page 87.

3. Drag the event from the events panel to the cluster tree view panel (the upper left-hand panel of the window) and drop it on the cluster element you want the event to apply to.

For example, if you want to monitor the cluster for any cluster events, drag **All Cluster Events** from the events panel and drop it on the cluster icon in the cluster tree view. This opens the Alert Configuration window for the selected cluster element (see Figure 26). The window will have the name of the selected cluster element in the title bar.

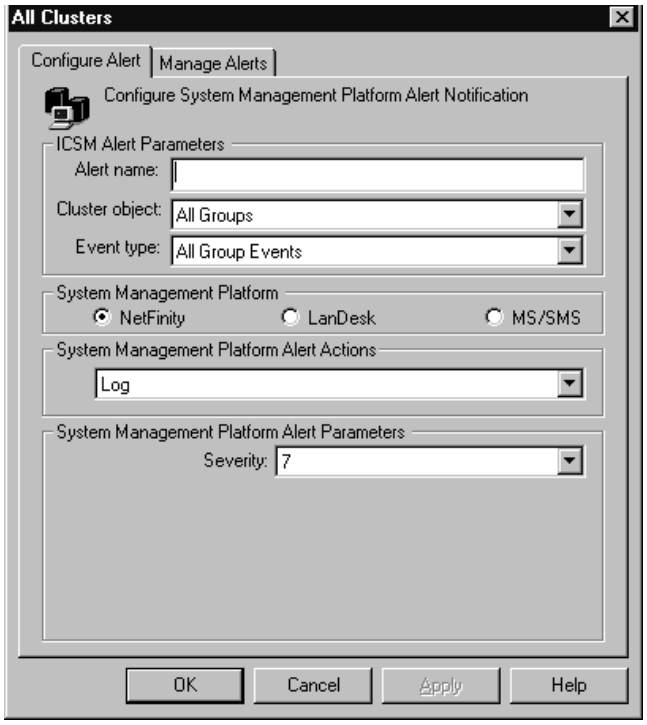

Figure 26. The Alert Configuration window

4. Type in the **Alert Name** field a name for the alert.
5. Select from the **Cluster object** selection list a cluster element to monitor (optional).

   The name of the cluster element you selected will be displayed in this window.
6. Select from the **Event type** selection list the cluster event you want to monitor (optional).

The name of the cluster event you selected from the cluster events tree will be displayed in this window.

7. Select **Netfinity** from the **System Management Platform** button group.

   This determines the format of the alert that will be generated and the actions that are available to be taken in response to the alert. If you also have Intel LANDesk or Microsoft SMS installed on your system, buttons will be available for these products as well. This publication covers Netfinity functions only. For information about other systems-management platform alerts and actions that are available, see the Cluster Manager online help or refer to the *IBM Cluster Systems Management User's Guide.*

8. Select from the **System Management Platform Alert Action** selection list the alert action that will be taken in response to the alert and provide any additional parameters needed.

   When you select an alert action, additional parameter fields might appear beneath the **System Management Platform Alert Action** selection list. Provide the additional needed information to configure alert actions that require additional parameters.

   For information about Netfinity alert actions that can be used with Cluster Manager Alert Service, see "Available Cluster Alert Actions" on page 89.

9. Specify an Alert Severity

   The Severity is a number from 0 through 7 that indicates how serious a generated alert is. A severity of 0 represents a very serious alert, while a severity of 7 is relatively minor.

10. Select **OK** to save this cluster alert action.

When a cluster alert is defined and saved, it appears in the Alert Service alerts information panel (the bottom half of the Alert Service window).

Select **Cancel** at any time to close this window without saving any cluster alert information.

Deleting Cluster Alerts

To delete a previously defined cluster alert action:

1. Start the Alert Service (or open the Cluster Discovery window).
2. Double-click on any event in the Alert Service events panel (the upper right-hand panel of the window).

   This opens the Alert Configuration window for the selected element.
3. Select the **Manage Alerts** tab in the Alert Configuration window. This changes the view of the Alert Configuration window to a view of all events and alerts that are currently defined for the cluster (see Figure 27).

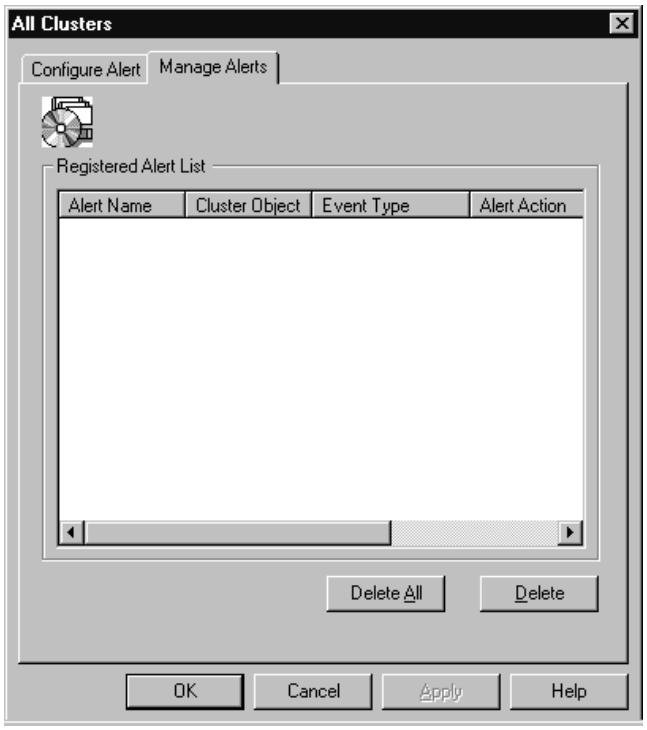

Figure 27. The Manage Alerts view

4. Select one (or more) cluster alerts that you want to delete.

5. Select **Delete**.

To delete **all** previously defined cluster alerts, select, **Delete All**.

Available Cluster Events

You can use Cluster Manager to monitor any of the following cluster events. If one of these events occurs and you have configured a cluster alert using the Alert Service, a Netfinity alert automatically will be generated and an alert action taken in response to the alert.

- All Cluster Events

  The alert will be generated if *any* Cluster event occurs.

- All Node Events

  The alert will be generated if any node event (Node State, Node Added, Node Deleted) occurs.

- Node State (Up, Down, Paused)

  The alert will be generated if the node changes state.

- Node Added

  The alert will be generated if a node is added to the cluster.

- Node Deleted

  The alert will be generated if the node is deleted from the cluster.

- All Group Events

  The alert will be generated if any group event (Group State, Group Added, Group Deleted) occurs.

- Group State (Online, Offline, Failed)

  The alert will be generated if the group changes state.

- Group Added

  The alert will be generated if a group is added to the node.

- Group Deleted

The alert will be generated if the group is deleted from the node.

- All Resource Events

  The alert will be generated if any resource event (Resource State, Resource Added, Resource Deleted) occurs.

- Resource State (Online, Offline, Failed)

  The alert will be generated if the resource changes state.

- Resource Added

  The alert will be generated if a resource is added to the group.

- Resource Deleted

  The alert will be generated if the resource is deleted from the group.

- All Network Events

  The alert will be generated if any network event (Network State, Network Added, Network Deleted) occurs.

- Network State (Up, Partitioned, Down)

  The alert will be generated if the network changes state.

- Network Added

  The alert will be generated if a network is added to the cluster.

- Network Deleted

  The alert will be generated if a network is deleted from the cluster.

- All Net Interface Events

  The alert will be generated if any network interface event (Network Interface State, Network Interface Added, Network Interface Deleted) occurs.

- Network Interface State (Up, Unreachable, Failed)

  The alert will be generated if the network interface changes state.

- Network Interface Added

The alert will be generated if a network interface is added to the cluster.

- Network Interface Deleted

  The alert will be generated if the network interface is deleted from the cluster.

Available Cluster Alert Actions

The following Netfinity alert actions are available for use with the Cluster Manager Alert Service:

- Log

  Select **Log** to send the alert to the Netfinity alert log.

- NT Event Log

  Select **NT Event Log** to use Netfinity to enter the alert into the NT Event Log.

- Digital Pager

  Select **Digital Pager** to use Netfinity to use a modem attached to your system to dial out and deliver the information using a digital pager service.

  Additional Parameters

  – <P1> Modem COM Port

    The COM port that the modem is configured to use. The COM port parameter *must* be typed in the parameter field as COM *x*, where *x* is the number of the COM port.

  – <P2> Pager number

    The telephone number that must be dialed by the modem to forward the information to the digital pager.

  – <P3> Digital pager display

    The numeric data that will be displayed on the pager.

  Note: Depending on your paging service, you might need to increase the amount of time that this alert action waits after dialing the telephone number in parameter field **<P2>** before it transmits the numeric data in parameter

field **<P3>**. To increase the amount of time that will pass before the numeric data is transmitted, add one or more commas (,) to the end of the telephone number in field **<P2>**. Each comma will cause the modem to wait two seconds before transmitting the numeric data.

- Alphanumeric Pager

  Select **Alphanumeric Pager** to use a modem attached to your system to send all alert information and additional text (if needed) to an alphanumeric pager using telocator alphanumeric protocol (TAP).

  Additional Parameters

  – <P1> Modem COM Port

    The COM port that the modem is configured to use. The COM port parameter *must* be typed in the parameter field as COM *x*, where *x* is the number of the COM port.

  – <P2> TAP Access Number

    The telephone number that must be dialed by the modem to forward the information to the alphanumeric pager.

  – <P3> Pager ID

    The identification number of the pager to which the data will be sent.

  – <P4> Additional text to send

    Any additional text that you want to send along with the alert data. This parameter is optional.

  Notes:

  1. This action will work only with pager services that use the telocator alphanumeric protocol (TAP).
  2. You *must* provide your pager's Pager ID.

- Execute a Command

  Select **Execute a Command** to execute a command when the alert is received.

  Additional Parameters

– <P1> Command

  The command that will be executed on the system.

- Message Popup

  Select **Message Popup** to display the alert in a popup window.

Cluster Expert Wizard

You can use the Cluster Manager Cluster Expert Wizard to quickly and easily create several commonly used resource groups, including:

- File-share resource group
- Internet Information Server (IIS) resource group
- Print spooler resource group

With Cluster Expert Wizard you can create groups by defining new resource groups into already existing resource groups. This is especially useful when you have a limited number of physical disks that need to serve multiple purposes for your environment. For example, a single physical disk can be used to store data for multiple file share groups and multiple IIS groups.

During startup of the system, Cluster Manager prompts you for a range of virtual IP addresses. A sequential range of IP addresses is created for use in the system.

Note: When you add the range of numbers, do not include any numbers that are currently active. For example, if the address of 9.9.9.10 is assigned, do not use the range of 9.9.9.1–9.9.9.100, start with 9.9.9.11–9.9.9.109.

If an IP address is deleted, Cluster Expert Wizard automatically adds that number to the list of IP addresses that are available for use by the cluster.

To start the Cluster Expert Wizard, select **Cluster Expert Wizard** and then the type of resource group you want to create from the Utilities pull-down menu.

Creating or Changing File Share Resource Groups

A File Share Resource Groups shares the directory of the server, on one of the shared disks in your configuration. The configuration of a file-share group is identical to the configuration of a file-share group in Windows NT Explorer. For example, you can store files in a shared directory on the server and give access only to a group of clients.

You can create a file share resource group or change an existing file share resource group.

Note: Before creating a file share resource, ensure that a disk drive is available. If a hard disk drive is not available, the default is to change a file share resource.

To create a new file-share resource group:

1. Select **Cluster Expert Wizard** and then **File Share** from the Utilities pull-down menu.

   The Expert Wizard window appears with information pertaining to file-share resources available for use (see Figure 28).

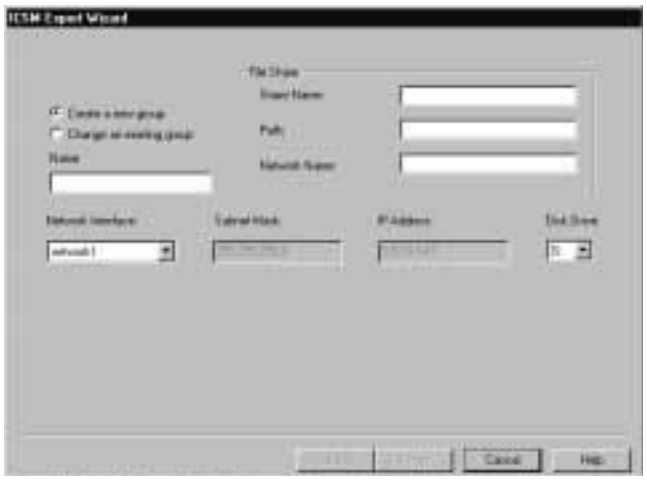

Figure 28. The Cluster Expert Wizard File Share Resource window

2. Select **Create a new group**

3. Specify the Share Name, Path, and Network Name for the file share resource group.
4. Specify the Network Interface for the file-share resource group.
5. Choose the Disk Drive for the file share resource group.
6. Select **Finish**.

To change a file share resource group:

1. Select **Cluster Expert Wizard** and then **File Share** from the **Utilities** pull-down menu.

   The Expert Wizard window appears with information pertaining to file share resources available for use (see Figure 28 on page 92).
2. Select **Change an existing group**
3. Select from the **File Share Resource** selection list the name of the file-share resource you want to change.
4. Change file-share properties as desired.
5. Select **Finish**.

Creating Internet Information Server Resource Groups

An Internet Information Server (IIS) resource group provides high availability to the World Wide Web, FTP, and Gopher components of the Microsoft Internet Information Server. If a node fails, another node will supply the client with the data.

To create an Internet Information Server resource group:

1. Select **Cluster Expert Wizard** and then **IIS** from the **Utilities** pull-down menu.

   The Expert Wizard window appears with information pertaining to IIS resources available for use (see Figure 29 on page 94).

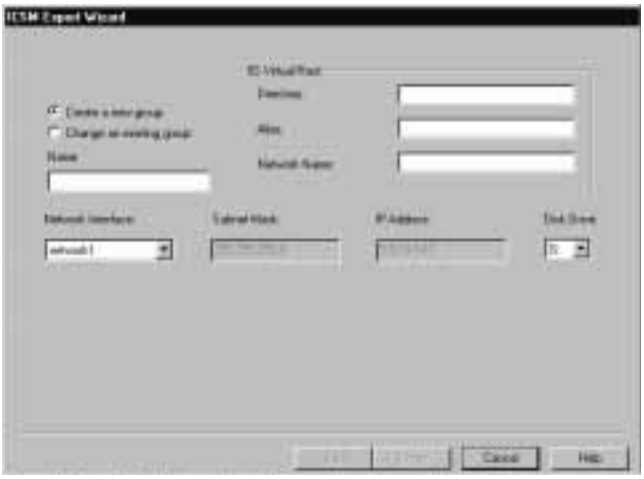

Figure 29. The Cluster Expert Wizard IIS resource group window

2. Select **Create a new group**.
3. Specify the Directory, Alias, and Network Name for the IIS resource group.
4. Specify the Network Interface for the IIS resource group.
5. Choose the Disk Drive for the IIS resource group.
6. Select **Finish**.

Creating or Changing Print Spooler Resource Groups

When a server functions as a print spooler, the server must specify where the print spooler stores its data. A print spooler resource group provides a spool directory on the shared storage disk where print jobs will be spooled.

You can create a print spooler resource group or change an existing print spooler resource group.

To create a print spooler resource group:

1. Select **Cluster Expert Wizard** and then **Print Spooler** from the **Utilities** pull-down menu.

The Expert Wizard window appears with information pertaining to print spooler resources available for use (see Figure 30 on page 95).

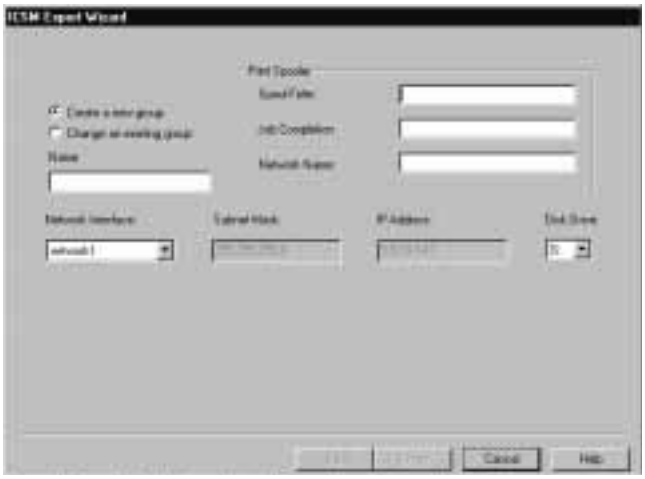

Figure 30. The Cluster Expert Wizard print spooler resource group window

2. Select **Create a new group**.
3. Specify the Spool Folder, Job Completion, and Network Name for the print spooler.
4. Specify the Network Interface for the print spooler.
5. Choose the Disk Drive for the print spooler.
6. Select **Finish**.

To change a print spooler resource group:

1. Select **Cluster Expert Wizard** and then **Print Spooler** from the **Utilities** pull-down menu.

   The Expert Wizard window appears with information pertaining to rprint spooler resources available for use.

2. Select **Change an existing group**
3. Select from the **Print Spooler Resouce** selection list the name of the print spooler resource you want to change.

4. Change print spooler properties as desired.
5. Select **Finish**.

Chapter 6. Critical File Monitor

Critical File Monitor can warn you whenever critical system files on the systems in your network are deleted or altered. The Critical File Monitor service makes it simple for you to generate Netfinity alerts when an important system file (such as the CONFIG.SYS file) changes date, time, size, is deleted (when it was present previously), or is created (when it was not present previously). Critical File Monitor can also be used to monitor any other files that reside on a Netfinity system.

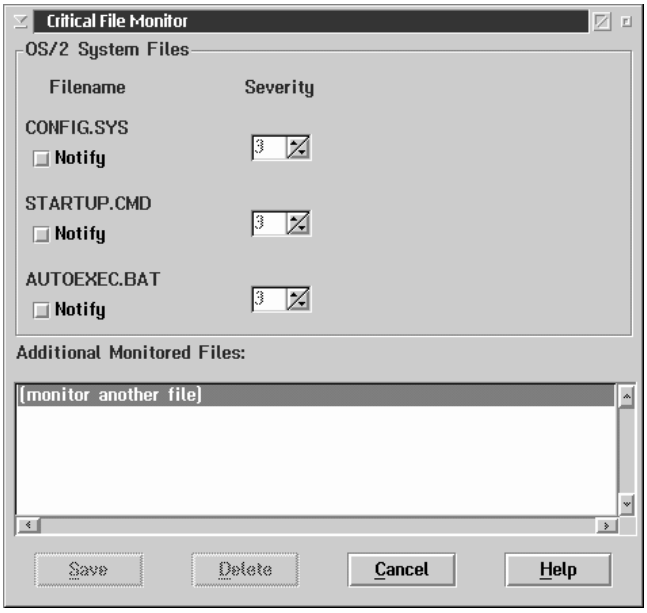

Figure 31. Critical File Monitor

Monitoring System Files

The system files that can be monitored by the Critical File Monitor are operating-system-specific. The name of the operating system that is in use by the system that you are accessing appears in the title area of the System Files field group. The names of the system files that can be monitored appear beside the check boxes.

Notes:

1. You can use Critical File Monitor to monitor *any* file on the system. The system files that appear at the top of the Critical File Monitor window are important files that you would be most likely to want to monitor. To monitor other files, see "Monitoring Other Files" on page 99.
2. Files located on network drives cannot be monitored.

OS/2 System Files

The OS/2 system files that appear in the System File field group are:

- CONFIG.SYS
- STARTUP.CMD
- AUTOEXEC.BAT

Windows 3.1, Windows for Workgroups, and Windows 95 System Files

The Windows system files that appear in the System File field group are:

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

Windows NT System Files

The Windows NT system files that appear in the System File field group are:

- WIN.INI
- SYSTEM.INI

NetWare System Files

The NetWare system files that appear in the System File field group are:

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

To monitor one or more system files:

1. Select the system files that you want to monitor.

   Select the **Notify** check boxes below the names of the system files that you want to monitor. A check mark appears in the box.

2. Select a Severity.

   Each system file in the System File field group has a Severity field beside its name. Use the spin buttons to select a Severity value for each of the system files that you want to monitor. This severity value will be assigned to the Netfinity alert that will be generated if the system file is created, deleted, or changed. You can choose a severity value from 0 (most severe) to 7 (least severe).

3. Select **Local Notify** (optional).

   Select the **Local Notify** if you want to direct the alert to the Alert Manager on the system which you are monitoring.

4. Select **Save** to save the Critical File Monitor settings.

To close Critical File Monitor without saving any changes, select **Cancel**.

Monitoring Other Files

Critical File Monitor can monitor any file on the Netfinity system that you are accessing. The **Additional Monitored Files** field contains a list of all other files that are currently being monitored.

To select a file to monitor:

1. Select **(monitor another file)** from the **Additional Monitored Files** field (see Figure 31 on page 97).

   This will open the Monitor window (see Figure 32).

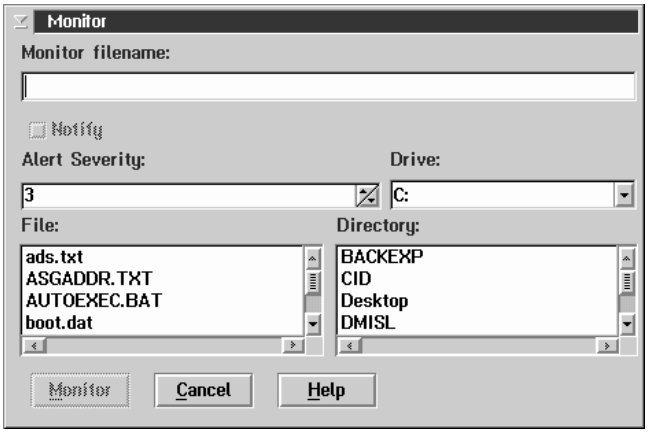

Figure 32. Critical File Monitor — Monitor window

2. Select from the **Drive** list the drive letter that contains the file that you want to monitor.
3. Select from the **Directory** field the directory that contains the file that you want to monitor.
4. Select from the **File** list the name of the file that you want to monitor.
5. Use the spin buttons beside the **Severity** field to set the Severity of the alert that will be generated if the selected file is altered or deleted.
6. Select **Local Notify** (optional).

   Select the **Local Notify** if you want to direct the alert to the Alert Manager on the system which you are monitoring.
7. Select **Monitor** to initiate the monitoring process on the selected file.

To close the Critical File Monitor service without saving any changes, select **Cancel**.

Note: Critical File Monitor can be set to alert you if a specific file that does not exist on the system is created. For more information, see "Monitoring for File Creation."

Monitoring for File Creation

Critical File Monitor can also generate alerts when specified files are created. To configure the Critical File Monitor to generate an alert in this case:

1. Select from the **Drive** field the letter of the disk drive that you want to monitor for file creation.
2. Type in the **Monitor Filename** field the fully qualified path and name of the file that you want to monitor.

   For example, if you want the Critical File Monitor to generate an alert if a file named ERROR.LOG appears in the directory named PROGRAM, you would type in the **Monitor Filename** field

   ```
   PROGRAM\ERROR.LOG
   ```

3. Use the spin buttons beside the **Severity** field to set the Severity of the alert that will be generated if the file is created.
4. Select **Local Notify** (optional).

   Select the **Local Notify** if you want to direct the alert to the Alert Manager on the system which you are monitoring.
5. Select **Monitor** to initiate the monitoring process on the specified file.

Chapter 7. DMI Browser

You can use the Netfinity Desktop Management Interface (DMI) Browser Service to examine information about the DMI-compliant hardware and software products (called *DMI components*) installed in or attached to the system.

You can use the DMI Browser to:

- View information about DMI components
- Receive notification of problems or errors with products from the DMI Service Layer
- View the log of problems or errors concerning DMI components

Notes:

1. This service is available only on systems that have the DMI Service Layer installed and operational. DMI Service Layers are available for most of the operating systems that are supported by Netfinity. If a DMI Service Layer is not installed and operational on your system when you install Netfinity, neither the DMI Browser nor the Netfinity-specific DMI components will be installed on your system. If you install a DMI Service Layer after you install Netfinity, you must reinstall Netfinity in order to install and use Netfinity's DMI Component Instrumentation.
2. The Netfinity DMI Browser service is a special version of the DMI Browser that comes with the DMI Service Layer. Some functions that are available with the DMI Browser are not available in Netfinity's DMI Browser service.

What is DMI?

The Desktop Management Interface (DMI) is an industry standard that simplifies management of hardware and software products attached to, or installed in, a computer system. The computer system can be a standalone desktop system, a node on a network, or a network server. DMI is designed to work across desktop operating systems, environments, hardware platforms, and architectures.

DMI provides a way to provide or obtain, in a standardized format, information about hardware and software products. Once this data is obtained, desktop and network software applications can use that data to manage those computer products. As DMI technology evolves, installation and management of products in desktop computers will become easier, and desktop computers will become easier to manage in a network.

How Does DMI Work?

The complete DMI structure consists of three separate elements:

- DMI components
- DMI Service Layer
- DMI-compliant management applications

DMI Components

Each DMI component contains information about the product with which it is associated. This information is organized into product-specific groups. This information is contained in a Management Information File (*MIF*). The MIF describes the manageable attributes of the DMI component or product.

Each group contains a variety of group-specific attributes. The attributes that are found within a group are entirely dependent on the group itself. For example, the Component ID group for a software product might include the following attributes:

- Manufacturer
- Product
- Version
- Serial Number
- Installation
- Verify

However, the attributes found in the Processor group included in a PC system's component might contain these attributes:

- Type
- Processor Family
- Version Information

- Maximum Speed
- Current Speed
- Processor Upgrade

Each of a group's attributes is fully defined by a series of data items. The items available for a group vary according to the type of product, but most attributes include the following data items:

ID The attribute's **ID** is a sequential number unique to the attribute's group.

Type The data **type** can be one of eight defined by DMI. These data types are:
- Integer
- 64-Bit Integer
- Counter
- 64-Bit Counter
- Gauge
- Display String
- Octet String
- Date

Access The ways in which this attribute's data can be accessed. Access values can be:
- Read-Only
- Read-Write
- Write-Only

Note: Attributes that have Read-Write or Write-Only access values can have certain other attributes changed. For more information, see "Changing Attribute Information" on page 109.

Name The **name** of the attribute is derived from DMI standards or is provided by the manufacturer.

Value A **value** is a specific occurrence of an attribute. For example, an attribute value of 2.1 could be provided for the version number of an application. In a few cases, a value is read-only and will never change. The value can be specified directly in the MIF file. However, most values will change over time.

	Updating usually occurs automatically, managed by programs supplied by the manufacturer of the component. A value can also be an enumeration value (ENUM), indexing into a table of possible values defined in the MIF file.
Description	The **description** of the component is technical information supplied by the manufacturer.

Netfinity DMI Component Instrumentation

The Netfinity DMI Component Instrumentation provides DMI-based management applications with information from Netfinity's Remote System Manager, System Monitors, and System Information Tool. The MIF files required by DMI-based management applications are installed as part of Netfinity's DMI Instrumentation when Netfinity is installed.

Notes:

1. If a DMI Service Layer is not installed and operational on your system when you install Netfinity, neither the DMI Browser nor the Netfinity-specific DMI components will be installed on your system.
2. DMI-based Netfinity data is available to other DMI-based application only when the Netfinity Support Program is running.

DMI Service Layer

The DMI Service Layer is a program that gathers and organizes the DMI component information into a standardized format. Once this data has been organized and is available, a DMI-compliant component agent (Netfinity's DMI Browser service, for example) can access the DMI service layer and request information about any of the DMI components.

Note: Your system *must* have the DMI Service Layer installed and operational for Netfinity's DMI Browser to function.

The DMI Service Layer gathers configuration information from the installed MIF files, builds a database, and, upon request, passes the information to management applications. Management applications are programs that are capable of receiving data from the DMI Service Layer and providing this data for desktop or network management purposes.

In addition to gathering and configuring the MIF data, the DMI Service Layer also collects information about problems or errors that the various DMI components have encountered. You can use the Netfinity DMI Browser to receive notification of problems or errors concerning your DMI components and to view a log of problems or errors concerning your DMI components.

The Netfinity DMI Browser works with the following DMI Service Layers:

Operating System	Supported DMI Service Layer
OS/2 Warp 3.0 or later	IBM SystemView Agent version 1.4.2 or later
Windows NT 3.51 with Service Pak 5 or later	IBM SystemView Agent version 1.3.2 for WIN32, Intel DMI Service Provider 2.0
Windows 95	IBM SystemView Agent version 1.3.2 for WIN32, Intel DMI Service Provider 2.0
Windows 3.1	Intel® DMI SDK version 2.0 or later

Management Applications

A management application is any DMI-compliant systems-management application that is capable of interfacing with the DMI Service Layer in order to gather and make use of the DMI component information.

Using the DMI Browser

The Netfinity DMI Browser service enables you to:

- View information about DMI components, groups, and attributes of installed DMI-compliant products
- Receive notification of problems or errors with your products from the DMI Service Layer
- View the log of problems or errors concerning your DMI components

The DMI Browser functions can be accessed by selecting menu choices from the menu bar, or by selecting the function's corresponding objects from the fast-path icon bar.

The menu bar includes the following functions:

- Options: View the event log or exit the DMI Browser service.
- Information: Display version information for the Service Layer and copyright notices for the DMI Browser.

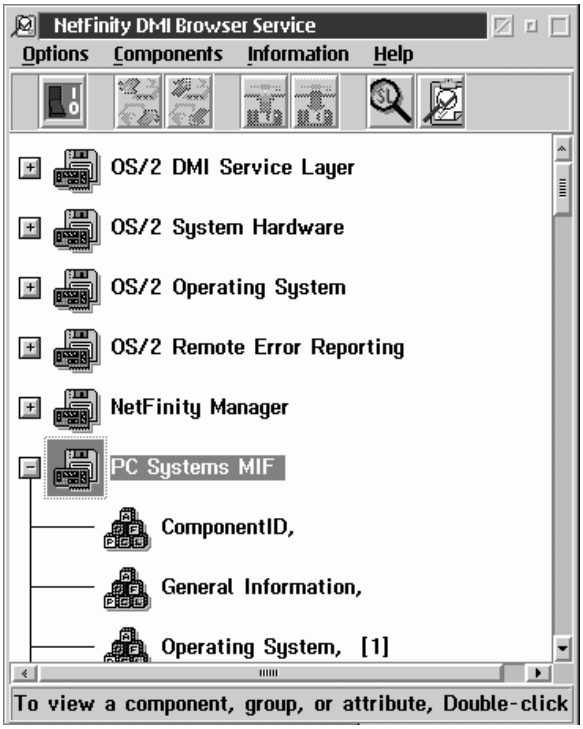

Figure 33. The DMI Browser window

For quickest operation, use the mouse to select the menu bar icon that you want. The alternative is to select a menu choice and then select a choice from the menu that drops down. If you are unsure about the meaning of an icon, just move the mouse pointer over it. A brief explanation of the icon will appear at the bottom of the window.

Viewing DMI Component Information

Using mouse button 1, double-click on the DMI component that you want to open. This will open the Component Information window.

When you are finished, select **Close** to close the Component Information window.

Viewing Group Information

To view information about one of a DMI component's individual groups:

1. Using mouse button 1, click on the plus sign (+) beside the DMI component that contains the group data that you want to view.
2. Using mouse button 1, double-click on the name of the group that you want to view. This will open a window that contains a list of the group's attributes.

Viewing Attribute Information

To view information about one attribute of a single group:

1. Using mouse button 1, click on the plus sign (+) beside the DMI component that contains the group data that you want to view.
2. Using mouse button 1, double-click on the name of the group that you want to view. This will open a window that contains a list of the group's attributes.
3. Using mouse button 1, double-click on the name of the attribute that you want to view. This will open the Attribute Information window.

Changing Attribute Information

You can configure attributes that have Access values of *Read-Write* or *Write Only*. To change attribute information:

1. Using mouse button 1, double-click on the specific attribute that you want to change. This will open the Attribute information window.
2. Enter the new Attribute information. Note that not all Attribute information items can be changed.
3. Select **Apply** to change the attribute information.

If you decide not to make a change, select **Reset** to restore the attribute information to its last-saved value.

Select **Cancel** to close this window without saving any changes.

Receiving Notification of Problems or Errors

Upon request, the Service Layer notifies management applications of the occurrence of a problem or error. These problem and error messages are called *events*. The events are then stored in the Event Log, where they can be examined later to help rectify the problem or error.

The DMI Browser service automatically receives notification of DMI component events from the DMI Service Layer. If an event message is received by the DMI Browser service, a telephone object appears in the DMI Browser icon bar. Select the telephone icon (or select **View event log...** from the **Options** pull-down menu) to open the DMI Browser Event Log.

Chapter 8. ECC Memory Setup

You can use the Netfinity ECC Memory Setup to monitor and manage ECC memory. Options are:

- Single-Bit Error Scrubbing
- Single-Bit Error Counting
- Single-Bit Error Threshold Nonmaskable Interrupt (NMI)

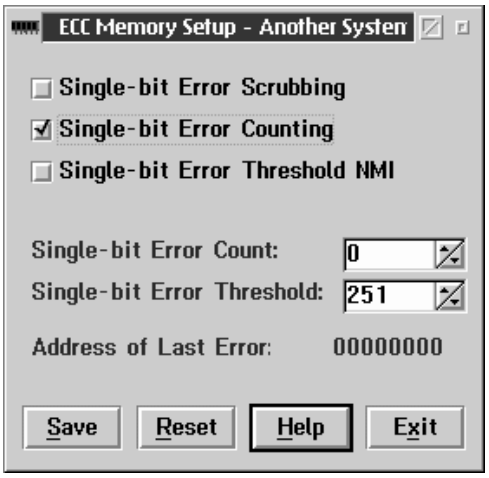

Figure 34. ECC Memory Setup

To configure the ECC Memory Setup:

1. Select the actions that you want ECC Memory Setup to perform.
   - Activate the Single-Bit Error Scrubbing option to automatically correct any single-bit errors that might occur. Selecting this option might cause slight performance delays on some systems, but ensures greater data integrity. Check your system documentation for more information.
   - Activate the Single-Bit Error Counting option to keep a running count of all ECC memory errors that occur.
   - Activate the Single-Bit Error Threshold NMI option to cause a nonmaskable interrupt (NMI) if the number of single-bit errors exceeds the user-specified threshold.

     Note: If an NMI occurs, it might halt your system.

2. Change the Single-Bit Error Count, if desired.

   The **Single-Bit Error Count** field displays the number of single-bit errors that have been detected by the ECC Memory Setup during the current session.

   Note: The single-bit error count is for the current session *only*. The count is reset to 0 when the computer is restarted. To carry a count over from a previous session, you must enter the error count manually from the configuration screen.

3. Set a Single-Bit Error Threshold value if you have chosen the Single-Bit Error Threshold NMI option.

   The **Single-Bit Error Threshold** field displays the number of ECC single-bit errors that will be allowed before a nonmaskable interrupt (NMI) will be triggered.

   Note: An NMI will occur only if the Single-Bit Threshold NMI option is activated.

4. Select **Save** when you are satisfied with the selections you have made.

5. Select **Exit** when you have finished configuring ECC Memory Setup.

Chapter 9. Event Scheduler

You can use the Event Scheduler service to easily automate many hardware systems-management tasks. Use the Event Scheduler to create scheduled events, execute these events automatically on multiple remote systems or entire system groups, and maintain detailed logs of the results of these scheduled events. You can also edit or delete previously created scheduled events as necessary.

With Event Scheduler, you can create scheduled events that will automatically perform one of the following tasks on one or more individual systems, or even on entire system groups:

- Use the System Information Tool to gather data from all specified systems, and then:
  - Save the information as a History File.
  - Print the information to a printer or save it to a file.
  - Export the data to a Netfinity database.
- Distribute files and directories among local and remote systems, or delete files locally and remotely.
- Execute commands on remote systems.
- Access and manage the System Partitions of remote systems.
- Use the Software Inventory service to gather data from all specified systems and then:
  - Save the gathered information to a file.
  - Export the gathered information to a Netfinity database.
- Export System Monitor data to a Netfinity database.
- Configure Netfinity services on remote systems using SCF files (created using Service Configuration Manager).
- Scrub RAID drives on remote RAID systems
- Start up, shut down, or power down remote systems
- Use Netfinity command-line interfaces on multiple remote systems
- Automatically generate Capacity Management reports

A scheduled event can be configured to execute repeatedly at a specified time interval (hourly, daily, weekly, monthly, or yearly)

for fully automated systems-management functions (such as simplified hardware inventorying), or can be executed once only for special situations (such as data collection and distribution or System Partition updating). Finally, Event Scheduler maintains a detailed log of all scheduled event results, so you can verify that your automated tasks were executed correctly.

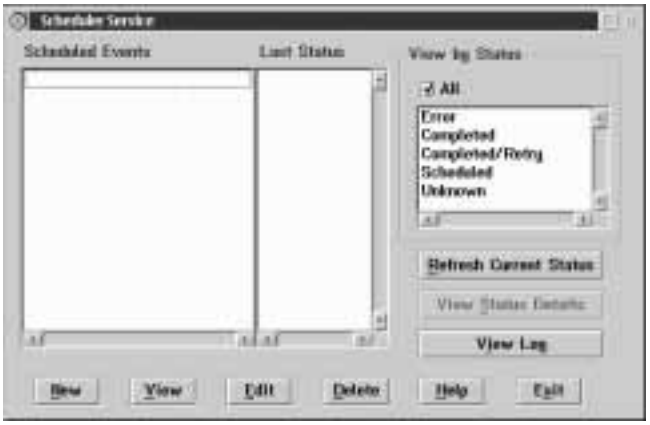

Figure 35. The Event Scheduler Service window

Use Event Scheduler to perform any of the following actions:

- Create a new scheduled event.
- Delete a previously created scheduled event.
- View a previously created scheduled event.
- Edit a previously created scheduled event.
- Refresh the Scheduled Event list.
- View the Scheduler Log.
- Check the status of currently configured scheduled events.

Select **Help** to access the Event Scheduler online helps.

Select **Exit** from the Event Scheduler Service window to close the Event Scheduler Service window and return to the Netfinity Service Manager.

Creating a New Scheduled Event

To create a new scheduled event:

1. Select **New** to open the Schedule New Event window (see Figure 36).

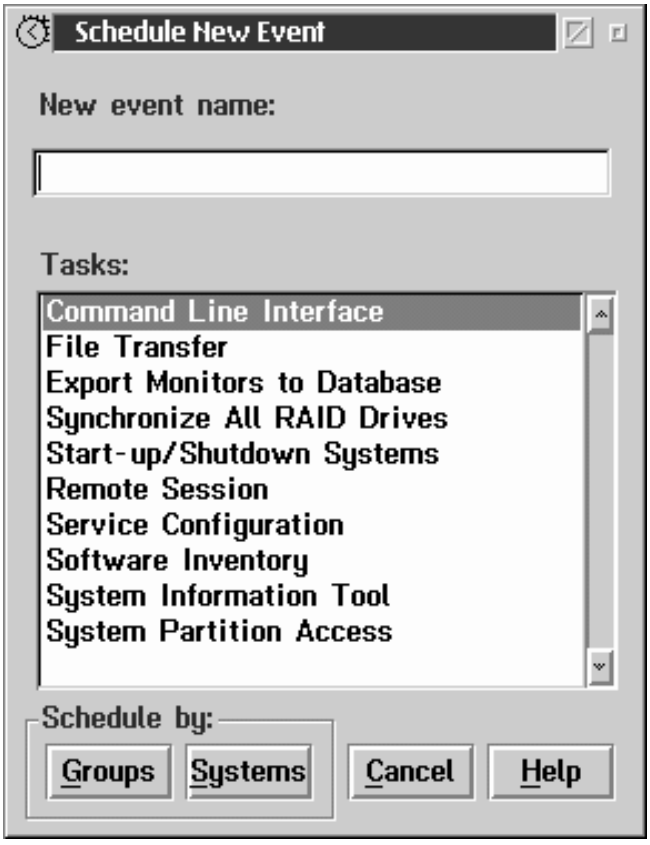

Figure 36. The Schedule New Event window

2. Type in the **New event name** field a name for the scheduled event.

3. Select the action to be performed by the scheduled event from the **Tasks** selection list. The available tasks are:

   - File Transfer

     Select **File Transfer** to automatically transfer files or directories between the local and remote systems, or to automatically delete files locally or remotely.

   - Remote Session

     Select **Remote Session** to automatically execute a command on all selected systems.

   - System Information Tool

     Select **System Information Tool** to gather hardware and configuration data from all selected remote systems. This data can be saved as a History File, printed to a printer, saved to a file, exported to a Netfinity database, or saved as a database file.

   - System Partition Access

     Select **System Partition Access** to automatically manage the System Partitions of all selected systems.

   - Software Inventory

     Select **Software Inventory** to gather data about the software that is installed on the selected remote systems. This data can be used to generate a simple summary of software installed on your networked systems or to generate a detailed report of what software is installed on each selected remote system. All data gathered by the Software Inventory service can also be automatically exported to a Netfinity database.

   - Monitor Database

     Select **Monitor Database** to export to a Netfinity database the data gathered by the System Monitors.

   - Scrub All RAID Drives

     Select **Scrub All RAID Drives** to automatically scrub the RAID drive array on any RAID systems.

- Start Up/Shut Down Systems

  Select **Start Up/Shut Down Systems** to attempt to restart, shut down, power down, or power up remote systems.

  Note: Some of these functions will work only on systems that have hardware or operating system support for these features.

- Service Configuration

  Select **Service Configuration** to use SCF files (created with Service Configuration Manager) to update or replace the configuration of specified Netfinity services on remote systems. For more information about SCF files and Service Configuration Manager, see Chapter 21, "Service Configuration Manager" on page 261.

- Command Line Interface

  Select **Command Line Interface** to use one of the Netfinity command line interfaces toperform systems management tasks on one or more systems. For more information on Netfinity command-line interfaces, see *Netfinity Manager Command Reference*.

4. Select **Groups** or **Systems**:

   - Select **Groups** to perform the selected task on entire System Groups.
   - Select **System** to perform the selected task on individual systems.

   Selecting either of these buttons opens the Schedule Groups or Systems window (see Figure 37 on page 118).

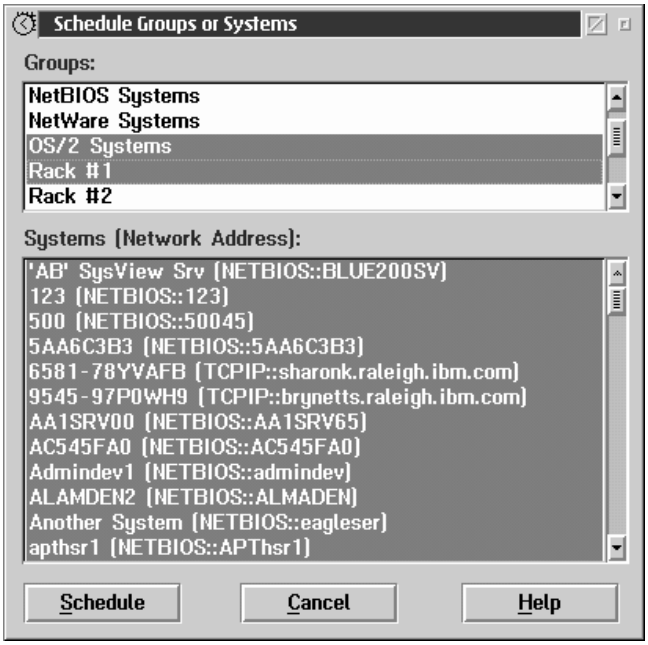

Figure 37. The Schedule Groups or Systems window

5. Select from the appropriate fields the system groups or systems on which the scheduled event will be performed. Then, select **Schedule** to save this information and open the task-specific window.

   The task-specific window that opens when you select **Schedule** depends upon the task that you selected in step 3 on page 116. Each of the task-specific windows is covered in greater detail at the end of this section.

   - If you need help with the File Transfer task-specific window, see "The File Transfer Task-Specific Window" on page 121.
   - If you need help with the Remote Session task-specific window, see "The Remote Session Task-Specific Window" on page 123.

- If you need help with the System Information Tool task-specific windows, see “The System Information Tool Task-Specific Windows” on page 123.
- If you need help with the System Partition task-specific window, see “The System Partition Access Task-Specific Window” on page 128.
- If you need help with the Software Inventory task-specific window, see “The Software Inventory Task-Specific Window” on page 134.
- If you need help with the Monitor Database task-specific window, see “The System Monitor Task-Specific Window” on page 139.
- If you need help with the Start Up/Shut Down Systems task-specific window, see “The Start Up/Shut Down System Task Specific Window” on page 141.
- If you need help with the Service Configuration task-specific window, see “The Service Configuration Task Specific Window” on page 142.
- If you need help with the Command Line Interface task-specific window, see “The Command Line Interface Task Specific Window” on page 143.
- If you need help with the Capacity Management task-specific window, see “The Capacity Management Task Specific Window” on page 143.

There is no task-specific window for the Scrub All RAID Drives task.

6. Enter any information required by the specific task that will be performed by the scheduled event. Then, select **Save** to save this information, close the task-specific window, and open the Schedule Time and Date window (see Figure 38 on page 120).

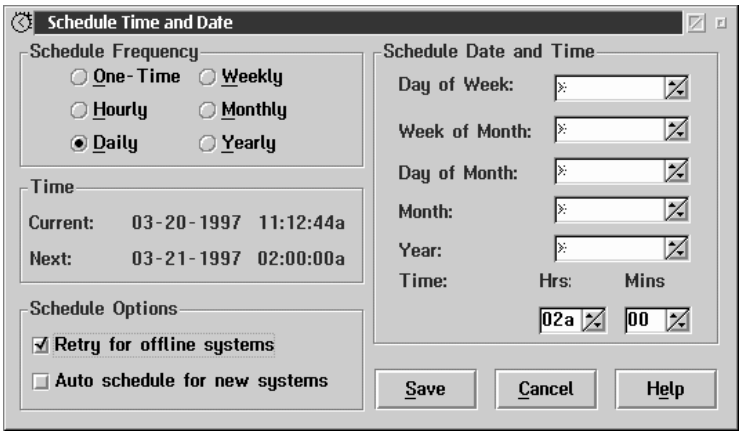

Figure 38. The Schedule Date and Time window

7. Use the Schedule Frequency buttons and **Schedule Date and Time** field group to configure time intervals and date- and time-specific settings for the scheduled event.

   The **Schedule Frequency** button group contains six radio buttons, each of which determines the time interval between executions of the scheduled event. The available selections are:

   - One-Time
   - Hourly
   - Daily
   - Weekly
   - Monthly
   - Yearly

   Note: As you select a button, only the fields necessary for proper configuration of this time interval remain active.

   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 depend on which **Schedule Frequency** you have selected. Each field offers a wildcard value, marked with an asterisk (*). If you select this

value, the Schedule Date and Time information is created for you, based on the current date and time.

Note: As you alter the **Schedule Date and Time** values, the **Next** value alters as well.

8. Select **Save** to save the scheduled event and return to the Event Scheduler Service window. Note that the name of the scheduled event you have just finished configuring now appears in the **Scheduled Events** list.

The File Transfer Task-Specific Window

Use this task-specific window to configure a scheduled event that will transfer an individual file, an individual directory, or entire directory trees between the local managing system and all selected remote systems. You can also use this window to configure a scheduled event to delete specific local or remote files.

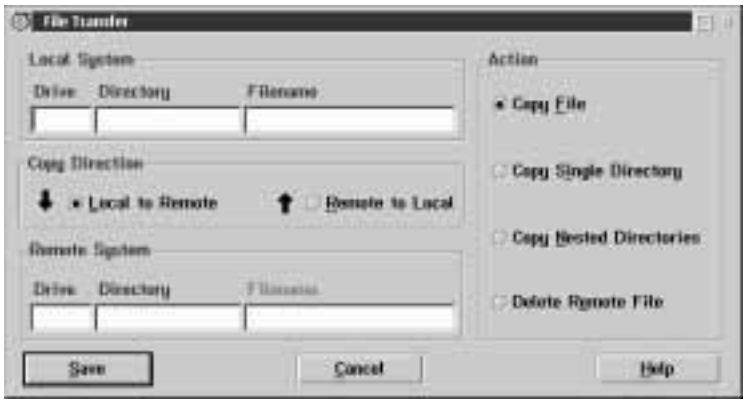

Figure 39. The File Transfer task-specific window

Attention

DOS does not support path names of more than 63 characters. If you will be using File Transfer to transfer nested directories to a system running Netfinity Manager for Windows or Client Services for Netfinity Manager for Windows, be sure that the complete path name does not exceed the maximum 63-character length. If the total length of the path name exceeds 63 characters, some nested subdirectories and the files they contain will be lost.

To configure your File Transfer scheduled event:

1. Select an Action.

   The fields that are active in the File Transfer task-specific window depend on which **Action** button you select. Available Actions are:

   - Copy File

     Select **Copy File** to create a scheduled event that will automatically transfer a specific file to or from the local system.

   - Copy Single Directory

     Select **Copy Single Directory** to create a scheduled event that will automatically transfer a specific directory to or from the local system.

   - Copy Nested Directories

     Select **Copy Nested Directories** to create a scheduled event that will automatically transfer a specific directory and all of its subdirectories to or from the local system.

   - Delete Remote File

     Select **Delete Remote File** to create a scheduled event that will automatically delete a specific file from remote systems.

   Note: As you select a button, only the fields and buttons necessary for proper configuration of this File Transfer scheduled event remain active.

2. Select a Copy Direction.

   If you are transferring a file or directory, select a Copy Direction (**Local to Remote** or **Remote to Local**). If you are deleting a file, you do not need to select a Copy Direction.

3. Enter Local System and Remote System information.

   Enter information regarding the source of the file to be transferred and the target area to which the file will be transferred. If you are deleting a file, you will only need to enter information regarding the location of the file to be deleted.

4. Save the task-specific information.

   Select **Save** to save this information and continue configuring the scheduled event.

The Remote Session Task-Specific Window

Use this task-specific window to create a scheduled event that will automatically execute a specific command on one or more remote systems.

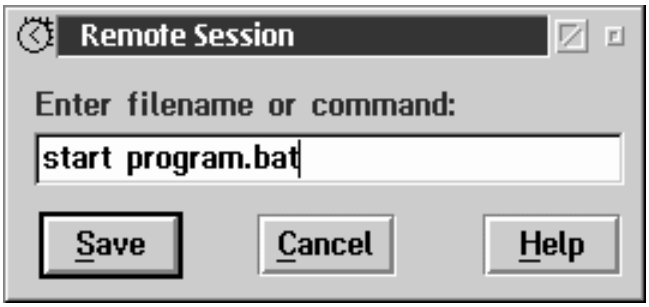

Figure 40. The Remote Session task-specific window

To configure your Remote Session scheduled event:

1. Type in the **Enter filename or command** field the command you want to execute on the selected systems.
2. Select **Save** to save the task-specific information and continue configuring the scheduled event.

The System Information Tool Task-Specific Windows

Use this action to create a scheduled event that will collect system hardware information from one or more remote systems. Once collected, this information can be saved as a history file and viewed later, printed to a printer, saved to a file, or exported to a database.

You can use this action to do one of the following actions for each selected system:

- Create a history file.
- Print the output or save it to a file.

- Send the output to a database.

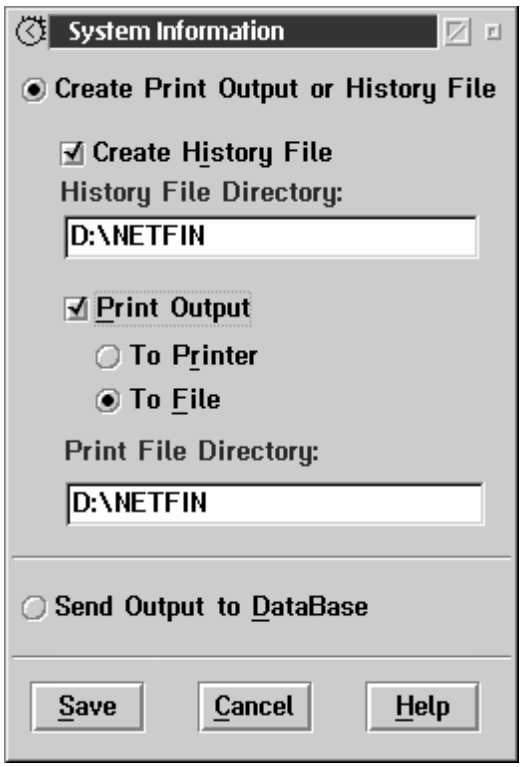

Figure 41. The System Information Tool task-specific window

Creating a History File

To configure the System Information scheduled event to create a history file for each system on which it is executed:

1. Select **Create Print Output or History File**.
2. Select **Create History File**.
3. Type in the **History File Directory** field the complete path for the local directory in which generated history files will be stored.
4. Select **Save** to continue configuring the scheduled event.

Note: The history file for each system from which information is gathered will have a different file name. This file name is generated by taking the first four letters of the system's System Name and then applying a mathematical algorithm to the entire System Name to generate a four digit alphanumeric string. These two parts are then combined to create the file name.

For example, a history file created by a Create History File scheduled event for a system named USER1 will always be named USER11BN.HST. This ensures that similarly named systems will not generate identically named history files, and that each system will generate the same file name each time the scheduled event is executed.

Printing Output or Saving Output in a File

To configure the System Information scheduled event to print output for each system on which it is executed:

1. Select **Create Print Output or History File**.
2. Select **Print Output**.
3. Select an output device.
   - Select **To Printer** to print the collected data to printer connected to LPT1.
   - Select **To File** to save the collected data in a printable file.

     If you select **To File**, type in the **Print File Directory** field the complete path of the directory in which generated print files will be stored.
4. Select **Save** to continue configuring the scheduled event.

Note: The print file for each system from which information is gathered will have a different and distinct file name. This file name is generated by taking the first four letters of the system's System Name and then applying a mathematical algorithm to the entire System Name to generate a four digit alphanumeric string. These two parts are then combined to create the file name.

For example, a print file created by a Print Output To File scheduled event for a system named USER1 will always be named USER11BN.RPT. This ensures that similarly named systems will not generate identically named print files, and that each system will generate the same file name each time the scheduled event is executed.

Sending Output to a Database

To configure the System Information scheduled event to send output from each system on which it is executed to a database:

1. Select **Send Output to Database**.
2. Select **Save** to save this information and open the Database Selection window (see Figure 42).

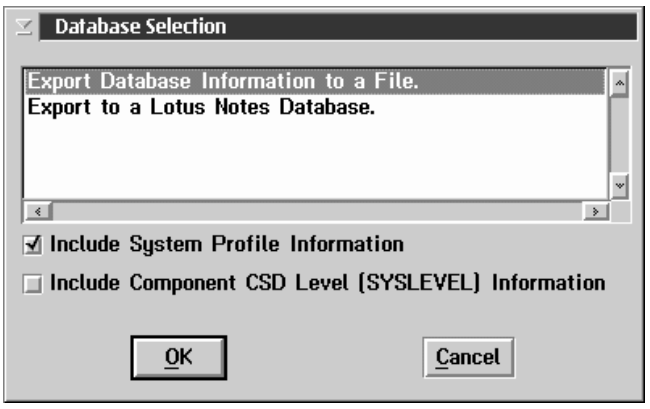

Figure 42. The Database Selection window

3. Select a database export function from the Database Selection field.

   The data can be exported to a file or to a supported database format.

   - To export the system information to a file, select **Export Database Information to a File**.
   - To export the system information to a supported database, select the export function for the database server to which your managing system is attached. If your managing

system is attached to more than one type of database server, then you will have an entry for each type of database in the Database Selection field. For example, if your system is configured to use both a Lotus Notes database server and a DB2 database server then the Database Selection field will contain two export to database selections: **Export to a Lotus Notes Database** and **Export to a DB2 Database**.

Note: This function will not be available if the managing system does not have access to or is not configured to use a database system. For more information, see "Netfinity Database Support" in *Netfinity Manager Quick Beginnings*

If you want the System Information Tool to gather information from the System Profile notebook and include it in the data set, select the **Include Profile information** check box.

4. Select **OK** to save this information.

   - If you selected **Export System Information to a File**, the Export To File window appears (see Figure 43).

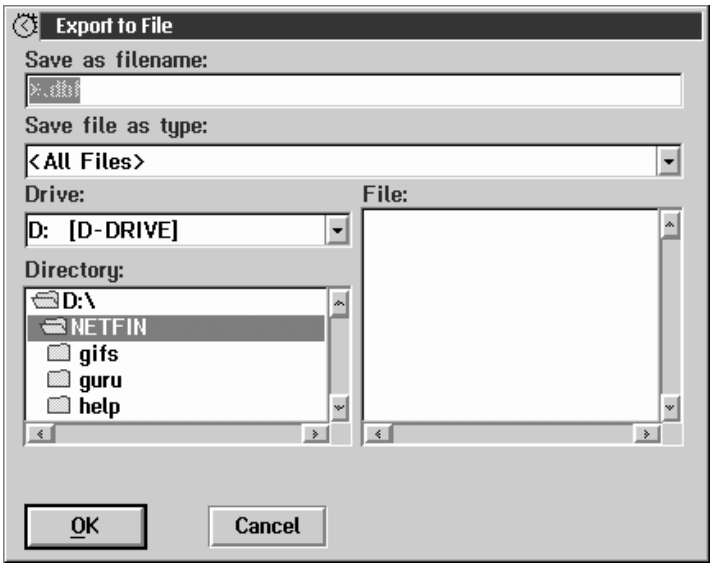

Figure 43. The Export To File window

Enter all file-specific information, and then select **OK** to continue configuring the scheduled event.

- If you selected **Export System Information to a Database**, the Server Selection window appears.

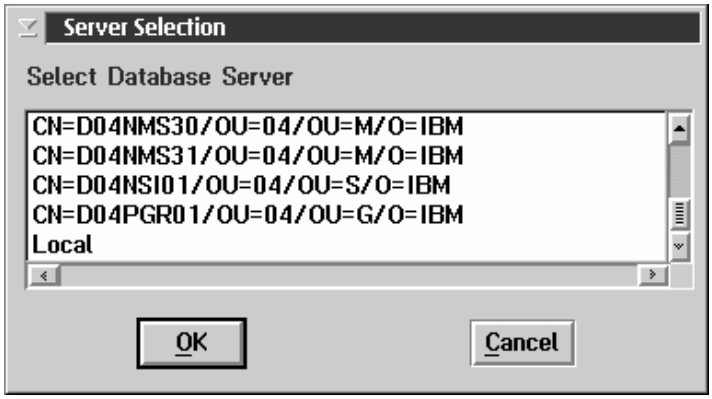

Figure 44. The Server Selection window

Select from the **Server Selection** field a database to export the data to, and then select **OK** to continue configuring the scheduled event.

The System Partition Access Task-Specific Window

Use the System Partition Access task to configure a scheduled event that will automatically update, back up, or delete specific files and directories from the the System Partitions of all selected systems.

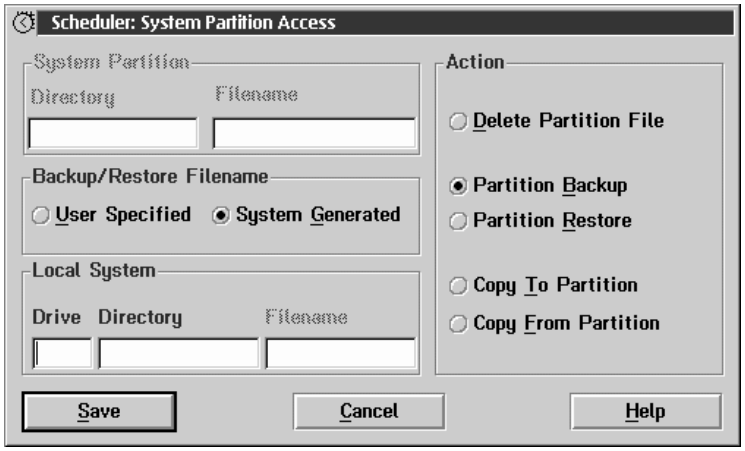

Figure 45. The System Partition Access task-specific window

You can configure a scheduled event to perform any one of the following actions:

- Delete Partition File

  Select **Delete Partition File** to erase a specific file from the System Partition of each selected system.

- Partition Backup

  Select **Partition Backup** to create a backup image of the System Partition of each remote selected system.

- Partition Restore

  Select **Partition Restore** to restore the System Partition of each remote selected system. The backup image is restored from an image located on the local system.

- Copy To Partition

  Select **Copy To Partition** to copy a specific file from the local system to the System Partition of all remote selected systems.

- Copy From Partition

  Select **Copy From Partition** to copy a specific file from the System Partition of all remote selected systems. The file is copied to a drive and directory located on the local system.

Deleting Partition Files

Select the **Delete Partition File** Action to erase a specific file from the System Partition of each remote selected system.

To configure a **Delete Partition File** Action:

1. Select the **Delete Partition File** radio button.
2. Type in the System Partition **Directory** field the name of the System Partition directory (if any) that contains the file to be deleted.
3. Type in the System Partition **Filename** field the name of the System Partition file that will be deleted by the scheduled event.
4. Select **Save** to save this information and continue configuring the scheduled event.

Backing Up System Partitions

Select **Partition Backup** to create a backup image of the System Partition of each remote selected system.

To configure a **Partition Backup** Action:

1. Select the **Partition Backup** radio button.
2. Select a Backup/Restore Filename option.

   There are two Backup/Restore Filename options to choose from:

   - User Specified
   - System Generated
3. Type in the Local System **Drive** field the drive letter of the local system's disk drive that will be used to store the backup image file.
4. Type in the Local System **Directory** field the name of the local system's directory that will be used to store the backup image.

5. If you have selected **User Specified**, enter in the Local System **Filename** field the name you want to assign to the backup image file.

   Note: If you selected **System Generated**, the System Partition Access task will create a system-specific file name for each system on which the scheduled event is performed. This file name is created by using the first four letters of a remote system's System Name, and then applying a mathematical algorithm to the entire System Name to generate a four digit alphanumeric string. These two parts are then combined to form a file name for the image.

   For example, a System Partition backup image file of a system named USER1 created by a Partition Backup scheduled event using the System Generated Filename option will always be named USER11BN.IMG. This ensures that similarly named systems will not generate identically named partition backup images files, and that each system will generate the same file name (or restore the same image) each time the scheduled event is executed.

6. Select **Save** to save this information and continue configuring the scheduled event.

Restoring System Partitions

Select **Partition Restore** to restore the System Partition of each remote selected system. The backup image is restored from a specified image located on the local system.

To configure a **Partition Restore** Action:

1. Select the **Partition Restore** radio button.
2. Select a Backup/Restore Filename option.

   There are two Backup/Restore Filename options to choose from:

   - User Specified
   - System Generated

3. Type in the Local System **Drive** field the drive letter of the local system's disk drive that contains the image file that will be used to restore the System Partition.
4. Type in the Local System **Directory** field the name of the local system's directory that contains the image file that will be used to restore the System Partition.
5. If you have selected **User Specified**, type in the Local System **Filename** field the name of the backup image file that will be used to restore the System Partition in the Local System **Filename** field.

   Note: If you selected **System Generated**, the System Partition Access task will create a system-specific file name for each system on which the scheduled event is performed. This file name is created by using the first four letters of a remote system's System Name, and then applying a mathematical algorithm to the entire System Name to generate a four digit alphanumeric string. These two parts are then combined to form a file name for the image.

   For example, a System Partition backup image file of a system named USER1 created by a Partition Backup scheduled event using the System Generated Filename option will always be named USER11BN.IMG. This ensures that similarly named systems will not generate identically named partition backup images files, and that each system will generate the same file name (or restore the same image) each time the scheduled event is executed.

   If you have previously created System Partition images using the **System Generated** Backup/Restore Filename option, you should select **System Generated** when restoring these System Partitions.
6. Select **Save** to save this information and continue configuring the scheduled event.

Copying Files To Partitions

Select **Copy To Partition** to copy a specific file from the local system to the System Partition of all remote selected systems.

To configure a **Copy To Partition** Action:

1. Select the **Copy To Partition** radio button.
2. Type in the Local System **Drive** field the drive letter of the local system's disk drive that contains the file that will be copied to the System Partition.
3. Type in the Local System **Directory** field the name of the local system's directory that contains the file that will be copied to the System Partition.
4. Type in the Local System **Filename** field the name of the file that will be copied to the System Partition.
5. Select **Save** to save this information and continue configuring the scheduled event.

Copying Files From Partitions

Select **Copy From Partition** to copy a specific file from the System Partition of all remote selected systems to a specified drive and directory on the local system.

To configure a **Copy From Partition** Action:

1. Select the **Copy From Partition** radio button.
2. Type in the System Directory **Directory** field the name of the System Partition directory (if any) that contains the file that will be copied to the local system.
3. Type in the System Partition **Filename** field the name of the System Partition file that will be copied to the local system.
4. Type in the Local System **Drive** field the drive letter of the local system's disk drive that will be used to store the System Partition file.
5. Type in the Local System **Directory** field the name of the local system's directory that will be used to store the System Partition file.

6. Select **Save** to save this information and continue configuring the scheduled event.

The Software Inventory Task-Specific Window

Use the Software Inventory task to create a scheduled event that will gather data about software installed on one or more remote systems. Once collected, this information can be exported to a database, saved to a database file, or used to generate a variety of reports.

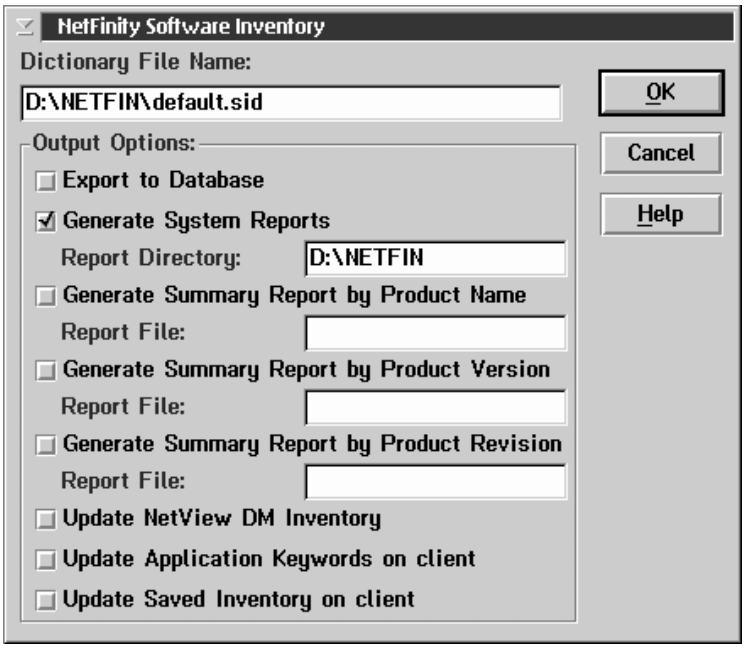

Figure 46. The Software Inventory task-specific window

To continue configuring your Software Inventory scheduled event:

1. Type in the **Dictionary File Name** field the name of the Software Inventory dictionary file that will be used to determine the presence of software products on each of the remote systems.
2. Select one or more Output Options:

You can select up to eight Output Options:

- Export to Database

  To export Software Inventory data to a database or database file:

  a. Select **Export to Database** and then select **OK**.

     Note: You can select other Output Options as well. The following steps do not need to be completed until after you have selected **OK** and closed the Netfinity Software Inventory task-specific window.

  b. Select from the **Database Selection** field the type of database data export you want to perform.

     The data can be exported to a file or to a supported database format.

     – To export the information to a file that can later be used to append the Software Inventory data to an existing Netfinity database:

       1) Select **Export Database Information to a File**.

       2) Select **OK** to open the Save as File window.

       3) Select a drive and directory where the file will be saved, and then type in the **Save as file name** field the name of the file that will be created.

     – To export the system information to a supported database:

       1) Select the export function for the database server to which your managing system is attached.

          If your managing system is attached to more than one type of database server, then you will have an entry for each type of database in the **Database Selection** field. For example, if your system is configured to use both a Lotus Notes database server and a DB2 database server then the **Database Selection** field will contain two

export to database selections: **Export to a Lotus Notes Database** and **Export to a DB2 Database**.

2) Select **OK** to open the Database Selection window.

3) Select the database to which the Softeare Inventroy data will be exported.

Note: This function will not be available if the managing system is not attached to or configured to use a supported database system. For more information, see "Netfinity Database Support" in *Netfinity Manager Quick Beginnings*.

If you select Export Information to a Database:

1) Select **OK** to open the Database Selection window.

2) Select the database to which the Software Inventory data will be exported.

c. Select **OK** to save this information and continue configuring the scheduled event.

- Generate System Reports

  Select this option to create a report of all software products detected on each remote system. This report is then stored in a specified directory on your local system.

  To generate a Software Inventory report for each system:

  a. Select **Generate System Reports**.

  b. Type in the **Report Directory** field the fully qualified path of the directory on the managing system that the system reports will be saved to.

  Note: The report for each system from which information is gathered will have a different and distinct file name. This file name is generated by taking the first four letters of the system's System Name and then applying a mathematical algorithm to the entire System Name to generate

a four digit alphanumeric string. These two parts are then combined to create the file name.

For example, a report file created by a Generate System Reports scheduled event for a system named USER1 will always be named USER11BN.RPT. This ensures that similarly named systems will not generate identically named reports, and that each system will generate the same report name each time the scheduled event is executed.

- Generate Summary Report by Product Name

  Select **Generate Summary Report by Product Name** to create a report that contains a summary of *all* software products found on all selected remote systems. This report will feature information on all distinct Product Names that are found by Software Inventory.

  To generate a Summary Report by Product Name:

  a. Select **Generate a Summary Report by Product Name**.

  b. Type in the **Report File** field the name of the report file that will be created.

- Generate Summary Report by Product Version

  Select **Generate Summary Report by Product Version** to create a report that contains a summary of *all* software products found on all selected remote systems. This report will feature information on all distinct Product Versions of distinct Product Names that are found by Software Inventory.

  To generate a Summary Report by Product Version:

  a. Select **Generate a Summary Report by Product Version**.

  b. Type in the **Report File** field the name of the report file that will be created.

- Generate Summary Report by Product Revision

  Select **Generate Summary Report by Product Revision** to create a report that contains a summary of *all* software

products found on all selected remote systems. This report will feature information on all distinct Revisions of distinct Versions of distinct Product Names that are found by Software Inventory.

To generate a Summary Report by Product Revision:

a. Select **Generate a Summary Report by Product Revision**.

b. Type in the **Report File** field the name of the report file that will be created.

- Update NetView DM Inventory

  Select **Update NetView DM Inventory** to update the NetView DM inventory files of any selected remote system that is running NetView DM. If the remote system is running NetView DM, Software Inventory will scan the currently loaded dictionary file for any product definitions that include an NetView DM Change Object and add them to the NetView DM software inventory import file (FNDSWINV). The location token information will be written into the NetView DM agent software base path into a file called FNDTKINV.

  This enables a user-written exit routine to then invoke the appropriate NetView DM INV and NetView DM UPDTG commands to move the data in this import file into that workstation's NetView DM software change history database.

- Update Application Keywords on Client

  Select **Update Application Keywords on Client** to update the application keyword list used by the remote client.

- Update Saved Inventory on Client

  Select **Update Saved Inventory on Client** to update the saved inventory list (for use by other management products, including products that use SNMP or DMI) on the remote client.

3. Select **OK** to save this information and continue configuring the scheduled event.

The System Monitor Task-Specific Window

Use the System Monitor task to create a scheduled event that will collect system monitor data for a specified time period from one or more remote systems. Once collected, this information can be exported to a database or saved to a database file.

To configure your System Monitor scheduled event:

1. Select from the **Monitors** list the names of the monitors whose recorded data will be exported to the database.
2. Use the spin buttons in the **Export for Time Period** fields to select the number of hours, days, or weeks of recorded data that will be exported to the database.
3. Select **OK** to save this information and open the Database Selection window.
4. Select from the Database Selection window the type of database data export you want to perform.

   You can use this scheduled event to handle the collected System Monitor data in the following ways.

   - Export Database Information to a File

     Select this option to export the information into a file that can later be used to append the System Monitor data to an existing Netfinity database.

     If you select Export Database Information to a File:

     a. Select **OK** to open the Save as File window.

     b. Select a drive and directory where the file will be saved, and then type in the **Save as file name** field the name of the file that will be created.

   - Export Information to a Database

     Select this option to export the information directly to a Netfinity database to which the managing system has access.

     Note: This option will not appear if the managing system does not have access to or is not configured to use a supported database system. For more information,

see “Netfinity Database Support” in *Netfinity Manager Quick Beginnings*.

If you select Export Information to a Database:

a. Select **OK** to open the Database Selection window.

b. Select the database to which the System Monitor data will be exported.

- Export Information to a Lotus Notes Database

  Select this option to export the information directly to a Netfinity Lotus Notes database.

  Note: This option will not appear if the managing system does not have access to or is not configured to use Lotus Notes.

  If you select Export Information to a Lotus Notes Database:

  a. Select **OK** to open the Server Selection window.

  b. Select from the **Select Database Server** field the Lotus Notes server to which the System Monitor data will be exported.

  c. Select **OK**. If you do not have access to the selected server, you will be asked to provide a password to enable access for this event.

5. Select **OK** to save this information and continue configuring the scheduled event.

The Start Up/Shut Down System Task Specific Window

Use the Start Up/Shut Down System task to restart, shut down, power up, or wake Wake on LAN systems remotely.

To configure your Start Up/Shut Down System scheduled event, select the Start Up/Shut Down System action you want to take from the Start Up/Shut Down System Options window, and then select **OK** and continue configuring the scheduled event.

The following Start Up/Shut Down System Options are available.

- Attempt System Restart

  This option attempts to restart any systems you specify, exactly as if you had selected **Restart System** from each system's context menu in Remote System Manager. This action will complete successfully only if you have access to the remote system's Security Manager service.

- Attempt System Shut Down

  This option attempts to shut down the operating system of any systems you specify. This action will complete successfully only if the remote system is running Windows 3.1, Windows 95, Windows NT 3.51 or later, or NetWare **and** if you have access to the remote system's Security Manager service.

- Attempt System Wake Up

  This option attempts to wake all specified systems that are enabled to support Wake on LAN. For more information on Wake-on-LAN configuration, see Appendix K, "Troubleshooting Wake-On-LAN Systems" on page 525.

- Attempt System Power Down

  This option attempts to power down all specified systems. This feature will complete successfully only on systems running Windows 95 that have Advanced Power Management enabled and on which you have access to the Security Manager service.

The Service Configuration Task Specific Window

Use the Service Configuration task to update or replace the configuration used by specific Netfinity services with Service Configuration Files (SCF) created using Service Configuration Manager.

To configure your Service Configuration scheduled event:

1. Type in the field provided the full name of the Service Configuration File that contains the service configuration data you want to propagate to other systems.

   The name you type must be a file name that appears in the SCF subdirectory of your Netfinity installation directory, and the file name must match exactly, including the file extension. For example, an SCF file named ALERT.SCF must be typed as ALERT.SCF. If you type just ALERT, the service configuration update will fail.

2. Select a **Merging** setting.

   Service Configuration events can apply changes specified in SCF files in one of two ways:

   - Overwrite Existing Configuration

     Select **Overwrite Existing Configuration** if you want to completely replace the service-specific configuration on each remote system with the configuration defined in the specified SCF file.

   - Add to Existing Configuration

     Select **Add to Existing Configuration** to append any configuration records that appear in the SCF file to the service conifguration that already exists on the remote system.

3. Select **Save** to save this information and continue configuring the scheduled event.

The Command Line Interface Task Specific Window

Use the Coomand Line Interface Service window to initiate a Netfinity command-line interface task on all specified systems. For information on using Netfinity command-line interfaces, see *Netfinity Manager Command Reference.*

To configure your Command Line Interface scheduled event:

1. Type in the **Command Line Intereface EXE** field the name of the Netfinity command you want to use.
2. Type in the **Command Line Parameters** field any additional parameters that you want to use with this Netfinity command. Do **not** include the /N or /S parameters. Ordinarily, these parameters are used to determine the network address and system name of the system on which the command will be run. Event Scheduler will provide this information for all systems automatically.
3. Select **Send CLI Output to File** to direct all command-line output to file on the managing system (optional).
4. Select **OK**. If you do not have access to the selected server, you will be asked to provide a password to enable access for this event.

The Capacity Management Task Specific Window

Use the Capacity Management task automatically create Capacity Managment reports.

To configure your Capacity Management scheduled event:

1. Select a Report Definition.

   The Report Defintions page of the Generate Reports notebook contains all previously defined Report Defintions. Report Definitions specify the data that is collected for a Capacity Management report. You can:

   - Select a previously generated Report Definition

     To select a previously defined Report Definition, select the Report Definiton and then select **Next**. This opens the

Generate Reports notebook to the Systems page. If you are using a previously created report, go to 3 on page 145.

- Edit a previously defined Report Definition

  To edit a previously defined Report Definition, select the Report Definiton and then select **Edit**. This opens the Report Definition window (see Figure 47).

- Create a new Report Definition

  To create a new Report Defintion, select **New**. This opens the Report Definition window (see Figure 12 on page 52).

Figure 47. Report Definition window

2. Create (or edit) the Report Definition.

   Use the selections available on the Report Definitions window to configure the Report Definition. You will need to specify:

   - The time period for which data will be collected
   - The amount of data to collect
   - The time-period for which the data will be collected

- The specific monitored data that will be included in the report

Select **Next** to continue.

3. Select systems to include in the report.

Figure 48. Report Generator notebook — Systems page

Select Netfinity groups or systems that will be included in the report. Then, select **Next** to continue configuring the scheduled event.

Deleting Scheduled Events

To delete a previously configured scheduled event:

1. Select from the **Scheduled Events** field in the Scheduler Service window the scheduled event you want to delete from the **Scheduled Events** list.
2. Select **Delete**. After confirmation, the scheduled event is deleted.

Viewing Scheduled Events

To view a previously created scheduled event:

1. Select from the **Scheduled Events** field in the Scheduler Service window the scheduled event you want to view from the **Scheduled Event** list.

2. Select **View**. This opens the View Scheduled Event window (see Figure 49 on page 146).

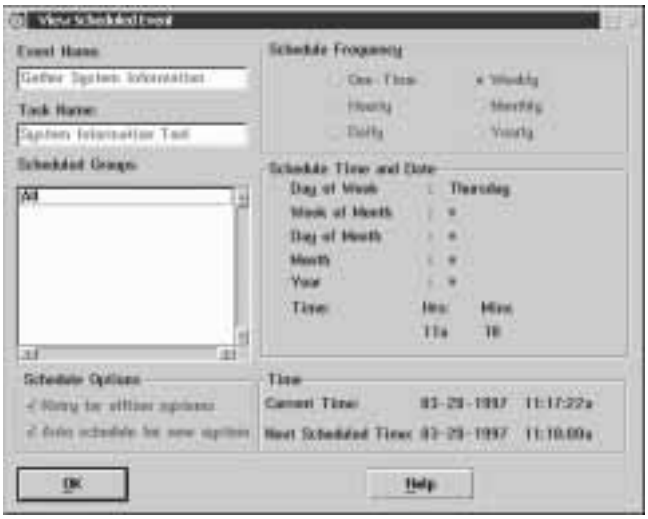

Figure 49. The View Scheduled Event window

The View Scheduled Event window contains information specific to the selected scheduled event (including name, task to be performed, systems on which the task will be performed, and when the event will be performed again).

Note: You cannot change any of the information displayed in the View Scheduled Event window.

3. Select **OK** to close the View Scheduled Event window.

Editing Scheduled Events

To edit a previously configured scheduled event:

1. Select from the **Scheduled Events** field in the Scheduler Service window the scheduled event you want to edit from the **Scheduled Events** list.
2. Select **Edit**. This opens the Edit Scheduled Event window (see Figure 50 on page 147).

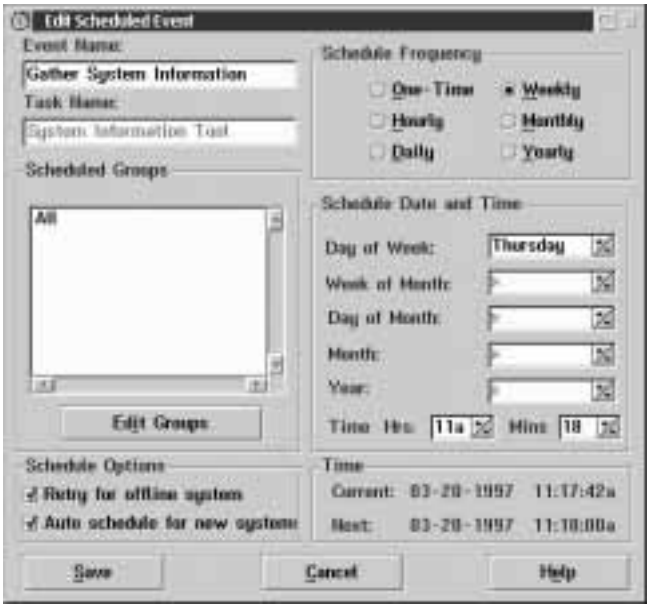

Figure 50. The Edit Scheduled Event window

The Edit Scheduled Event window contains information specific to the selected scheduled event. From this window, you can:

a. Change the scheduled event's name.

   To change the name of the selected event, enter the new name in the **Event Name** field.

b. Change the systems or system groups on which the selected event's task will be performed.

   To change the systems or system groups on which the task will be performed, select **Edit Groups/Systems**. This will open the Schedule Groups or Systems window (see Figure 37 on page 118). Select or deselect systems and then select **Schedule** to return to the Edit Scheduled Event window.

c. Change the **Schedule Frequency** of the scheduled event.

   Select the new frequency for the scheduled event from the **Schedule Frequency** button group.

d. Change the **Schedule Date and Time** settings of the scheduled event.

   Adjust the date and time setting fields in the **Schedule Date and Time** field group.

3. When you have finished editing the scheduled event, select **Save** to save the new scheduled event information.

Refreshing the Scheduled Event List

If other Netfinity Managers have access to your Event Scheduler service, they can create, edit, and delete scheduled events on your system remotely. This could cause changes to the **Scheduled Event** list that would not ordinarily appear until the Event Scheduler Service window was closed and reopened. Select **Refresh** from the Scheduler Service window to update the **Scheduled Events** list immediately.

Viewing the Scheduler Log

The Scheduler Log contains a record of all actions taken by the Event Scheduler service, including the name of any scheduled event, the name of the Netfinity service that was used to execute the scheduled event, the date and time at which the event was executed, the name of each system on which the event was executed, and the results (success or failure) of the scheduled event on each system.

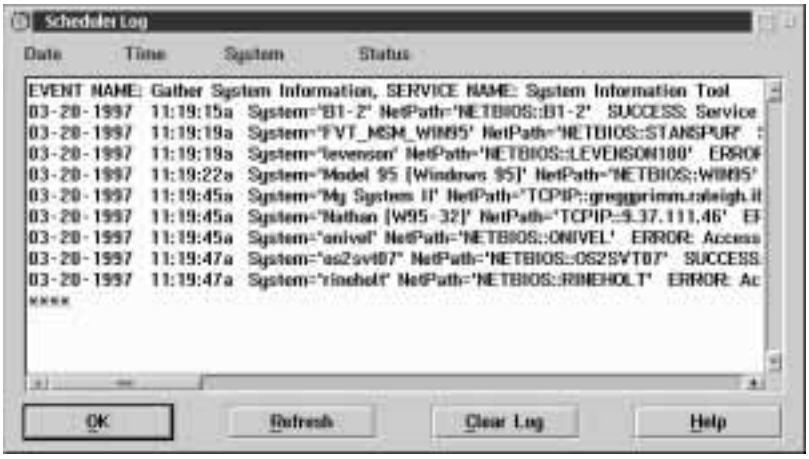

Figure 51. The Scheduler Log window

To view the Scheduler Log, select **View Log** from the Scheduler Service window. To erase the contents of the log, select **Clear Log**. To update the contents of the Scheduler Log while you are viewing it, select **Refresh**. To close the Scheduler Log window, select **OK**.

Chapter 10. File Transfer Service

Use File Transfer to transfer files and directories among your local system and remote Netfinity systems. In addition to these basic file and directory management functions, File Transfer also includes a Cleanup Assistance function that you can use to search the contents of a remote system's hard disks for duplicate files, files greater than a certain size, old or outdated files, or specific file types. Once these files are detected, you can selectively delete them. Finally, you can use File Transfer to synchronize the contents of specified directories, ensuring that the contents of entire directories on your local and remote systems match exactly.

For detailed information about File Transfer functions, see the following topics:

- "Receiving Directories or Files from a Remote System" on page 153
- "Sending Directories or Files to a Remote System" on page 154
- "Deleting Local Directories or Files" on page 155
- "Deleting Remote Directories or Files" on page 155
- "Synchronizing Local and Remote Directories" on page 155
- "Cleanup Assistance" on page 157

Notes:

1. File Transfer is a *remote only* service. This service will be available only when you are accessing a remote system. The File Transfer service object will *not* appear in your local Service Manager.
2. File Transfer uses an automatic file-compression process to minimize the amount of time it takes to move files or directories across slower networks. However, if you are using a fast network, File Transfer will not use any compression, as the time required to process the data for compression will actually increase the amount of time it takes to transfer the data. This process is automatic, and requires no input. If you want to disable File Transfer data-compression capabilities, see "Disabling Data Compression" on page 161.

3. The extended file names of any high performance file system (HPFS) files that are transferred to a file allocation table (FAT) drive will be changed to an appropriate FAT file name.

Attention:

- Improper use of File Transfer can lead to data loss locally or remotely. If you are concerned about potential data loss, use Security Manager to limit use.
- DOS does not support path names of more than 63 characters. If you will be using File Transfer to transfer nested directories to a system running Client Services for Netfinity Manager for Windows, be sure that the complete path name does not exceed the maximum 63-character length. If the total length of the path name exceeds 63 characters, some nested subdirectories and the files they contain will be lost.

Selecting Drives, Directories, and Files

Before you can use File Transfer features on another system, you must first select that system from a Remote System Manager system group. Then, select the remote system's File Transfer object. You are now ready to transfer files or directories to and from the selected system. Note that the left half of the File Transfer window represents your local system, and the right half represents the remote system you have accessed. The remote system's name is displayed above the remote system fields and in the window's title bar.

Before you can use any File Transfer directory or file-handling functions, you must select the local and remote directories or files that will be transferred, synchronized, or deleted. All directory and file selection is done in the File Transfer window (Figure 52 on page 152). As you select drives, directories, and files, you will notice that File Transfer automatically enables or disables buttons and fields that can be used with the currently selected directory or file.

Figure 52. The File Transfer window

Selecting Drives or Volumes

Drives and volumes on the local or remote system are listed in the **Drive/volume** selection list in the Local group and Remote group, respectively. To select a drive, select the small arrow at the right side of the **Drive/volume** field and then select a drive or volume from the list. The contents of the **Directories** and **Files** fields will be updated automatically when you select a new drive or volume.

Selecting Directories

Directories on the local or remote system are listed in the **Directories** field in the Local group and Remote group, respectively. To select a directory, click on the name of the directory. To select multiple directories, press **Ctrl** and then click on additional directories. To open a directory, double-click on the directory you want to open. When you open a directory, the contents of the **Directories** and **Files** fields are updated automatically.

You can use the **All Dirs** button to select or deselect all directories listed in the **Directories** field.

Selecting Files

Files on the local or remote system are listed in the **Files** field in the Local group and Remote group, respectively. To select a file, click on the name of the file. To select multiple files, press **Ctrl** and then click on additional file names.

You can use the **All Files** button to select or deselect all files listed in the **Files** field.

Receiving Directories or Files from a Remote System

To receive one or more directories or files from a remote system:

1. Select a target drive and directory from the Local group.

   The *target drive* and *directory* are the drive and directory on your system that remote directories or files will be transferred to.

2. Select a source drive and one (or more) source directories from the Remote group.

   The *source drive* and *directory* are the drive and directory on the remote system that contain the directories or files that will be transferred.

3. Select a transfer mode.

   You can select one of the two available transfer modes:

   Copy Directories or files transferred from the source system are left on the source system and copied to the target system.

   Move Directories or files transferred from the source system are removed from the source system and moved to the target system.

4. Check the **Nested** check box if you are transferring directories and want to receive subdirectories that are nested within selected source directories.

5. Select **Receive Dir** to transfer the selected remote directories to your local system, or select **Receive File** to transfer the selected files to your local system.

Sending Directories or Files to a Remote System

To send one or more directories or files to a remote system:

1. Select a source drive and one (or more) source directories or files from the Local group.

   The *source drive* and *directory* are the drive and directory on your system that contain the directories or files that will be transferred.

2. Select a target drive and one target directory from the Remote group.

   The *target drive* and *directory* are the drive and directory on the remote system that local directories or files will be transferred to.

3. Select a transfer mode.

   You can select one of the two available transfer modes:

   Copy Directories or files transferred from the source system are left on the source system and copied to the target system.

   Move Directories or files transferred from the source system are removed from the source system and moved to the target system.

4. Check the **Nested** check box if you are transferring directories and want to send subdirectories that are nested within selected source directories.

5. Select **Send Dir** to transfer the selected local directories to the remote system, or select **Send File** to transfer the selected files to the remote system.

Deleting Local Directories or Files

To delete one or more local directories or files:

1. Select a source drive and one (or more) source directories or files from the Local group.

   The *source drive* and *directory* are the drive and directory on your system that contain the directories or files that will be deleted.

2. Select **Delete Dir** to delete all selected directories, or select **Delete File** to delete all selected files.

Deleting Remote Directories or Files

To delete one or more remote directories or files:

1. Select a source drive and one (or more) source directories or files from the Remote group.

   The *source drive* and *directory* are the drive and directory on the remote system that contain the directories or files that will be deleted.

2. Select **Delete Dir** to delete all selected directories, or select **Delete File** to delete all selected files.

Synchronizing Local and Remote Directories

You can use the File Transfer synchronization process to ensure that the contents of a local and a remote directory are identical. File Transfer offers three synchronization modes:

Local is master Use **Local is master** mode to synchronize the contents of the remote system directory with those of the local system directory. Any files that are contained in the remote system directory that are not found in the local system directory are deleted.

Remote is master Use **Remote is master** mode to synchronize the contents of the local system directory with those of the remote system directory. Any files that are contained in the local system directory

that are not found in the remote system directory are deleted.

Peers Use **Peers** mode to synchronize the remote and local directories with the latest versions of any files found in either directory. In this mode, synchronization will update any files found in *both* directories to the most recent version of the file. Also, files that are found in only one of the directories are copied to the other directory.

To synchronize the contents of a directory on your local system with a directory on a remote system:

1. Select a drive and directory from the Local group.
2. Select a drive and directory from the Remote group.
3. Select **Synchronize**.

   This opens the Directory Synchronization (Figure 53) window. From this window, you can specify the synchronization mode (using the **Sync mode** radio buttons) and the synchronization action (using the **Sync action** check boxes).

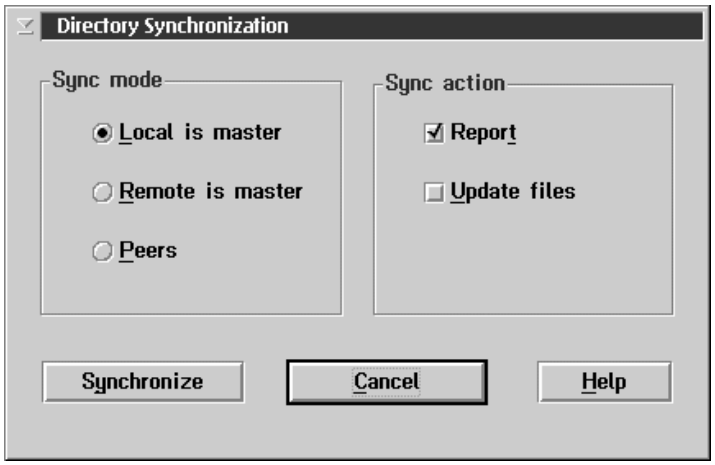

Figure 53. The Directory Synchronization window

4. Select a synchronization mode.
5. Check at least one synchronization action.

   Check one or more of the available synchronization action check boxes in the **Sync action** group.

   - Report

     Check the Report check box to receive information on what files need to be changed or removed for the selected synchronization process to be successful. If you check *only* the **Report** check box, you will receive information regarding which files need to be updated, replaced, or deleted for the selected synchronization mode to be completed. However, unless you check the **Update files** synchronization action, the contents of the selected directories will not be altered.

   - Update files

     Check the **Update files** check box to enable the directory synchronization process to alter the contents of the selected directories. The contents of the selected directories will be updated *only* if the **Update files** check box is checked.
6. Select **Synchronize** to complete the synchronization procedure.

Cleanup Assistance

Select **Remote Cleanup...** to perform a file cleanup procedure on the remote system. You can use this procedure to scan the remote system's hard disks for files that may be:

- Unnecessary
- Old or out-of-date
- Very large
- Duplicated in other directories

Once these files are detected, you can choose to delete some or all of them, or simply to save or print the results of the scan for reference later. To start the cleanup procedure, select **Remote Cleanup...**. This opens the Cleanup Assistance window (Figure 55 on page 160).

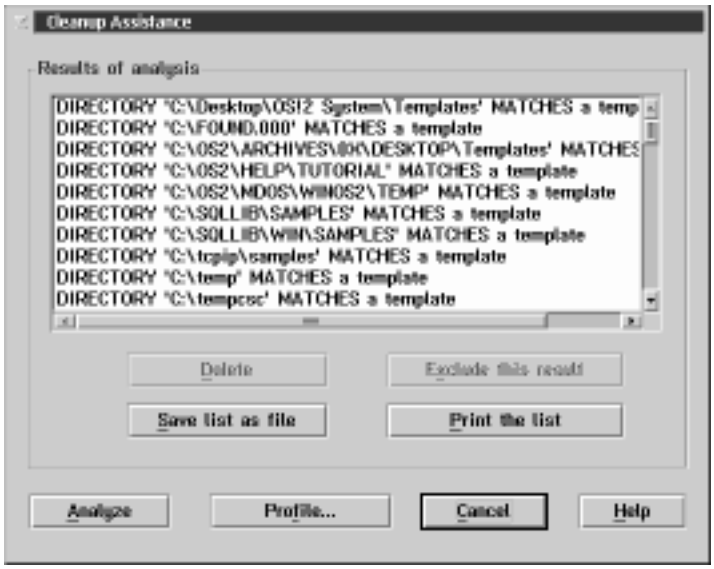

Figure 54. The Cleanup Assistance window

From the Cleanup Assistance window, you can initiate a Cleanup Assistance scan of the remote system's hard disks by selecting **Analyze**.

When you select **Analyze**, Cleanup Assistance uses the currently defined Cleanup Assistance profile to determine which files will be detected and reported. To review or edit the currently defined Cleanup Assistance profile, select **Profile...**.

Cleanup Assistance Profiles

Use the Cleanup Assistance Profile window to specify the criteria that will be used by File Transfer to determine if a file on the remote system's hard disks is to be included in the list of files reported by Cleanup Assistance.

To configure the Cleanup Assistance Profile:

1. Select **Remote Cleanup** from the File Transfer window.

   This opens the Cleanup Assistance window (see Figure 55 on page 160).

2. Select **Profile...** from the Cleanup Assistance window.

   This opens the Cleanup Assistance Profile window.

3. Select one or more criteria for use by Cleanup Assistance.

   The following criteria are available for use by Cleanup Assistance:

   - Report duplicate files

     Check the **Report Duplicate files** check box to include in the Cleanup Assistance report any files that have identical names, dates, times, and sizes.

   - Report files larger than

     Check the **Report files Larger than** check box to include in the Cleanup Assistance report any files that are larger than the number of units specified in the fields beside this selection.

   - Report files older than

     Check the **Report files Older than** check box to include in the Cleanup Assistance report any files that exceed the number of units specified in the fields beside this selection.

   - Match templates

     Check the **Match templates** check box to include in the Cleanup Assistance report any files that match any of the file types shown in the **Templates** field. For more information on configuring and using templates, see "Cleanup Assistance Profile Templates" on page 161.

   Note: All Cleanup Assistance options work independently. Therefore, if you select more than one option, it is possible that the same file might be reported more than once (if it matches more than one option).

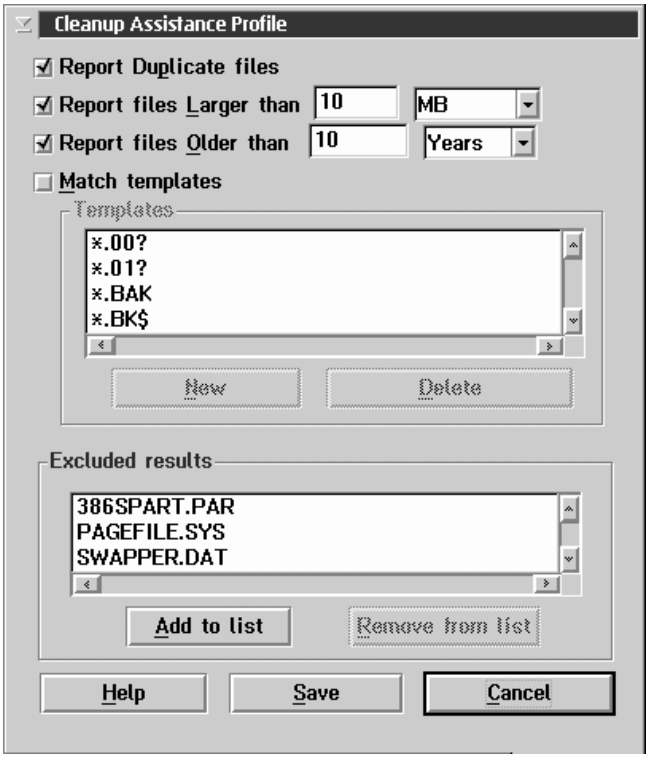

Figure 55. The Cleanup Assistance Profile window

You can select any or all of these options, but you must select at least one. Cleanup Assistance will report files or directories that meet *any* option selected in the Cleanup Assistance Profile window.

4. Configure the **Excluded results** list (optional).

   Cleanup Assistant will not include files that appear in the **Excluded results** list. This list enables you to instruct Cleanup Assistance to ignore certain files or directories on the remote system.

   - To add an entry to the **Excluded results** list, select **Add to list**, type in the name of the file you want to exclude from Cleanup Assistance scans, and then select **Save**.

- To remove an entry from the list, select the entry and then select **Remove from list**.

5. Select **Save** to save the new profile and return to the Cleanup Assistance window.

Cleanup Assistance Profile Templates

A Cleanup Assistance template is a file that will be included in the Cleanup Assistance report if it is found when Cleanup Assistance scans the remote system's hard disks. This template can consist of a specific file name and file type (for example, README.TXT), files with a specific file-type extension (for example, *.EXE), drive and directory path information (for example D:\NETFIN\) and so forth, using all standard file-name wildcards characters. For example, a Cleanup Assistant template that specifies files named A*.DOC would result in a report including all file names that start with the letter A and that have DOC as a file type.

Note: The amount of time needed to perform the Cleanup Assistance scan is directly proportional to the number of templates in use. To make the Cleanup Assistance scan as quick as possible, keep the template list small or if you are mainly interested in duplicate files temporarily disable the **Match templates** check box.

Disabling Data Compression

To disable the File Transfer automatic data compression process, add the following environment variable to your system:

```
SET NFFTCL=0
```

The manner in which this environment variable is added depends on your operating system.

- To set this environment variable on an OS/2 or Windows 95 system, add the variable to your CONFIG.SYS file and then restart your system.
- On NT systems:

  1. Open the Windows NT Control Panel, then double-click on **System**.

2. Click on the **Environment** tab.
3. Click anywhere in the **System Environment Variable** field.
4. Type in the **Variable** field

   `NFFTCL`
5. Type in the **Value** field the value (0 or 1).
6. Select **Set**.
7. Select **Apply**.
8. Select **OK**.
9. Shutdown and restart the Netfinity Support Program.

Once you have added this environment variable, File Transfer will not use its automatic data compression capabilities under any circumstances.

Chapter 11. Power-On Error Detect

Power-On Error Detect takes full advantage of IBM's Micro Channel architecture and power-on self-test (POST) technology. When your Micro Channel system is powered on, the POST process is initiated. During POST, your Micro Channel system performs an extensive and thorough examination of the system's hardware and its configuration. This examination includes confirming that all components are working properly, and that the system's hardware configuration is the same as it was when the system was last powered-on.

If any problems or discrepancies are noted, POST generates a warning message, and then takes some appropriate action (such as starting the System Configuration utilities in the System Partition). Unfortunately, if the system's user is not present or does not know what to do once these errors have been reported, valuable time is wasted while technical personnel are notified, the problem diagnosed, and the appropriate actions are taken.

However, if a system is enabled to use the Power-On Error Detect drivers, it loads the network adapter's support program (or *driver*), and then sends an "SOS"-style message out over the network. This message includes information that positively identifies the system that is sending the message (MAC address of the system's LAN adapter, System Information, VPD if available) as well as information about the POST error that was reported. This way, you and your technical personnel are notified as soon as the problem occurs, and are simultaneously given all the information needed to diagnose the problem and prepare a solution, before you've even left your desk.

The Power-On Error Detect service receives these messages and interprets them, enabling you to quickly determine:

- Which 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 to help you with rapid problem determination and recovery, minimizing system downtime and loss of productivity.

For information on how to enable your LAN-attached systems to use the Power-On Error Detect feature during POST, see Appendix C, "Power-On Error Detect Enablement" on page 458.

The Power-On Error Detect Service Window

The Power-On Error Detect Service window contains a list of all remote POST errors and System Partition access messages that Power-On Error Detect has received (see Figure 56). POST error entries start with a red circle that contains an exclamation point; System Partition access entries start with a blue circle that contains the letter *i* (for *information*).

Note: System Partition access messages can be disabled. For more information, see "Options Pull-Down Menu Selections" on page 167.

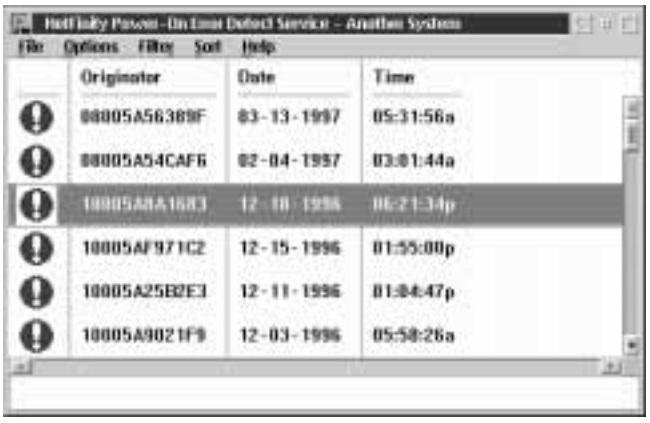

Figure 56. The Power-On Error Detect Service window

Each entry in the Power-On Error Detect Log consists of a Date, Time, and an Originator value. The Date and Time values are the date and time at which the remote POST error was reported. If the system that generated the POST error message is a system that has been discovered or added to a System Group in the Netfinity

Manager's Remote System Manager service (see Chapter 16, "Remote System Manager" on page 199), then the Originator value displayed will be the remote system's System Name. If the system that generated the POST error message is *not* a system that has been discovered or added to a System Group in the Netfinity Manager's Remote System Manager service, then the Originator value displayed will be the *media access code* (MAC) address of the network adapter card of the system that sent the remote POST error message. Use the Originator value to confirm the identity of the system that generated the POST error message.

All of the Power-On Error Detect service's functions can be accessed from the Power-On Error Detect Service window. From this window, you can:

- View information about an individual error message.

  To view more detailed information about an entry, select the entry from the Power-On Error Detect Service window. This will open the Power-On Error Detect Entry Contents window. For more information see "The Power-On Error Detect Contents Window" on page 170.

- Print the entries, clear the entries, or exit the service.

  Use the selections available from the File pull-down menu to print or clear the contents of the Power-On Error Detect Service window, or to close the Power-On Error Detect service. For more information see "File Pull-Down Menu Selections" on page 166.

- Control the Power-On Error Detect service's options.

  Use the selections available from the Options pull-down menu to control Power-On Error Detect's alert-generation, to automatically start the Power-On Error Detect interface when Power-On Error Detect messages are received, and to access message logging options. For more information see "Options Pull-Down Menu Selections" on page 167.

- Filter the contents of the Power-On Error Detect Service window.

Use the selections available from the Filter pull-down menu to configure the Power-On Error Detect Service window to display entries according to a variety of criteria. For more information see “Filter Pull-Down Menu Selections” on page 168.

- Sort the contents of the Power-On Error Detect Service window.

  Use the selections available from the Sort pull-down menu to sort the contents of the Power-On Error Detect Service window by time and date or by Originator value. For more information see “Sort Pull-Down Menu Selections” on page 169.

- Access online help.

  Use the selections available from the Help pull-down menu to access Power-On Error Detect’s online help facility.

File Pull-Down Menu Selections

Use the selections available in the File pull-down menu to:

- Close the Power-On Error Detect service.

  Select **Exit** to close the Power-On Error Detect service.

- Clear the Power-On Error Detect Service window.

  Select **Clear** to erase the contents of the Power-On Error Detect Service window.

- Print a report on the entries contained in the log.

  Select **Print Log** to print information regarding the entries currently stored in the Power-On Error Detect Log. This report can be one of two types:

  – Summary

    Select **Summary** to print a short report containing the following information on each entry in the Power-On Error Detect Service window:

    - Date reported
    - Time reported
    - Originator value
    - POST error code reported

– Full

  Select **Full** to print a detailed report of all entries in the Power-On Error Detect service window. This report will contain the following information on each entry:

  - Date reported
  - Time reported
  - Originator value
  - POST error code reported
  - Extensive system information, which will include:
    - Adapters
    - Memory
    - Hardware Error Log (if present)
    - Vital Product Data (VPD - if available)

Options Pull-Down Menu Selections

Use the selections available in the Options pull-down menu to:

- Generate Netfinity Alerts when remote POST error messages are received.

  Select **Alert on Error** to enable Power-On Error Detect to generate a Netfinity alert when a remote POST error message is received. The generated alert will be received by the 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

  For information on how to configure a response to generated alerts, see Chapter 2, “Alert Manager” on page 11.

- Automatically start the Power-On Error Detect service's graphical user's interface (GUI) when remote POST errors messages are received.

  Select **Start GUI on Error** to automatically start the Power-On Error Detect service when a remote POST error message is received.

- Log (or ignore) System Partition access messages.

  Select **Log Access Entries** if you want your Power-On Error Detect Log to include Power-On Error Detect messages that are produced when users access their System Partitions during system startup. If you want to ignore these messages, do not select the Log Access Entries option.

Filter Pull-Down Menu Selections

Use the selections available in the Filter pull-down menu to configure the Power-On Error Detect Service window to display entries according to a variety of criteria. Available selections are:

- All

  Select **All** to display all entries in the Power-On Error Detect Service window.

- Date

  Select **Date** to configure the Power-On Error Detect Service window to display remote POST errors messages received within a specified date range.

- Time

  Select **Time** to configure the Power-On Error Detect Service window to display remote POST errors messages received within a specified time range.

- Filter - Combination

  Select **Combination** to configure the Power-On Error Detect Service window to display remote POST errors messages received within a specified date range *and* within a specified time range.

- Filter - Settings

  Select **Settings** to set default date and time ranges for entries that are displayed in the Power-On Error Detect Service window. These values are used when you select the **All** filter to determine which entries to display.

  Note: The Date, Time, and Combination filters override the Settings.

Sort Pull-Down Menu Selections

Use the selections available in the Sort menu to sort the entries in the Power-On Error Detect Service window by the time and date when they were received, or by their Originator value. Available selections are:

- Date/Time

  Select **Date/Time** to sort the entries according to the date and time when they were reported. The entries can be assorted in ascending or descending order.

  – Select **Ascending** to sort the entries contained in the Power-On Error Detect Service window by date and time with the oldest entries listed first.

  – Select **Descending** to sort the entries contained in the Power-On Error Detect Service window by date and time with the newest entries listed first.

- Originator

  Select **Originator** to sort the entries in the Power-On Error Detect Service window according their Originator values. They can be sorted in ascending or descending order:

  – Select **Ascending** to sort the entries contained in the Power-On Error Detect Service window by Originator value with the lowest Originator values listed first.

  – Select **Descending** to sort the entries contained in the Power-On Error Detect Service window by Originator value with the highest Originator values listed first.

The Power-On Error Detect Contents Window

To view more detailed information about an entry, select the entry from the Power-On Error Detect Service window. This will open the Power-On Error Detect Entry Contents window (see Figure 57).

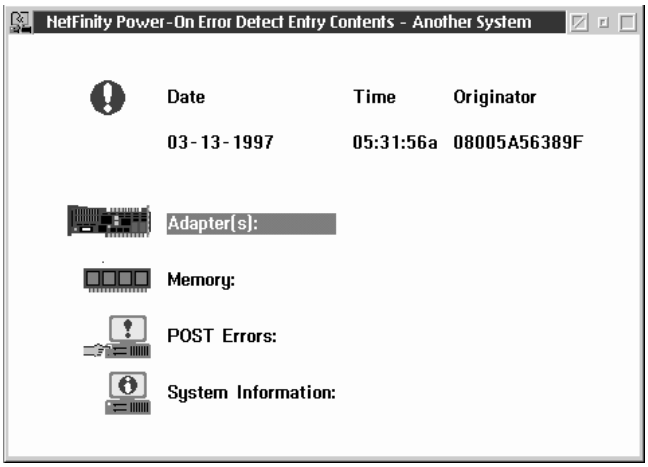

Figure 57. The Power-On Error Detect Entry Contents window

From this window, you can access detailed information about the remote POST error message that you received and the configuration of the system that sent it. You can obtain information on any of the following topics:

- Adapter information, including adapter name, slot location, actual and configured POS IDs
- Memory information, including actual and configured amounts of extended and base memory
- Hardware Error Log entries

  Note: This topic will not appear if the hardware error log is empty.
- POST Error Code number and description

  Note: This topic will not appear if the selected entry is a System Partition access message.

- System Information, including model, submodel, system board POS ID, and BIOS revision number and date, as available
- Vital Product Data (VPD)

  Note: Not all systems will provide VPD. If this information is not provided, this topic will not appear.

You can use the System Information and Vital Product Data (if available) topics to help confirm the identity of the system on your network that generated the POST Error message.

When Power-On Error Detect determines that there is a discrepancy between actual and configured values in one of these topics, it will alert you to this by displaying a red arrow beside the appropriate topic. This topic contains the information you need to diagnose and resolve the problem that caused the POST error.

Selecting a topic from this window opens a Power-On Error Detect Details window with information about the system displayed (see Figure 58).

Figure 58. The Power-On Error Detect Details window

More arrows will indicate other discrepancies between actual and configured data.

Chapter 12. Predictive Failure Analysis

Use the Predictive Failure Analysis (PFA) service to monitor all PFA-enabled disk drives installed locally on your system. With this service, you will instantly be notified when a PFA-message is generated by a PFA-enabled drive. Also, you can configure this service to automatically generate a Netfinity Alert when a PFA message is received.

Note: PFA-messages generated by PFA-enabled disk drives that are in use as part of a RAID array **cannot** be detected by the Predictive Failure Analysis service. However, PFA-messages can be monitored and reported by using the System Monitor service's attribute monitors for the PFA-enabled disk drive. For more information, see "Attribute Monitors" on page 368.

The Predictive Failure Analysis Window

Each PFA-enabled physical drive is represented by an object in the Predictive Failure Analysis window. Predictive Failure Analysis service uses two objects to help you quickly determine the status of each disk drive. These objects are:

Object	Description
Solid disk drive	Normal: The drive has not reported any predictive failure analysis messages.
Shattered disk drive	Warning: The drive has reported one or more predictive failure analysis messages and might be failing.

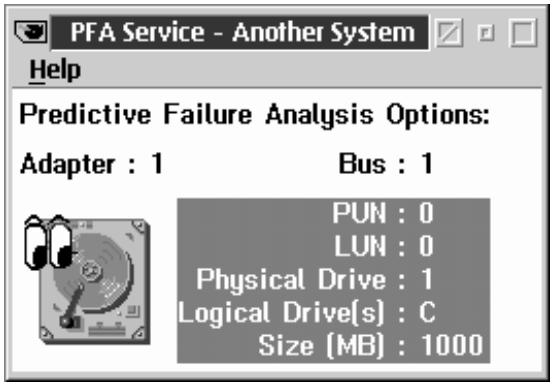

Figure 59. The Predictive Failure Analysis service. The PFA Drive shown represents a drive that has not reported any predictive failure analysis messages.

Information that will help you identify the drive is listed beside its icon. This information includes:

- Adapter

  The **Adapter** is the value of the adapter card that the disk drive is connected to.

  When Predictive Failure Analysis detects PFA-enabled hard disk drives in your system, it also scans your system for SCSI hard disk drive controllers. The **Adapter** value is the number of the SCSI adapter to which the PFA-enabled hard disk drive is attached. For example, if your system has two SCSI hard disk drive adapters installed, and each SCSI adapter has one PFA-enabled disk drive attached, you will have two PFA-enabled disk drive objects in the PFA Service window. The first PFA-drive object would have an Adapter value of 1, because it is the first SCSI hard disk drive adapter detected by Predictive Failure Analysis. The second PFA-drive object would have an Adapter value of 2, because it is the second SCSI hard disk drive adapter detected by Predictive Failure Analysis.

- PUN and LUN

  The physical unit number (PUN) and logical unit number (LUN) are values assigned to the hard disk drive to uniquely identify it within a system.

  Note: If an individual physical drive is partitioned into two or more logical drives, each logical drive will have the same PUN, LUN, and physical drive value.

- Physical Drive value

  The **Physical Drive** value is a numeric value assigned to each hard disk drive in your system. These values begin with 0 and increase with each additional hard disk drive installed (for example, if you have two hard drives in your system, their Physical Drive values will be 0 and 1).

- Logical Drive values

  The **Logical Drive** value is a letter assigned to each hard disk drive or partition you create on a hard disk drive. For example, if you have a 1 GB* drive, and you divide this drive into 5 partitions of 200 MB each, they will have **Logical Drive** values of C, D, E, F, and G. However, each **Logical Drive** will share the same PUN, LUN, and Physical Drive values.

- Size

  The **Size** value is the capacity of the physical drive.

  Note: **Size** does *not* represent space remaining on the individual drive.

To obtain more detailed information on an individual PFA-enabled drive, or to configure Predictive Failure Analysis service options for an individual drive, select the drive from the Predictive Failure Analysis window. This will open the PFA Options for Drive window (see Figure 60 on page 175).

* When referring to hard-disk-drive capacity, GB means 1 000 000 000 bytes; total user-accessible capacity may vary depending on operating environment.

The PFA Options for Drive Window

Use the PFA Options for Drive window to view additional information about the selected PFA-enabled drive, and to configure Predictive Failure Analysis service options specific to the selected drive.

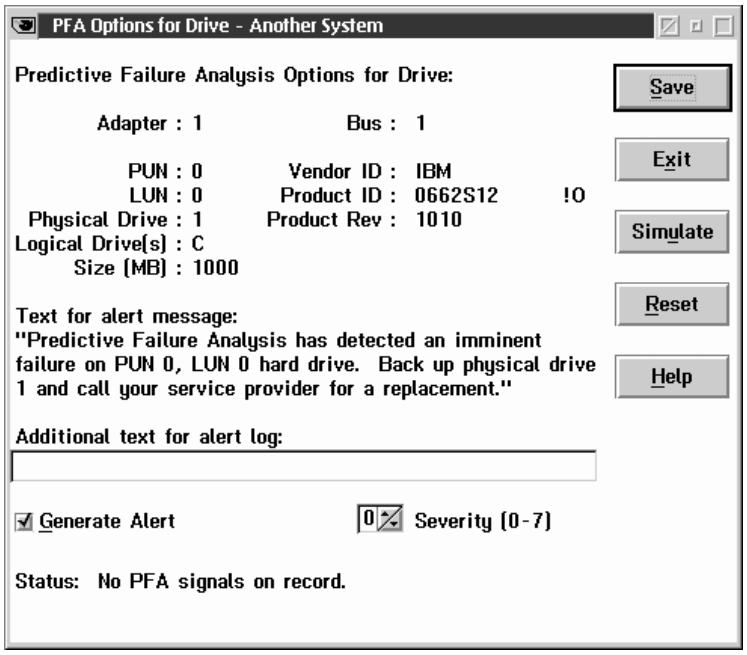

Figure 60. The PFA Options for Drive window

Detailed Disk Drive Information

The PFA Options for Drive window duplicates the drive-specific information from the Predictive Failure Analysis window, and also provides the following additional information:

- Vendor ID

  The Vendor ID is the name of the drive manufacturer reported by the disk drive.

- Product ID

  The Product ID is the drive-specific product number reported by the disk drive.

- Product Revision

  The Product Revision is the product revision level reported by the disk drive.

- Status

  The Status shows the most recent information reported by the disk drive. If a PFA message has been generated by the disk drive, the Status data will show the day, date, and time at which the PFA message was generated.

Predictive Failure Analysis Options

In addition to providing detailed drive information, the PFA Options for Drive window enables you to:

- Configure Predictive Failure Analysis' alert generation options for this drive.
- Simulate a Predictive Failure Analysis warning message for this drive.
- Reset the drive from "Warning" status to "Normal" status.

Generating Alerts

Select the **Generate Alert** check box to enable Predictive Failure Analysis to generate a Netfinity alert whenever this disk drive generates a Predictive Failure Analysis message. You can customize some of the alert-specific information.

- Alert Text

  The standard Alert Text that will appear in the generated alert appears in the center of the window. If you would like to add information to this text, type it in the **Additional text for alert log** field.

- Severity

  Use the spin buttons beside the **Severity** field to set the alert severity value. This value can be an integer from 0 (most severe) to 7 (least severe).

Simulating a Predictive Failure Analysis Message

To simulate a Predictive Failure Analysis failure warning message for this drive, select **Simulate**. The Predictive Failure Analysis service will behave exactly as if an actual warning message had been received (it will change the drive status in the Predictive Failure Analysis window and in the PFA Options for Drive window, and will generate an alert if **Alert Generation** is selected). However, both the Status reported in the PFA Options for Drive window and the Alert Text will state that the PFA message was simulated and was not caused by a real PFA message.

Resetting a Drive's Status

Select **Reset** to change the drive's status from "Warning" to "Normal."

Chapter 13. Process Manager

You can use the Netfinity Process Manager service to view detailed information about all processes that are currently active on a system. With Process Manager, you can execute commands on the system, halt individual processes, and monitor any process that you've specified, generating a Netfinity Process Alert if the process starts, stops, or fails to start within a specified amount of time from startup.

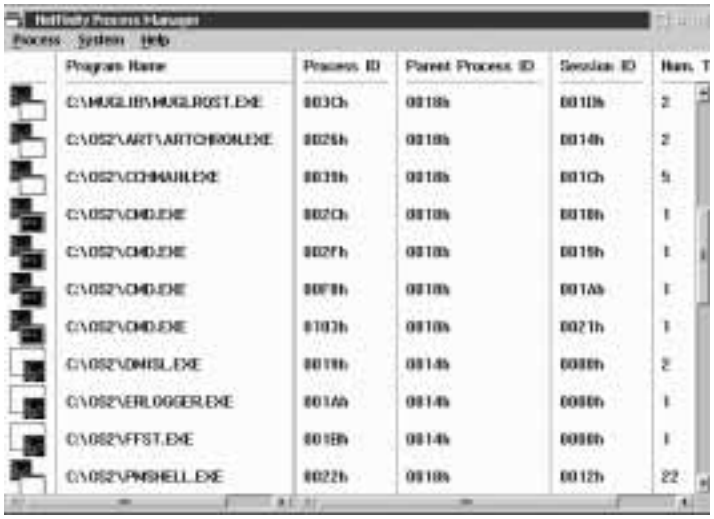

Figure 61. The Process Manager window

Gathering Process Information

When you start Process Manager on your system or on a remote system, it will immediately gather information about all currently active processes on the system. This information is then displayed in the Process Manager window (see Figure 61). Each process is signified by an icon depicting the type of process that is running (OS/2 window or full screen, Presentation Manager application, Windows application, 32-bit Windows application, NetWare Loadable Module (NLM), or DOS session), followed by data specific to the session type. The following information is available for each process:

- Program Name (all operating systems)

  The name of this process, as well as the fully qualified path (if applicable) showing where the program resides on the system.

- Process ID (OS/2, Windows, Windows 95, and Windows NT)

  The operating system's internal identification value for this process.

- Parent Process ID (OS/2, Windows)

  The operating system's internal identification value for the process or program that started this process.

- Number of Threads (OS/2, NetWare, and Windows NT)

  The number of program threads that this process is using.

- Priority (Windows 95 and Windows NT only)

  The relative importance of the process with regard to receiving attention from the system’s processor.

- Session ID (OS/2 only)

  The operating system’s internal identification value for the session that is supporting this process.

- User ID (Windows NT only)

  The logon ID of the user that started the process.

- Description (NetWare only)

  A brief description of the NLM.

- Version (NetWare only)

  The NLM version number.

- Date (NetWare only)

  The date of the NLM.

Notes:

1. Available information about the process depends on the type of process and the operating system under which the process is running.
2. Windows and DOS processes running under OS/2 or Windows NT will appear as DOS sessions.

Running Commands

You can use Process Manager to send individual commands to the Netfinity system that you are accessing. Unlike the Remote Session service, Process Manager can issue only a single command at a time, and you will not receive any feedback or confirmation messages.

To run a command:

1. Select **Run command...** from the Process Manager window's **Process** pull-down menu.
2. Type in the **Enter command line to be executed** field the command that you want to execute on this system.
3. Select **Run** to execute the command.

Select **Cancel** at any time to close the Run Command window without executing a command.

Halting Processes

Attention:
Use Process Manager's process-halting capabilities carefully. With Process Manager, you can halt almost any process that is running on a system. Irresponsible use of Process Manager can result in loss of data and could halt the operating system.

The method by which a process is halted depends on the operating system that the process is running under. For more information

about the operating system, select **Operating System Information** from the System pull-down menu.

To halt a process that is running on a system:

1. Select from the Process Manager window the process that you want to halt.
2. Select **Process** from the Process Manager window's menu bar, or use mouse button 2 on the selected process to open the process's pop-up menu.
3. Select the appropriate halt process action for the system's operating system.
   - If the system is running OS/2, you can select one of three process halting actions:
     - Select **Send Ctrl+C** to send a Ctrl+C command to the selected process.
     - Select **Send Ctrl+Break** to send a Ctrl+Break command to the selected process.
     - Select **Send Kill Process** to send a Kill Process command to the selected process.

     Most processes will respond to a Ctrl+C command and will close gracefully. However, some programs will ignore Ctrl+C commands, and you will need to use a Ctrl+Break to halt them. If the process does not respond to Ctrl+C or Ctrl+Break, use the Kill Process command. The Kill Process command will halt most any OS/2 process.
   - If the system is running Windows, select **Close Application** to halt the selected process.
   - If the system is running NetWare, select **Send Unload Module** to halt the selected process.

Process Alerts

Process Manager can generate a Netfinity alert when any specified process:

- Starts running

- Stops running
- Fails to start running within a specified amount of time after system startup

To configure Process Manager to generate an alert when a process starts, stops, or fails to start, select **Process Alerts...** from the Process pull-down menu. This opens the Process Alerts window. The Process Alerts window contains in the **Alert conditions** field a list of all currently configured Process Manager Alert conditions. Each **Alert condition** includes the name of the process that will trigger a Netfinity Process Alert, and the conditions under which the alert will be generated.

From the Process Alerts window, you can:

- **Add** a Process Alert.
- **Edit** a Process Alert.
- **Delete** a Process Alert.

Adding a Process Alert

Select **Add** to open the Add Process Alert window. In this window you can configure a Process Alert for a specific process that will generate a Netfinity Alert whenever the process:

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

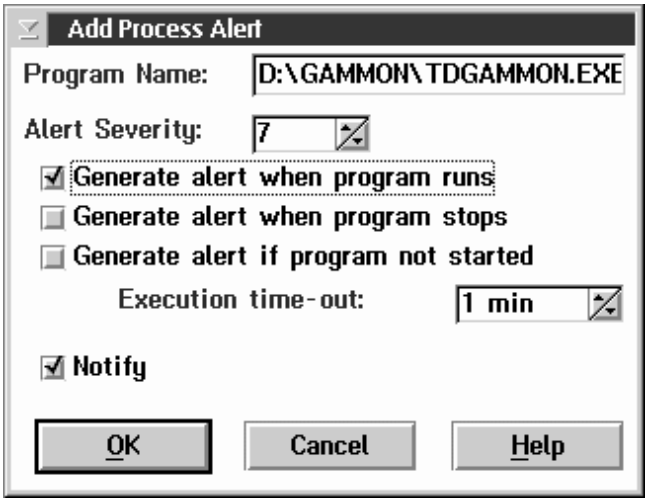

Figure 62. Process Manager — The Add Process Alert window

To add a new Process Alert:

1. Type in the **Program Name** field the name of the process that you want to monitor.
   - If you want to monitor a specific process that is run from a specific directory, type in the fully qualified path where the program resides (for example, C:\APP\PROGRAM.EXE).
   - If you want to monitor any process with a specific name, type in only the name of the program (for example, PROGRAM.EXE).
2. Type in the **Alert Severity** field a severity value for the Netfinity Alert that will be generated by Process Manager.
3. Select one (or more) **Generate alert** check boxes.
   - Select **Generate alert when program runs** to generate an alert if the specified process is started.
   - Select **Generate alert when program stops** to generate an alert if the specified process is stopped.
   - Select **Generate alert if program not started** to generate an alert if the specified process does not start within a specified amount of time after system startup. The amount of time

that Process Manager will wait before generating the alert is specified in the **Execution timeout** field.

4. Select **Notify** to have this alert forwarded directly to your system's Alert Manager (optional).

   This is important if your are configuring this alert on a remote system and want your system to receive the alert that is generated for the Process Alert.

5. Select **Local Notify** to have this alert generated locally on the system (optional).

   This is important if your are configuring this alert on a remote system and want the user of that sysem to receive the alert that is generated for the Process Alert.

6. Select **OK** to save this Process Alert.

Select **Cancel** at any time to close the Add Process Alert window without saving any changes.

Editing a Process Alert

To edit a previously configured Process Alert:

1. Select from the Process Alert window's **Alert condition** field the name of the Process Alert that you want to edit.
2. Select **Edit** to open the Edit Process Alert window.
3. Change the configuration of the selected Process Alert.
4. Select **OK** to save your changes.

Select **Cancel** at any time to close the Edit Process Alert window without saving any changes.

Deleting a Process Alert

To delete a previously configured Process Alert:

1. Select from the Process Alert window's **Alert condition** field the name of the Process Alert that you want to delete.
2. Select **Delete**.

Chapter 14. RAID Manager

RAID (*redundant array of independent disks*) is a technology whereby several physical storage devices are grouped into an array that appears to the operating system as one or more physical drives. Using RAID technology, you can configure the RAID array drives into a variety of data configurations. These configurations (called *RAID levels*) provide varying levels of data-integrity protection and storage capacity. Some RAID levels provide greater data integrity through the use of data mirroring.

Ordinarily, you must take your RAID system offline in order to perform most RAID management tasks. However, with Netfinity's RAID Manager service, you can easily gather information about your system's RAID adapter, physical drives in the array, and virtual drives that are defined by the array. You can also perform a variety of important RAID management tasks quickly and easily. These tasks include:

- Scrubbing virtual drives
- Formatting and rebuilding RAID physical devices
- Gathering data about all RAID adapters, devices, virtual drives, and enclosures

Notes:

1. Irresponsible use of RAID Manager can seriously harm your system and its data. Use RAID Manager only if you are familiar with RAID arrays and RAID systems management.
2. RAID Manager is not designed to operate simultaneously with other RAID management utilities. Running other RAID management utilities while running RAID Manager may cause your system to become unstable.
3. This service is available for use only on systems that have a supported RAID adapter installed. For a list of supported RAID adapters, see Appendix E, "Supported RAID Adapters" on page 462.

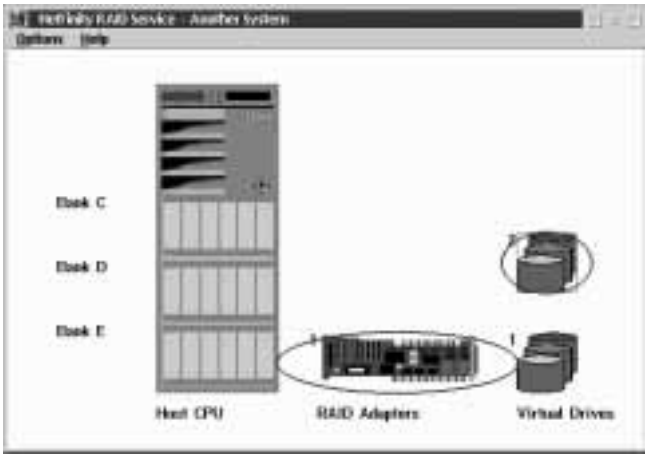

Figure 63. The RAID Manager service

RAID Manager Window Options

The RAID Manager window shows a graphical representation of your RAID system enclosure, RAID adapters, and logical disk drives. You can:

- Change the scale of the graphical representations
- Change the number of virtual drives that are shown in each column
- Change the enclosure configuration
- Refresh the current information

Changing the Viewing Scale

To change the scale of the graphics shown in the RAID Manager window:

1. Select **Viewing Scale** from the Options pull-down menu.
2. Use the spin buttons to select a scale for the RAID Manager graphics.
3. Select **OK** to apply this change.

The RAID Manager graphics are resized according to the scale you have specified.

Changing the Virtual Drives Representation

To change the number of virtual drives shown per column:

1. Select **Virtual Drive Representation** from the Options pull-down menu.
2. Use the spin buttons to select the number of virtual drives that will be shown in each column.
3. Select **OK** to apply this change.

The number of virtual drives in each column will be adjusted according to the value you selected.

Changing the Enclosure Configuration

Select **Enclosure Configuration** from the Options pull-down menu to open the Enclosure Configuration window (see Figure 64 on page 188). From this window, you can:

- Add an enclosure
- Delete an enclosure
- Configure the bank and adapter configuration for your enclosures
- Configure the device numbers for each bank in your enclosures

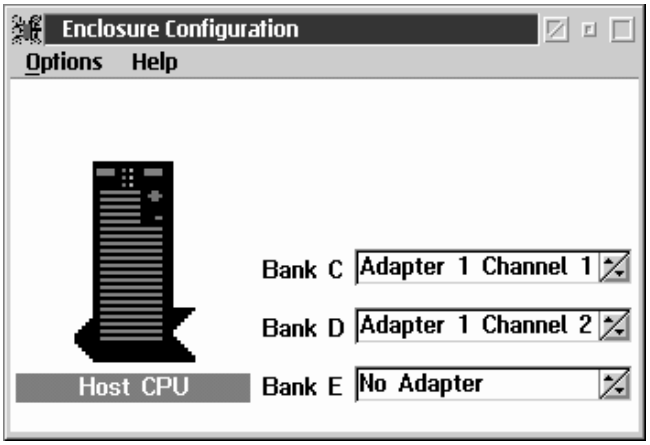

Figure 64. The Enclosure Configuration window

Adding an Enclosure

To add an enclosure:

1. Select **Enclosure Configuration** from the Options pull-down menu in the RAID Manager window.

   This opens the Enclosure Configuration window.

2. Select **Add Enclosure** from the Options pull-down menu in the Enclosure Configuration window.

   This opens the Select Enclosure window (see Figure 65 on page 189).

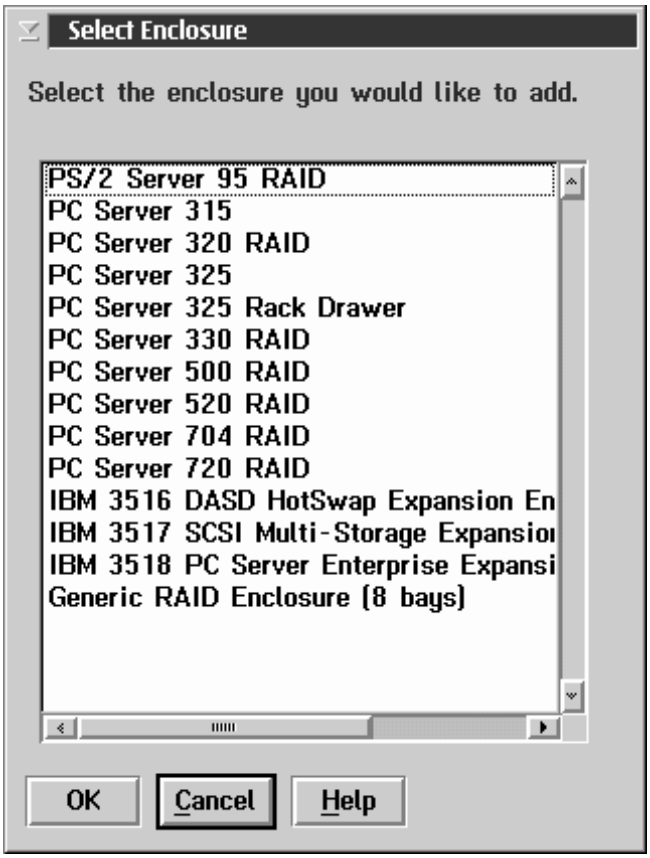

Figure 65. The Select Enclosure window

3. Select the name of the enclosure you want to add.
4. Select **OK**.

Deleting an Enclosure

To delete an enclosure:

1. Select **Enclosure Configuration** from the Options pull-down menu in the RAID Manager window.

   This opens the Enclosure Configuration window.

2. Using mouse button 2, select the enclosure that you want to delete.

This opens a context menu for the elected enclosure.

3. Select **Delete Enclosure** from the context menu.

Configuring RAID

To specify which RAID adapter controls which bank of RAID drives in your enclosure:

1. Select **Enclosure Configuration** from the Options pull-down menu in the RAID Manager window.

   This opens the Enclosure Configuration window.

2. Use the spin buttons beside each **Bank** field to specify which adapter and channel controls the bank.

3. When you have finished configuring the enclosure bank, close the Enclosure Configuration window to save your new settings.

Configuring RAID Bank Device Numbers

To specify the device numbers for each RAID device in a selected bank:

1. Select **Enclosure Configuration** from the Options pull-down menu in the RAID Manager window.

   This opens the Enclosure Configuration window.

2. Select the **Bank** field for the bank that contains the devices for which you want to specify a device number configuration.

3. Select **Configure Device Numbers** from the Options pull-down menu.

   This opens the Device Number Configuration window (see Figure 66 on page 191).

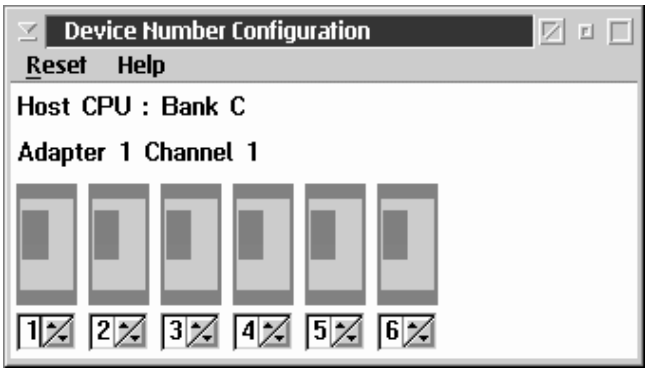

Figure 66. The Device Number Configuration window

4. Use the spin buttons associated with each device in the bank to specify a device number for that device.
5. When you have finished configuring the device numbers, close the Device Number Configuration window to save your new settings.

Refreshing RAID Information

Select **Refresh** from the Options pull-down menu to update all information displayed in the RAID Manager window.

Viewing RAID Information

You can use RAID Manager to view general information on your RAID system's devices, including the RAID enclosure, physical RAID devices, RAID adapters, and logical RAID drives.

Viewing Enclosure Information

Use RAID Manager to quickly gather information about any RAID enclosures attached to this system. Available information includes:

- Enclosure model
- Enclosure manufacturer
- Number of RAID adapters
- Enclosure function

To view information about a RAID enclosure:

1. Use mouse button 2 to select the enclosure that you want to examine. This opens the enclosure's context menu.
2. Select **View Enclosure** from the enclosure's context menu.

Select **OK** to close the Enclosure Information window.

Viewing Physical Device Information

Use RAID Manager to gather a variety of information about the physical devices that are part of your RAID array. Available information includes:

- Device status
- Device number
- Channel number
- Device type
- Device size
- Sectors
- Manufacturer
- Model, version
- Serial number

To view information about a physical RAID device:

1. Use mouse button 2 to select the device that you want to examine. This opens the adapter's context menu.
2. Select **View Device** from the device's context menu.

Select **OK** to close the Standard Device Information window.

Viewing General Adapter Information

Use RAID Manager to quickly gather information about any installed RAID adapters. Available information includes:

- Adapter identifier
- Slot
- Buses available
- Configured devices
- Device I/O
- Host bus

- Adapter status
- Manufacturer
- Model
- Serial number (if available)

To view information about a RAID adapter:

1. Use mouse button 2 to select the adapter that you want to examine. This opens the adapter's context menu.
2. Select **View Adapter**.
3. Select **General Info**.

Select **OK** to close the Adapter Information window.

Viewing Adapter-Specific Information

Use RAID Manager to quickly gather more detailed information about any installed RAID adapters. Available adapter-specific information includes:

- Stripe size
- Rebuild control
- Parity storage
- Read Ahead

To view adapter-specific information:

1. Use mouse button 2 to select the adapter that you want to examine. This opens the adapter's context menu.
2. Select **View Adapter**.
3. Select **Specific Info**.

Select **OK** to close the Adapter-Specific Information window.

Viewing Virtual Drive Information

Use RAID Manager to quickly gather information about any virtual drives defined by your RAID adapters. Available information includes:

- Virtual drive number
- Virtual drive size

- Virtual drive status
- Virtual drive RAID level
- Virtual drive write policy

To view information about a virtual drive:

1. Use mouse button 2 to select the virtual drive that you want to examine. This opens the virtual drive's context menu.
2. Select **View Virtual Drive Information**.

Select **OK** to close the Virtual Drive Information window.

RAID Device Management

Use RAID Manager to manage the storage devices that make up your RAID array. Use RAID Manager to:

- Add a device
- Remove a device
- Replace a device
- Rebuild a device
- Rebuild to another device
- Stop a device
- Set a device to standby
- Set a device to Hot Spare

To perform any of these RAID device management functions, use mouse button 2 to select the RAID device from the RAID Manager window, and then select the RAID Management function from the selected device's pop-up menu.

RAID Adapter Configuration Backup

You can use RAID Manager to back up the configuration of your RAID adapter. To back up your RAID adapter configuration:

1. Use mouse button 2 to select the adapter you want to back up.
2. Select **Backup Configuration** from the adapter's context menu.
3. Insert a blank, formatted diskette and select **OK**.

RAID Virtual Drive Management

Use RAID Manager to alter a variety of virtual drive parameters. The following logical drive management options are available:

- Initialize virtual drives
- Scrub virtual drives

Initializing Virtual Drives

Select **Initialize** to write binary zeroes to all bits on the logical drive and recompute proper parity information. This operation is required for RAID Level 1 and RAID LEvel 5 virtual drives.

Note: This feature is not available on RAID systems running NetWare.

Scrubbing Virtual Drives

Select **Scrub** to recompute the parity information on a RAID Level 1 or RAID Level 5 virtual drive. The data on the drive is not changed.

Chapter 15. Remote Session

Using the Remote Session you can establish a fully active, remote command-line window session with a client system. The Remote Session window session is capable of all command-line functions that are available under the remote system's operating system, allowing for significant remote system management and troubleshooting capabilities.

Notes:

1. Remote Session returns only standard text. If you enter a command that starts a graphic application on the remote system, your Remote Session will appear to "hang." If this occurs, close the Remote Session window and begin again.
2. Remote Session is a *remote only* service. This service will be available for use only when you are accessing a remote system. The Remote Session service object will *not* appear in your local Service Manager.
3. Remote Session performs somewhat differently when used to access a remote NetWare server. For more information, see "Remote Session on NetWare Systems" on page 198.

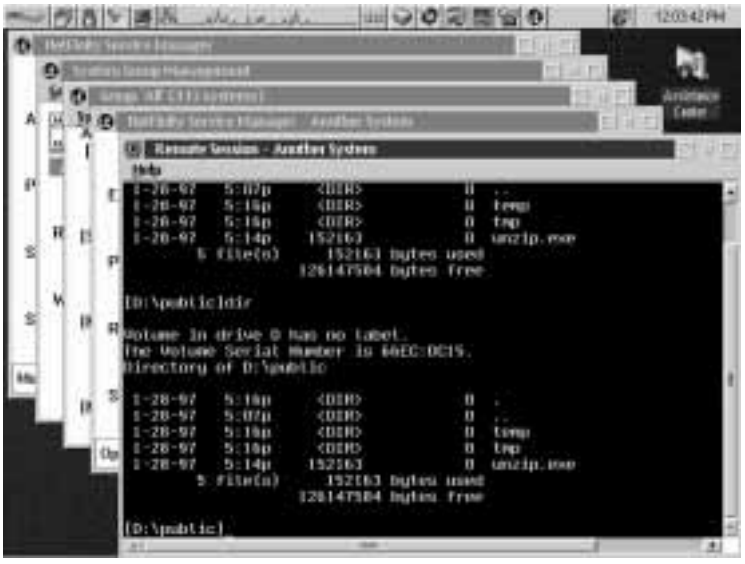

Figure 67. Remote Session

Remote Session on OS/2 and Windows Systems

When you are using Remote Session on a system running Client Services for Netfinity Manager for OS/2, Client Services for Netfinity Manager for Windows, Client Services for Netfinity Manager for Windows 95, or Client Services for Netfinity Manager for Windows NT, all local keystrokes are passed through to the remote system. However, some keystroke combinations are available for your system. These combinations are:

Keystroke	Result
[Alt+Esc]	Switches to the next open window, full-screen session, or object that is minimized on the Desktop.
[Alt+Shift+Tab]	Makes the Desktop window active.
[Ctrl+Alt+Del]	Restarts the operating system on the local system.
[Ctrl+Esc]	Displays the Window List on the local system.
Print Screen	If you are running OS/2, this prints the contents of the remote window to the default local printer. If you are running Windows 95 or Windows NT, this copies the contents of the window to the clipboard.

Note: The effect that these keystroke combination will have on the remote system is dependent on the remote system's operating system.

Keystrokes within the Remote Session, other than those listed, are treated as they would be under the remote system's default command shell. If the remote system is running OS/2 or Windows NT, the default command shell is CMD.EXE. If the remote system is running Windows 3.1 or Windows 95, the default command shell is the remote system's DOS COMMAND.COM. For more information, see the OS/2 *User's Guide* or the Windows *User's Guide*.

Remote Session on NetWare Systems

Using Remote Session you can take over the System Console of a remote NetWare server. This function is similar to the remote console capabilities of the RCONSOLE.EXE utility included with NetWare. You can use Remote Session to load and unload NLMs remotely, and to check the status of all currently available screens.

Remote Session will pass all standard alphanumeric keystrokes through to the remote NetWare server. However, only the following key combinations will be passed through:

Alt+F3 Switches to the **next** NetWare screen. The Plus (+) key on your numeric keypad will perform the same function.

Alt+F4 Switches to the **previous** NetWare screen. The Minus (-) key on your numeric keypad will perform the same function.

Note: Remote Session cannot pass through the Ctrl+Esc keystrokes that would ordinarily bring up the NetWare Current Screens list. You cannot access the Current Screen list with Remote Session.

Chapter 16. Remote System Manager

You can use Netfinity Remote System Manager to link with and remotely access Netfinity services installed on systems within your network.

Remote systems are divided into *system groups*. For example, a network administrator could create a system group named "Development" for all systems used by software developers.

Individual systems are then added to these system groups using an informal System Name (for example, "John's System"), Network Type (any system-supported and configured communication protocol, including NetBIOS, IPX, and TCP/IP), and the Network Address of the system.

The Remote System Manager also features a keyword-based *discovery* process. This *discovery* process uses preassigned keywords to identify Netfinity systems on your network. With the discovery process, you can add multiple systems to a system group based solely on these keywords. In addition to user-defined keywords, Netfinity features many automatically defined keywords that can help simplify system organization. All systems running Netfinity Manager or Client Services for Netfinity Manager version 5.0 or later will automatically respond to predefined keyword strings that describe specific system configurations, use of a specified communications protocol or operating system, and the availability of specified Netfinity services. For information on automatically defined keywords, see "Automatically Defined Keywords" on page 212. For more information on keyword assignment and the discovery process, see "Using the Discovery Process" on page 224.

If remote systems are installed in a rack-mounting unit (such as the IBM PC Server Rack), you can define *rack groups* that contain only systems that are mounted in specified server rack units. A rack group uses information contained in the rack configuration file (a file with an *.rk$ file extension; the file must be in the root directory of any hard disk drive in a rack-mounted system) to selectively add to a group only systems that have certain rack-specific information associated with them. The rack configuration file can be created using a system-configuration program such as the PC Server Rack Configurator, or you can create the file using a text editor.

Rack-specific information that can be used to define a rack group includes rack name, rack ID, rack suite name, rack suite ID, rack collection name, and rack collection ID. For more information see "Creating a Rack Group" on page 203.

If your network includes systems running Windows NT Server 4.0 Enterprise Edition in a cluster configuration, you can define *cluster groups* that contain only systems that are part of a specified cluster. Each cluster must have a unique cluster name, and systems that are part of the cluster will be identified and discovered using this unique cluster name. For more information, see "Creating a Cluster Group" on page 205.

System, Rack, and Cluster Groups

Netfinity Remote System Manager organizes all Netfinity remote systems into groups. Three types of groups are available for your use: *system groups*, *rack groups*, and *cluster groups*.

A *system group* is a group of individual, network-attached systems that can be accessed, managed, and monitored by the Remote System Manager. Individual systems can be added to a system group by using either of the following two methods:

- Enter the system name, network address, and network type.
- Use the discovery process, which uses assigned system keywords.

A *rack group* is a group of systems that are installed in a rack-mounting unit such as the IBM PC Server Rack. Rack-mounted systems can be configured to include a rack configuration file. This file contains information regarding the name of the rack, location of the system within the rack, name of the rack collection suite that the rack is part of, and so forth. If this file is present on a system that has Netfinity installed, Netfinity will use the information contained in this file to identify rack-mounted systems and group them in user-defined rack groups. Using rack groups, you can specify that only systems that are configured for inclusion in a rack-mounting unit can appear in the group. Otherwise, systems included in a rack group behave exactly like systems included in a system group.

A *cluster group* is a group of systems running Windows NT Server 4.0 Enterprise Edition that a in a cluster configuration. All systems in a cluster use a common, unique *cluster name* to identify themselves as part of a specific cluster. Using cluster groups, you can specify that only systems that are configured for inclusion in a specific cluster can appear in the group. Otherwise, systems included in a cluster group behave exactly like systems included in a system group.

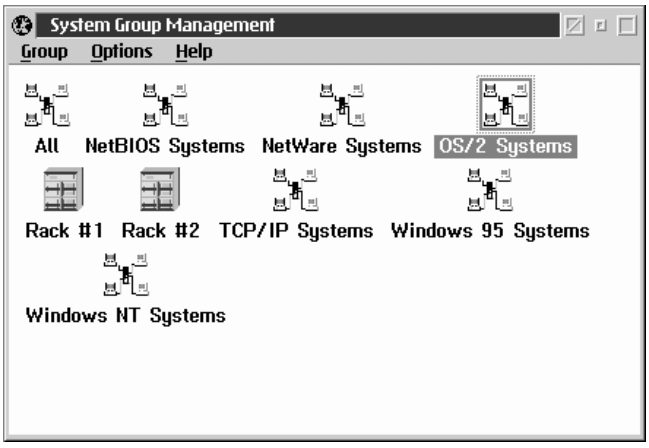

Figure 68. Remote System Manager — System Group Management Window

Creating a System Group

You can create as many or as few system groups as you need. Each system group has its own user-defined name, and can have its own system-discovery conditions and system-group keywords to control the addition of remote systems during the discovery process. The name of the system group is for your reference, and has no effect on Remote System Manager's functions. System discovery conditions are discussed in greater detail in "Using the Discovery Process" on page 224.

To create a system group:

1. Start the Remote System Manager by selecting its object from the Netfinity Service Manager.

2. Select the **Add Group** option from the Group pull-down menu.
3. Choose a name for the system group and enter it in the **Group Name** field.

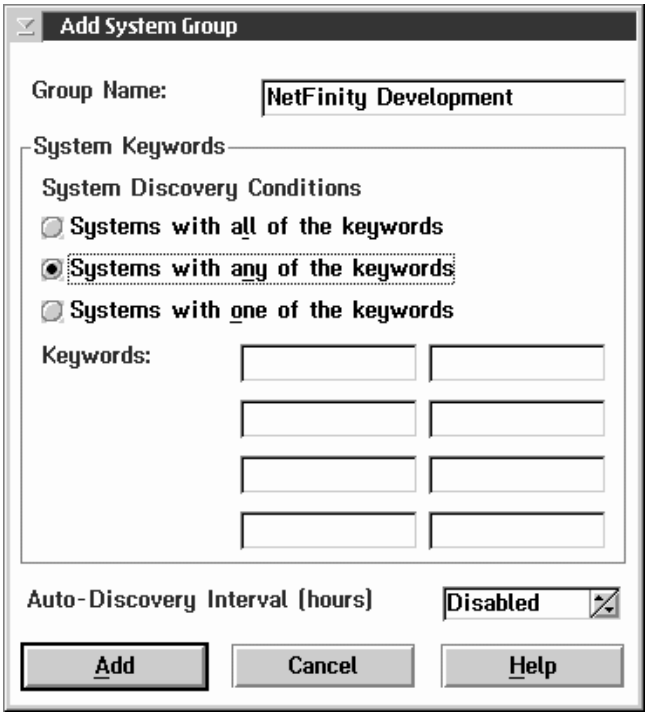

Figure 69. Remote System Manager — Add System Group Window

4. Select a **System Discovery Condition**. There are three to choose from:
   - Systems with all of the keywords
   - Systems with any of the keywords
   - Systems with only one of the keywords
5. Enter one or more keywords. These will determine what remote systems are to be added to the system group you are creating.
6. Specify an auto-discovery interval (optional). Use the spin buttons beside the **Auto-Discovery Interval** field to specify the amount of time between auto-discovery attempts. Using

auto-discovery, you can automatically add new Netfinity systems to your system groups. Auto-discovery is disabled by default.

7. Select **Add** to create the system group. This returns you to the System Group Management window. A system group object with the system group name that you specified now appears in the System Group Management window.

Next, you must add remote systems to the system group. This can be done in one of two ways. You can add an individual system, or you can use the Remote System Manager discovery process to add all remote systems that fit the system group's system discovery condition. To add individual systems, see "Adding Individual Systems to a System or Rack Group" on page 206. To add systems using the discovery process, see "Using the Discovery Process to Add Multiple Systems" on page 207.

Creating a Rack Group

You can create as many or as few rack groups as you need. Each rack group has its own user-defined name and can include one or more rack-specific identifiers. These identifiers are used to control the addition of remote systems during the discovery process. Only the rack-mounted units that match the identifiers are included in a rack group. The name of the rack group is for your reference, and has no effect on Remote System Manager's functions. System discovery conditions are discussed in greater detail in "Using the Discovery Process" on page 224.

To create a rack group:

1. Start the Remote System Manager by selecting its object from the Netfinity Service Manager.
2. Select the **Add Rack Group** option from the Group pull-down menu.
3. Choose a name for the rack group and enter it in the **Group Name** field.
4. Specify one or more rack attributes.

Each rack attribute corresponds to an entry in the rack configuration file. The rack configuration file is a file with an *.rk$ extension; the file must be located in the root directory of any hard disk drive of a rack-mounted unit. This file contains information about the rack in which the system is mounted and is created either by using a configuration file generation program (such as the PC Server Rack Configurator) or by using a text editor and placing one or more rack attribute definitions in the file.

The available rack attributes are:

Rack Name
Name string defined for the rack associated with the rack group. This attribute corresponds to the

`RACKNAME="name"`

entry in the rack configuration file on the system.

Rack ID ID string defined for the rack associated with the rack group. This attribute corresponds to the

`RACKID=ID_number`

entry in the rack configuration file on the system.

Rack Suite Name
Name string defined for the rack suite associated with the rack group. This attribute corresponds to the

`SUITENAME="name"`

entry in the rack configuration file on the system.

Rack Suite ID
ID string defined for the rack suite associated with the rack group. This attribute corresponds to the

`RACKSUITE=ID_number`

entry in the rack configuration file on the system.

Rack Collection Name
Name string defined for the rack collection associated with the rack group. This attribute corresponds to the

COLLECTIONNAME="*name*"

entry in the rack configuration file on the system.

Rack Collection ID

ID string defined for the rack collection associated with the rack group. This attribute corresponds to the

SUITECOLLECTION=*ID_number*

entry in the rack configuration file on the system.

Only systems that match **all** defined rack attributes can be added to the rack group.

5. Specify an auto-discovery interval (optional). Use the spin buttons beside the **Auto-Discovery Interval** field to specify the amount of time between auto-discovery attempts. Using auto-discovery, you can automatically add new Netfinity systems to your system groups. Auto-discovery is disabled by default.
6. Select **Add** to create the rack group. This returns you to the System Group Management window. A rack group object with the rack group name that you specified now appears in the System Group Management window.

Creating a Cluster Group

You can create as many or as few cluster groups as you need. Each cluster group has its own user-defined name and uses a unique cluster name to control the addition of remote systems during the discovery process. Only the clustered systems that match the unique cluster name are included in a cluster group. The name of the cluster group is for your reference, and has no effect on Remote System Manager's functions. System discovery conditions are discussed in greater detail in "Using the Discovery Process" on page 224.

To create a cluster group:

1. Start the Remote System Manager by selecting its object from the Netfinity Service Manager.

2. Select the **Add Cluster Group** option from the Group pull-down menu.
3. Choose a name for the cluster group and enter it in the **Group Name** field.
4. Type in the **Cluster Name** field the unique cluster name that is used by all systems included in the cluster.

   Only systems that are part of the uniquely named cluster can be added to the cluster group.
5. Specify an auto-discovery interval (optional). Use the spin buttons beside the **Auto-Discovery Interval** field to specify the amount of time between auto-discovery attempts. Using auto-discovery, you can automatically add new Netfinity systems to your system groups. Auto-discovery is disabled by default.
6. Select **Add** to create the cluster group. This returns you to the System Group Management window. A cluster group object with the cluster group name that you specified now appears in the System Group Management window.

Adding Individual Systems to a System or Rack Group

To add an individual remote system to the system group:

1. Open a system group.

   Double-click on the system group to which you are adding the individual system.
2. Select **Add System** from the System pull-down menu.
3. Type a name for the system in the **System Name** field. This name is for your reference only.
4. Enter a network address for the remote system in the **Network Address** field. This must be the network address for the network protocol you will be using.
5. Select a network type from the supported network protocols listed in the **Network Type** selection list.
6. When you are satisfied with the information you have entered, select **Add** to add the system to the system group. This closes

the Add System window and returns you to the Group window. An object representing the system has been added to the Group window. If the system is not online, the object will be colored light gray. If the system is online, you can access it by double-clicking on the object.

The Group window has two View Settings that can be selected from the Group window's View pull-down menu. For more information see "Group View Settings" on page 214.

Using the Discovery Process to Add Multiple Systems

To add multiple systems to the system group using the Remote System Manager discovery process:

1. Open a system group.

   Double-click on the system group to which you are adding the individual system.

2. Select **Discover Systems** from the System pull-down menu.

   Once Discover Systems is selected, Netfinity Remote System Manager sends a short message out over your network, using your enabled communications drivers. This message commands all Netfinity systems on your network that have the correct keywords to respond.

   The remote systems that have the correct keywords then send a response to the system that initiated the discovery process. This response contains all of the information necessary to add the individual system to the system group (system name, network address, and network type). The individual remote systems are then automatically added to the system group. Objects representing each of the remote systems then appear in the System Group window, sorted alphabetically by System Name. This entire process takes approximately 45 seconds to complete.

   The discovery process is discussed in greater detail in "Using the Discovery Process" on page 224.

   The Group window has two View Settings that can be selected from the Group window's View pull-down menu. For more information see "Group View Settings" on page 214.

Discovering Systems in Remote TCP/IP Subnets

If you are using the TCP/IP protocol driver, Remote System Manager will discover remote Netfinity systems using TCP/IP only on your TCP/IP subnet. If you want to discover Netfinity systems in other TCP/IP subnets, you must create a text file named TCPADDR.DSC in your Netfinity directory. This file must contain the following information in the format shown:

```
tcpipaddress subnetmask
```

where *tcpipaddress* is the numeric TCP/IP address of **one** Netfinity system in the remote subnet, and *subnetmask* is the TCP/IP subnet mask for the remote subnet. For example:

```
200.100.50.25 255.255.240.0
```

The space between the TCP/IP address and the subnet mask is required. The TCPADDR.DSC can contain multiple subnet entries.

Discovering Other Systems Using SNA

The SNA protocol does not support broadcasting of messages in the manner that TCP/IP, NetBIOS, and IPX do. For a system to communicate with other remote systems using SNA, the SNA stack must be configured with the remote system's SNA-specific address. Because of this, if your system is using the SNA protocol to communicate with remote systems the auto-discovery process will discover only those remote systems that your SNA stack has been configured to communicate with. For SNA stack configuration information, see the documentation that came with your SNA stack.

Dynamic Address Options

Dynamic address options control Remote System Manager handling of systems that have network addresses that can change over time. For example, systems which use Dynamic Host Configuration Protocol (DHCP) for acquiring TCP/IP addresses will often have different TCP/IP addresses assigned when the system attaches to the network, while other systems will be assigned new addresses due to physical location changes or installation of a new network adapter.

By default, dynamic addressing is disabled. When dynamic addressing is disabled, systems are tracked using their network address. This can result in incorrect system identification and management when the system changes address (such as when DHCP is used). However, when dynamic addressing is enabled, Remote System Manager will use the *System Unique ID*, a random 16 character identification string that is assigned to the system when Netfinity is installed, to track systems as they change addresses. This enabled Remote System Manager to correctly identify and manage systems despite any address or location changes.

Note: The System Unique ID is stored in the NFUNIQUE.ID file in the Netfinity directory. If Remote System Manager is using dynamic addressing support to locate and manage a system, the Unique System ID *must* not change. If you reinstall Netfinity, be sure to save the NFUNIQUE.ID file and copy it into the Netfinity directory after you have finished reinstalling. Failing to do so will prevent Remote System Manager from properly identifying the system with any pre-existing system objects.

When Netfinity's dynamic addressing support is enabled, Remote System Manager will continue to ping and discover systems as normal. However, pings are typically sent directly to a system's address, and this is ineffective when systems frequently change address (such as when they use DHCP). This problem is addressed by enabling Netfinity's dynamic ping support.

Dynamic ping greatly improves the Remote System Manager's ability to find previously discovered systems when they change address. This is done by periodically sending broadcast messages requesting a response from any systems that Remote System Manager has previously discovered but cannot find on the network. This is similar to discovery requests, but is more efficient, as only the specific systems which are missing will respond to the request (as opposed to all systems which match a discovery request). The frequency of these requests is controlled by the **Dynamic Ping Interval** setting.

To enable and configure Netfinity's dynamic addressing support:

1. Select **Dynamic Address Options...** from the Options menu in the System Group Management window.
2. Select **Enable Dynamic Addressing** to activate Netfinity dynamic addressing support.
3. Select the **Enable Dynamic Ping** option to activate the Netfinity dynamic ping support.

   Dynamic addressing support must be enabled for dynamic ping to function.
4. Specify a dynamic ping interval.

   The dynamic ping interval is the number of minutes between dynamic ping discovery attempts. Use the spin buttons to set the number of minutes.
5. Select **OK**.

Using Group Discovery Filters

You can use the Remote System Manager to discover systems that are using only a specified operating system or communications protocol. This is accomplished by using group discovery filters. When you apply a group discovery filter to one of your System Groups, only systems that are using one of the specified operating systems and one of the specified communications protocols will be added to the group by the discovery process.

To apply a discovery filter to one of your system groups:

1. Open the system group's pop-up menu.

   Using mouse button 2, click on a group to open the group's pop-up menu.
2. Select **Group Discovery Filters**.

   Selecting **Group Discovery Filters** opens the Group Discovery Filters window (see Figure 70 on page 211).

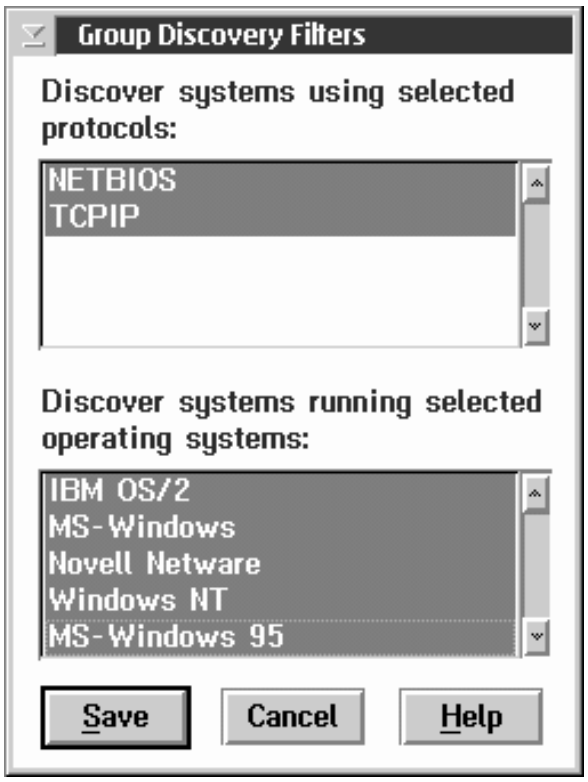

Figure 70. Remote System Manager — Group Discovery Filters window

3. Select from the **Discover systems using selected protocols** list one or more communications protocols.

   All available communications protocols are selected by default.

4. Select from the **Discover systems running selected operating systems** list one or more operating systems.

   All available operating systems are selected by default.

5. Select **Save** to save your selections and apply the group discovery filter.

Once applied, the group discovery filter will allow the discovery process to add a system to the system group only if the system is

using one of the selected communications protocols *and* one of the selected operating systems *and* has any required system keywords.

Automatically Defined Keywords

Systems running Netfinity Manager or Client Services for Netfinity Manager version 5.0 or later support keywords that can be used in addition to keywords that are defined during installation. These keywords can be used to limit discovery to systems that feature specific hardware, that use a specified communications protocol or operating system, that have specified software products installed, or that have specific Netfinity services available for use. A list of these automatically defined keywords follows.

Keyword	**Keyword added if remote system:**
NF:WAKEUP	Has Wake-on-LAN feature enabled For more information on Wake-on-LAN configuration, see Appendix K, “Troubleshooting Wake-On-LAN Systems” on page 525.
NF:SERVER	Appears to be a file server
NF:MANAGER	Is a Netfinity Manager
OS:NETWARE	Is a Novell NetWare server
OS:OS2	Is running OS/2
OS:WIN_NT	Is running Windows NT
OS:WINDOWS	Is running Windows or Windows-95
PROTO:NETBIOS	Has NetBIOS protocol driver enabled
PROTO:IPX	Has IPX protocol driver enabled
PROTO:TCPIP	Has TCP/IP protocol driver enabled
PROTO:SERIPC	Has Netfinity serial driver enabled
PROTO:SNA_APPC	Has SNA protocol driver enabled
SVC:ProfileBase	Has System Profile service available

SVC:Gatherer3.0	Has System Information Tool service available
SVC:SCH_BASE_NODE	Has Event Scheduler service available
SVC:PFAServiceBase	Has PFA service available
SVC:RAID_BASE	Has RAID Manager service available
SVC:SecMgr	Has Security Manager service available
SVC:DMIBrowserBase	Has DMI Browser service available
SVC:AlertMgr	Has Alert Manager service available
SVC:MonSvc	Has System Monitor service available
SVC:ScreenID	Has Screen View service available
SVC:PartionBase	Has System Partition service available
SVC:ECCMemory	Has ECC Memory Setup service available
SVC:FileBase	Has File Transfer service available
SVC:NetMgr	Has Remote System Manager service available
SVC:ShriekerServiceBase	Has Power On Error Detect service available
SVC:SerialBase	Has Serial Control service available
SVC:ProcMgr	Has Process Manager service available
SVC:SoftInvB	Has Software Inventory service available
SVC:CFMBase	Has Critical File Monitor service available
SVC:WebFin	Has Web Manager service available
SVC:RCSHD	Has Remote Session service available

SVC:ProfileBase	Has System Profile service available
SVC:CAPMGT	Has Capacity Management service available
SVC:RWCService	Has Remote Workstation Control service available
SVC:DiagMgr	Has System Diagnostic Managerservice available
SVC:SCFMgr	Has Service Configuration Manager service available
SVC:ServiceProcessorBase	Has Service Processor Manager service available
SVC:UpdateConnector	Has Update Connector Manager interface available.
SVC:UpdateConnectorClient	Has Update Connector Manager interface or client available.
APP:*appkey*	Has an application with Application Keyword *appkey* present (for information on Application Keywords, see "Using Application Keywords" on page 339)

Notes:

1. Keywords are case-sensitive and must match exactly for a remote system to be discovered.
2. A Netfinity service is considered available if the service's base program is installed on the remote system. However, remote users can configure Security Manager to permit access to services only to users that provide specified user ID/password combinations. Therefore, a service that is considered available is not necessarily accessible.

Group View Settings

After you have added systems to a system group, you can select a system group view setting. There are two view settings available:

- Icon View

  For more information on the Icon view setting see “Icon View.”

- Detail View

  For more information on the Detail view setting see “Detail View” on page 216.

Icon View

In Icon view, each system is displayed as a large icon depicting the system. The system name is displayed below the icon (see Figure 71). If a remote system is running server software, such as Novell NetWare or IBM OS/2 LAN Server, **(Server)** will be displayed below the system name. If a remote system is running Netfinity Manager, **(Manager)** will be displayed below the system name. All systems are sorted alphabetically by system name.

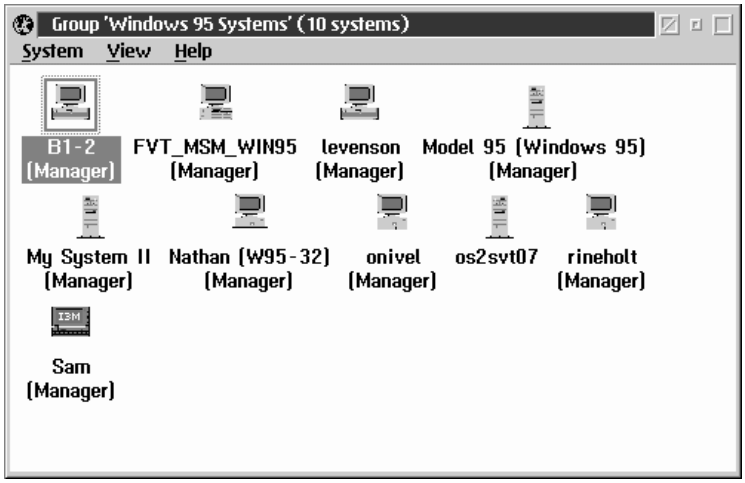

Figure 71. Remote System Manager — Group window, Icon View

To select Icon view:

1. Open a system group.

   Double-click on the system group to which you are adding the individual system.

2. Select **Icon View** from the View pull-down menu.

Detail View

In Detail view, systems in the group are displayed in a table, with each row containing extensive information about an individual system. In Detail view, the following information is available about each system in the system group:

- System Name
- Network Type (the communications protocol being used to talk to this system)
- Network Address
- System Model (available only from IBM systems that have Client Services for Netfinity Manager or Netfinity Manager *and* that provide the appropriate vital product data to positively identify the system)
- Operating System (available only from IBM systems that have Client Services for Netfinity Manager or Netfinity Manager)
- Presence Check Interval (for more information, see "Presence Check" on page 219)
- Online/Offline Notification Severity (for more information, see "System Notifications" on page 220)
- System Unique ID (available only on systems that have Netfinity Manager or Client Services for Netfinity Manager version 5.0 or later)

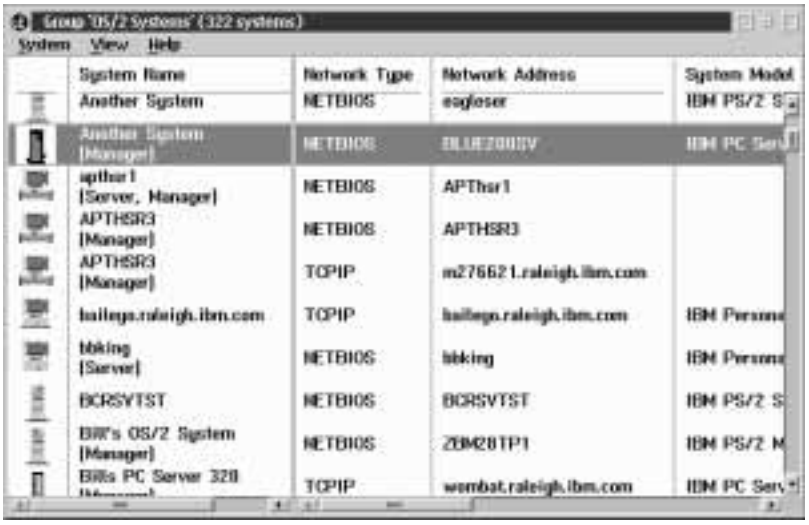

Figure 72. Remote System Manager — Group window, Detail View

If a remote system is running server software, such as Novell NetWare or IBM OS/2 LAN Server, **(Server)** will be displayed below the system name. If a remote system is running Netfinity Manager, **(Manager)** will be displayed below the system name. All systems are sorted alphabetically by system name.

To select Detail view:

1. Open a system group.

   Double-click on the system group to which you are adding the individual system.

2. Select **Detail View** from the View pull-down menu.

Accessing Remote Systems

You can access any remote system's available Netfinity services by opening the individual system's object. The remote system's security configuration determines which services are available for your use. This is covered in greater detail in Chapter 19, "Security Manager" on page 240. To access the Netfinity services on an individual system, open the system's object.

If your system has access to the remote system (as determined by the Security Manager), the remote system's Service Manager window appears on your screen. You will notice that the remote system's name appears in the Service Manager's title bar. To use any of the available services, open the service's object.

Additional Features

There are a number of other actions that you may perform from the System Group window. Each of these actions directly affects an individual remote system that is present in the system group. These actions are accessed from the individual system object's pop-up menu. To open a system's pop-up menu, use mouse button 2 to click on the individual system object. Available actions are:

- Open System
- Edit System
- Delete System
- System Restart
- Presence Check
- Login System
- System Notifications
- Set User ID and Password
- Set Keywords and System Name
- Error Conditions
- Attempt System Wake-Up (available only on Wake on LAN capable systems. For more information, see Appendix K, "Troubleshooting Wake-On-LAN Systems" on page 525)
- Attempt System Shut Down (available only on systems running Windows 3.1, Windows 95, Windows NT 3.51, Windows NT 4.0, or NetWare)
- Attempt System Power-Down (available only on systems running Windows 95 that have Advanced Power Management enabled)

Note: If an individual system is currently offline or unresponsive, some of these selections will not be available.

A description of each of these actions follows.

Open System

Select **Open System** to access the selected remote system's Service Manager.

Edit System

Select **Edit System** to change any of the remote system's identifying information (system name, network address, network type).

Delete System

Select **Delete System** to remove the selected remote system from the system group.

System Restart

Select **System Restart** to restart the selected remote system. You will not be able to perform this function unless you have access to the remote system's Security Manager.

When a system is restarted using the **System Restart** function, Netfinity first checks the Netfinity directory on the target system for a file named NFREBOOT.BAT (NFREBOOT.CMD if the system is running OS/2, NFREBOOT.NCF if the system in running NetWare). If this file is present, Netfinity will process the file (and execute any commands within the file) prior to restarting the system. If the file is not present, Netfinity will restart the system immediately. If there are systems in your network that run applications that do not respond well to system restarts, use the NFREBOOT.BAT file to execute commands that will shut down these programs prior to system restart.

Presence Check

Select **Presence Check** to query the remote system's presence on the network. If a remote system becomes inactive during operations, its object will be grayed out and it cannot be opened for communication. When the system becomes active again, your local system will recognize that it is active and change the object to reflect this. However, it can take several minutes before the Remote System Manager recognizes that the remote system is active again. Presence Check forces Remote System Manager to check the remote system's status immediately.

Login System

Select **Login System** to override an outgoing User ID/Password (outgoing User ID/Passwords are discussed in Chapter 19, "Security Manager" on page 240) for that system. If the system has more than one User ID/Password combination to allow access to the system's services, this option can be used to try a combination without destroying the current outgoing User ID/Password combination.

System Notifications

Select **System Notifications** if you want to be notified when the selected remote system goes online or offline. Remote System Manager automatically checks each of the systems in your system groups to see if they are active, according to a predetermined Presence Check Interval.

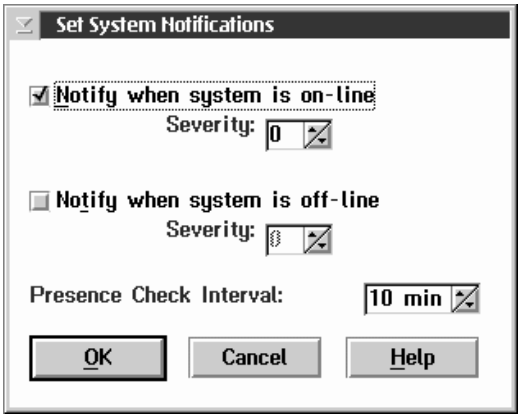

Figure 73. Remote System Manager System Notifications Window

If you want to be notified when a selected system goes online or offline, follow these steps:

1. Select **System Notifications** from the selected remote system's pop-up menu.
2. To be notified when the selected system is active and accessible, select the **Notify when system is online** check box.

If you have selected the **Notify when system is online** check box, set a Severity value for the alert that will be generated when the system comes online (for more information on alert Severity see "Severity" on page 15). When you do this, the Remote System Manager will generate an alert when the selected remote system comes online and is accessible. The alert that is generated will have an Application ID of NetMgr, an Application Alert Type of 10, and the Severity value that you selected from the Severity spin button below the check box.

3. To be notified when the selected system is inactive or inaccessible, select the **Notify when system is offline** check box.

   If you select the **Notify when system is offline** check box, set a Severity value for the alert that will be generated when the system goes offline. When you do this, the Remote System Manager will generate an alert when the selected remote system goes offline and is inaccessible. The alert that is generated will have an Application ID of NetMgr, an Application Alert Type of 11, and the Severity value that you selected from the Severity spin button below the check box.

4. Set a Presence Check Interval.

   The **Presence Check Interval** field shows the length of time Remote System Manager waits between automatic Presence Checks. The Presence Check Interval default value is 10 minutes. The Presence Check Interval selections include 15 seconds, 30 seconds, 45 seconds, and from 1 to 120 minutes.

   Note: Frequent presence checks on many systems can reduce the speed of data transfer on your network. Only perform frequent presence checks on systems that are crucial to your network's performance.

5. Select **OK** to save the notification configuration for this system.

For more information on alerts, see "The Alert Log" on page 14. For information on how to use Application ID, Application Alert Type, and Severity to trigger actions in response to generated alerts, see "The Alert Log" on page 14.

Set User ID and Password

Select **Set User ID and Password** to set the User ID/Password combination that will be used automatically when opening this remote system. Using the Set User ID and Password option yields the same results as using the Set Outgoing User ID and Password option in Security Manager. For more information see "Setting Outgoing User ID/Password Combinations" on page 244.

Set Keywords and System Name

Select **Set Keywords and System Name** to view or change the selected system's keywords or name. Changing the system's keywords and system name can enable you to better organize your System Groups through effective use of the discovery process.

Notes:

1. To view a system's keywords, you must have at least PUBLIC access to one or more of the system's Netfinity services.
2. To change a system's keywords or system name, you must have access to the system's Security Manager service, or you must have a specific Login ID and Password configured and saved for that system.

   For more information on User ID and Password combinations, see Chapter 19, "Security Manager" on page 240.

Error Conditions

Select **Error Conditions** to open the system's error condition log window. This selection will not be available if the error condition log is empty.

Error conditions are generated by the Netfinity Alert Manager in response to Netfinity alerts. Error conditions simply notify the Remote System Manager that a notable event has occurred on one of the Netfinity systems in the network. When you bind an alert profile to the Set Error Condition alert action, you must specify a name for the error condition (see "Error Conditions"). Then, when the Alert Manager generates an error condition it will place an error condition entry, using the name you specified, in the system's error condition log.

If a system currently has one or more entries in its error condition log, its individual system object will be replaced by a generic system icon with a red "circle and slash" symbol. Any system groups in the System Group Management window that contain this system will also change. This will help to alert you that the system group contains one or more systems that have entries in their error condition logs.

Error conditions can be cleared in either of two ways:

1. Generate a **Clear Error Condition** message with the Alert Manager.

   When the Alert Manager generates a **Clear Error Condition** message, it will clear only one identically named error condition from the log (see "Error Conditions" on page 222).

2. Select **Reset** from the Error Condition Log window.

   This will clear *all* error conditions from the log.

Note: This function can be performed only on remote systems that are running Client Services for Netfinity Manager or Netfinity Manager version 3.0 or later.

System Wake-Up

Select **System Wake-Up** to attempt to "wake up" Wake on LAN enabled systems. For more information, see Appendix K, "Troubleshooting Wake-On-LAN Systems" on page 525.

Note: This function can be performed only on remote systems that feature Wake on LAN hardware and that are running Client Services for Netfinity Manager or Netfinity Manager version 5.0 or later

System Shut Down

Select **System Shut Down** to shut down the selected remote system. You will not be able to perform this function unless you have access to the remote system's Security Manager.

Note: This function can be performed only on remote systems that are running Windows 3.1, Windows 95, Windows NT 3.51, Windows NT 4.0, or NetWare and that are running Client

Services for Netfinity Manager or Netfinity Manager version 5.0 or later.

System Power Down
Select **System Power Down** to power down the selected remote system. You will not be able to perform this function unless you have access to the remote system's Security Manager.

Note: This function can be performed only on remote systems that are running Windows 95, that have Advanced Power Management enabled, and that are running Client Services for Netfinity Manager or Netfinity Manager version 5.0 or later.

Using the Discovery Process

Using the Netfinity Remote System Manager's discovery process you can quickly and easily add multiple remote systems to a selected system group. The discovery process uses keywords that are assigned to all systems during the Netfinity installation process.

When a system group is created, system group keywords can be specified, along with a system discovery condition. When the discovery process is initiated, the Netfinity Remote System Manager sends a short message out over your network, using your enabled communications drivers. This message requests that any remote systems that have the Netfinity programs installed and running and that have the proper keywords, as determined by the system discovery condition and keywords that you selected when you created the system group, acknowledge their presence on the network.

The remote systems that have the correct keywords then send a response to the system that initiated the discovery process. This response contains all of the information necessary to add the individual system to the system group (system name, network address, and network type). The individual remote systems are then automatically added to the system group. Objects representing each of the remote systems then appear in the System Group

window, sorted alphabetically. This entire process takes approximately 45 seconds to complete.

The discovery process has been designed to be open-ended and flexible, thus allowing for its use over a broad range of work group sizes.

The process by which you organize your Netfinity system groups is dependent on the environment in which you will be using it. For example, if you are using Netfinity in a peer-to-peer work group, where every individual system has complete access to all other systems in the work group, only one system group is necessary, and keyword assignment is fairly simple.

However, in a larger organization (such as a small company that has several departments, each of which will be a separate work group, but all of which will be managed by an individual Netfinity Remote System Manager) more intricate keyword assignment might be necessary. This section provides you with a series of examples of keyword assignment, system-discovery condition selection, and the effect that these have on the discovery process.

Assigning Keywords During Installation

When the Netfinity installation process is complete, you can enter system-specific keywords. Keywords are a series of descriptive words that identify the individual system within the group. For example, a system might have keywords identifying the company name, the department name, the building number, the department manager's name, and the primary user's name. The main goal of keyword assignment is to offer a broad variety of criteria by which to identify a system.

Using the example system keywords, you could:

- Add all of the systems in a company.
- Add all of the systems in a department.
- Add all of the systems that are in a building and that are used by employees who are supervised by a particular manager.
- Add the systems that are used by three specific employees, regardless of location.

These are just some of the possible combinations of systems that could be added using the discovery process. Which Netfinity systems are added to the system group is determined by the keyword list and the system-discovery condition that you selected when you created the individual system group.

Assume that there are four remote systems that you can potentially add to any system group. Each of these four systems uses NetBIOS communication drivers and has only three system-specific keywords assigned. The three keywords represent the company name, the department the system is located in, and the primary user's last name. The keywords for each system are as follows:

System Number	System Keywords
System #1	IBM, DEVELOPMENT, JONES
System #2	IBM, DEVELOPMENT, SMITH
System #3	IBM, MARKETING, O'BRIAN
System #4	IBM, MANAGEMENT, JEFFERSON

System Discovery Conditions

When you want to create a system group, decide which keywords to look for during the discovery process, and set a system-discovery condition. The system-discovery condition determines how many of the remote system's keywords must match the Remote System Manager system group keywords if they are to be included in the system group. There are three possible system-discovery conditions. They are:

- Systems with all of the keywords

  When the discovery process is initiated, this system-discovery condition includes a remote system in the system group only if that system's keyword list contains *all* of the keywords specified in the keyword list.

- Systems with any of the keywords

  When the discovery process is initiated, this system-discovery condition includes a remote system in the system group only if that system's keyword list contains at least *one* of the keywords specified in the keyword list.

- Systems with only one of the keywords

  When the discovery process is initiated, this system-discovery condition includes a remote system in the system group only if that system's keyword list contains *one and only one* of the keywords specified in the keyword list.

Here are some examples of how you could use each of these system discovery conditions to add some or all of the four remote systems to a system group. For the purposes of these examples, assume that you are a network administrator for IBM Corporation.

System Discovery Condition #1: Systems with all of the keywords. You are creating a system group named **IBM**. You want this system group to contain all Netfinity systems in IBM Corporation's NetBIOS network. This could be accomplished by selecting the first system discovery condition, **Systems with all of the keywords**, and by entering the keyword **IBM** in one of the **Keywords** fields. Your Add System Group window would look like this.

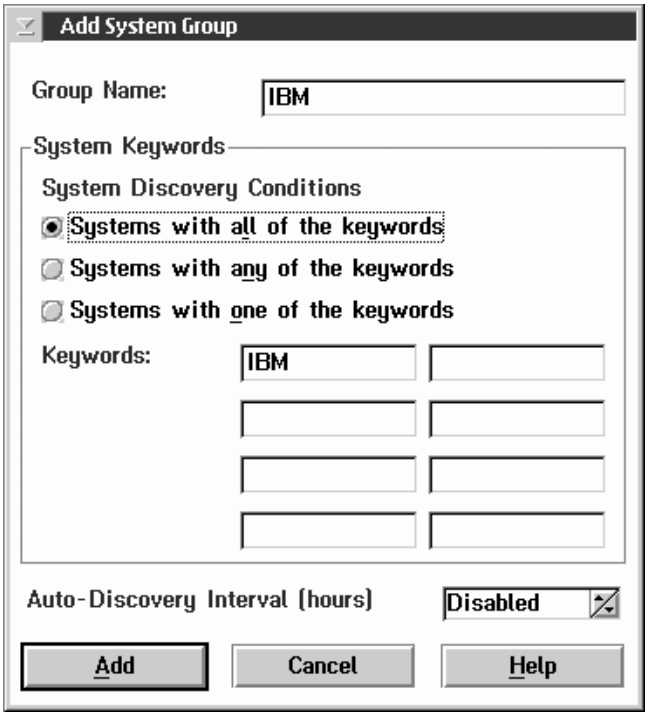

Figure 74. System Discovery Condition #1: Example #1

Select **Add** to add this system group to your System Group Manager window. Next, select the system group to open it. It will be empty, as you have not yet added any remote systems.

Select **Discover Systems** from the System pull-down menu. Remote System Manager sends out a message to all Netfinity systems on the network asking for any systems that have the keyword **IBM** to acknowledge their presence on the network. All four of the

example systems fit this criteria, so all four of these systems would appear within the IBM system group.

If you had entered two keywords and selected the same system discovery condition (**Systems with all of the keywords**), the results would be different. Enter the keywords **IBM** and **DEVELOPMENT**. Your Add System Group window would look like this.

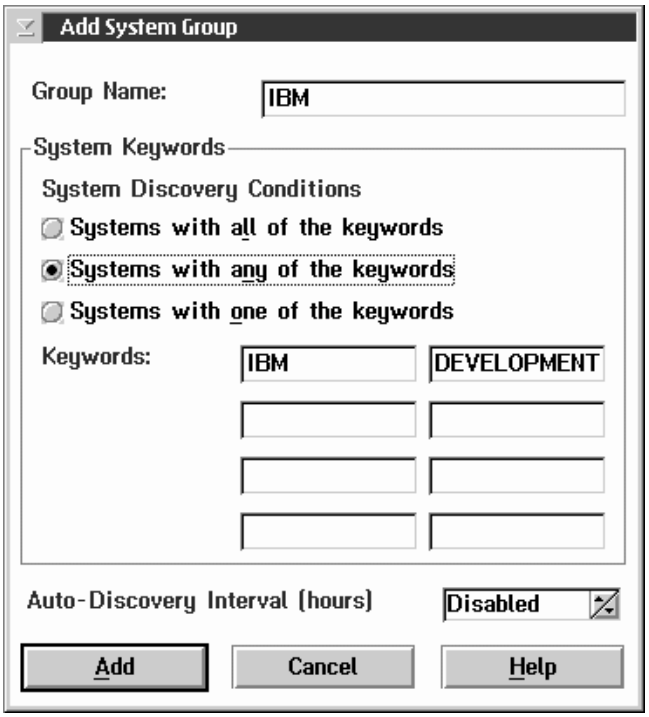

Figure 75. System Discovery Condition #1: Example #2

This time, only example systems #1 and #2 would be added to the system group. This is because, of the four Netfinity systems on the network, they are the only ones that have all of the keywords that the system group requires.

System Discovery Condition #2: Systems with any of the keywords

You are creating a system group named **IBM Development and Marketing**. You want this system group to contain all Netfinity systems in the IBM Corporation's NetBIOS network that are part of the Development department or of the Marketing department. This could be accomplished by selecting the second system discovery condition, **Systems with any of the keywords**, and by the entering the keywords **DEVELOPMENT** and **MARKETING** in the **Keywords** fields. Your Add System Group window would look like this.

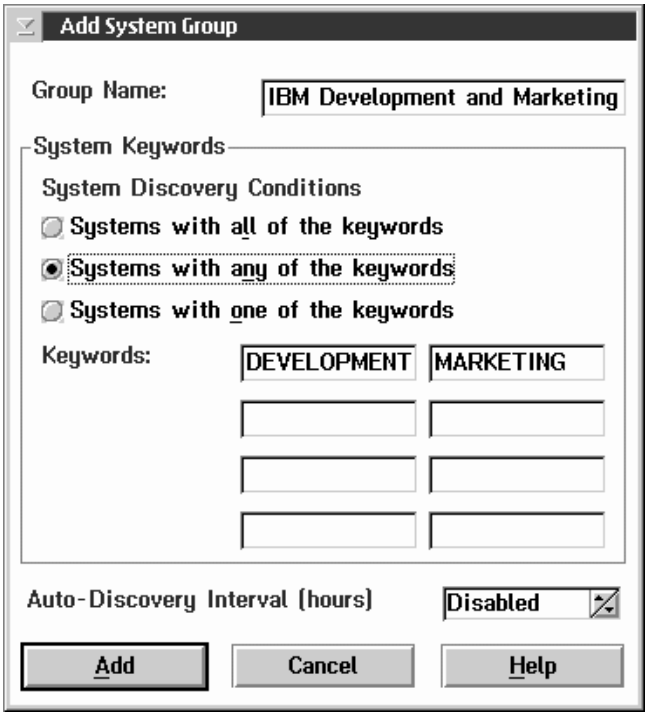

Figure 76. System Discovery Condition #2

Select **Add** to add this system group to your System Group Manager window. Next, select the system group to open it. It will be empty, as you have not yet added any remote systems.

Select **Discover Systems** from the System pull-down menu. Remote System Manager sends out a message to all Netfinity systems on the network asking for any systems that have the keyword **DEVELOPMENT** or the keyword **MARKETING** to acknowledge their presence on the network. Only three of the four example systems fit this criteria, so only systems #1, #2, and #3 would appear in the IBM Development and Marketing system group.

Note: When the **Systems with any of the keywords** system discovery condition is selected, a system can have more than one of the keywords on the system group keyword list and still be added by the discovery process.

System Discovery Condition #3: Systems with only one of the keywords.

Create a system group named **IBM: Non-Development** that will contain all Netfinity systems in the IBM Corporation's NetBIOS network that are not part of the Development department. This could be accomplished by selecting the third system discovery condition, **Systems with only one of the keywords**, and by the entering the keywords **IBM** and **DEVELOPMENT** in the **Keyword** fields. Your Add System Group window would look like this.

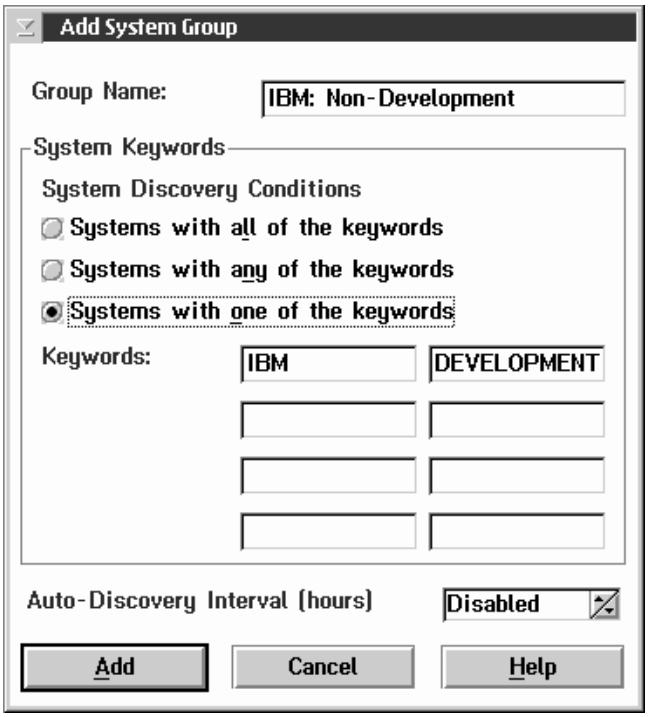

Figure 77. System Discovery Condition #3

Select **Add** to add this system group to your System Group Manager window. Next, select the system group to open it. It will be empty, as you have not yet added remote systems.

Now, select **Discover Systems** from the System pull-down menu. Remote System Manager sends out a message to all Netfinity

systems on the network asking for any systems that have either the keyword **DEVELOPMENT** or the keyword **IBM** to acknowledge their presence on the network. For a system to be added to the system group, it must have only one of these keywords. If it has both, it is not added to the system group. Only two of the four example systems fit this criteria, so only systems #3 and #4 would appear in the IBM:Non-Development system group.

Note: If you create a system group and do not assign any keywords, all Netfinity systems on your network will be added to the system group when the Discover Systems option is selected, regardless of what system discovery condition you select.

Chapter 17. Remote Workstation Control

Using Remote Workstation Control you can monitor or control the screen display of a remote Netfinity system. Once you initiate a Remote Workstation Control session with another Netfinity system, you can passively monitor events that are occurring on the display of the remote system or actively control the remote system's desktop. When you initiate an active Remote Workstation Control session, all mouse clicks and keystrokes entered on your system are automatically passed through to the remote system. With Remote Workstation Control, you can remotely start programs, open and close windows, enter commands, and much more.

Notes:

1. Remote Workstation Control is a *remote only* service. This service will be available for use only when you are accessing a remote system. The Remote Workstation Control service object will *not* appear in your local Service Manager.
2. Remote Workstation Control is not designed to work in conjunction with other remote workstation desktop-control products. Running Remote Workstation Control with other similar products might cause your system to become unstable.
3. Do not use Remote Workstation Control over a serial connection. Due to the large amount of data that must be transferred by this service, use Remote Workstation Control only on systems connected to a fast network.
4. To reduce the amount of data that is transferred from the remote system, Remote Workstation Control reduces the display information of all images to 16 colors. As a result, the image shown on the Netfinity Manager display might differ from the actual appearance of the remote system desktop. This has no effect on Remote Workstation Control functions.

Figure 78. Remote Workstation Control

Remote Workstation Control Sessions

Once you establish a Remote Workstation Control session with a remote Netfinity system, you are presented with a window depicting the remote system's display. The window can be in any of the following states:

- Active

  When the Remote Workstation Control window is in Active state, you have control over the remote system's display. All mouse clicks and keyboard input entered from your system are passed through to the remote system. This window will update automatically whenever there is a change on the remote system's display.

- Monitor

  When the Remote Workstation Control window is in Monitor state, the remote system's user has control of the remote system. The window will update automatically whenever there is a change on the remote system's display.

- Suspend

  When the Remote Workstation Control window is in Suspend state, the remote system's user has control of the remote system. However, the window will not show any changes that occur on the remote system's display.

When you first initiate a Remote Workstation Control session with a remote system, the display window is placed in Active state. To change to another state, select the state from the Session pull-down menu. To close the Remote Workstation Control service, select **Terminate** from the Session pull-down menu.

The remote system's user can change the state of the Remote Workstation Control session by pressing **Alt+T** and then selecting a new state.

Remote Workstation Control Keystrokes

When Remote Workstation Control is in an Active state, nearly all keystroke and keystroke combinations will be automatically passed through to the remote system. However, due to operating system requirements some keystroke combinations (such as **Ctrl+Alt+Del**) cannot be passed through to a remote system automatically. This is because the operating system on your system intercepts and uses these keystroke combinations locally, preventing Remote Workstation Control from passing them to the remote system. However, with Remote Workstation Control you can send these normally intercepted keystroke combinations by selecting the combination from the Keystrokes pull-down menu. The following selections are available:

- Send Alt+Esc
- Send Alt+Tab
- Send Crtl+Esc
- Send Ctrl+Alt+Del

Note: The effect that these keystroke combinations will have on the remote system depends on the remote system's operating system.

With the exception of these keystroke combinations, all keystrokes and keystroke combinations that are typed on the local system keyboard will be passed through to the remote system. If you need to type keystroke combinations for the local system, you must change the Remote Workstation Control keystroke mode. To change the keystroke mode:

1. Select **Change Keystroke Mode** from the Keystroke pull-down menu.
2. Select **Keystrokes Local** from the Change Keystroke Mode submenu.

To resume passing keystrokes through to the remote system, select **Keystrokes Remote** from the Change Keystroke Mode submenu.

The keystroke mode can also be switched by pressing **Alt+T**.

Chapter 18. Screen View

You can use Screen View to view a “snapshot” of any remote system’s current screen display. The remote system’s desktop image is converted into a bit-map (BMP) file, compressed, and transmitted to the network administrator’s system, which then decodes the data and displays a scalable window depiction of the remote system’s display. This is useful for remote system troubleshooting.

Use Screen View to:

- Save a screen shot to a file for later reference.

  Select **Save** from the Options pull-down menu to create a data file of the screen-shot information for later reference.

- Refresh your screen shot on demand.

  Select **Capture New Screen** from the Options pull-down menu to collect another screen shot from the remote system.

Figure 79. Screen View Service

- Load previously saved screen shots.

  Select **Load** from the Options pull-down menu to load a previously saved screen shot.

- Scale a screen shot to any size up to full screen

  To scale the screen shot, drag the Screen View window's corner until the window is the size you desire.

Note: Screen View cannot capture full–screen DOS or Win-OS/2 sessions.

Chapter 19. Security Manager

The Netfinity Security Manager is designed to limit remote access to some or all of the Netfinity services installed on an individual system. Irresponsible or careless use of the Netfinity services can lead to data loss or system damage. To avoid this, limit remote access to some or all of these services on the Netfinity systems in your network.

Note: The following Netfinity services pose the most potential risk if used irresponsibly:

- File Transfer
- Process Manager
- RAID Manager
- Remote Session
- Remote System Manager
- System Partition Access

The Netfinity Security Manager uses a User ID/Password combination to determine security clearance on a system. Incoming User ID/Password combinations determine which of your are available to a user accessing your system remotely. Outgoing User ID/Password combinations can be set to provide default User ID/Password combinations when you attempt to remotely access other systems.

If your outgoing User ID/Password combination for a target system matches a configured incoming User ID/Password combination on the target system, you are automatically granted access to the services that have been selected for that User ID/Password combination. If you have configured appropriate outgoing User ID/Password combinations for all Netfinity systems operating in your network, all security checking is done passively and without interruption.

Security Manager features a default incoming User ID/Password feature. It is called the <PUBLIC> setting, and automatically allows access to any services that you select. For more information on the <PUBLIC> incoming User ID/Password, see “Setting Incoming User ID/Password Combinations” on page 242.

Once you have established incoming and outgoing User ID/Password combinations on all of the systems in your network, security operates passively. When a user attempts to gain access to another system, the outgoing User ID/Password combination is automatically checked against the target system's incoming User ID/Password combinations.

You will encounter security checks only if:

- A change is made to the security configuration of a given system.
- A new system is added and is not properly configured.
- You use Remote System Manager's Login System action to override your default outgoing User ID/Password combination for a particular system.

Use the Login System action to establish multiple levels of security for the Netfinity systems within your network. For example, you might want to configure a <PUBLIC> incoming User ID/Password combination on the Netfinity systems within your network that permits access to all Netfinity services except the System Partition Access.

However, you want to be able to access the System Partition Access when necessary. You would then set an incoming User ID/Password combination on each of the systems in your network that would allow access to the System Partition Access. Once this configuration is saved, all Netfinity systems in your network automatically receive the limited <PUBLIC> access to the other system's .

To access the System Partition Access, you would have to select Remote System Manager's **Login System** action and enter the User ID/Password combination you created. You would then receive access to all , including System Partition Access.

Netfinity Security Manager also generates alerts to help you maintain a record of who has accessed or attempted to access your system. For more information on the alerts generated by the Security Manager, see "Security Access Alerts" on page 247.

Setting Incoming User ID/Password Combinations

If the Security Manager has not been preconfigured, there will be a User ID called <PUBLIC>. This is a general security access default setting. It allows any system using the <DEFAULT> outgoing User ID/Password combination to access all Netfinity services on your system.

If a remote system user attempts to use the Remote System Manager Login System action to access your system and fails to match a corresponding incoming User ID/Password combination, the user will be given access to any services in your <PUBLIC> configuration.

Initially, *all* Netfinity services are available for <PUBLIC> access. To edit the list of services available from the <PUBLIC> User ID/Password combination:

1. Double-click on **Edit/Display Incoming Passwords** to open the Incoming Passwords window.
2. Select <PUBLIC> from the User ID selection list.
3. Deselect the services you do not want available for public access.
4. Deselect the **Security Manager Access** check box to restrict public access to Security Manager.
5. Select **Set** to save your configuration.

Note: If you do not have a <PUBLIC> default configured as part of your incoming User ID/Password security configuration, only users with valid outgoing User ID/Password combinations will be able to access the Netfinity services on your system.

If an invalid User ID/Password combination is used when a user attempts to access your system, an alert is generated by the Security Manager. However, if you maintain a <PUBLIC> default on your system, users who attempt to access your system using an invalid outgoing User ID/Password combination will automatically be granted

access to your <PUBLIC> services. This will also generate an alert. For more information on alerts generated by the Security Manager, see “Security Access Alerts” on page 247.

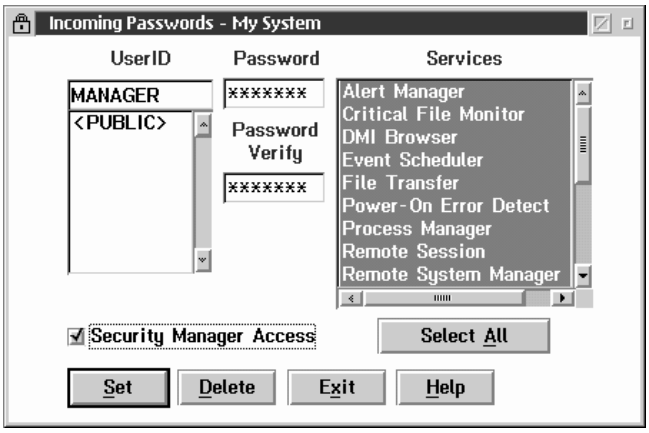

Figure 80. Incoming User ID/Password Configuration

To set a new incoming User ID/Password combination, and determine access to services:

1. Start Security Manager.
2. Select **Edit/Display Incoming Passwords**.
3. Enter a User ID.

   Enter the User ID that you are allowing access. You may select an ID from the User ID selection list, or enter a new ID in the entry field.
4. Enter a password.

   Type in the **Password** field a password that, when used in combination with the User ID you have specified, will allow access to all selected Netfinity services. The password must be from 1 to 8 characters in length. This password will not be displayed.
5. Verify the password.

   Type in the **Password Verify** field the same password that you typed in the **Password** field. These two passwords **must** match

to successfully create an incoming User ID/Password combination.

6. Select the accessible services.

   Select one or more services from the Services selection list. The selected services will be available to users who provide the User ID and password you have entered in the corresponding fields.

7. Determine access to the Security Manager.

   Select the **Security Manager Access** check box to allow access to your Security Manager.

   Note: Allowing access to the Security Manager enables the remote system to alter your incoming and outgoing User ID/Password combinations, and will also enable the Remote System Manager's Restart System action on your system. This will enable the remote user to restart your system on demand.

8. Save your incoming security configuration

   Select **Set** to save your configuration.

Deleting an Incoming User ID/Password Combination

To delete a previously set User ID/Password combination:

1. Start Security Manager.
2. Select **Edit/Display Incoming Passwords**.
3. Select the User ID you want to delete.
4. Select **Delete**. The User ID and its corresponding password are then deleted from your incoming User ID/Password combination configuration.

Setting Outgoing User ID/Password Combinations

If the Security Manager has not been preconfigured, there will be a <DEFAULT> outgoing User ID/Password combination. The

<DEFAULT> outgoing User ID/Password combination is used when you attempt to access a remote system for which you have not configured a User ID/Password combination. If the <DEFAULT> outgoing setting is used on a remote system that has a <PUBLIC> incoming User ID/Password setting configured, the remote system will automatically grant access to any services available from its <PUBLIC> incoming User ID/Password setting. However, the Netfinity services that are available on the accessed system may vary.

Note: Outgoing User ID/Password combinations can be edited or created only if you have the Netfinity Remote System Manager.

To set an outgoing User ID/Password combination:

1. Start Security Manager.
2. Select **Edit/Display Outgoing Passwords**. This opens the Outgoing Password window (see Figure 81).

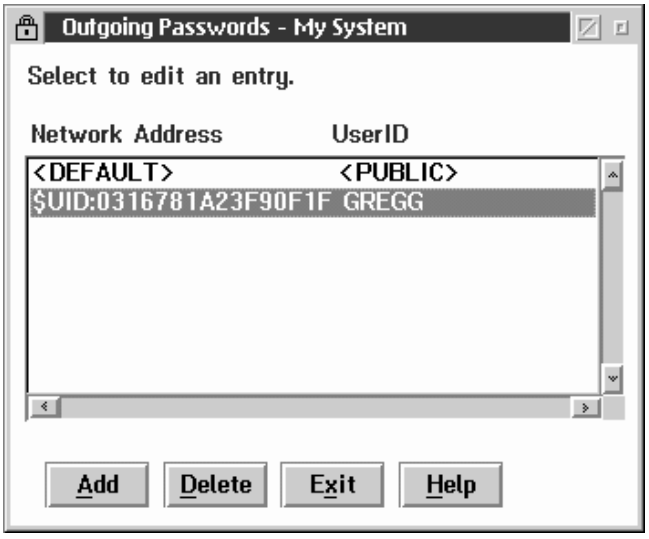

Figure 81. The Outgoing Password window.

3. Select **Add**. This opens the Edit Outgoing Passwords window (see Figure 82 on page 246).

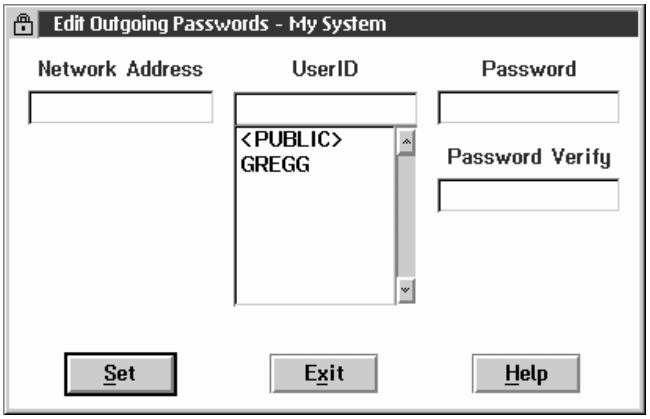

Figure 82. The Edit Outgoing Passwords window.

4. Enter a Network Address.

   Type in the **Network Address** field the network address of the system for which you are creating the outgoing User ID/Password combination. This address must be identical to the network address used by the Remote System Manager to locate the remote system.

5. Enter a User ID.

   Select a **User ID** from the selection list, or type a new ID in the **User ID** entry field. This ID will be used (along with the Password) when you attempt to access the remote system.

6. Enter a password.

   Type in the **Password** field the password that will be used in combination with the User ID you have specified to attempt to gain access to the remote system. The password must be from 1 to 8 characters in length. The password can contain any standard ASCII characters. The password will not be displayed.

7. Verify the password.

   Type in the **Password Verify** field the same password that you typed in the **Password** field. These two passwords **must** match to successfully create an outgoing User ID/Password combination.

8. Save your outgoing User ID/Password configuration.

   Select **Set** to save the outgoing User ID/Password combination.

Editing an Outgoing User ID/Password Combination

To edit a previously set User ID/Password combination:

1. Start Security Manager.
2. Select **Edit/Display Outgoing Passwords**.
3. Select the Network Address and User ID you want to edit.
4. Change the User ID, the Password, or both.
5. Select **Set** to save the new outgoing User ID/Password combination for this network address.

Deleting an Outgoing User ID/Password Combination

To delete a previously set User ID/Password combination:

1. Start Security Manager.
2. Select **Edit/Display Outgoing Passwords**.
3. Select the Network Address and User ID you want to delete.
4. Select **Delete**. The Network Address, User ID, and its corresponding password are then deleted from your outgoing User ID/Password combination configuration.

Security Access Alerts

The Security Manager can generate three alerts in response to specific security access conditions. These alerts are:

- Access Granted Alert

  Generated when Security Manager allows non-public access to a remote user.
- Public Access Granted Alert

Generated when Security Manager allows public access to one or more services to a remote user.

- System Access Denied Alert

  Generated when Security Manager denies access to the system to a remote user.

Detailed descriptions of the contents of each of these alerts follows.

Access Granted Alert

Explanation	Generated by the Security Manager service when access to one or more services is granted to a remote user that has used a UserID/Password combination to gain access.
Alert Text	User ID '*%P1*' from Address '*%P2*' on Network '*%P3*' has been granted system access
Type of Alert	Security Information
Severity	7
Application ID	SecMgr
Application Alert Type	20

Note: This alert supports the following macro parameter strings:

%P1	User ID requesting system access
%P2	Network Address of system requesting access
%P3	Network Type of system requesting access

If you have not altered the default configuration for your Alert Manager, this alert will not trigger an action. However, you can create a new action response to this specific alert.

Public Access Granted Alert

Explanation	Generated by the Security Manager service when **Public** access to one or more services is granted to a remote user.
Alert Text	User ID '*%P1*' from Address '*%P2*' on Network '*%P3*' has been granted public system access
Type of Alert	Security Information
Severity	6
Application ID	SecMgr
Application Alert Type	21

Note: This alert supports the following macro parameter strings:

%P1	User ID requesting system access
%P2	Network Address of system requesting access
%P3	Network Type of system requesting access

If you have not altered the default configuration for the Alert Manager, this alert will not trigger an action. However, you can create a new action response to this specific alert.

System Access Denied Alert

Explanation	Generated by the Security Manager service when access to the system is denied to a remote user.
Alert Text	Logon attempt by User ID '*%P1*' from Address '*%P2*' on Network '*%P3*' has been rejected
Type of Alert	Security Warning
Severity	5
Application ID	SecMgr
Application Alert Type	22

Note: This alert supports the following macro parameter strings:

%P1	User ID requesting system access
%P2	Network Address of system requesting access
%P3	Network Type of system requesting access

If you have not altered the default configuration for the Alert Manager, this alert will be added to the Alert Manager's log file. You can create additional action responses to this specific alert.

System Restart Alerts

The Security Manager can generate two alerts in response to System Restart attempts. These alerts are:

- System Restart Initiated Alert
- System Restart Request Rejected Alert

Detailed descriptions of the contents of each of these alerts follows.

System Restart Initiated Alert

Explanation Generated by the Security Manager service when a remote Netfinity Manager uses the Remote System Manager's Restart System option to restart your system.

Alert Text System Restart initiated by User ID '*%P1*' from Address '*%P2*' on Network '*%P3*'.

Type of Alert Security Information

Severity 5

Application ID SecMgr

Application Alert Type 41

Note: This alert supports the following macro parameter strings:

%P1	User ID requesting system restart
%P2	Network Address of system requesting restart
%P3	Network Type of system requesting restart

If you have not altered the default configuration for the Alert Manager, this alert will be added to the Alert Manager's log file. You can create additional action responses to this specific alert.

System Restart Request Rejected Alert

Explanation Generated by the Security Manager service when a remote Netfinity Manager attempts to use the Remote System Manager's Restart System option to restart your system, but does not have adequate security access to do so.

Alert Text System Restart request by User ID '*%P1*' from Address '*%P2*' on Network '*%P3*' rejected rejected.

Type of Alert Security Error

Severity 3

Application ID SecMgr

Application Alert Type 40

Note: This alert supports the following macro parameter strings:

%P1	User ID requesting system restart
%P2	Network Address of system requesting restart
%P3	Network Type of system requesting restart

If you have not altered the default configuration for the Alert Manager, this alert will be added to the Alert Manager's log file **and** will generate a pop-up window notifying you of the System Restart attempt. You can create additional action responses to this specific alert.

Chapter 20. Serial Connection Control

Use the Netfinity Serial Connection Control service to use your system's modem to remotely access another Netfinity system. Once properly configured, you can access and manage other Netfinity systems using only a modem, just as if they were attached to your LAN. If you use Serial Connection Control to connect with a Netfinity Manager, you can then use the remote system's Remote System Manager to pass through that system and manage any other Netfinity system on the remote system's network.

Also, if your system is not LAN-attached, the Netfinity Serial Connection Control service will enable your system administrator to manage your system using any of Netfinity's applications without having to visit your office or interrupt your work.

Note: Your system *must* have a properly installed and configured modem that supports at least 9600 baud for the Serial Connection Control service to function.

Modem Configuration

Before you can use the Serial Connection Control service to access remote systems or to enable remote access of your own system through your modem, you must ensure that your modem is properly configured.

To configure your system's modem:

1. Select **Modem Settings** from the Serial Connection Control window.

   This will open the Netfinity Modem Settings window (see Figure 84 on page 255).

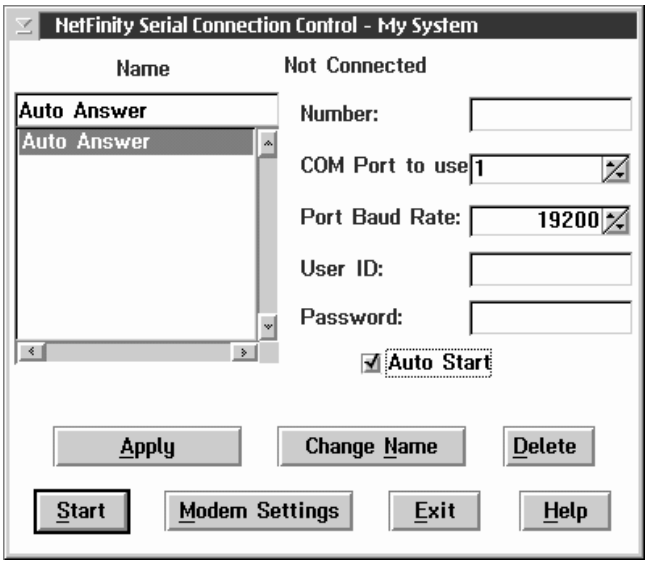

Figure 83. The Serial Connection Control service

2. Select the **COM Port** for the modem that you are configuring.

   Use the spin buttons beside the **COM Port** field to select the modem's COM port.

3. Select a **Modem Name**, or type in a new one.

   Select from the **Modem Name** field the name of your system's modem, or type in a new one. Netfinity comes preconfigured with settings for some popular modem types. However, if your modem is not listed in the **Modem Name** field, or if you do not know what kind of modem your system has, select **Default**. If your modem does not function properly when using the **Default** settings, see "Initialization String Guidelines" on page 259.

   Note: Selecting a preconfigured Modem Name or **Default** will automatically fill in the other modem configuration information.

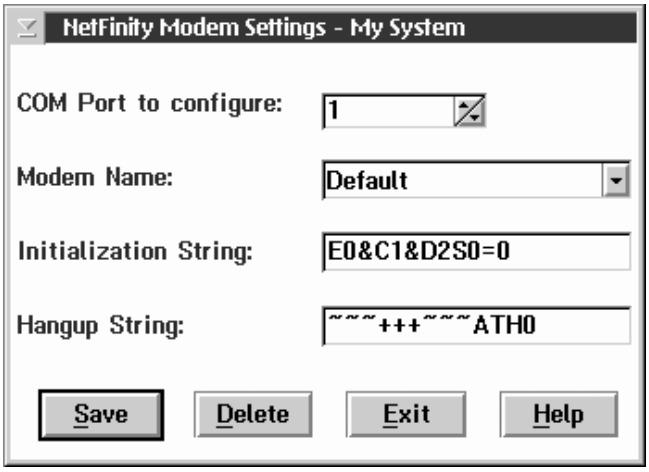

Figure 84. Serial Connection Control — The Netfinity Modem Settings window

4. If you typed in a modem name, type in the proper **Initialization String** for your system's modem.

   If you selected one of the preconfigured Modem Names, this field will be filled in for you. However, you might need to edit this field if Netfinity did not come with preconfigured settings for your modem. If you need more information, see "Initialization String Guidelines" on page 259.

5. Type in the proper **Hangup String** for your system's modem.

   The **Hangup String** field contains the command that will be sent to the modem to instruct it to close the connection to the phone line. This string will function properly on most modems. If your modem does not respond correctly to the default hangup string, see the documentation that came with your modem for more information.

6. Select **Save** to save these settings and enable this modem to be used by the Serial Connection Control service.

Enabling Remote Access

Once you have configured your modem for use with Serial Connection Control, you must grant access to your system to your

network administrator or other authorized users. Authorized users can then use Serial Connection Control to access your system. To grant access to your system:

1. Set the Serial Connection Control service to AutoAnswer mode.
2. Use Security Manager to configure a User ID/Password combination for the authorized user to use when logging on to your system.

For information on how to configure a User ID/Password combination to enable remote access to your system, see "Setting Incoming User ID/Password Combinations" on page 242.

To set the Serial Connection Control service to AutoAnswer mode:

1. Start the Netfinity Serial Connection Control service.
2. Select **AutoAnswer** from the Serial Connection Control window's **Name** field.

   The AutoAnswer setting will enable the Serial Connection Control service to automatically answer incoming phone calls through the modem. Once it has answered the telephone, it will attempt to establish a link with the calling system.
3. Select **Null Modem** if the connection will be established using a null modem connection.

   Note: The **Null Modem** checkbox **must** be checked if remote systems will be using a null modem connection to communicate with this system.
4. Set the Serial Connection Control User ID and Password.

   Type in the **User ID** and **Password** fields the user ID and password that a remote system, using Serial Connection Control, must provide in order to gain access to your system using Serial Connection Control.
5. Select **Start**.

   Once you select **Start**, the Serial Connection Control service will begin waiting for an incoming call. Once "Waiting for call" appears in the Serial Connection Control window status field,

you can select **Exit**. Serial Connection Control will continue to wait in the background for incoming calls.

Note: If you want the Serial Connection Control service to automatically start and begin waiting for incoming calls when Netfinity is started, select **AutoAnswer**, and then select the **Auto Start** check box.

Once you have configured your system's modem for use with the Serial Connection Control service, you can create Serial Connection Control entries that will enable you to remotely access other Netfinity systems.

Creating Serial Connection Control Entries

Serial Connection Control entries are added by filling in the appropriate fields in the Netfinity Serial Connection Control window. To add a new Serial Connection Control entry:

1. Assign a name to the entry.

   Type in the **Name** field a unique name for the Serial Connection Control entry that you are creating for an individual system. For example, the System Name of the system that you are configuring for Serial Connection access would be a good entry. However, the Name entry is purely descriptive, and can be anything at all.

2. Enter the remote system's telephone number.

   Type in the **Number** field the telephone number of the system that you will be accessing. Be sure to include the area code and any prefixes that might be necessary to reach this system (for example, some phone systems require that you dial a 9 to get an external phone line).

   Note: Do not use parentheses or dashes in the telephone number.

3. Assign a COM Port.

   Select the **COM Port** of the modem that you will be using to access the remote system.

4. Specify the modem's baud rate.

Select the **Baud Rate** of the modem that you will be using to access the remote system.

Notes:

a. If your serial connections fail frequently, try lowering the baud rate. Higher baud rates are more sensitive to line noise.

b. For best performance, select a baud rate that equal to or greater than your modem's maximum speed.

5. Enter a User ID for logging on to the remote system.

   Type in a **User ID** that will allow access to the remote system. This must match the User ID setting in the remote system's AutoAnswer setup.

6. Enter a password for logging on to the remote system.

   Type in a **Password** that will allow access to the remote system. This must match the Password setting in the remote system's AutoAnswer setup.

7. Select **Null Modem** if the connection will be established using a null modem connection.

   Note: The **Null Modem** checkbox **must** be checked if you will be using a null modem connection to communicate with the remote system.

8. Save the Serial Connection Control entry.

   Select **Apply** to save this entry.

Accessing Remote Systems

Once you have created one or more Serial Connection Control entries, you are ready to access remote systems.

Remote systems are accessed from the Netfinity Serial Connection Control window (see Figure 83 on page 254). To access a remote system:

1. Select from the **Name** field the Serial Connection Control entry for the remote system that you want to access.

2. Select **Start** to initiate the serial connection process.

Once you have initiated the serial connection process, your system will initialize your modem, dial the telephone number for the selected entry, wait for an answer, and then attempt to use the User ID/Password combination to access the remote system. If the connection is successful, you can add (or discover) the remote system with Remote System Manager. Then, you can remotely access and manage the remote system just as if it were part of your network.

Notes:

1. The remote system *must* have its own Serial Connection Control service running in AutoAnswer mode. If the remote system is not in AutoAnswer mode, your telephone call will not be answered by the remote system's modem.
2. If you want the Serial Connection Control service to automatically start and attempt to access a specific remote system when Netfinity is started, select the remote system's entry, and then select the **Auto Start** check box. Only one entry can be configured to start automatically.

Initialization String Guidelines

Although most modems share similar initialization string codes, there are differences from modem to modem. Therefore, it is very difficult to provide appropriate initialization strings for *all* modems. In some cases you might need to create your own initialization string for your modem. If you do, consult the documentation that comes with your modem for the appropriate initialization string codes.

- Required Initialization Codes

  For a modem to operate correctly with the Netfinity Serial Connection Control service, the initialization string must configure the modem as follows:

  – Command echoing OFF
  – Online character echoing OFF
  – Result codes ENABLED

- Verbal result codes ENABLED
- All codes and connect messages with BUSY and DT detection
- Protocol ind added - LAPM/MNP/NONE V42bis/MNP5
- Normal CD operations
- DTR ON-OFF hangup, disable AA and return to command mode
- CTS hardware flow control
- RTS control of received data to computer
- Queued and nondestructive break, no escape state
- Auto-answer off

Example: The initialization string for a U.S. Robotics Sportster modem using only the settings required for correct operation would be:

```
E0F1Q0V1X4&A3&C1&D2&H1&R2&Y3S0=0
```

- Additional Initialization Codes

  In addition to the required initialization codes, you can optimize the operation of the Netfinity Serial Connection Control service by configuring your modem with the following additional settings:

  - Speaker ON until carrier detected
  - Software flow control disabled
  - Auto-error control
  - Variable data rate

  Example: The initialization string for a U.S. Robotics Sportster modem using all the required and additional settings would be:

```
E0F1M1Q0V1X4&A3&C1&D2&H1&I0&K1&M4&
N0&R2&Y3S0=0
```

Chapter 21. Service Configuration Manager

You can use Service Configuration Manager to save the configuration of a Netfinity service from a selected system. The configuration is saved in a service configuration file (SCF). Once created, SCF files can be used by Event Scheduler to restore the configuration back to the same system, or they can be used (in conjuction with the Event Scheduler) to propagate that configuration to whatever other similar systems you choose.

Once you configure various Netfinity services (for example, Alert Manager or Critical File Monitor) on a particular system, you can use Service Configuration Manager to save the configuration of a service on that system. Then, using Event Scheduler or the command line interface, you can use the service configuration file (SCF) created with Service Configuration Manager to:

- Replace the service configuration on one or more remote systems, replicating the configuration of the service across multiple systems
- Back up the service configuration on a specific system in case of the loss of a service configuration
- Quickly change the configuration of a specific system's services
- Augment or replace the existing service configuration on a system, permitting standardization or addition of administrative facilities as required

The Service Configuration Manager window (see Figure 85 on page 262) presents the service configuration files that exist in the SCF directory. You can:

- Create a new service configuration file using the Service Configuration File Generator.

  For more information, see “Creating Service Configuration Files” on page 262.

- Edit an existing service configuration file using the Service Configuration File Editor.

  For more information, see “Editing Service Configuration Files” on page 264.

- Delete existing service configuration files.

For more information, see “Deleting Service Configuration Files” on page 266.

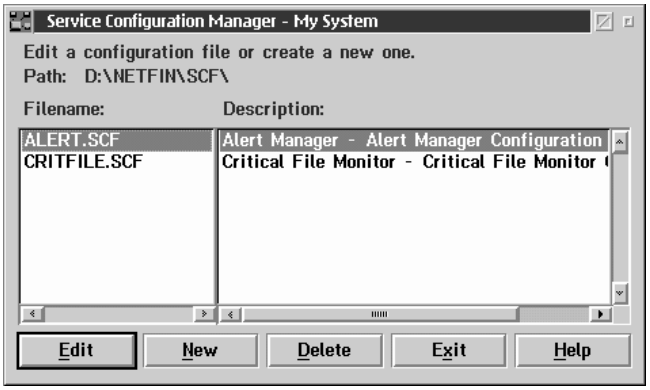

Figure 85. The Service Configuration Manager window.

Creating Service Configuration Files

To create a new Service Conifguration File:

1. Select **New**.

   This opens the Service Configuration File Generator window (see Figure 86 on page 263).

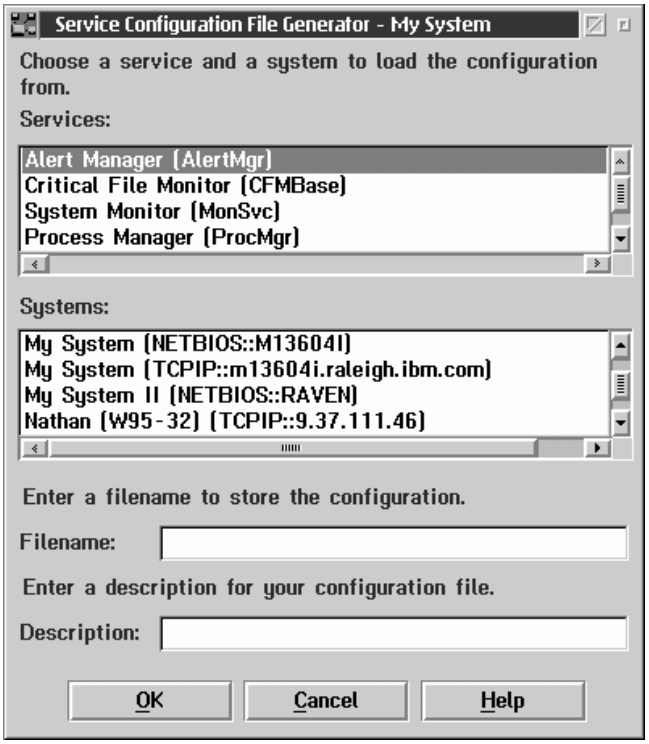

Figure 86. The Service Configuration File Generator window.

2. Select a Netfinity service from the **Services** selection list.

   Select the Netfinity service that has a configuration that you want to save as an SCF file.

3. Select a Netfinity system from the **Systems** selection list.

   Select a system that contains the service configuration that you want to save as a SCF file for use by Event Scheduler.

4. Type in the **File name** field a name for the SCF file. This file name must be a valid file name for storage in the Netfinity SCF subdirectory.

5. Type in the **Description** field a description of the SCF file (optional).

6. Select **OK**.

Sometimes the creation of the service configuration file is unsuccessful. This failure is often due to the source system being offline or to the source service being protected by security. If the service configuration file creation is unsuccessful, use Remote System Manager to ensure that the remote system is online and that you have access to the service.

If the service configuration file creation is successful, you will be asked whether you wish to view or edit the new SCF file. Select **Yes** to open the Service Configuration File Editor window. Select **No** to return to the Service Configuration Manager window. For more information on editing Service Configuration Files, see "Editing Service Configuration Files."

Editing Service Configuration Files

You can use Service Configuration File Editor to view the detailed information about a service configuration file (SCF) and to remove any undesired configuration records from the file.

To edit a Service Configuration File:

1. Select a Service Configuration File from the Service Configuration Manager window.
2. Select **Edit**.

   This opens the Service Configuration File Editor window (see Figure 87 on page 265).

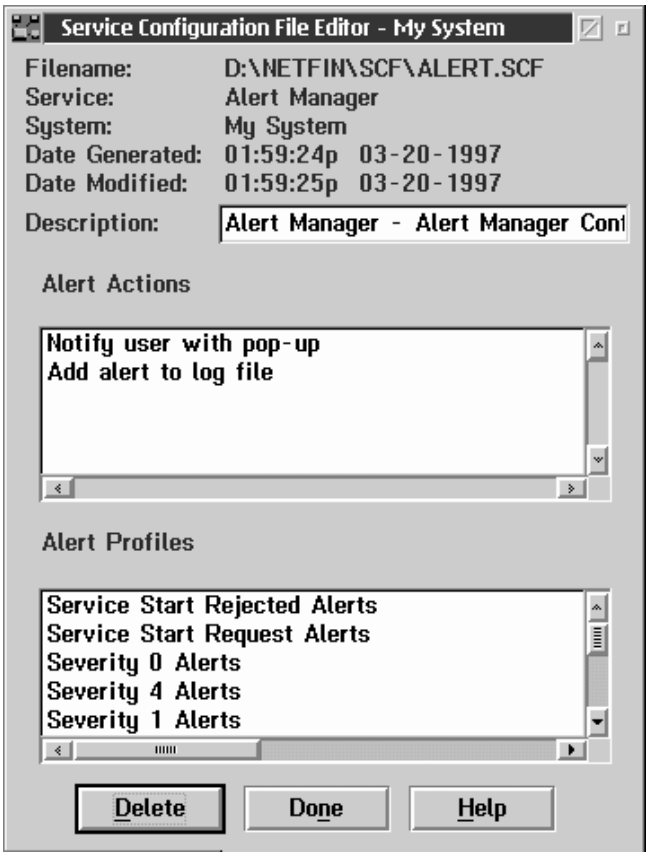

Figure 87. The Service Configuration File Editor window.

The top of the window displays the following information:

- The full path name of the file
- The Netfinity service that the configuration apllies to
- The name of the system from which the file was generated
- The date and time at which the file was generated
- The description given to the file when it was created, if any

The rest of the window contains one or more record selection lists. These lists show descriptive labels for all the records saved from the service configuration. This window contains the

records associated with the configuration file for the selected Netfinity service. For example, an SCF file created for Alert Manager will feature record selection lists for configured Alert Actions and Alert Profiles.

You can select these records and **Delete** them in order to remove them from the service configuration file permanently. You may do this if you want only a subset of the configuration contained on the original system to be restored to other systems you configure using this SCF. For example, if a service configuration file for Alert Manager contains 2 alert profiles that you want to propagate to other Netfinity systems, but also contains many other records (additional alert actions and alert profiles in this case) that you do not require, you can delete all of the records in the service configuration file except for the two alert profiles you need.

3. Select one or more service records that you wish to remove from the SCF file.
4. Select **Delete** to remove the selected records from the SCF file.

Deleting Service Configuration Files

To delete a Service Configuration File, select a Service Configuration File from the Service Configuration Manager window and then select **Delete**.

Chapter 22. Advanced System Management

Use the Advanced System Management service to configure and monitor many features of supported IBM system management subsystems. The Advanced System Management service works with the following system management subsystems:

- Advanced Systems Management Adapter
- System Management Processor (included with the Netfinity 5500)

With Advanced System Management you can configure system management events (such as POST, loader, and operating system timeouts or critical temperature, voltage, and tamper alerts). If any of these events occurs, the Advanced System Management service can be configured to automatically forward a Netfinity alert in one of three ways:

- Alert forwarded to another Netfinity system
- Alert forwarded to a standard numeric pager
- Alert forwarded to an alphanumeric numeric pager

With this service, you can dialout and directly access and control a remote system's system management subsystem.

In addition, with Advanced System Management you can remotely monitor, record, and replay all textual data generated during power–on self–test (POST) on a remote system that includes a supported system management subsystem. While monitoring a remote system during POST, you can enter key commands on your keyboard that will then be relayed to the remote system.

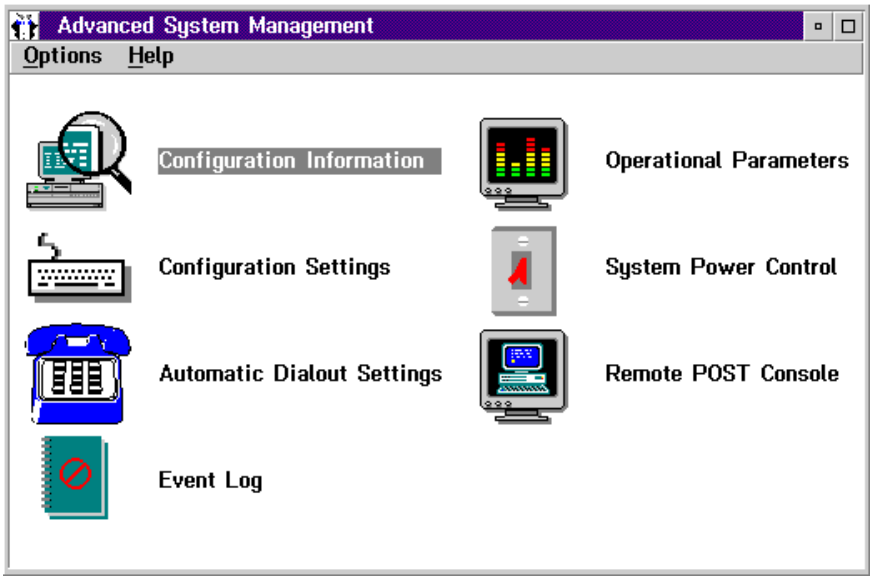

Figure 88. The Advanced System Management service

To start the Advanced System Management service, double-click on the Advanced System Management icon in the Netfinity Service Manager window. Then double-click on any of the selections available in the Advanced System Management window to access the function or configuration information you need.

- Select **Configuration Information** to view detailed information about the system management subsystem, including RAM microcode, ROM microcode, and device driver information. If you are managing the system management subsystem of an IBM Netfinity 5500 you will also have access to extensive system information. For more information on Configuration Information, see "Configuration Information" on page 270.
- Select **Configuration Settings** to configure many features of the system management subsystem. These features include system identification data, dial-in security settings, the time and date reported by the system management subsystem clock, timeout and delay values, and advanced modem settings. For more information on Configuration Settings, see "Configuration Settings" on page 272.

- Select **Automatic Dialout Settings** to configure the system management subsystems automatic dialout functions. For more information on Automatic Dialout Settings, see “Automatic Dialout Settings” on page 286.
- Select **Event Log** to view the contents of the system management subsystem Event Log. Information about all remote access attempts and dialout events that have occurred is recorded in the system management subsystem Event Log. For more information on the Event Log, see “Event Log” on page 297.
- Select **Operational Parameters** to view the current values or status of many system components monitored by the system management subsystem. For more information on Operational Parameters, see “Operational Parameters” on page 298.
- Select **System Power Control** to instruct the system management subsystem to power off the system, restart the system, or power on the system. For more information on System Power Control, see “System Power Control” on page 299.
- Select **Remote POST Console** to use the system management subsystem to remotely monitor, record, and replay all textual output generated during POST on a remote system that has a supported system management subsystem. For more information on using Remote POST, see “Remote POST Console” on page 301.
- To update the microcode on your system management subsystem, from the **Options** pulldown menu select **Update Microcode...** and then select **System Management Subsystem**. For more information on updating microcode, see “Updating System Management Subsystem Microcode” on page 304.

Using a Serial Connection to Manage Remote System Management Subsystems

If you want to use your system’s modem to dial out and access the system management subsystem on a remote system, use Serial Connection Control to establish a connection with the remote system

and then start the Advanced System Management service. You can also use Serial Connection Control to establish a null modem connection to another system. For more information on Serial Connection Control, see the *Netfinity Manager User's Guide*.

Notes:

1. Be sure to check the **System Management Processor** check box in the Netfinity Serial Connection Control window when you create the Serial Connection Control entry. If this check box is not checked the connection with the remote system management subsystem will fail.
2. When using Serial Connection Control to configure a Dialout Entry for use by the Advanced System Management service, be sure to enter the Login ID and Password for access to the remote system's system management subsystem, not the User ID and Password for access to Netfinity services on the remote system.
3. When creating a Serial Connection Control entry to establish a null modem connection to a remote system's System Management Processor, make sure that the **Port Baud Rate** value (configured using the Serial Connection Control service) is set to match the **Baud Rate** value (configured using the Advanced System Management control service) of the target system. If the **Port Baud Rate** and the **Baud Rate** values do not match, the connection will fail.

Configuration Information

The Configuration Information window (shown in Figure 89 on page 271) contains detailed information about the system management subsystem, including RAM microcode, ROM microcode, and device driver information.

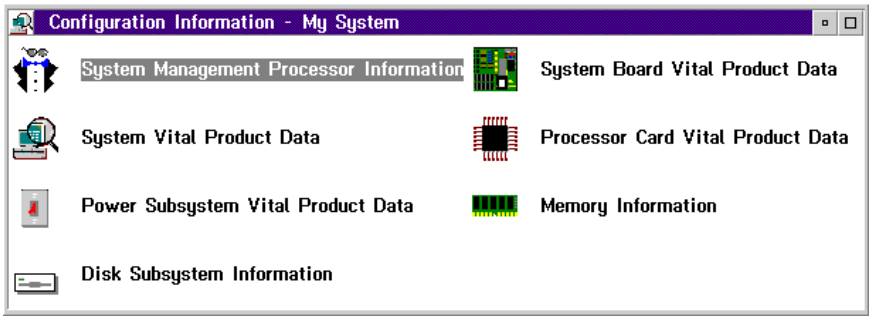

Figure 89. The Configuration Information window

Configuration Settings

Use the selections available in the Configuration Settings window (see Figure 90 on page 273) to configure many features of the system management subsystem. These features include system identification data, dial-in security settings, the time and date reported by the system management subsystem clock, timeout and delay values, and advanced modem settings.

This window contains:

- System Identification group
- Dial-in settings group
- System Management Subsystem Clock group
- POST timeout, Loader timeout, O/S timeout, and Power off delay fields

This window also includes the Modem button. Select **Modem** to open the Modem Settings window (see "Modem Settings" on page 281).

The System Identification Group

The System Identification group contains two fields to help you identify the system that contains the system management subsystem.

Field	Description
Name	Can be used to provide a name for the system, the name of the system's user, or the name of a contact.
Number	Can be used to identify the system with a specific serial or identification number, to record the phone number used to dial into the system, or to provide the phone number of a contact.

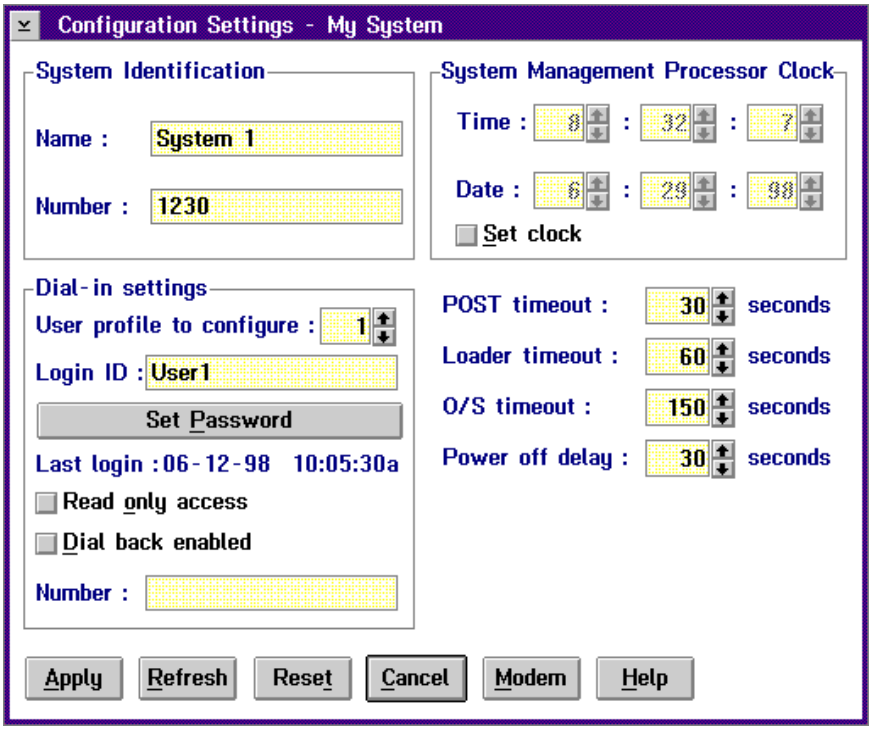

Figure 90. The Configuration Settings window

To change the information provided by these fields:

1. In the **Name** or **Number** field, type the system information you want to record.
2. Select **Apply** to save this information.

The Dial-In Settings Group

Use the selections available in the Dial-In Settings group to enable or disable dial-in support, and to enable users to dial in and access the system management subsystem. The Dial-In Settings group contains the following items.

Item	Description
User profile to configure	Use the spin buttons to select the user profile you want to configure. This service supports up to six separate user profiles on systems with an Advanced Systems Management Adapter, and up to twelve separate profiles on IBM Netfinity 5500 systems.
Login ID	Type in this field the login ID that will be used by the remote user. Up to six Login IDs can be configured. (This field is case sensitive.) *Note:* A Login ID *must* be specified to remotely access the system management subsystem.
Set Password	A password must be provided along with the Login ID to allow a remote user to access the system management subsystem. After providing a Login ID, click on **Set Password** to open the Set Password window. (The fields in the Set Password window are case sensitive.)
Last login	Shows the date and time of the last successful login by a remote user.
Read only access	If the **Read only access** check box is checked, the users whose profile is selected will not be able to alter any of the system management subsystem settings when access is granted. The user will, however, be able to see all currently configured settings and values except passwords.
Dial back enabled	If the **Dial back enabled** check box is checked, the system management subsystem will automatically terminate the connection as soon as the user whose profile is selected logs in, and will then use the telephone number that is entered in the **Number** field to dial out and attempt to connect with a remote system.

If necessary, select **Modem** to access the Modem Settings window (see "Modem Settings" on page 281). From the Modem Settings window you can specify modem settings and dialing settings.

To create a new login ID for a remote user:

1. In the **Login ID** field, type the ID that will be used by the remote user. This ID can be up to 8 characters.
2. Remote users must provide a password along with a login ID in order to access the system management subsystem. Select **Set Password** to open the Set Password window.

   From the Set Password window:

   a. In the **Enter Password** field, type a password.

      Note: This password must be 5–8 characters in length and must contain at least one nonalphanumeric character.

   b. In the **Re-enter Password** field, type the same password that you typed in the **Enter Password** field.

   c. Click on **OK** to save this password and close the Set Password window.
3. Click on **Apply** to save the new user ID.

To delete the currently selected login ID:

1. Use the spin buttons beside the **User ID to configure** field to select a previously configured User profile.
2. Click on the **Login ID** field.
3. Using the Backspace or Delete key, delete the currently displayed login ID.
4. Click on **Apply** to remove the user ID.

The System Management Subsystem Clock Group

Use the selections available in the System Management Subsystem Clock group to set the time and date that is reported by the system management subsystem.

To change the currently set time or date:

1. Verify that there is a check in the **Set System Management Subsystem Clock** check box. This check box *must* be checked to enable the Advanced System Management to change the currently stored time and date values.
2. Use the spin buttons beside each field to set the time or date.
   - The **Time** fields represent, when viewed from left to right, hours, minutes, and seconds.
   - The **Date** fields represent, when viewed from left to right, month, date, and year.
3. Click on **Apply** to save the new time and date.

POST Timeout

Note: This function requires a specially architected POST routine and is available only on some IBM systems. For a list of systems that support this feature, see "Supported Advanced Functions" on page 305.

The **POST timeout** field shows the number of seconds that the system management subsystem will wait for the system's power-on self-test (POST) to complete before generating a POST Timeout event. If POST takes longer than the configured amount of time to complete and the **POST timeout** check box (found in the **Enabled Alerts Dialout** group on the Automatic Dialout Settings window) is checked, the system management subsystem will automatically restart the system one time and will attempt to forward an alert to all enabled Dialout Entries. Once the system is restarted **POST timeout** is automatically disabled.

To set the POST timeout value, use the spin buttons beside the **POST timeout** field to set the number of seconds that the system management subsystem will wait for POST to complete. Then, click on **Apply** to save this value.

For more information on the Automatic Dialout Settings window, see "Automatic Dialout Settings" on page 286.

Loader Timeout

Note: This function requires a specially architected POST routine and is available only on some IBM systems. For a list of systems that support this feature, see "Supported Advanced Functions" on page 305.

The **Loader timeout** field shows the number of seconds that the system management subsystem will wait for the system's loading process to complete before generating a Loader Timeout event. The Loader Timeout measures the amount of time that passes between the completion of POST and the end of operating system (O/S) startup. If this takes longer than the configured amount of time to complete and the **Loader timeout** check box (found in the **Enabled Alerts Dialout** group of the Automatic Dialout Settings window) is checked, the system management subsystem will automatically restart the system one time and will attempt to forward an alert to all enabled Dialout Entries. Once the system is restarted **Loader timeout** is automatically disabled.

To set the Loader timeout value, use the spin buttons beside the **Loader timeout** field to set the number of seconds that the system management subsystem will wait between POST completion and O/S startup before generating a timeout event. Then, click on **Apply** to save this value.

For more information on the Automatic Dialout Settings window, see "Automatic Dialout Settings" on page 286.

O/S Timeout

The **O/S timeout** field shows the number of seconds that the system management subsystem will wait for the system's operating system to respond before generating a O/S Timeout event. If the O/S takes longer than the configured amount of time to respond and the device driver is installed and running correctly, the system management subsystem will attempt to restart the system, and if the **O/S timeout** check box (found in the **Enabled Alerts Dialout** group of the Automatic Dialout Settings window) is checked, the system management subsystem will automatically restart the system one time and will attempt to forward an alert to all enabled Dialout Entries.

To set the O/S timeout value, use the spin buttons beside the **O/S timeout** field to set the number of seconds that the system management subsystem will wait for the system's operating system to respond before generating a O/S Timeout event. Then, click on **Apply** to save this value.

For more information on the Automatic Dialout Settings window, see "Automatic Dialout Settings" on page 286.

Power Off Delay

The **Power off delay** field shows the number of seconds that the system management subsystem will wait for the system's operating system shutdown process to complete before powering off the system.

When the system management subsystem initiates a power down procedure and the **Power off** check box (found in the **Enabled Alerts Dialout** group of the Automatic Dialout Settings window) is checked, the system management subsystem will automatically attempt to forward an alert to all enabled Dialout Entries. This alert is forwarded after the system is powered off and the **Power off delay** time has passed.

To set the power off delay value, use the spin buttons beside the **Power off delay** field to set the number of seconds that the system management subsystem will wait for the system's operating system shutdown to complete before powering off the system. Then, click on **Apply** to save this value.

For more information on the Automatic Dialout Settings window, see "Automatic Dialout Settings" on page 286.

Other Configuration Settings Functions

The Configurations Settings window also includes three additional buttons:

Button	Description
Refresh	Select **Refresh** to update all data that is shown on the System Management Subsystem Configuration Settings window, including date, time, and last login.
Reset	Select **Reset** to set *all* Advanced System Management settings back to their default values, including configuration settings, dialout settings, and advanced dialout settings. *Important:* All previously configured system management subsystem settings will be permanently lost.
Cancel	Select **Cancel** to close this window without saving any changes.

Modem Settings

Use the Modem Settings window to specify advanced modem and dialing settings. To open this window, click on **Modem** from the Configuration Settings window (see "Configuration Settings" on page 272).

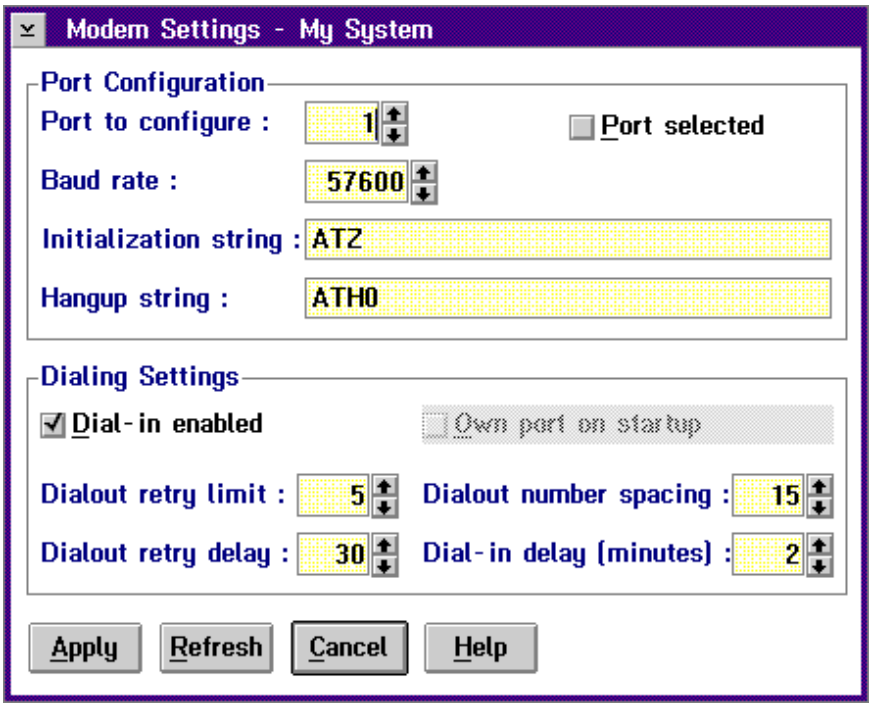

Figure 91. The Modem Settings window

The Port Configuration Group

Use the Modem Settings group to specify and configure the modem that will be used to forward the alert when a System Management Subsystem Dialout Event occurs. The Port Configuration group contains the following items.

Item	Description
Port to configure	Use the spin buttons to select the port that your modem is configured to use. This spin button will show only values that are available for use by your system management subsystem. The port that you select to use affects the availability of the modem for use by either the system management subsystem or the operating system. You can select Port A, Port B, or Port C. • If you select Port A, the modem will be available for use by the operating system until the system management subsystem uses the modem for the first time. After the system management subsystem takes control of the modem, the operating system will not be able to access or use the modem until the operating system is restarted. • If you select Port B, the modem will be dedicated for use by the operating system only. The system management subsystem will not be able to access a modem that is configured to use Port B. • If you select Port C, the modem will be dedicated for use by the system management subsystem only. The operating system will not be able to access a modem that is configured to use Port C.
Baud rate	Use the spin buttons to specify the baud rate of the modem.
Initialization string	Type the initialization string that will be used for the specified modem. A default string is provided (ATE0). Do not change this string unless your dialout functions are not working properly. If you need to change the initialization string, see “Initialization String Guidelines” on page 285.
Caller ID string	Type the initialization string that will be used to get Caller ID information from the modem.

Item	Description
Port selected	This check box indicates whether the port number currently displayed in the **Port to configure** field is the port that is currently designated for use by the system management subsystem. Check this check box if you want to configure the System Management Subsystem to use the currently displayed port number.
Null modem	Check this check box to use a null modem connection to allow access from a remote Netfinity system. *Note:* If the **Null modem** check box is checked, you cannot send dialout alerts to other systems using a modem or receive dialout alerts from other systems.
Return to factory settings string	Type the initialization string that returns the modem to its factory settings when the modem is initialized. The default is AT&F0.
Query string	Type the initialization string that is used to find out if the modem is attached. The default is AT.
Escape string	Type the initialization string that returns the modem to command mode when it is currently talking to another modem (connected). The default is +++.
Escape guard time	Type in this field the length of time before and after the escape string is issued to the modem. This value is measured in 10 millisecond intervals. The default value is 1 second.
Dial prefix string	Type the initialization string that is used before the number to be dialed. The default is ATDT.
Dial postfix string	Type the initialization string that is used after the number is dialed to tell the modem to stop dialing. The default is the Carriage Return character or ¬M.
Auto-answer string	Type the initialization string that is used to tell modem to answer the phone when it rings. The default is to answer after two rings or ATS0=2.
Auto-answer stop	Type the initialization string that is used to tell the modem to stop answering the phone automatically when it rings. The default is ATS0=0;

The Dialing Settings Group

Use the Dialing Settings group to specify settings related to the modem, and to configure the modem that is used to forward an alert when a System Management Subsystem Dialout Event occurs. The Dialing Settings group contains the following items.

Item	Description
Dial-in enabled	Check this check box to enable remote users to dial into and access the system management subsystem. If this box is unchecked, remote users will be unable to remotely access the system management subsystem. Click on **Apply** after checking or unchecking this check box to save the new setting.
Dialout retry limit	Use the spin buttons to select the number of additional times that the Advanced System Management will attempt to forward the alert.
Dialout retry delay	Use the spin buttons to specify the number of seconds that the Advanced System Management will wait before retrying a dialout attempt.
Own port on startup	Check this check box to reserve a serial port for exclusive use by the system management subsystem. If the system management subsystem is built into your system, checking this box will reserve one of your system's serial ports. If the system management subsystem is an adapter, checking this box will reserve one of the adapter's integrated communications ports. Click on **Apply** after checking or unchecking this check box to save the new setting. *Note:* Check this box if you are configuring your system for dial-in access. If this check box is not checked, you will be unable to dial into this system unless the system management subsystem has reclaimed the port for a dialout. If you want to configure the system management subsystem to always be dial-in enabled, regardless of whether the system is currently powered up, you must check this check box. When this check box is checked, you cannot configure the specified port for use by your system.

Item	Description
Dialout number spacing	If you have configured more than one Dialout Entry to forward alerts, the system management subsystem will attempt to contact each of these entries sequentially. Use the spin buttons to specify the number of seconds for the system management subsystem to wait between dialout attempts for separate Dialout Entries.
Dial-in delay (minutes)	The **Dial-in delay (minutes)** field shows the number of minutes that must pass after an incorrect User ID or Password has been used in five successive dial-in attempts before valid dial-in access will be permitted. After the fifth successive login failure, dial-in access is disabled for the number of minutes you specify, the system management subsystem adds an entry in the Event Log noting that dial-in access was suspended due to five successive login failures, and the system management subsystem attempts to forward an alert if the **Tamper** Enabled Alerts Dialout check box has been checked (see Figure 92 on page 287).

Initialization String Guidelines

If you need to provide a new initialization string, refer to the user's guide that came with your modem. Your initialization string must contain commands that configure your modem as follows:

- Command echoing OFF
- Online character echoing OFF
- Result codes ENABLED
- Verbal result codes ENABLED
- All codes and Connect messages with BUSY and DT detection
- Protocol identifiers added - LAPM/MNP/NONE V42bis/MNP5
- Normal CD operations
- DTR ON-OFF hang-up, disable AA and return to command mode
- CTS hardware flow control
- RTS control of receive data to computer
- Queued and nondestructive break, no escape state

Changing Dialout Entry Settings

To apply settings to a selected Dialout Entry:

1. Specify Modem Settings.
2. Specify Dialing Settings.
3. Click on **Apply** to save these settings and return to the Automatic Dialout Settings window.

Automatic Dialout Settings

Use the Automatic Dialout Settings window (shown in Figure 92 on page 287) to configure the system management subsystem's automatic dialout functions. If you configure a Dialout Entry, the system management subsystem will attempt to forward an alert to a remote Netfinity system, a numeric pager, or an alphanumeric pager when any of the events selected from the **Enabled Alerts Dialout** group occur. This alert will contain information about the nature of the event that occurred, the time and date at which the event occurred, and the name of the system that generated the alert.

If the system management subsystem is currently performing a dialout function, the **Dialout status** text will read DIALOUT ON. If you want to halt a currently active dialout function, click on **Stop Dialout**.

Your system management subsystem can be configured with up to six separate Dialout Entries.

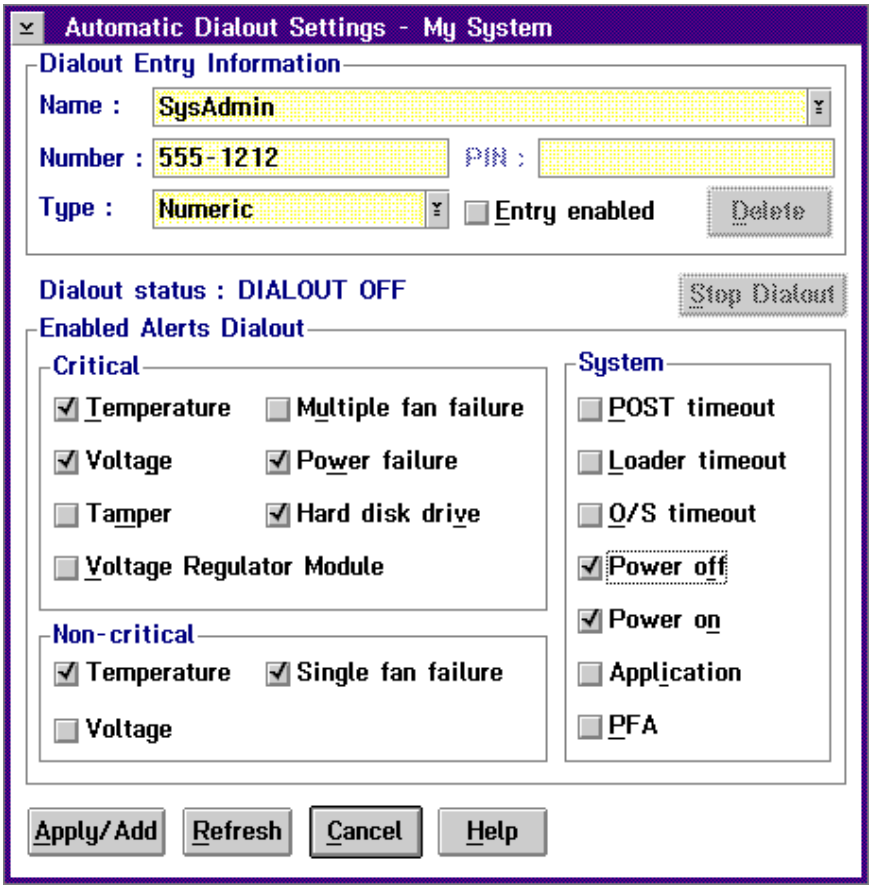

Figure 92. The Automatic Dialout Settings window

Dialout Entry Information Group

To edit or create a Dialout Entry:

1. In the **Name** field, type the name of the person or system that the alert will be forwarded to. The information in the **Name** field is strictly for your use in identifying the Dialout Entry. If you are editing a previously configured Dialout Entry, select the entry that you want to edit from the **Name** selection list.

2. In the **Number** field, type the telephone number that will be used by the system's modem to dial out to a digital pager service. After the modem connects to the pager service, it will send numeric data pspecific to the dialout event.

   Note: Depending on your paging service, you might need to increase the amount of time that this alert action waits after dialing the telephone number before it transmits the numeric data. To increase the amount of time that will pass before the numeric data is transmitted, add one or more commas (",") to the end of the telephone number. Each comma will cause the modem to wait two seconds before transmitting the numeric data.

3. In the **PIN** field, type the personal identification number required by your alphanumeric pager provider. This field will be active only if you select Alpha-numeric in the **Type** field.

4. From the **Type** selection list, select the type of connection the system management subsystem will attempt to make in order to forward the event notification. You can select Numeric (for standard pagers), Alpha-numeric (for alphanumeric pagers), or Netfinity (for connecting to a remote Netfinity system).

5. Check the **Entry enabled** check box to activate this Dialout Entry. If the **Entry enabled** check box is not checked, no dialouts will be made to this entry.

6. Select dialout events from the **Enabled Alerts Dialout** group. If any of the checked events occur, the system management subsystem will dial out to the telephone number specified in the **Number** field and forward an alert describing the event using the method selected in the **Type** field. For more detailed information about dialout events, see "Enabled Alerts Dialout Group" on page 289.

7. Click on **Apply/Add** to save these settings.

To remove a previously configured Dialout Entry, select the name of the entry from the **Name** selection list and then select **Delete**.

Enabled Alerts Dialout Group

Use the selections available in the Enabled Alerts Dialout group to specify which system management subsystem events will result in all currently configured Dialout Entries being contacted by the system management subsystem. Any selected items will, if detected by the system management subsystem, result in an alert describing the event being forwarded, using the method selected in the **Type** field, to the recipient specified by the Dialout Entry.

If the alert is being forwarded to a pager, Advanced System Management will include information about the event that triggered the alert. If the alert is forwarded to a numeric (or standard), pager, the page will include a code number that corresponds to the triggering event. If the alert is forwarded to an alphanumeric pager, the page will include both a code number and a text string that describe the triggering event. For more information on the nurmeic codes and text strings that are transmitted to pgers, see "Enabled Alerts Dialout Group."

The Enable Alerts Dialout group is divided into **Critical**, **Non-critical**, and **System** groups. The **Critical** Enabled Alerts Dialout group contains the following items.

Item	Description (if checked)	Numeric Code	Text String
Temperature	The system management subsystem will dial out and then automatically initiate a system shutdown if any monitored temperatures exceed their threshold values.	00	TEMPERATURE
Voltage	The system management subsystem will dial out if the voltages of any monitored power sources fall outside their specified operational ranges.	01	VOLTAGE

Item	Description (if checked)	Numeric Code	Text String
Tamper	The system management subsystem will dial out if six consecutive remote login attempts fail.	02	TAMPER
Multiple fan failure	The system management subsystem will dial out if two (or more) of the system's cooling fans fail *and* will automatically initiate a system shutdown. *Note:* This function is available only on some IBM systems. For a list of systems that support this feature, see "Supported Advanced Functions" on page 305.	03	MULTIPLE FAN FAILURE
Power failure	The system management subsystem will dial out if the system's power supply fails. *Note:* This function is available only on some IBM systems. For a list of systems that support this feature, see "Supported Advanced Functions" on page 305.	04	POWER FAILURE

Item	Description (if checked)	Numeric Code	Text String
Hard disk drive	The system management subsystem will dial out if one or more of the hard disk drives in the system fail. *Note:* This function is available only on some IBM systems. For a list of systems that support this feature, see "Supported Advanced Functions" on page 305.	05	HARD DRIVE
Voltage regulator module failure	The system management subsystem will dial out and then automatically initiate a system shutdown if the voltage regulator module (VRM) fails. *Note:* This function is available only on some IBM systems. For a list of systems that support this feature, see "Supported Advanced Functions" on page 305.	06	VRM FAILURE

The **Non-critical** Enabled Alerts Dialout group contains the following items.

Item	Description (if checked)	Numeric Code	Text String
Temperature	The system management subsystem will dial out if any monitored temperatures exceed their threshold values. However, unlike the Critical Temperature event, this Alerts Dialout will *not* initiate a system shutdown automatically. *Note:* This function is available only on some IBM systems. For a list of systems that support this feature, see "Supported Advanced Functions" on page 305.	12	Non-critical Temperature

Item	Description (if checked)	Numeric Code	Text String
Single fan failure	The system management subsystem will dial out if one of the system's cooling fans fail. *Note:* This function is available only on some IBM systems. For a list of systems that support this feature, see "Supported Advanced Functions" on page 305.	11	Single Fan Failure
Voltage	The system management subsystem will dial out if any of the monitored voltages exceed their threshold values.	13	Non-critical Temperature

The **System** Enabled Alerts Dialout group contains the following items.

Item	Description (if checked)	Numeric Code	Text String
POST timeout	The system management subsystem will dial out if the **POST timeout value** (specified in the System Management Subsystem Configuration Settings window) is exceeded.	20	POST Hang
Loader timeout	The system management subsystem will dial out if the **Loader timeout value** (specified in the System Management Subsystem Configuration Settings window) is exceeded.	26	Loader Watchdog Failure

Item	Description (if checked)	Numeric Code	Text String
O/S timeout	The system management subsystem will dial out if the **O/S timeout value** (specified in the System Management Subsystem Configuration Settings window) is exceeded.	21	OS Hang
Power off	The system management subsystem will dial out if the system is powered off.	23	System Power Off
Power on	The system management subsystem will dial out if the system is powered on.	24	System Power On

Item	Description (if checked)	Numeric Code	Text String
Application	The system management subsystem will dial out if it receives a Netfinity alert (Netfinity can forward alerts directly to the system management subsystem using the Alert Manager **Forward Alert to System Management Subsystem** action)	22	Application Logged Event
PFA	The system management subsystem will dial out if it receives a PFA alert from the system.	27	PFA

Event Log

Use Event Log to open the System Management Subsystem Logs window (shown in Figure 93). This window contains all entries that are currently stored in the system management subsystem event log. Information about all remote access attempts and dialout events that have occurred is recorded in the system management subsystem event log.

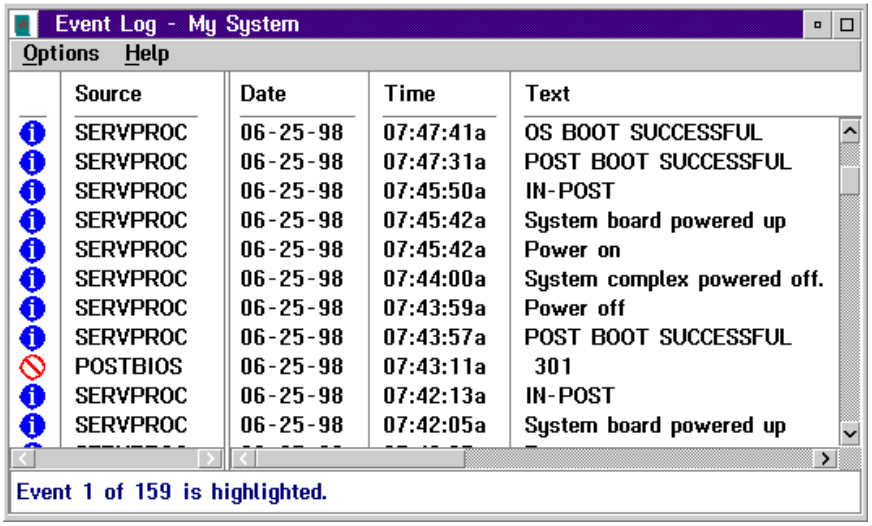

Figure 93. The System Management Subsystem Logs window

Notes:

1. If you are using the Advanced System Management service with an Advanced Systems Management Adapter installed in a Netfinity 7000 system, the event log might contain entries that begin with the text "I2C Message." These messages are normal and are intended for use by IBM servicers in the event of system problems.
2. If you are using the Advanced System Management service with a Netfinity 5500, the event log will also include any POST error messages.

The following functions are available from the Options pulldown menu in the System Management Subsystem Logs window:

- Load

  Refreshes the contents of the System Management Subsystem Logs window.

- Print to File

  Saves the contents of the System Management Subsystem Logs window to a text file.

- Print to Printer

  Sends the contents of the System Management Subsystem Logs window to a printer attached to your system.

- Clear Log

  Erases all entries that are currently stored in the system management subsystem Event Log (including any entries that are not currently visible in the System Management Subsystem Log window).

  Note: Once you use **Clear Log** to erase the entries in the system management subsystem Event Log, they are permanently erased and cannot be retrieved.

Operational Parameters

The Operational Parameters window (see Figure 94 on page 299) shows the current values or status of many system components monitored by the system management subsystem. Available values include:

- Power supply voltages (including +5 V ac, +12 V ac, -3.3 V ac, -12 V ac; Netfinity 5500 systems feature additional -5 V ac and Voltage Regulation Module VRM“ monitors).
- Current temperatures and threshold levels for system components such as far-end adapter, center adapter, microprocessors, system board, and DASD backplane.

  Note: Monitored system components vary by system management subsystem.

- System state (including O/S started, O/S running, POST started, POST stopped (error detected), and system powered off/state unknown).
- System power status (on or off).
- Power on hours; the total number of hours that the system has been powered on. (This is a cumulative count of all powered-on hours, not a count of hours since the last system restart).

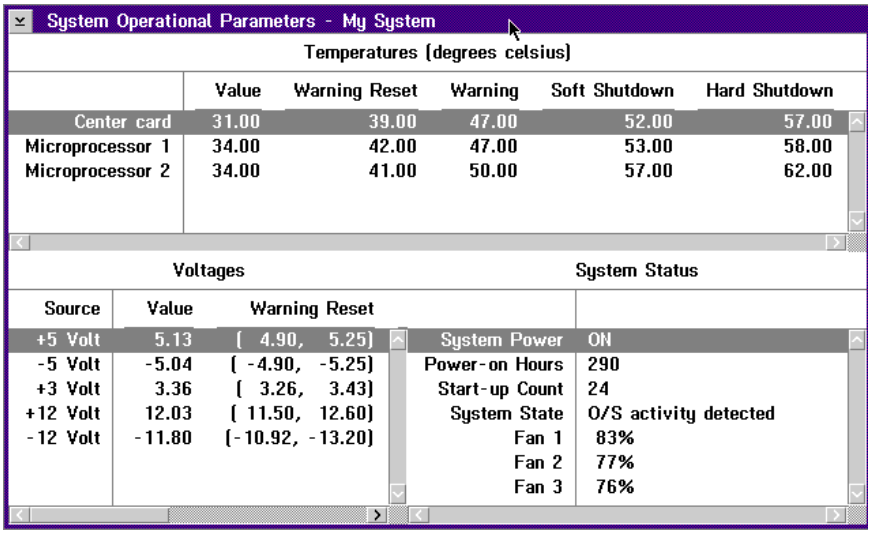

Figure 94. The Operational Parameters window

Note: Some temperature monitors are available only on some IBM systems. For a list of systems that support additional temperature monitors, see "Supported Advanced Functions" on page 305.

System Power Control

Use the System Power Control window to instruct the system management subsystem to power off the system, restart the system, or power on the system. To initiate any of the power control options, you must first check the **Enable power control options** check box. If this check box in unchecked, the **Power Control Options** field will not be available.

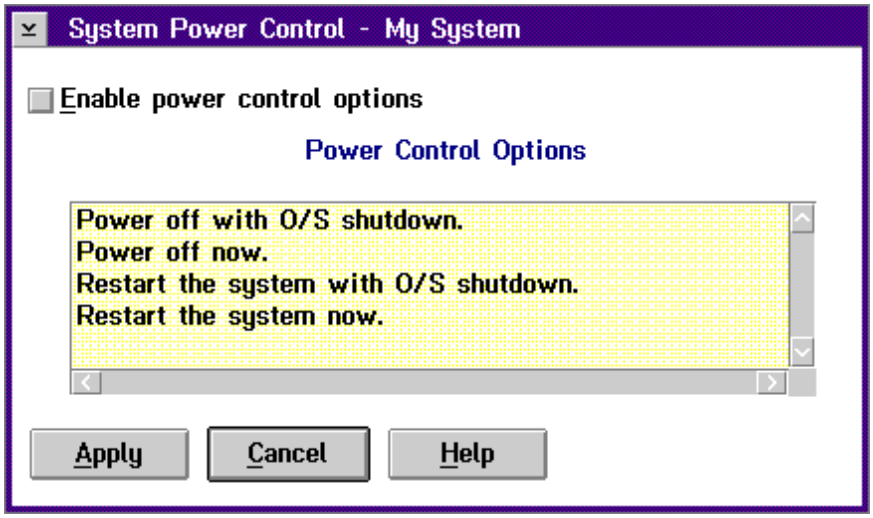

Figure 95. The System Power Control window

The following System Power Control functions are available at all times.

Function	Description
Power off with O/S shutdown	Performs an O/S shutdown before removing power from the system.
Power off now	Immediately removes power from the system.
Restart the system with O/S shutdown	Performs an O/S shutdown, removes power from the system, and then restores power to the system.
Restart the system now	Immediately removes and then restores power to the system.

If you are connected to the system management subsystem through a modem, the **Power on now** selection will also be available. This function powers up the system and allows the microprocessor to perform POST, loading, and O/S startup procedures.

To initiate a Power Control Option:

1. Check the **Enable power control options** check box.

   Note: To initiate any of the power control options, you must first check the **Enable power control options** check box. If this check box in unchecked, the **Power Control Options** field will not be available.

2. From the **Power Control Options** field, select the Power Control Option you want to activate.
3. Click on **Apply**.

Remote POST Console

You can use the Advanced System Management Remote POST Console function to remotely monitor, record, and replay all textual output generated during POST. To monitor and record the POST data on a remote system:

1. Connect to the remote system's system management subsystem.
2. Open the Remote POST window.
3. Restart the remote system (using the Advanced System Management's System Power Control functions).

All POST data will be displayed in and recorded by the Remote POST Console as the remote system completes POST. While you are monitoring POST on a remote system all local keystrokes are relayed automatically to the remote system, enabling you to interact with the POST process on the remote system.

To review data after POST completes, disconnect from the remote system and use the Replay functions.

Figure 96. The Remote POST window

Use the selections available in the Replay pull-down menu to replay the textual output that was captured during the last Remote POST operation. All text that was displayed by the remote system during POST will be displayed as it appeared on the remote system.

- To begin playing the recorded POST data, or to resume playing the recorded POST data after stopping playback, click on **Replay Last POST**.
- To halt playback of the recorded POST data, click on **Stop**.
- To resume viewing the recorded POST data from the beginning, click on **Restart**.
- Select **Fast**, **Medium**, or **Slow** to specify the speed at which the recorded POST data is displayed in the Remote POST window.

Notes:

1. Remote POST data can be replayed only when you are *not* connected to a remote system's system management subsystem.
2. This function requires a specially architected POST routine and is available only on some IBM systems. For a list of systems that support this feature, see "Supported Advanced Functions" on page 305.

Updating System Management Subsystem Microcode

To update the system management subsystem microcode:

1. From the **Options** pulldown menu select **Update Microcode...** and then select **System Management Subsystem**.

   A file selection window appears.

2. Use the file selection window to select the source disk drive (or diskette drive) and directory where the system manamgent subsystem microcode update is located.

3. Select **OK** to continue.

4. Warning notices will appear, asking that you verify that you want to continue. Select **OK** to continue or **Cancel** to stop the microcode update process.

5. When you have verified that you want to proceed with updating the system management subsystem microcode, the Advanced System Management service will apply the microcode update to the system management subsystem.

   During this process, some of the monitoring functions of some system management subsystems (such as the environmental monitors available with the Netfinity 550 System Management Processor) will be disabled. Once the microcode update is complete, all system monitoring will resume.

Supported Servers

Advanced System Management will function with an Advanced Systems Management Adapter (with microcode revision 10 or later) that is installed in any of the following IBM servers:

- PC Server 310 (all ISA models)
- PC Server 315
- PC Server 320 (all EISA models)
- PC Server 325
- PC Server 330
- PC Server 520 (all EISA models)

- PC Server 704 with PC Server Systems Management Cable (94G6970)
- Netfinity 7000

Advanced System Management also functions on Netfinity 5500 servers. These servers feature an integrated system management subsystem called System Management Processor

Supported Advanced Functions

Some advanced Advanced System Management functions require specially architected microcode or hardware to be present on the server. Unless noted in the following sections, a Advanced System Management function is available for use on *all* supported servers that have an Advanced Systems Management Adapter installed.

Note: Check the IBM PC Server World Wide Web page at http://www.pc.ibm.com/us/netfinity/ for the latest information about supported servers and supported advanced functions.

POST Timeout

POST Timeout is available only on the following systems:

- PC Server 325
- PC Server 330
- Netfinity 7000

Loader Timeout

Loader Timeout is available only on the following systems:

- PC Server 325
- PC Server 330

Power Supply Failure Automatic Dialout Setting

Power Supply Failure dialout is available only on the Netfinity 7000.

Fan Failure Automatic Dialout Setting

Fan Failure dialout is available only on the following systems:

- PC Server 325

- PC Server 330
- Netfinity 7000

Hard Disk Drive Failure Automatic Dialout Setting

Hard Disk Drive Failure dialout is available only on the Netfinity 7000.

Non-Critical Temperature Automatic Dialout Setting

Non-Critical Temperature dialout is available only on the Netfinity 7000.

Remote POST Console, Replay, and Remote Diagnostics

Remote POST console, replay, and remote diagnostics are available only on the following systems:

- PC Server 325 (remote diagnostics available on models PTO, PTW, PBO, and RBO)
- PC Server 330 (remote diagnostics available on models PTO, PTW, and PBO)
- Netfinity 7000 (remote diagnostics not available)

Additional Temperature Monitors

Temperature monitors for the system board, microprocessor area, microprocessor 1, and microprocessor 2 are available only on the following systems:

- PC Server 325
- PC Server 330

Accessing the System Management Subsystem without Netfinity Manager

If for some reason you are unable to use Netfinity Manager to access and manage your system management subsystem, you can use a terminal program and a modem to connect directly to the system management subsystem. This modem should be connected to management port C (for more information on configuring the system management subsystem modem, see “Modem Settings” on page 281). When connected, you will be able to access a variety of

monitor, configuration, and error log data. You can also power the remote system on or off, shutdown and restart the server, and initiate remote video mode on the system management subsystem. Remote video mode enables you to remotely monitor all textual output generated during POST. All POST data will be displayed in the terminal program window as the remote system completes POST. While you are monitoring POST on the remote system, all local keystrokes are relayed automatically to the remote system, enabling you to use POST utilities (such as system configuration, RAID mini-configuration program, and diagnostic programs) that can be accessed during POST.

To use a terminal program to establish a connection with the system management subsystem:

1. Use a terminal program to establish a connection with the system management subsystem modem.

   The modem settings you should use are:

   Baud 57.6 k
   Data Bits 8
   Parity None
   Stop Bits 1
   Flow Control Hardware

2. Log in to the system management subsystem.

   When you have established a connection with the system management subsystem, you will be prompted for a username and password. You must provide a username and password combination that has been previously configured for use with the system management subsystem.

   You can use one of two username and password combinations:

   - The default username (USERID) and password (PASSW0RD)

     Note: The default username and password is case sensitive. You must use all caps, and the "0" in PASSW0RD is the numeral zero.

   - A username and password that you define using the Advanced System Management service and Netfinity Manager

Important

For security purposes, change the username and password using the Advanced System Management service. For more information, see "Configuration Settings" on page 272.

If you update the system management subsystem microcode, the default username (USERID) and password (PASSW0RD) are reset. If you had previously changed them, you will need to change them again.

When you have logged into the system management subsystem, the following main menu appears:

```
2 Monitors
3 Error Logs
4 Service Processor Configuration
5 System Services
6 System Power
7 Boot
B Remote Terminal Status
Y Disconnect Current Logon
Z Start Remote Video
```

To access a menu item, press the number or letter that corresponds to the information you want to access. After you select a menu item, subsequent menus will offer more specific information that pertains to the selection you made from the main menu.

Note: Selecting **Y Disconnect Current Logon** ends the current session and requires you to enter a new username and password before continuing.

Menu Selection	Data Available for Viewing
Monitors	System board temperature, CPU temperatures, power supply temperatures, voltage readings, voltage regulator module readings, fan status, redundant power supply status
Error Logs	Contents of system error log

Menu Selection	Data Available for Viewing
Service Processor Configuration	System management subsystem modem configuration, dial-out entries, dial-out alerts, dial-in logins, system status, thresholds, system statistics, VPD information and system state
System Services	Status of system management subsystem watchdog timers and event alerts sent to the host system.
System Power	Current system power status, power-off configuration and power-off delay values. *Note:* You can use selections available from the **System Power** menu to power the system on or off. For more information, see "System Power Menu Selections" on page 309.
Boot	You can use selections available from the **Boot** menu to shutdown and restart your system or to restart the system management subsystem. For more information, see "Boot Menu Selections" on page 311.
Remote Terminal Status	Current remote terminal status
Start Remote Video	Use **Start Remote Video** to enable your terminal program to remotely monitor and manage the server during POST. For more information, see "Using Remote Video Mode to Monitor and Access POST" on page 313.

When you are finished accessing the system management subsystem using a terminal program, select **Disconnect Current Logon** from the main menu and then use your terminal program to close the connection to the system management subsystem.

System Power Menu Selections

You can use the selections available from the System Power menu to:

- View data regarding the current server power status
- View data regarding the server power configuration

- Power the server off
- Power the server on

To access these functions:

1. Use a terminal program to establish a connection with the system management subsystem modem.
2. Log in to the system management subsystem.

   When you have established a connection with the system management subsystem, you will be prompted for a username and password. You must provide a username and password combination that has been previously configured for use with the system management subsystem. You can use one of two username and password combinations:

   - The default username (USERID) and password (PASSW0RD)

     Note: The default username and password is case sensitive. You must use all caps, and the "0" in PASSW0RD, is the numeral zero.

   - A username and password that you define using the Advanced System Management service and Netfinity Manager

   Important

   For security purposes, change the username and password using the Advanced System Management service. For more information see "Configuration Settings" on page 272.

   If you update the system management subsystem microcode, the default username (USERID) and password (PASSW0RD) are reset. If you had previously changed them, you will need to change them again.

   When you have logged into the system management subsystem, the following main menu appears:

```
2 Monitors
3 Error Logs
4 Service Processor Configuration
5 System Services
6 System Power
7 Boot
B Remote Terminal Status
Y Disconnect Current Logon
Z Start Remote Video
```

3. Select **6 System Power**.

   The following System Power menu appears:

   ```
   1 Current Power Status
   2 Power Configuration
   3 Power On
   4 Power Off
   ```

4. Select a System Power menu item.

   - Select **1 Current power Status** for information about the current server power status.
   - Select **2 Power Configuration** for information about the server power configuration.
   - Select **3 Power On** to power the server on (if it is currently powered off).
   - Select **4 Power Off** to power the server off (if it is currently powered on).

Boot Menu Selections

You can use the selections available from the Boot menu to:

- Shutdown the server operating system and then restart the server
- Restart the server immediately, without first performing an operating system shutdown
- Restart the system management subsystem

To access these functions:

1. Use a terminal program to establish a connection with the system management subsystem modem.
2. Log in to the system management subsystem.

   When you have established a connection with the system management subsystem, you will be prompted for a username and password. You must provide a username and password combination that has been previously configured for use with the system management subsystem. You can use one of two username and password combinations:

   - The default username (USERID) and password (PASSW0RD)

     Note: The default username and password is case sensitive. You must use all caps, and the "0" in PASSW0RD, is the numeral zero.

   - A username and password that you define using the Advanced System Management service and Netfinity Manager

   Important

   For security purposes, change the username and password using the Advanced System Management service. For more information see "Configuration Settings" on page 272.

   If you update the system management subsystem microcode, the default username (USERID) and password (PASSW0RD) are reset. If you had previously changed them, you will need to change them again.

   When you have logged into the system management subsystem, the following main menu appears:

```
2 Monitors
3 Error Logs
4 Service Processor Configuration
5 System Services
6 System Power
7 Boot
B Remote Terminal Status
Y Disconnect Current Logon
Z Start Remote Video
```

3. Select **7 Boot**.

   The following Boot menu appears:

   ```
   1 Reboot w/OS Shutdown
   2 Reboot immediately
   3 Restart SP
   ```

4. Select a Boot menu item.

   - Select **1 Reboot w/OS Shutdown** to shutdown the server operating system and then restart the server.
   - Select **2 Reboot immediately** to restart the server immediately, without first shutting down the operating system.
   - Select **3 Restart SP** to restart the system management subsystem.

Using Remote Video Mode to Monitor and Access POST

You can use a terminal program to remotely monitor all textual output generated during POST. All POST data will be displayed in the terminal program window as the remote system completes POST. While you are monitoring POST on the remote system, all local keystrokes are relayed automatically to the remote system, enabling you to use POST utilities (such as system configuration, RAID mini-configuration program, or diagnostic programs) that can be accessed during POST.

To use Remote Video Mode to monitor and access POST on the server:

1. Use a terminal program to establish a connection with the system management subsystem modem.
2. Log in to the system management subsystem.

   When you have established a connection with the system management subsystem, you will be prompted for a username and password. You must provide a username and password combination that has been previously configured for use with the system management subsystem. You can use one of two username and password combinations:

   - The default username (USERID) and password (PASSW0RD)

Note: The default username and password is case sensitive. You must use all caps, and the "0" in PASSW0RD, is the numeral zero.

- A username and password that you define using the Advanced System Management service and Netfinity Manager

Important

For security purposes, change the username and password using the Advanced System Management service. For more information see "Configuration Settings" on page 272.

If you update the system management subsystem microcode, the default username (USERID) and password (PASSW0RD) are reset. If you had previously changed them, you will need to change them again.

When you have logged into the system management subsystem, the following main menu appears:

```
2 Monitors
3 Error Logs
4 Service Processor Configuration
5 System Services
6 System Power
7 Boot
B Remote Terminal Status
Y Disconnect Current Logon
Z Start Remote Video
```

3. Start (or restart) the server.
   - If the remote server is currently powered off:
     a. Select **6 System Power** from the main menu.
     b. Select **4 Power On** from the System Power menu.
   - If the server is currently powered on, you must restart the server. You can use selections from the System Power menu or the Boot menu to restart the server in several ways.

     To restart the server using System Power menu selection:

     a. Select **6 System Power** from the main menu.

b. Select **3 Power Off** from the System Power menu.

c. Once the server has powered off, select **4 Power On** to restore power to the server.

To restart the server using Boot menu selections:

a. Select **7 Boot** from the main menu.

b. Select either **1 Reboot w/OS Shutdown** or **2 Reboot Immediately** to restart the server.

Note: For information on the System Power and Boot menus, see "System Power Menu Selections" on page 309 and "Boot Menu Selections" on page 311.

4. After you restart the server, return to the main menu and select **Z Start Remote Video**.

Once you have started Remote Video mode on the system management subsystem, all textual output generated during POST will be sent to your terminal window. Your terminal will also act as a fully-active remote session, enabling you to enter keyboard commands that will be sent to the remote server. In this way, you can enter key commands and key-combinations that access POST operations and utilities such as system setup or the RAID mini-configuration program.

When you have finished using Remote Video mode, press **Ctrl+R**, then press **Ctrl+E**, and then press **Ctrl+T**. This will end Remote Video mode and return you to the main menu.

Chapter 23. Software Inventory

You can use Software Inventory to quickly and easily scan any Netfinity system for the presence of installed software products. Its flexible scanning methods can be used to search for specific products, types of products (for example, word processors or graphics viewers), or to compile a record of all recognized software on a system. Reports can be printed to a file, sent to your printer, or exported to a Netfinity database.

System Inventory comes complete with a dictionary file with many predefined software product profiles (called *product definitions*), so you can start keeping track of the software installed on your networked systems right away.

Software Inventory is designed with a simple graphical interface that enables you to add or edit product definitions quickly and easily. Products can be defined and identified by the presence of specified file names (including files that are of a specific size or that were created on specific date, enabling you to search for only certain versions of software) or by the presence of a SYSLEVEL file.

Software Inventory is designed to work with other IBM and non-IBM systems management software applications. Software Inventory provides a mechanism to integrate a workstation's existing software inventory information into the NetView Distribution Manager/6000 or NetView DM for NetWare software distribution database, if the appropriate NetView DM agent software is installed on the workstation. This is accomplished by the creation of the NetView DM FNDSWINV software change history import file, which contains a listing of the NVDM change object names that where discovered on that workstation by the Software Inventory service.

Software Inventory also provides a software dictionary import function for existing QSoft dictionary files (used by IBM's Network Door/2 product), NetView DM inventory list files (used by the INVSCAN utility), SPAudit dictionaries (a publicly available dictionary, used with the Software Publishers Association SPAudit tool. This dictionary can be obtained on the World Wide Web at http://www.spa.org), and other Software Inventory dictionaries

(enabling you to easily combine multiple Software Inventory dictionaries).

Software Inventory can also be used in conjunction with the Remote System Manager. With Software Inventory, you can assign keywords to specific applications. If an application that has a defined application keyword is found during a dictionary search, the application keyword can be added to the list of other keywords that are currently defined for this system. Once an application keyword has been added to the list of system keywords, a Netfinity Manager can use the Remote System Manager discovery feature to add only systems that have specified application keywords to a system group. For example, using an application keyword a Netfinity Manager could create a group that contains only systems that have a specific word processor program that needs upgrading. For more information on keyword assignment and the discovery process, see “Using the Discovery Process” on page 224.

Figure 97. The Software Inventory service

The Software Inventory Dictionary File

Software Inventory uses a software product data file (called the *dictionary file*) to determine the presence of a software product on a system. The dictionary file contains the names of many software

products and *matching attributes*. Matching attributes are characteristics of the software product that enable Software Inventory to identify the software product when the specified attributes are found. Software Inventory uses two kinds of matching attributes:

- File names (can include file size and file date)
- SYSLEVEL files (can include SysID and Component ID)

As Software Inventory searches your hard disk drives, it checks for the presence of specified files or SYSLEVEL files. If it finds a SYSLEVEL file or other file that is defined as a matching attribute in the loaded dictionary file, it reports the product as installed on the system.

Loading a Dictionary File

To load a Software Inventory dictionary file:

1. Select **Open...** from the Dictionary pull-down menu in the Software Inventory window.

   This opens the Open Existing Dictionary... window.

2. Type in the **Open filename** field the fully qualified path and file name of the dictionary file that you want to open, **or** select from the appropriate fields the drive and directory that contain the dictionary file, and then select the dictionary file name.

3. Select **OK**.

Creating a New Dictionary File

To create a new dictionary file:

1. Select **New...** from the Dictionary pull-down menu in the Software Inventory window.

   This opens the New Dictionary... window.

2. Type in the **Save as filename** field the name of the new dictionary file.

3. Select from the **Drive** and **Directory** fields the drive and directory where the new dictionary file will be created.

4. Select **OK**.

Editing the Dictionary File

To edit the currently loaded Software Inventory dictionary file, select **Edit...** from the Dictionary pull-down menu. This opens the Edit Dictionary window (see Figure 98). From this window, you can:

- Change the dictionary description.

  The dictionary file description appears at the bottom of the Software Inventory window and can be used to help you identify the contents of the currently loaded dictionary file. The description is for your use only, and can be anything at all.

  To change the dictionary file description, type in the **Description** field the new description for the dictionary file and then select **Exit**.

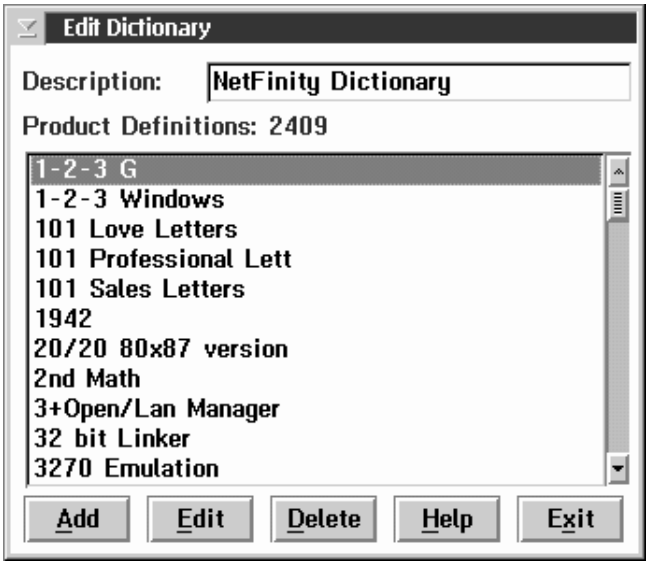

Figure 98. The Edit Dictionary window

- Add a Product Definition.

  For information on how to add a product definition, see "Adding a Product Definition" on page 320.

- Edit a Product Definition.

For information on how to edit a product definition, see “Editing a Product Definition” on page 332.

- Delete a Product Definition.

  To delete a product definition form the dictionary file, select the product definition from the **Product Definitions** selection list, and then select **Delete**.

Adding a Product Definition

Select **Add** to add a new product definition to the currently loaded Software Inventory dictionary file. This opens the New Product Definition Type window (see Figure 99 on page 321). Product definitions can be added based on either of two criteria:

- Product defined by one or more required files

  Select **Product defined by one or more required files** to configure a Software Inventory product definition that will determine whether a product is installed on a system by checking for one or more files of your choosing. In addition to the name of the file or files that Software Inventory will search for, you can specify minimum (or maximum) file size and exact date or date ranges for the file.

  To add a product definition by defining one or more required files, see “File-List Product Definitions” on page 321.

- Product defined by SYSLEVEL file

  Select **Product defined by SYSLEVEL file** to configure a Software Inventory product definition that will determine whether a product is installed on a system by checking for a specified SYSLEVEL file. In addition to the name of the SYSLEVEL file, you can specify a SysID Value or Component ID.

  To add a product definition by requiring the presence of a specified SYSLEVEL file, see “SYSLEVEL File Product Definitions” on page 327.

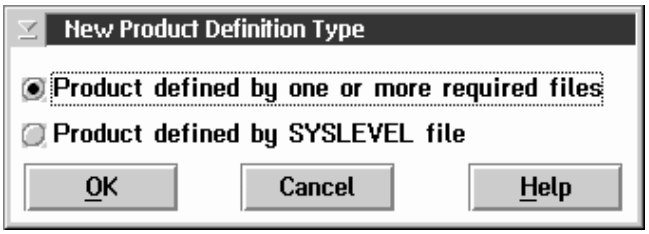

Figure 99. The New Product Definition Type window

File-List Product Definitions

A file-list product definition enables Software Inventory to search your system's drives for specific files that are found in specific products. If the files are found, then the Software Inventory service will report that the software package that contains the files is installed on the system.

To add a file list product definition to the currently loaded Software Inventory dictionary file:

1. Select **Edit** from the Dictionary pull-down menu in the Software Inventory window.
2. Select **Add** from the Edit Dictionary window.
3. Select **Product defined by one or more required files** from the New Product Definition Type window, and then select **OK** to open the Add File List Product Definition window (see Figure 100 on page 322).

Figure 100. The Add File List Product Definition window

4. Fill in the product data fields and select a **Product Type**.

   This information will appear in the Software Inventory window and in any reports Software Inventory generates when the product is found during a search. The Product Type can also be used by the Software Inventory service when Search by Product Type searches are performed. For more information on Search by Product Type searches, see "Search by Product Type" on page 334.

   The product data fields include:

   - Product Name

     This is the name of the software product.

- Vendor Name

  This is the name of the manufacturer of the software product.

- Description

  This is a brief description of the software product.

- Product Type

  This is a brief description of what function the software product performs. The selections available are:

  – Default
  – Network
  – Communications
  – Word Processing
  – Desktop Publishing
  – Database
  – Mail
  – Server
  – Spreadsheet
  – Financial
  – Entertainment
  – Multimedia
  – Graphics Viewer/Editor
  – Education
  – Operating System
  – Software Development
  – Presentation Graphics
  – System Management
  – Documentation
  – CAD/CAM

- Version

  This is the software product version number.

- Revision

  This is the software product revision number.

- NetView DM Change Object (NetView DM users only)

  This is the NetView Distribution Manager change object that will be added to the workstation's installation history. It does not have to match an existing change object in the NetView DM server's database, but it should follow your naming conventions for change objects. After the invocation of Software Inventory on a workstation, this change object name will be added to your NetView DM catalog if it does not already exist.

  Note: This data is used only for the **Update NetView DM Inventory** function. For more information on the NetView DM Change Object, see "Updating a NetView Distribution Manager Inventory" on page 337, or see your NetView DM documentation.

- NetView DM Location Token (NetView DM users only)

  This is the NetView Distribution Manager location token string for use with the software product you are defining. This is commonly used to denote where the application is installed on the workstation. For example, if you are creating a product definition for Netfinity, you would enter a location token of NETFINDIR. The maximum length allowed is 11 characters. This field is optional.

  Note: This data is used only for the **Update NetView DM Inventory** function. For more information on the NetView DM Change Object, see "Updating a NetView Distribution Manager Inventory" on page 337 or your NetView documentation.

- Application Keyword

  The application keyword, when used in conjunction with the Remote System Manager, enables a Netfinity Manager to discover only systems that have specified applications installed on them. For more information on using application keywords, see "Using Application Keywords" on page 339.

Although you do not need to fill in all of these fields, fill in as many as possible in order to maximize the information available

to you when a product is found by the Software Inventory service.

5. Specify the Matching Attributes

   Matching Attributes are the data items used by the Software Inventory service in order to detect whether the software product you are defining is installed on a system. Because you are creating a File List Product Definition, the Matching Attributes will be one (or more) specified files. You can Add, Edit, or Delete files from the **Matching Attributes** field.

   To add a file:

   - If you have the product that you are defining on your system:

     a. Select **Use Files**.

     b. Select the **Drive** and **Directory** where the files that Software Inventory will search for are located. Then, select a **File** and select **OK**.

        This will add the selected file to the **Matching Attributes** field, and then reopen the Use File for Matching File window so you can add other files from this directory. When you have finished adding files, select **Cancel**.

     c. **Optional:** In order to differentiate between different releases or versions of an individual product, you might need to specify that particular files were created on or after a specific date, or that the file is a certain size or within a range of sizes. If you want Software Inventory to look for files that are a specified size or within a range of sizes, or that were created on a specific day or during a specific date range, select the file from the **Matching Attributes** field and then select **Edit** to open the Edit Matching File window (see Figure 101 on page 326). Specify the **File Size** and **File Date** information, and then select **Save** to continue.

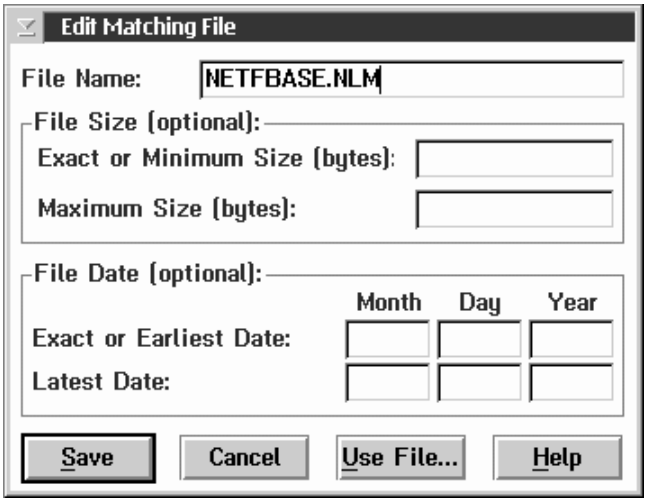

Figure 101. The Edit Matching File window

d. Select **Create** to save this Product Definition to the currently loaded Software Inventory dictionary file.

- If you do *not* have the product that you are defining on your system:

  a. Select **Add** to open the Add Matching File window.

  b. Type in the **File Name**, **File Size** data (optional), and **File Date** data (optional).

     In order to differentiate between different releases or versions of an individual product, you might need to specify that a particular file was created on or after a specific date, or that the file is of a certain size or within a certain range of sizes. If you want Software Inventory to look for files that are a specified size or within a range of sizes, or that were created on a specific day or during a specific date range, specify the **File Size** and **File Date** information.

  c. Select **Save** to add this file to the Matching Attributes list.

Repeat this process until you have added as many Matching Attributes as you want.

d. Select **Create** to save this Product Definition to the currently loaded Software Inventory dictionary file.

SYSLEVEL File Product Definitions

A SYSLEVEL file product definition enables Software Inventory to search your system's drives for a specific SYSLEVEL file that is found in a specific product. If the SYSLEVEL file is found, then the Software Inventory service will report that the software package that contains the SYSLEVEL is installed on the system.

To add a SYSLEVEL file list product definition to the currently loaded Software Inventory dictionary file:

1. Select **Edit** from the Dictionary pull-down menu in the Software Inventory window.
2. Select **Add** from the Edit Dictionary window.
3. Select **Product defined by SYSLEVEL file** from the New Product Definition Type window, and then select **OK** to open the Add SYSLEVEL Product Definition window (see Figure 102 on page 328).

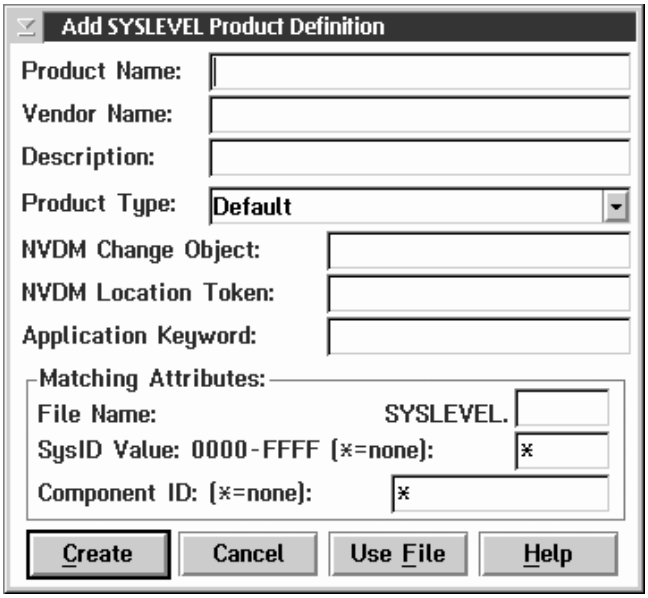

Figure 102. The Add SYSLEVEL Product Definition window

4. Fill in the product data fields and select a **Product Type**. This information will appear in the Software Inventory window and in any reports Software Inventory generates when the product is found during a search. The Product Type can also be used by the Software Inventory service when Search by Product Type searches are performed. For more information on Search by Product Type searches, see "Search by Product Type" on page 334.

   The product data fields include:

   - Product Name

     This is the name of the software product.

- Vendor Name

  This is the name of the manufacturer of the software product.

- Description

  This is a brief description of the software product.

- Product Type

  This is a brief description of what function the software product performs. The selections available are:

  – Default
  – Network
  – Communications
  – Word Processing
  – Desktop Publishing
  – Database
  – Mail
  – Server
  – Spreadsheet
  – Financial
  – Entertainment
  – Multimedia
  – Graphics Viewer/Editor
  – Education
  – Operating System
  – Software Development
  – Presentation Graphics
  – System Management
  – Documentation
  – CAD/CAM

- NetView DM Change Object (NetView DM users only)

  This is the NetView Distribution Manager change object that will be added to the workstation's install history. It does not have to match an existing change object in the NetView DM server's database, but it should follow your naming conventions for change objects. After the invocation of Software Inventory on a workstation, this change object

name will be added to your NetView DM catalog if it does not already exist.

Note: This data is used only for the **Update NetView DM Inventory** function. For more information on the NetView DM Change Object, see "Updating a NetView Distribution Manager Inventory" on page 337, or see your NetView DM documentation.

- NetView DM Location Token (NetView DM users only)

  This is the NetView Distribution Manager location token string for use with the software product you are defining. This is commonly used to denote where the application is installed on the workstation. For example, if you are creating a product definition for Netfinity, you would enter a location token of NETFINDIR. The maximum length allowed is 11 characters. This field is optional.

  Note: This data is used only for the **Update NetView DM Inventory** function. For more information on the NetView DM Change Object, see "Updating a NetView Distribution Manager Inventory" on page 337, or see your NetView DM documentation.

- Application Keyword

  The application keyword, when used in conjunction with the Remote System Manager, enables a Netfinity Manager to discover only systems that have specified applications installed on them. For more information on using application keywords, see "Using Application Keywords" on page 339.

Although you do not need to fill in all of these fields, fill in as many as possible in order to maximize the information available to you when a product is found by the Software Inventory service.

5. Specify the Matching Attributes

   Matching Attributes are the data items used by the Software Inventory service in order to detect whether the software product you are defining is installed on a system. Because you are creating a SYSLEVEL File Product Definition, the Matching Attributes will be the SYSLEVEL file name, the SysID, and the Component ID.

   To add Matching Attributes for a SYSLEVEL file:

   - If you have the SYSLEVEL file for the product you are defining on your system:

     a. Select **Use File**.

     b. Select the **Drive** and **Directory** where the SYSLEVEL file is located, select the SYSLEVEL **File** and then select **OK**.

     c. Select **Create** to save this Product Definition to the currently loaded Software Inventory dictionary file.

   - If you do **not** have the SYSLEVEL for the product you are defining on your system:

     a. Type in the **File Name** field the three character file name extension for the product's SYSLEVEL file.

     b. If possible, type in the **SysID Value** and the **Component ID**.

        Note: These values are stored in the SYSLEVEL file, and can be difficult to obtain without the SYSLEVEL file itself.

     c. Select **Create** to save this Product Definition to the currently loaded Software Inventory dictionary file.

Editing a Product Definition

Software Inventory dictionary file product definitions can be edited in much the same as they are added. To edit a product definition:

1. Select **Edit** from the Dictionary pull-down menu in the Software Inventory window.
2. Select from the **Product Definitions** field the name of the product whose definition you want to edit, and then select **Edit**.
   - If the selected product definition is a File List Product Definition, the Edit File List Product Definition window opens.
   - If the selected product definition is a SYSLEVEL File Product Definition, the Edit SYSLEVEL Product Definition window opens.
3. Edit the product information and Matching Attributes as needed.

   The process used to edit the product information and Matching Attributes is the same as that used when adding a new product definition. See "File-List Product Definitions" on page 321 and "SYSLEVEL File Product Definitions" on page 327 for more information.
4. Select **Save** to save the changes to this product definition.

Performing a Search

Software Inventory can perform three types of software searches on the system. The three kinds of searches are:

- Full Dictionary Search
- Search by Drive
- Selected Product Search
- Search by Product Type

Full Dictionary Search

Software Inventory's Full Dictionary Search enables you to search for any software product that is defined in the currently loaded Software Inventory dictionary file. Depending on the speed of your system, the number of files on your system, the products installed

on your system, and the number of products defined in the currently loaded Software Inventory dictionary file, the Full Dictionary Search can take from just seconds to several minutes to complete. Once the search is complete, results will be displayed in the Software Inventory window.

To perform a Full Dictionary Search, select **Full Dictionary Search** from the Inventory pull-down menu in the Software Inventory window.

For information on generating reports or exporting this information to a database, see "Generating Reports and Exporting Data" on page 336.

Search by Drive

Software Inventory enables you to perform full dictionary searches on specified hard disk drives. If you want to search to for products only on one disk drive on a system, select **Search by Drive...** from the Inventory pull-down menu in the Software Inventory window, and then select the letter of the disk drive you want to search. Software Inventory will then search for any products defined in the currently loaded Software Inventory dictionary on only the specified disk drive.

Once the search is complete, results will be displayed in the Software Inventory window. For information on generating reports or exporting this information to a database, see "Generating Reports and Exporting Data" on page 336.

Selected Product Search

In some cases, you might want to search for specific software products on your networked systems. To search for one or more specific products:

1. Select **Selected Product Search...** from the Inventory pull-down menu in the Software Inventory window.

   This opens the Selective Inventory window (see Figure 103 on page 334).

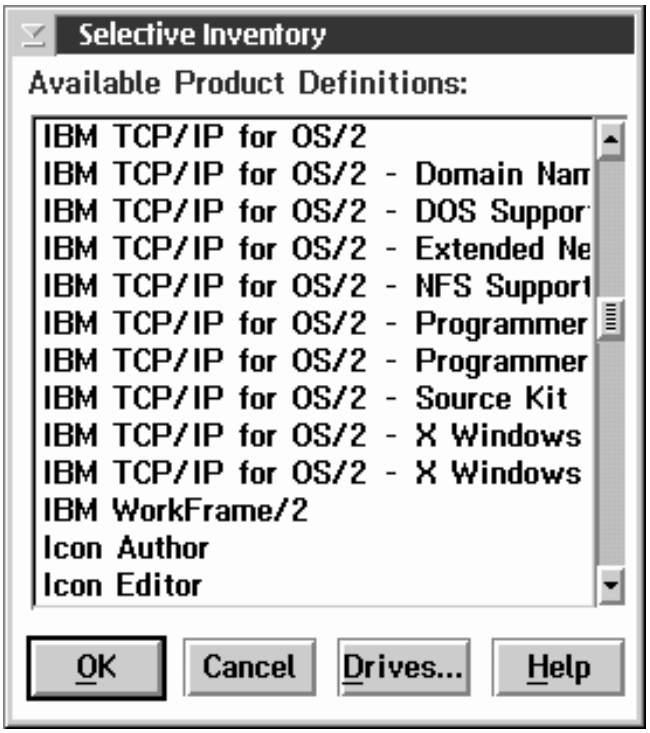

Figure 103. The Selective Inventory window

2. Select from the **Available Product Definitions** window the names of all products that you want to search for.
3. Select **OK** to begin the search for the selected products.

Once the search is complete, results will be displayed in the Software Inventory window. For information on generating reports or exporting this information to a database, see "Generating Reports and Exporting Data" on page 336.

Search by Product Type

When defining products for use with the Software Inventory dictionary file, you can specify a Product Type. This is a brief description of the product's main function. For example, Netfinity's Product Type is *Systems Management*. Software Inventory enables

you to search your networked systems for all products of the same Product Type.

To search only for specified Product Types:

1. Select **Search by Product Type** from the Inventory pull-down menu in the Software Inventory window.

   This opens the Search by Product Type window.

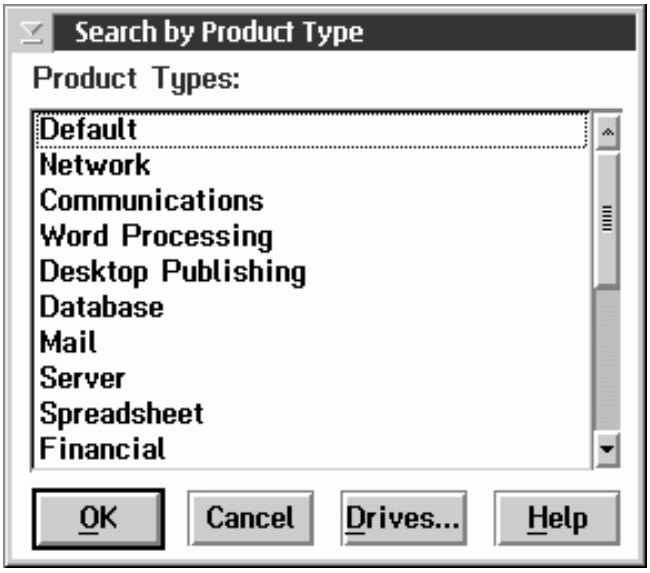

Figure 104. The Search by Product Type window

2. Select from the **Product Type** list one or more product types.
3. Select **OK** to initiate your search.

Once the search is complete, results will be displayed in the Software Inventory window. For information on generating reports or exporting this information to a database, see "Generating Reports and Exporting Data" on page 336.

Generating Reports and Exporting Data

The information gathered by Software Inventory can be:

- Printed to a file
- Printed to a printer
- Exported to a Netfinity database

Print to File

To save the information gathered by Software Inventory to a file:

1. Initiate a Software Inventory search.
2. When the search is complete, select **Print to File** from the Inventory pull-down menu.
3. Name the file, select a drive and directory to which it will be saved, and then select **OK**.

Print to Printer

To print the information gathered by Software Inventory on a printer attached to your system:

1. Initiate a Software Inventory search.
2. When the search is complete, select **Print to Printer** from the Inventory pull-down menu.

The information is then sent to the default printer attached to your system.

Export to Database

To export the information gathered by Software inventory to a Netfinity database, or to save the data to a supported database format file:

1. Initiate a Software Inventory search.
2. When the search is complete, select **Export to Database...** from the Inventory pull-down menu.

3. Select the type of database export you want to perform (export the data to an attached database, or save the data to a database file).
4. Select **OK** to export or save the data.

Updating a NetView Distribution Manager Inventory

You can use Software Inventory to create the NetView Distribution Manager (*NetView DM*) software inventory import file. If your system is running NetView DM agent software, select **Update NetView DM Inventory...** from the Inventory pull-down menu. Software Manager will scan the currently loaded dictionary file for any product definitions that include an NetView DM Change Object and add them to the NetView DM software inventory import file (FNDSWINV). The location token information will be written into the NetView DM agent software base path into a file called FNDTKINV.

This enables a user-written exit routine to then invoke the appropriate NetView DM INV and NetView DM UPDTG commands to move the data in this import file into that workstation's NetView DM software change history database.

Note: This choice is only available if NetView DM agent software is installed and running on the system.

Importing Software Dictionaries

Software Inventory provides a software dictionary import function for existing QSoft dictionary files (used by IBM's Network Door/2 product), NetView DM inventory list files (used by the INVSCAN utility), SPAudit dictionaries (a publicly available dictionary, used with the Software Publishers Association SPAudit tool. This dictionary can be obtained on the World Wide Web at http://www.spa.org), and other Software Inventory dictionaries (enabling you to easily combine multiple Software Inventory dictionaries).

To import a software dictionary file:

1. Open the Software Inventory dictionary file to which new data will be imported.

   To open a Software Inventory dictionary file, select **Open...** from the Dictionary pull-down menu, select a dictionary file, and then select **OK**.

2. Select an import function from the Dictionary pull-down menu.

   The following software dictionary import functions are available:

   - Import from Software Inventory Dictionary...

     Select **Import from Software Inventory Dictionary...** to import all data from another Software Inventory dictionary file into the currently loaded Software Inventory dictionary file.

   - Import from SPAudit Dictionary...

     Select **Import from SPAudit Dictionary...** to import all data from an SPAudit dictionary file into the currently loaded Software Inventory dictionary file.

   - Import from QSoft Dictionary...

     Select **Import from QSoft Dictionary...** to import all data from a QSoft dictionary file into the currently loaded Software Inventory dictionary file.

   - Import from Dictionary...

     Select **Import from NetView DM Inventory List...** to import all data from a NetView DM Inventory List into the currently loaded Software Inventory dictionary file.

Notes:

1. Depending on the speed of your system and the size of the dictionary file you are importing, import functions can take a considerable amount of time to complete.
2. Import functions import **all** data in the file you select, including entries that could already exist in the loaded Software Inventory

dictionary file. Importing identical product definitions will result in multiple, identical entries for products in your dictionary file and will also result in single products being discovered multiple times. To remove identical entries from your Software Inventory dictionary file, edit the dictionary file using the Software Inventory dictionary edit function (for more information see “Editing the Dictionary File” on page 319).

Using Application Keywords

Software Inventory enables you to add application keywords to specific software applications. Once defined, these keywords can then be used by Remote System Manager to create system groups that contain only systems that have specified applications installed.

To add an application keyword to a product definition in your Software Inventory dictionary file:

1. Load a Software Inventory dictionary file.

   To load a dictionary file select **Open** from the Dictionary pull-down menu, select the dictionary file you want to load, and then select **OK**.

2. Edit the Software Inventory dictionary file.

   Select **Edit...** from the Dictionary pull-down menu to edit the currently loaded dictionary file.

3. Edit the Product Definition.

   Select the product to which you will assign an application keyword from the **Product Definitions** field and then select **Edit**.

4. Assign an application keyword.

   Type in the **Application Keyword** field the keyword that will be used to identify this product. The application keyword can be up to 12 characters long.

5. Select **Save** to save this information to the dictionary file.

Products with application keywords that are discovered on a system following a dictionary search will have the application keyword

displayed along with other software product information in the Software Inventory window following the dictionary search. Once a product that has an application keyword defined is discovered on a system, the application keyword can be added to the system's keyword list. To update the system keyword list with application keywords for discovered and defined products, select **Update Application Keywords** from the Inventory pull-down menu.

Notes:

1. To differentiate application keywords from other system keywords, the application keyword will has the characters APP: added to the beginning of the application keyword. Remote System Manager system groups that use the application keyword as part of the group's system discovery criteria must include APP: as well as the text that is entered in the **Application Keyword** field to successfully discover the system.

   For example, if a product definition uses the application keyword SOFTWARE, the keyword that must be used by Remote System Manager to discover systems using the product that is defined using this application keyword would be APP:SOFTWARE.

2. The **Update Application Keywords** function adds only application keywords that are currently displayed in the Software Inventory window to the system's keyword list. If you add an application keyword to the product definition of an application that is installed on your system, the application keyword will not be added to the keyword list until you perform another dictionary search and then select **Update Application Keywords**.

Chapter 24. System Diagnostics Manager

You can use System Diagnostics Manager to initiate a variety of diagnostic tasks on systems that support ROM-based diagnostics. The results of all previously run diagnostic sessions are stored on the system and can be examined using System Diagnostics Manager to help diagnose and resolve system problems.

The System Diagnostics Manager can run diagnostics on any of the following system components:

- System board
- Memory
- Keyboard
- Video
- Diskette
- Alternate (2nd) microprocessor
- Parallel port
- Serial port
- Ethernet
- SCSI
- RAID controller
- Mouse

The System Diagnostics Manager window features seven columns of data for each available diagnostic routine. These columns are:

- Diagnostic Test
- Result
- Time of Failure
- Error Code
- Failure Explanation
- Failure Address
- Failure Data

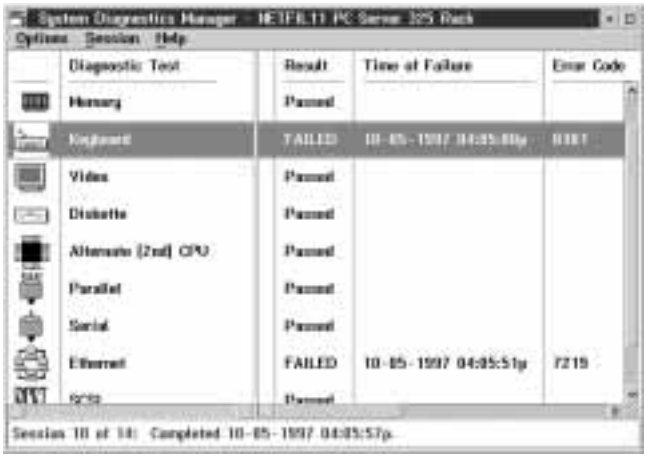

Figure 105. The System Diagnostics Manager window

Supported Systems

System Diagnostics Manager will function on the following systems:

- IBM PC Server 325 (models PTO, PTW, PBO, KTO, and RBQ only)
- IBM PC Server 330 (models PTO, PBO, and PMO only)

Using System Diagnostics Manager

The System Diagnostics Manager window shows the results of the currently loaded diagnostic session. Use the choices available from the System Diagnostics Manager window pull-down menus to:

- Run diagnostics

  For information on how to run diagnostics on a system, see "Running Diagnostics" on page 343.

- Refresh the contents of the window

  For information on how to refresh the contents of the window, see "Refreshing Displayed Data" on page 344.

- View results of previous diagnostic sessions

For information on how to view the results of previous diagnostic sessions, see “Viewing Previously Gathered Results” on page 344.

Running Diagnostics

To run diagnostics on a system, select **Run Diagnostics** from the Options pull-down menu. This will open the Run Diagnostics window (see Figure 106).

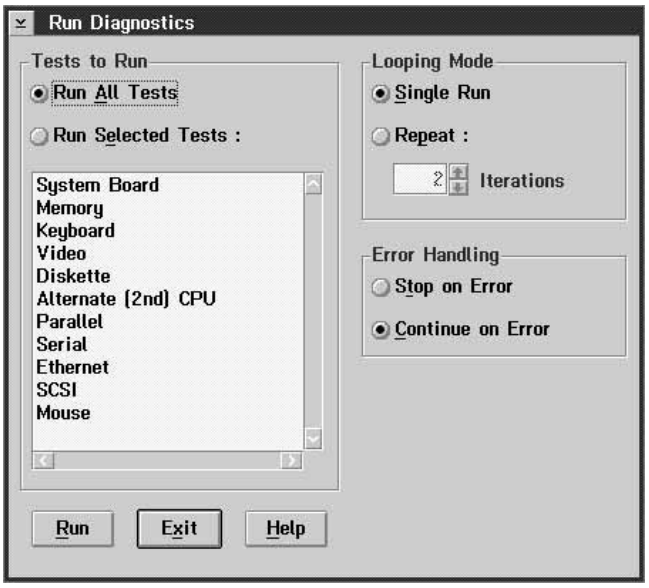

Figure 106. The Run Diagnostics window

Use the Run Diagnostics window to select which diagnostic tests to run on the system, to specify whether the tests will be run in looping mode, and to set the System Diagnostics Manager error handling for this diagnostic session.

To configure a System Diagnostics Manager session:

1. Use the selections available in the **Tests to Run** group to select which tests to run.

To run all of the available diagnostic routines, select **Run All Tests**. If you want to test only specific subsystems, select **Run Selected Tests** and then select one or more tests from the **Tests to Run** selection list.

2. Use the selections available in the Looping Mode group to select an error handling mode.

   To run the diagnostic routines only once, select **Single Run**. To run the diagnostic routines 2 or more times, select **Repeat** and use the spin buttons beside the **Iterations** field to specify the number of times that the diagnostic routines are to be run.

3. Use the selections available in the Error Handling group to select an error handling mode.

   To halt the diagnostic routines when an error is encountered, select **Stop on Error**. To record the error and continue with the specified diagnostic routines, select **Continue on Error**.

4. Begin the diagnostic session.

   Select **Run** to initiate the diagnostic session you have configured.

Select **Exit** at any time to close the Run Diagnostics window without initiating a diagnostics session.

Refreshing Displayed Data

To refresh the data that is currently displayed in the System Diagnostics Manager window, select **Refresh** from the Options pull-down menu.

Viewing Previously Gathered Results

To view the results of previous diagnostic sessions, select **Select** from the Session pull-down menu. This opens the Select Session window (see Figure 107 on page 345).

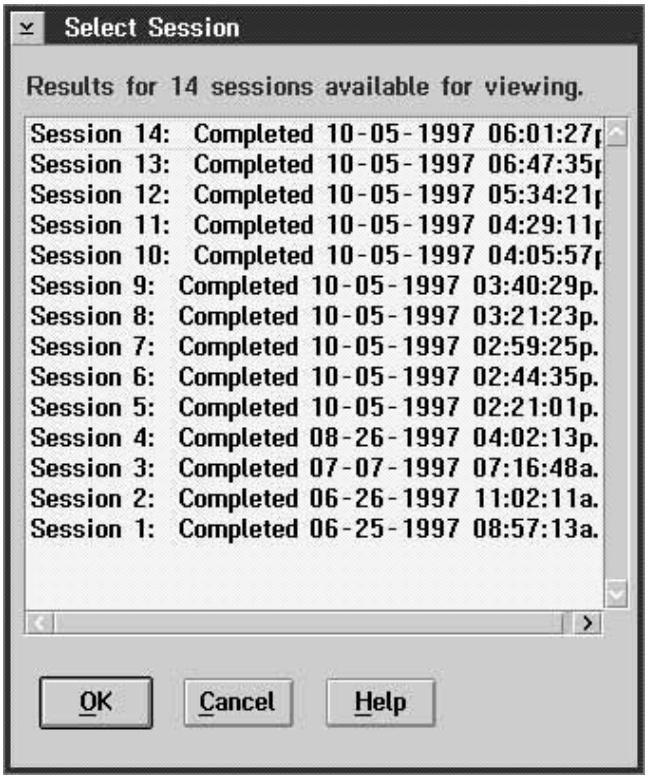

Figure 107. The Select Session window

Use the Select Session window to collect and view the results of a previously run diagnostic session. This window shows all previously run diagnostic sessions that are currently stored on the system. To view the results of one of these sessions, select the session from the **Select Session** field and then select **OK**. After you select **OK**, the Select Session window closes and the results of the selected diagnostic session are displayed in the System Diagnostics Manager window.

Chapter 25. System Information Tool

System Information Tool is designed to gather and display a broad variety of information about the hardware and software configuration of your local system or of a remote system or workstation. System Information Tool is primarily designed for use on IBM systems, but many features will function on systems from other manufacturers.

System Information Tool Features

The System Information Tool gathers hardware and software configuration information. This information can be viewed online or directed to a file or printer. The gathered information also can be exported to a Netfinity database. For information on the Netfinity database, see Appendix I, "Netfinity Relational Database Tables" on page 480 and "Netfinity Database Support" in *Netfinity Manager Quick Beginnings.*

Depending on your system's hardware, software, or operating system configuration, System Information Tool provides information on some or all of the the following system features:

- Pentium® processor information, including automatic detection of flawed Pentium processors
- Micro Channel, EISA, and PCI adapter identity, with configuration information available on many common adapters
- Drive information, including file-system type, available space on the disk drive, disk-drive size, and partition layout
- Error-log display and interpretation
- Keyboard information
- Memory configuration, including total physical memory, installed single inline memory module identification, and supported memory upgrades
- Mouse type and settings
- Operating system information, including version, DOS support, session limits, current task list, and CONFIG.SYS information
- Model and microprocessor information, including model name, processor type and speed, and BIOS date

- Parallel and serial port configuration
- Video system information, including adapter type, screen resolution, and video-display identification
- Printer configuration, including data on installed printer drivers
- SCSI, ESDI, IDE/ST506, or other disk adapter information, including devices attached, device sizes, and adapter data
- System security features, including power-on password and secondary security features
- RAID subsystems
- VPD data
- PCMCIA devices
- Plug and Play configuration
- Network (NDIS) devices and data (available only on systems running OS/2)

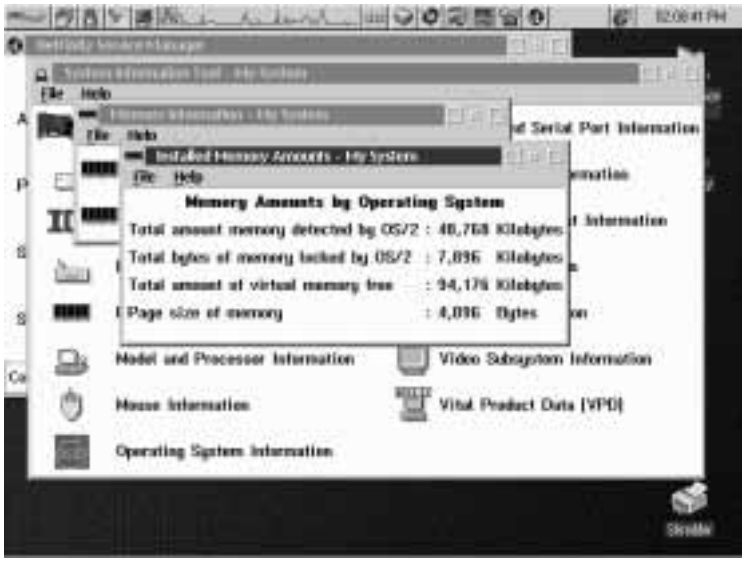

Figure 108. System Information Tool

Using System Information Tool

To display information gathered by System Information Tool, select the object or name of the component from the System Information Tool window. This action opens a window that contains more specific information regarding the component you selected.

If more information is available, one or more words or objects within the new window will be highlighted. You may then select another object or topic to open a window with more device-specific information. If there is no further information available, no highlighted items will appear within the window.

System Information Tool provides you with three options for generating output of the gathered and displayed data. To access these options, select the **File** pull-down menu at the top of the System Information Tool window, and then do the following:

- Select **Print All System Data To File** to generate a textual report of all of the system configuration data which has been collected by the System Information Tool, and then save the report to a user-selected file. You are given a standard file window to select the file name.
- Select **Print All System Data To Printer** to generate a textual report of all of the system configuration data that has been collected by the System Information Tool, and then send the report to the default printer.
- Select **Generate History File** to create a binary file that contains all of the information displayed in the program as well as the current time and date. The history file can be viewed later by using the **/F** command line parameter when starting the System Information Tool from a command line. For more information on System Information Tool's command-line functions, see "System Information Tool Command Line Operations" on page 468.
- Select **Database** to export the gathered information to the Netfinity database. For more information, see "Database Functions" on page 349.

Database Functions

To export the System Information Tool data to a database:

1. Select **Database...** from the File pull-down menu.
2. Select a database export function from the **Database Selection** field.

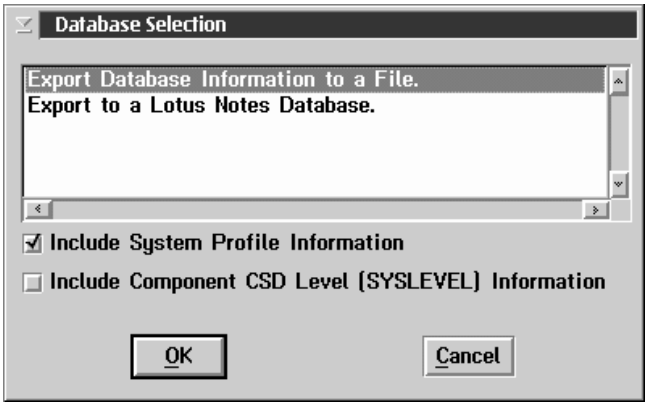

Figure 109. The Database Selection window

The data can be exported to a file or to a supported database format.

- To export the system information to a file, select **Export Database Information to a File**.
- To export the system information to a supported database, select the export function for the database server to which your managing system is attached. If your managing system is attached to more than one type of database server, then you will have an entry for each type of database in the Database Selection field. For example, if your system is configured to use both a Lotus Notes database server and a DB2 database server then the Database Selection field will contain two export to database selections: **Export to a Lotus Notes Database** and **Export to a DB2 Database**.

  Note: This function will not be available if the managing system does not have access to or is not configured to use a database system. For more information, see

"Netfinity Database Support" in *Netfinity Manager Quick Beginnings*

If you want the System Information Tool to gather information from the System Profile notebook and include it in the data set, select the **Include Profile information** check box.

3. Select **OK** to save this information.

   - If you selected the **Export System Information to a File** option, the Export To File window appears (see Figure 110).

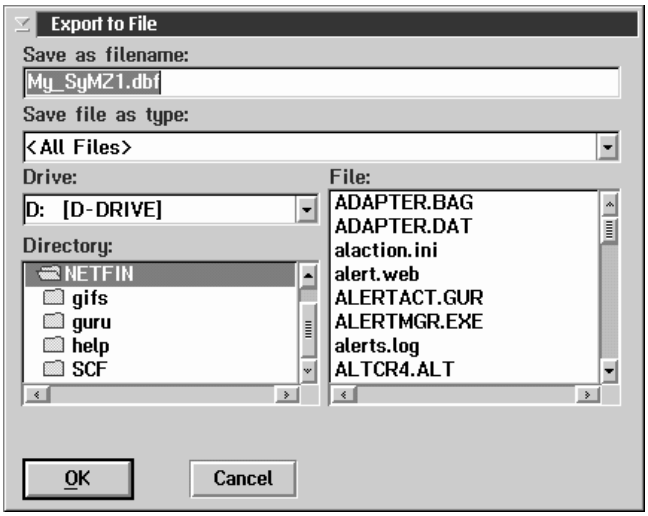

Figure 110. The Export To File window

Enter all file-specific information, and then select **OK**.

   - If you selected the **Export System Information to a Database** option, the Server Selection window appears.

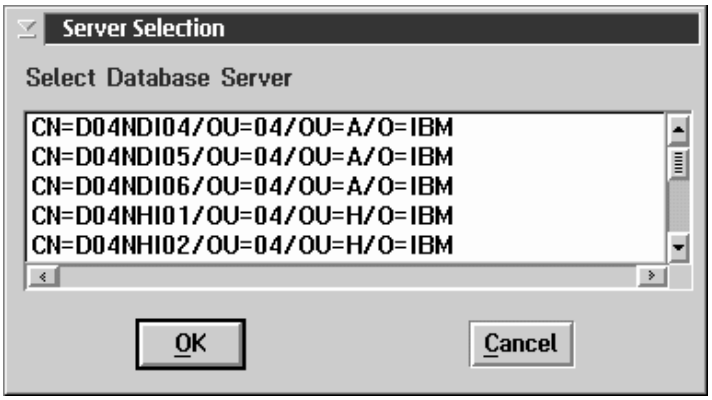

Figure 111. The Server Selection window

Select from the **Server Selection** field a database to export the data to, and then select **OK**.

All collected data will then be added or appended to the existing database. For more information on the Netfinity database, see Appendix I, "Netfinity Relational Database Tables" on page 480 and "Netfinity Database Support" in *Netfinity Manager Quick Beginnings*.

Protecting Confidential System Data

In addition to extensive hardware configuration information System Information Tool gathers detailed operating system information. The data collected is operating system-dependent, and typically includes the contents of the system's CONFIG.SYS or AUTOEXEC.BAT files. Depending on your system's configuration, these files might contain confidential information. For example, your CONFIG.SYS file might contain the following command, used to logon to a network-accessible disk drive:

```
LOGON MY_USER_ID /D:MY_DRIVE /P:MY_PASSWORD
```

To automatically protect sensitive or confidential system data, create an ASCII file named SIKEYWD.INI in your Netfinity directory. This file should contain one or more alphanumeric strings. If this file is present, System Information Tool will automatically replace all

alphanumeric characters (other than the keyword itself) that are on any line that contains one of the keywords specified in the SIKEYWD.INI file with asterisks.

Using the previous example, if your SIKEYWD.INI file contains the keyword LOGON the CONFIG.SYS information shown above would appear to the user as

```
LOGON************************************
```

Notes:

1. The SIKEYWD.INI file can contain as many keywords as needed. Keywords must be separated by a space.
2. SIKEYWD.INI string entries are case-sensitive. Only strings that exactly match the SIKEYWD.INI entries will be replaced in the System Information Tool data.
3. Because of the additional processing that must be done, adding keywords to the SIKEYWD.INI file can degrade System Information Tool performance. Users should add keywords to the SIKEYWD.INI file with care.

Chapter 26. System Monitor

The System Monitor provides a convenient method of charting and monitoring the activity of a number of components in a system. Standard features include:

- Continuous monitoring of systems, including:
  - Locked memory use
  - Virtual memory use
  - Microprocessor use
  - DASD space available and space remaining
  - DASD use
  - TCP/IP protocol functions
  - Processes running
  - Threads running
  - Pentium processor computations
  - RAID device attributes
  - Read/write errors (Netfinity Manager only)
- The ability to export System Monitor data to a Netfinity database
- Detachable, scalable, and user-configurable monitors
- User-definable thresholds that will generate Netfinity alerts when exceeded
- Choice of line-graph, text, and real time graphic representations of system activity

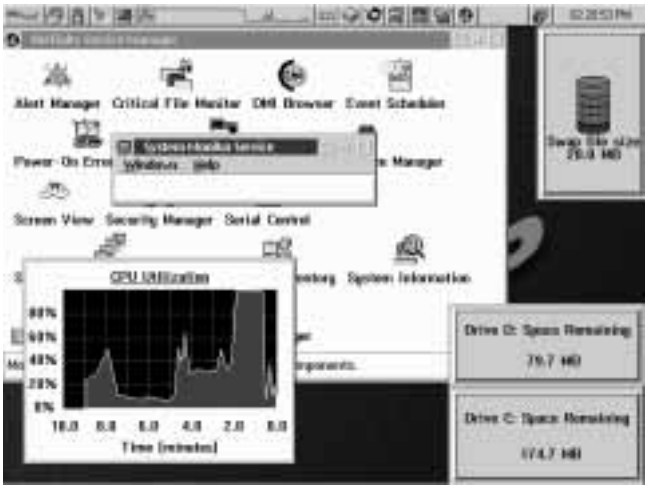

Figure 112. System Monitor Service

Note: System Monitor uses a data-handling technique that allows for both long-term, system activity profiles and short-term, high-resolution system activity monitoring.

As samples of system activity are taken, they are stored and displayed. However, after a number of samples have been taken, their individual values are weighed, several concurrent samples are averaged, and they are posted as a single, long-term value.

Primarily, this is done to prevent System Monitor data files from taking up a large amount of space on a system. This data-handling technique also allows for a more reasonable measurement of average long-term system load values without sacrificing short-term monitoring abilities. This data-handling technique accounts for the initial "spiking" you may see on line graphs when the System Monitor is started.

If you do not need records of a monitor's previous activity, or do not want to use disk drive space to maintain these records, you can use the System Monitor's Record Data option to disable record keeping.

The System Monitor Service Window

When the System Monitor service is started, all monitors currently set to be visible appear on your display, along with the System Monitor Service window.

Figure 113. The System Monitor Service window

The System Monitor Service window controls the service as a whole. If the System Monitor Service window is closed, all of the monitors will close as well.

Use the choices in the System Monitor Service window's **Windows** pull-down menu to:

- Show monitors that are available.

  Select **Show Monitors** to open the Select Visible Monitors window. Use this window to select which of the System Monitors you want to be visible on your Desktop.

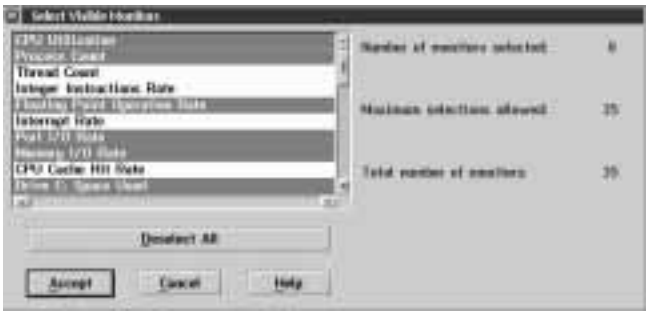

Figure 114. The Select Visible Monitors window

To select the monitors that will be visible on the Desktop:

1. Select the monitors that you want to have visible on the Desktop.

   To select *all* available monitors, click on **Select All**. If all monitors are currently selected and you want to deselect all monitors, click on **Deselect All**.

   There is no enforced limit to the number of monitors that can be active at one time. However, due to system restraints, a default maximum of 50 monitors can be displayed at a time. The maximum number of monitors visible can be changed by setting a system environment variable as follows:

   ```
   SET NF_MAX_MON_DISP=n
   ```

   where *n* is an integer greater than zero. The manner in which the environment variable is set depends on your operating system.

- To set this environment variable on an OS/2 or Windows 95 system, add the variable to your CONFIG.SYS file and then restart your system.
- On NT systems:
  a. Open the Windows NT Control Panel, then double-click on **System**.
  b. Click on the **Environment** tab.
  c. Click anywhere in the **System Environment Variables** field.
  d. Type in the **Variable** field

     `NF_MAX_MON_DISP`

  e. Type in the **Value** field the *n* value (an integer greater than zero).
  f. Select **Set**.
  g. Select **Apply**.
  h. Select **OK**.
  i. Shutdown and restart the Netfinity Support Program.

Note: If you increase the number of monitors that can be displayed at a time, you system could run out of resources. To prevent this problem, display only as many monitors as needed.

2. If any monitors are selected that you do not want to be visible on the Desktop, deselect them.
3. Select **Accept** to display or hide monitors as appropriate.

- Bring specific monitors to the foreground.

  Select the name of the monitor you want to bring to the foreground. If a monitor is not currently hidden, you can select the monitor's name to bring it to the foreground. If a monitor is hidden, its name will be grayed out. Hidden monitors cannot be brought to the foreground.

- Export data from multiple monitors to a Netfinity database

  The current time, date, and reported value of any selected monitors can be exported to a Netfinity database. To export monitor data from one or more component monitors:

  1. Select **Export to Database...** from the System Monitor Service window's Windows pull-down menu.
  2. Select from the **Monitors** field the names of the monitors from which the data will be exported.

     To select *all* available monitors, click on **Select All Monitors**. If all monitors are currently selected and you want to deselect all monitors, click on **Deselect All**.
  3. Select **OK**.
  4. Select the Netfinity database to which the monitor data will be exported.
  5. Select **OK** to export the data.

Each monitor has a number of monitor-specific options that can be accessed from the monitor's pop-up menu. Using mouse button 2, click on the monitor. This opens the monitor's pop-up menu.

Monitor Pop-Up Menus

Each monitor has its own pop-up menu. To open the pop-up menu, use mouse button 2, and click on the monitor. Use the selections in individual monitor's pop-up menu to:

- Change System Monitor settings

  Select **Settings** to open the Settings page of the individual monitor's notebook. For more information see "Monitor Settings" on page 364.

- Configure System Monitor thresholds

  Select **Thresholds** to open the Thresholds page of the individual monitor's notebook. For more information see "Setting Thresholds" on page 360.

- Change the System Monitor that is displayed

  Select **View** to choose the appearance of monitor that will is displayed. The available monitor types are:

  – Line Graph

  – Real Time

  – Text Display

  For more information on the available monitor types see "Changing Monitor Views" on page 365.

- Bring the Main Window to the foreground

  Select **Main Window** to bring the System Monitor Service window to the foreground.

- Enable or disable recording of data

  Select **Record Data** to enable System Monitor to keep records of this monitor's previous activity. If this option is not selected, monitor data is not saved and line-graph monitors are not available. Disabling this option on monitors that you do not use frequently, or from which you do not need long-term data, can help you save space on your disk drive.

- Access online help

  Select **Help** to access System Monitor's online help facility.

- Move

  Select **Move** to move the selected monitor around the Desktop. When you have moved the selected monitor to the new location, click again to drop it. Monitors can also be moved by dragging the monitor to a new location.

- Size the monitor

  Select **Size** to resize the selected monitor. After you select **Size**, move the mouse until the window outline is the size that you want the selected monitor to be. Then, click again to resize the monitor. You can also resize monitors by dragging the sides or corners of the monitor windows.

Note: If you make a monitor too small for the monitor's text to be shown fully, the text will disappear. However, this has no effect on the monitor's function.

- Hide the monitor

  Select **Hide** to make the selected monitor invisible. The monitor will continue to function and collect data, but it will not be seen on the Desktop. To make a monitor that you have hidden visible again, you must open the System Monitor Service window, and then select **Show Monitors...** to open the Select Visible Monitors window. For more information on the Show Visible Monitors window see "The System Monitor Service Window" on page 354.

- Export to Database...

  Data from any of the System Monitors can be exported to a Netfinity database. The exported data is the values being reported by the monitor for the user-specified time range, the time, and the date. To export data from an individual monitor:

  1. Select **Export to Database...**
  2. Select a Netfinity database to which the monitor data will be exported.
  3. Select **OK** to export the data.

  For information on how to export data from multiple monitors simultaneously, see "The System Monitor Service Window" on page 354.

System Monitor Notebooks

Use each monitor's System Monitor notebook to:

- Set thresholds at which alerts will be generated.

  For more information on setting thresholds, see "Setting Thresholds" on page 360.

- Configure monitor-specific settings. For more information on configuring monitor settings, see "Monitor Settings" on page 364.

To open the System Monitor notebook:

1. Open the individual monitor's context menu (using mouse button 2, click on the monitor).
2. Select **Open**.
3. Select the page of the notebook you want to open:
   - Select **Thresholds** to open the notebook to the Thresholds page.
   - Select **Settings** to open the notebook to the Settings page.

Setting Thresholds

The Thresholds page of the System Monitor notebook enables you to set threshold values for this monitored system component. If the monitored value of this system component falls outside of the configured threshold values, the System Monitor will generate a Netfinity alert.

System Monitor also automatically monitors any *redundant arrays of independent disks* (RAIDs) that may be present on your system. You can monitor RAID subsystems and other attribute-based devices with System Monitor's Attribute Monitors. For more information on Attribute Monitors, see "Attribute Monitors" on page 368.

System Monitor will automatically generate alerts if a RAID system change is detected. For more information on RAID alerts, see Appendix F, "RAID Alerts" on page 463.

Figure 115. The System Monitor Notebook Threshold Page

To create (or edit) a threshold for this system component:

1. Open the System Monitor notebook to the Threshold page.

   Using mouse button 2, select the monitor for which you will create the threshold. Then, select **Open**, and then **Thresholds** from the monitor's context menu.

2. Name the threshold (or select the Threshold Name to be edited).

   Type the name of the threshold in the **Threshold Name** field. If you are editing an existing threshold, select the threshold from the **Threshold Name** selection list.

3. Set the threshold's duration.

   Type a number and select a unit of measurement (for example, "seconds") to create a duration value. This will specify the length of time that the monitor's threshold value must be exceeded before an alert is generated.

4. Set the resend delay.

   Type a number and select a unit of measurement (for example, “seconds”) to create a resend delay value. This will specify the length of time that the System Monitor will wait, after sending an alert, before resending a duplicate alert if the threshold Value continues to be violated.

5. Set the threshold’s values.

   Enter one or more threshold Values for this monitor. You can set up to four different threshold Values, each of which will generate a different Netfinity alert.

   - Error if above or equal to

     The threshold value entered in the **Error if above or equal to** field is the minimum value that will trigger an alert. If the parameter being monitored is greater than or equal to this value, System Monitor will generate and “Error” alert type. The threshold value must be less than or equal to the maximum value for this system component (for example, 100.0 for CPU Utilization or 214.0 for the space on a 214 MB logical drive), and must be greater than or equal to the **Warning if above or equal to**, **Warning if below or equal to**, and **Error if below or equal to** Values (if any). If the entered value does not conform to these requirements, System Monitor will “beep” and reject the entered value.

   - Warning if above or equal to

     The threshold value entered in the **Warning if above or equal to** field is the minimum value that will trigger an alert. If the parameter being monitored is greater than or equal to this value, System Monitor will generate and “Warning” alert type. The threshold value must be less than or equal to the maximum value for this system component (for example, 100.0 for the CPU monitor), less than or equal to the value (if any) assigned for **Error if above or equal to**, and must be greater than or equal to the assigned values (if any) for **Warning if below or equal to** and **Error if below or equal to**. If the entered value does not conform to these requirements, System Monitor will “beep” and reject the entered value.

- Warning if below or equal to

  The threshold value entered in the **Warning if below or equal to** field is the maximum value that will trigger an alert. If the parameter being monitored is less than or equal to this value, System Monitor will generate and "Warning" alert type. The threshold value must be less than or equal to the maximum value for this system component (for example, 100.0 for the CPU monitor), less than or equal to the value (if any) assigned for **Error if above or equal to** and **Warning if above or equal to**, and must be greater than or equal to the assigned value (if any) for **Error if below or equal to**. If the entered value does not conform to these requirements, System Monitor will "beep" and reject the entered value.

- Error if below or equal to

  The threshold value entered in the **Error if below or equal to** field is the maximum value that will trigger an alert. If the parameter being monitored is less than or equal to this value, System Monitor will generate and "Error" alert type. The threshold value must be less than or equal to the maximum value for this system component (for example, 100.0 for the CPU monitor), and less than or equal to the values (if any) assigned for **Error if above or equal to**, **Warning if above or equal to**, and **Warning if below or equal to**. If the entered value does not conform to these requirements, System Monitor will "beep" and reject the entered value.

6. Set the threshold's severity

   A default severity is provided for each of the threshold Values. You can adjust these values by selecting the spin buttons at the right of the field.

7. Select Notify or Local Notify (optional).

   Select **Notify** to instruct the monitor to notify you if the threshold is violated. If you do not select **Notify**, the threshold will be saved and will be active, but it will not generate an alert on your system. However, a Netfinity Manager could remotely access your system and select **Notify**. In this case, the Manager

would be notified when the threshold was violated, but you would not.

If you are using Remote System Access to configure a System Monitor threshold on a remote system, another check box (called **Local Notify**) is available. If you select **Local Notify**, System Monitor will generate an alert on the local system on which you configured the threshold when the threshold is exceeded. If you select **Local Notify** *and* one or more **Notify** check boxes, alerts will be generated on your system *and* on the remote user's system when the threshold is exceeded.

Note: The **Local Notify** check box will not appear on the Thresholds page if you are using System Monitor locally.

8. Save the threshold.

   If you have been configuring a new threshold, select **Create** to save these threshold values. If you have been editing a previously configured threshold, select **Change** to save the new threshold values.

Monitor Settings

Use the Settings page of the System Monitor notebook to enable or disable the title bar for this monitor, select the type of monitor that is displayed, or to configure the line-graph settings for this monitor.

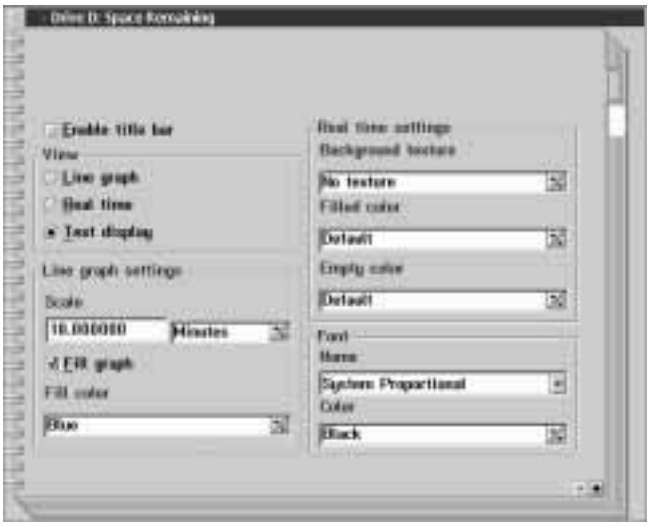

Figure 116. The System Monitor Notebook Settings Page.

Enabling and Disabling the Title Bar (available on OS/2 systems only)

Select the **Enable Title Bar** check box to activate a title bar on this monitor. This title bar shows the System Name of the system on which the System Monitor is being run (this will only appear if the service is being run on a remote system), and the name of the monitor itself (for example, "CPU Utilization Monitor"). If you do not want a title bar, deselect the **Enable Title Bar** check box.

To save the new Settings, close the notebook by double-clicking in the upper-left corner.

Note: This feature is available only on systems running OS/2.

Changing Monitor Views

Select the type of monitor that will be displayed from the View button group. The available monitor types are:

- Line-graph

  Select **Line-graph** to display a "heartbeat-style" chart of this system component's activity using user-specified Line-Graph Settings to determine the length of the graph and the units in

which it is measured. For more information on line-graph monitors, see “Configuring Line-Graph Settings” on page 366.

Note: If you have disabled the Record Data option (found in the monitor’s pop-up menu), line-graph monitors will not be available.

- Real time

  Select **Real time** to display a graphic representation of this system component’s current status. The real-time monitor that is displayed depends on what system component it is meant to represent. For example, the CPU monitor uses a speedometer-style real-time monitor to show percentage of CPU utilization, while hard disk drive Space Used monitors use a cylinder to depict how “full” the disk drive is.

- Text display

  Select **Text display** to display a textual readout of the system component’s current activity, without any graphical representation.

To save the new Settings, close the notebook by double-clicking in the upper left corner.

Configuring Line-Graph Settings

Use the selections available in the Line-graph settings field group to configure this component’s line-graph monitor. This field group enables you to:

- Set the line-graph scale

  Use the **Scale** fields to configure the length of time graphed when viewing this monitor’s line-graph. Enter a number in the first **Scale** field, and then use the spin buttons to the right of the second **Scale** to select the unit of time that the line-graph will use to graph component activity. The available units of time are:

  – Seconds
  – Minutes
  – Hours
  – Days

– Weeks

- Enable/disable line-graph fill

  Select **Fill graph** if you want to fill in this monitor's line graph with a specified color. If **Fill graph** is not selected, the line graph will show only a white line against the dark background. If you select **Fill graph**, you can then select from the **Fill color** field the color with which the line graph will be filled.

- Select the line-graph fill color

  Use the spin buttons at the right side of the **Fill color** field to select the color with which the line graph will be filled.

To save the new Settings, close the notebook by double-clicking in the upper left corner.

Configuring Real-Time Settings

Use the selections available in the Real-time settings field group to configure this component's real-time monitor. This field group enables you to:

- Select a background texture (available on OS/2 systems only)

  Use the spin buttons at the right side of the **Background texture** field to select a background bit map for use with this monitor.

- Select the filled color

  Use the spin buttons at the right side of the **Filled color** field to select the color that will be used for the foreground part of the real-time monitor.

- Select the empty color

  Use the spin buttons at the right side of the **Empty Color** field to select the color that will be used for the background part of the real-time monitor.

To save the new Settings, close the notebook by double-clicking in the upper left corner.

Configuring Font Settings

Use the selections available in the Font field group to select the font and font color for use with all text in all views for this monitor. This field group enables you to:

- Select a font

  Use the spin buttons at the right side of the font **Name** field to select the font that will be used for text in each of this component's views.

- Select a font color (available on OS/2 systems only)

  Use the spin buttons at the right side of the **Color** field to select the color of the font that will be used for text in each of this component's views.

To save the new Settings, close the notebook by double-clicking in the upper left corner.

Attribute Monitors

Attribute Monitors are used where a numerical value is meaningless. For example, the current status of a RAID device is expressed as a descriptive word (Online, Offline, or Defunct), rather than as a numeric value. Attribute Monitors enable you to view the current status of such a device, and to assign thresholds based on changes in state. Attribute monitors can also have a variety of settings assigned to them.

Note: Attribute monitors are similar to, but not the same as, the RAID alerts described in Appendix F, "RAID Alerts" on page 463. RAID alerts are automatically generated by Netfinity whenever a RAID device changes state, but offer no simple way for you to visually check the current state of a RAID device. Attribute monitors enable to you visually monitor the current state of any RAID device and to create additional thresholds for these devices, if necessary.

Attribute Monitor Thresholds

Attribute monitor thresholds are set from the Attribute Monitor notebook's Threshold page. To open the notebook, use mouse button 2 to click on the monitor for which you want to set a threshold. From the monitor's context menu, select **Open**, and then select **Thresholds**.

To configure a threshold for an Attribute Monitor:

1. Select the attribute that you want to monitor.

   Each Attribute Monitor will contain one or more attributes that can be monitored. The names of these attributes are determined by the type of device. Select from the **Attribute to Monitor** field the name of the attribute that you will monitor.

2. Name the threshold.

   Type in the **Threshold Name** field a name for this threshold and then press **Enter**.

3. Set the threshold's duration.

   Type a number and select a unit of measurement (for example, "seconds") to create a duration value. This value specifies the length of time after the monitored attribute changes state before the alert is generated.

4. Set the resend delay.

   Type a number and select a unit of measurement (for example, "seconds") to create a resend delay value. This value specifies the length of time that the System Monitor will wait, after sending an alert, before resending a duplicate alert if the attribute's state remains unchanged.

5. Select a violating state.

   Select from the **State** field the name of the state which, if reported by the the monitored **Attribute**, will generate an alert.

6. Select a severity value.

   Select a **Severity** for the alert that will be generated if the specified **State** is reported.

7. Specify an Application Alert Type value.

   The **Application Alert Type** is a four digit numeric value assigned to the generated alert. It can be used by the Alert Manager to differentiate this alert from other alerts for Alert Action responses. Type in the **Application Alert Type** field a four digit value to be used when this monitor's alert is generated.

8. Select an Alert Type.

   The **Alert Type** is a descriptive term assigned to the generated alert. It can be used by the Alert Manager to differentiate this alert from other alerts for Alert Action responses, and helps to describe the nature of the problem that caused the alert to be generated. Select from the **Alert Type** list an Alert Type to be used when when this monitor's alert is generated.

9. Select Notify (optional).

   Select **Notify** to cause a pop-up window to appear on this system whenever the violating state is reported. If you do not select **Notify**, the threshold will be saved and will be active, but a pop-up window will not automatically inform you if the violating state is reported.

10. Select **Create** to save these threshold values. If you have been editing a previously configured threshold, select **Change** to save the new threshold values.

Attribute Monitor Settings

Attribute Monitor settings are set from the Attribute Monitor notebook's Settings page. To open the notebook, use mouse button 2 to click on the monitor for which you want to set a threshold. From the monitor's context menu, select **Open**, and then select **Settings**.

Use the Attribute Monitor's Settings notebook to:

- Enable or disable the title bar (available on OS/2 systems only)

  Select the **Enable Title Bar** check box to activate a title bar on this monitor. This title bar shows the System Name of the system on which the System Monitor is being run (this will

appear only if the service is being run on a remote system), and the name of the monitor itself. If you do not want a title bar, deselect the **Enable Title Bar** check box.

- Enable or disable bit maps (available on OS/2 systems only)

  When the **Enable Bit Maps** check box is selected, a small icon will appear before each monitored attribute. This icon will indicate the attribute's current state.

- Change the monitor's view

  The following views are available for the Attribute Monitor:

  – Attribute History

    The Attribute History view shows the state reported by the attribute monitor over a specified period of time.
  – Real Time

    The Real Time view shows only the current state of the monitored device.

- Change the monitor's font

  Use the selections available in the Font field group to select the font and font color for use with all text in all views for this monitor. This field group enables you to:

  – Select a font

    Use the spin buttons at the right side of the **Font** field to select the font that will be used for text in each of this component's views.
  – Select a Font Color (available on OS/2 systems only)

    Use the spin buttons at the right side of the **Color** field to select the color of the font that will be used for text in each of this component's views.

To save the new Settings, close the notebook by double-clicking in the upper-left corner.

IBM PC Server 720 Monitors

Netfinity also includes several additional monitors that are specifically designed for use with the IBM PC Server 720. If Netfinity is installed on an IBM PC Server 720, you can use additional monitors that enable you to keep track of the:

- Power supply temperature (Celsius/Fahrenheit)
- System temperature (Celsius/Fahrenheit)
- Planar temperature (Celsius/Fahrenheit)
- Power supply voltage (+5Vac, +12Vac, -12Vac, and +3.3Vac)

Chapter 27. System Partition Access

The Netfinity System Partition Access allows for greatly simplified System Partition file handling on IBM computers. This service features:

- Extensive file-level manipulation
- Initial machine load (IML) image updating
- Adapter description program (ADP), adapter description file (ADF), and diagnostic (DGS) updating
- Set Configuration program updating
- User-confirmation security to prevent accidental deletion of the System Partition

The System Partition is a section of the hard drive on some IBM systems that contains the system's power-on self test (POST), basic input/output system (BIOS), and some system utility programs. If you are not using an IBM system that has a System Partition, you will not have access to, or a need for, this service.

Note: System Partition Access cannot access or manage the System Partitions on *enhanced small device interface* (ESDI) systems.

Netfinity System Partition Access offers a variety of System Partition file-manipulation actions. Available actions are:

- Copy from partition
- Copy to partition
- Delete directory
- Rename directory
- Delete file
- Rename file
- Partition backup
- Partition restore
- Delete partition
- Make directory
- Quit

The following sections provide detailed information on each available action.

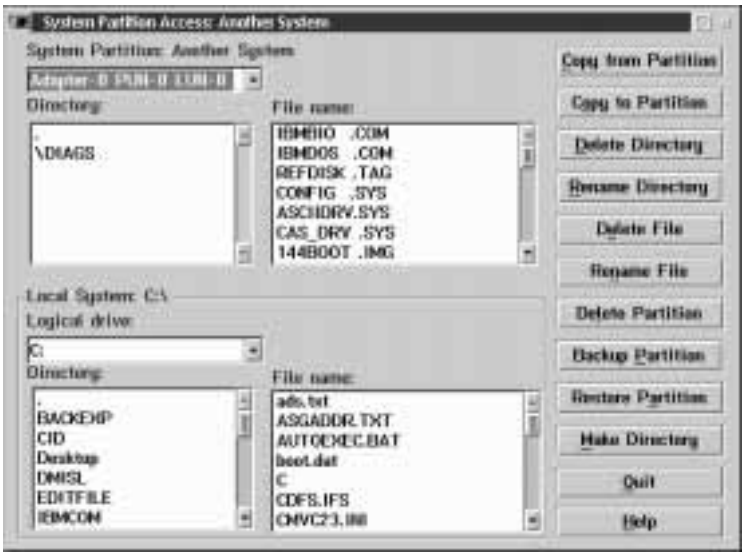

Figure 117. System Partition Access Service

Copy from Partition

You can use the Copy from Partition option to copy a specific file from within your System Partition to a selected directory on a local drive. To use this function:

1. If you have multiple System Partitions, select from the **System Partition** field the partition you want to access.
2. Select the System Partition directory you want to copy a file from by selecting the appropriate directory in the System Partition **Directory** field. When you have selected the directory, all files contained in that directory will be displayed in the System Partition **File name** field.
3. Select from the System Partition **File name** field the file that you want to copy.
4. Select a destination drive for the file. Select the arrow at the right side of the **Logical drive** field to display a list of all available drives. Select one of these drives as the file destination.

5. Select a destination directory for the file. All directories present on the selected logical drive are displayed in the Logical Drive **Directory** field. Select one of these directories. All files located in this directory will then be displayed in the Logical Drive **File name** field.
6. Select **Copy from Partition** to copy the selected System Partition file to the selected destination.

Copy to Partition

You can use the Copy to Partition option to copy a specific file from a local drive to your System Partition. To use this function:

1. If you have multiple System Partitions, select from the **System Partition** field the partition you want to access.
2. Select the System Partition directory you want to copy a file to by selecting the appropriate directory in the System Partition **Directory** field. When you have selected the directory, all files contained in that directory will be displayed in System Partition **File name** field.
3. Select the source drive for the file. Select the arrow at the right side of the **Logical drive** field to display a list of all available drives. Select one of these drives as the source drive.
4. Select the source directory for the file. All directories present on the selected logical drive are displayed in the Logical Drive **Directory** field. Select one of these directories. All files located in this directory will then be displayed in the Logical Drive **File name** field.
5. Select from the Logical Drive **File** field the file that you want to copy.
6. Select **Copy to Partition** to copy the selected file to the System Partition.

Delete Directory

You can use the Delete Directory option to delete a directory from your System Partition. To use this function:

1. If you have multiple System Partitions, select from the **System Partition** field the partition you want to access.
2. Select from the System Partition **Directory** field the System Partition directory you want to delete. Double-click on the directory name to open the directory.
3. Select **Delete Directory** to delete the selected directory from your system. To prevent accidental directory deletion, you must confirm this choice.

Note: The directory that you are deleting *must be empty* before the Netfinity System Partition Access will allow you to delete it. For information on deleting System Partition files, see "Delete File."

Rename Directory

You can use the Rename Directory option to select a new name for a directory within your System Partition. To use this function:

1. If you have multiple System Partitions, select from the **System Partition** field the partition you want to access.
2. Select the System Partition directory you want to rename. Double-click on the directory name to open the directory.
3. Select **Rename Directory**. The System Partition Access will ask you to enter the new name for the selected directory.
4. Enter the new directory name and press **Enter**. System Partition Access will rename the directory.

Delete File

You can use the Delete File option to delete individual files from within your System Partition. To use this function:

1. If you have multiple System Partitions, select from the **System Partition** field the partition you want to access.
2. Select from the System Partition **Directory** field the System Partition directory that contains the file you want to delete. When you have selected the directory, all files contained in that directory will be displayed in the System Partition **File** field.

3. Select from the System Partition **File name** field the file you want to delete.
4. Select **Delete File**. System Partition Access will then delete the selected file.

Rename File

You can use the Rename File option to rename individual files within your System Partition. To use this function:

1. If you have multiple System Partitions, select from the **System Partition** field the partition you want to access.
2. Select from the System Partition **Directory** field the System Partition directory that contains the file you want to rename. When you have selected the directory, all files contained in that directory will be displayed in the System Partition **File name** field.
3. Select from the System Partition **File name** field the file you want to rename.
4. Select **Rename File**. System Partition Access will then ask you what you want to rename the file. Enter the new name for the file and press **Enter**. The file is now renamed.

Delete Partition

Attention:
Deleting the System Partition on a system that requires a System Partition can render the system inoperative. Do not use the Delete Partition option unless you are certain that your system will function properly after the System Partition has been deleted.

You can use the Delete Partition option to remove a selected System Partition (displayed in the **System Partition** field) from your selected Logical Drive. When you have selected this option, System Partition Access will ask you to confirm that you want to delete the partition. To continue, select **OK** and the selected System Partition (as well as all directories and files within the partition) will be deleted.

Backup Partition

You can use the Backup Partition option to copy the System Partition to a file on any logical drive. To use this function:

1. If you have multiple System Partitions, select from the **System Partition** field the partition you want to access.
2. Select a destination drive for the System Partition backup file to be written to. Select the arrow at the right side of the **Logical drive** field to display all available logical drives, and then select the appropriate drive.
3. Select a destination directory. Directories present on the selected logical drive are displayed in the Logical Drive **Directory** field.
4. Select **Partition Backup** to write a file of the selected System Partition to your specified destination.

Restore Partition

You can use the Restore Partition option to restore your System Partition using backup diskettes or files created with the Backup Partition function. To use this function:

1. Select the source drive where the System Partition backup file is located. Select the arrow at the right side of the **Logical drive** field to display all available logical drives, and then select the appropriate drive..
2. Select the source directory where the backup file is located. All directories present on the selected logical drive are displayed in the Logical Drive **Directory** field. Select one of these directories. All files located in this directory will then be displayed in the Logical Drive **File name** field. Select the backup file that you want to use from the Logical Drive **File name** field.
3. Select **Restore Partition** to copy your backup file to the System Partition.

Make Directory

You can use the **Make Directory** option to add a directory to the selected System Partition (displayed in the **System Partition** field). After you have selected this option, System Partition Access will ask you to provide a name for the new directory.

Quit

Select **Quit** to exit System Partition Access.

Chapter 28. System Profile

System Profile provides you with an easy-to-organize repository for a variety of system- and user-specific information that might not be readily available otherwise. The System Profile service comes with many predefined fields to help simplify organization and entry of this data. The System Profile service also features many user-definable fields to help you customize the System Profile to meet your individual needs.

System Profile's data can be saved to an ASCII file. The combination of System Information Tool's sophisticated hardware information gathering abilities with System Profile's extensive selection of system- and user-specific data fields results in an extraordinarily flexible and useful system-inventorying and information facility.

Note: System Profile supports export of collected data to a Netfinity database. However, database export can be performed only by the Netfinity Manager. No database export functions are available for local use on systems running Client Services for Netfinity Manager.

Figure 118. The System Profile service window.

The System Profile service window is made up of five sections, each of which consists of two or more pages and is devoted to a specific type of system- or user-specific information. Each section is identified by its own tab. These sections are:

- System

  The System section of the System Profile service contains predefined fields to help you organize the information specific to your computer, display, printer, and modem.

- User

  The User section of the System Profile service contains predefined fields to help you organize the information specific to a system's primary user including name, phone number, home address, and emergency contact.

- Location

  The Location section of the System Profile service contains predefined fields to help you organize the information specific to the system's physical location, including office number, building number, site name, city, and country.

- Contacts

  The Contacts section of the System Profile service contains predefined fields to help you organize the information regarding various ways of contacting the system's primary user (telephone number, fax number, Email address, and so on) and other personnel associated with the primary user (for example, manager, secretary, and so on).

- Miscellaneous

  The Miscellaneous section of the System Profile service contains undefined fields that you can use to store additional information, such as nicknames and birthdays.

To enter and save data in the System Profile service:

1. Enter the data you want to save in the appropriate fields.

   Select a field and type in the appropriate data. To change pages, select one of the small arrows at the lower right corner of

the page (select the right-pointing arrow to advance one page, and the left-pointing arrow to go back one page). To change sections, select the section's tab from the right side of the service window. You do not need to fill in all of the available fields.

2. Close the System Profile service.

   When you have finished entering information, double-click on the upper-left corner of the System Profile service to save your information and close the service window.

Select **Undo** to reset the current page's fields to their last saved values. Selecting Undo will not have any affect on the other pages in the service window.

To close the service window without saving any changes, select **Close Without Saving** from the Options pull-down menu.

Other actions available from the Options pull-down menu are:

- Refresh

  Select **Refresh** to update the information that is displayed in the System Profile service window. Changes can be made to the service window's contents by other users while you are viewing it; selecting **Refresh** will update the data displayed in the System Profile service window's fields.

- Save to File

  Select **Save To File** to save all information contained in the System Profile service to an ASCII text file.

Chapter 29. Update Connector Manager

You can use Update Connector Manager to quickly and easily gather information about various updates that are available for your client systems. Once available updates are discovered, use Update Connector Manager to apply updates to your systems remotely. Updates can be applied to individual systems, or you can apply multiple updates to multiple systems, all from Netfinity Manager. You can also use Update Connector Manager to remove previously applied updates. Update Connector Manager also includes a scheduler that you can use to discover, apply, or remove updates automatically and periodically.

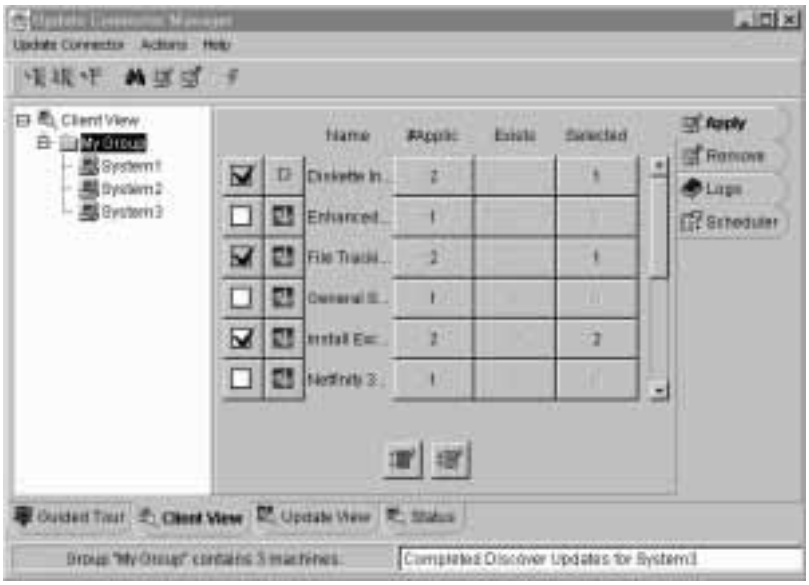

Figure 119. The Update Connector Manager window

Hardware and Software Requirements

To use the Update Connector Manager, you must have:

- A system containing a Pentium 100 MHz processor or faster with 64MB or more RAM running Windows NT 4.0 or later.
- A web browser installed on your system.

- A mouse or other pointing devide to use the Update Connector Manager interface.
- A connection to the Internet.

Notes:

1. The Update Connector Manager interface is available for use only on systems running Windows NT. However, data can be collected from and updates applied to remote systems running Client Services for Netfinity Manager on systems with a system containing a Pentium 100 MHz processor or faster with 32MB or more RAM running Windows 95 or Windows NT 4.0 or later.
2. The update packages that are used by Update Connector Manager are not provided or maintained by the Update Connector Manager or Netfinity Manager development teams.

The Update Connector Manager Interface

The Update Connector Manager interface is comprised of the following parts:

The Menu Bar — A series of pull-down menus found at the top of the window, just below the Update Connector Manager title bar. The 3 pull-down menus are named Update Connector, Actions, and Help. All Update Connector Manager functions can be accessed by using selections available from these pulldown menus.

The Toolbar — A row of buttons found just below the Menu Bar. You can use these buttons to quickly access the most commonly used Update Connector Manager functions. Each button also features tooltips to help you easily identify the function of the button. To see a tooltip, move your mouse pointed over the button but do not click on the button. After a few seconds a small window descirbing the button appears.

The Client View Tree A visual representation of the systems (and system groups) that can be updated and maintained using Update Connector Manager. The Client View tree appears only when the Client View tab is selected.

Note: An Update Connector Manager group must be added before systems can be added to the Client View tree. If you are running Update Connector Manager for the first time, there will not be any groups available from the Client View tree.

The Update View Tree A visual representation of all updates (and update pools) that are available for use on your systems. The Update View tree appears only when the Update View tab is selected.

Context Menus Pop-up menus that appear when the right-mouse button is clicked on any item in the Client View or Update View tree. You can use context menus to quickly select Update Connector Manager functions that are of use for the selected tree element.

The Status Bar The small box found at the bottom of the Update Connector Manager window that contains information about the current Update Connector Manager status.

View Tabs A series of tabs that run horizontally across the bottom of the window, above the status area. These tabs (labeled **Client View**, **Update View**, **Status**, and **Guided Tour**) control the appearance of the Update Connector Manager window, the manner in which the contents of the Update Connector Manager window are

displayed, and what Update Connector Manager functions are available.

Function Tabs

A series of tabs that run vertically along the right side of the window. The labels on these tabs vary, depending on which View Tab is selected.

- When **Client View** is selected, the following Function Tabs are available:
  - Apply
  - Remove
  - Logs
  - Scheduler

  For more information on Client View, see "Update Connector Manager Client View."
- When **Update View** is selected, the following Function Tabs are available:
  - Apply
  - Remove
  - Logs

  For more information on Update View, see "Update Connector Manager Update View" on page 388.
- No Function Tabs are available when the **Status** or **Guided Tour** view tabs are selected. For more information on Status, see "Update Connector Manager Status View" on page 390. Click on the Guided Tour tab for brief online tour of the basic Update Connector Manager functions.

Update Connector Manager Client View

The Client View presents Update Connector Manager information from a client system point of view. The Client View tree consists of all currently defined groups, and any defined systems. When you

select a system or group from the Client View tree, the Update Connector Manager window updates to display information about the updates that are available for use on the selected system or group (if the **Apply** function tab is selected) or updates that have already been applied and are available for removal (if the **Remove** function tab is selected). You can also select **Logs** (for information about previsouly completed Update Connector Manager tasks) or **Scheduler** (to create scheduled Update Connector Manager tasks).

The Update Connector Manager client view is shown in Figure 119 on page 383.

When the **Apply** or **Remove** function tab is selected, a list of updates that are available for use on your systems appears in the main body of the window. If the **Apply** function tab is selected, checkboxes appear beside all of the updates that are listed that have not yet been applied. Updates that have been applied to currently selected systems (or to systems that are part of a selected group) will not have a checkbox, signifying that the update has been applied. Beside the checkbox is an information button. Select this information button to display a brief description of the update in your web browser.

The list of updates includes the following information:

Name	The name of the update.
#Applic	The number of currently selected systems (or the number of systems within the currently selected group) to which this update applies. To see a list of the system names to which the update applies, select the number that appears in the #Applic. column to the right of the update name.
Exists	The number of currently selected systems (or the number of systems within the currently selected group) to which the update has already been applied. To see a list of the system names to which the update has already been applied, select

	the number that appears in the Exists column to the right of the update name.
Selected	The number of systems to which an update that is selected will be applied.

The list of updates also features buttons at the bottom of the list that enable you to quickly select or deselect all of the listed updates.

Update Connector Manager Update View

The Update View presents Update Connector Manager information from an update and update pool point of view. The Update View tree consists of all currently available updates, and any defined update pools. When you select an update or update pool from the Update View tree, the Update Connector Manager window updates to display information about the systems on which the selected update or update pool can be used. If the **Apply** function tab is selected, information about systems on which the selected update (or updates, if an update pool is selected from the Update View tree) can be applied is displayed. If the **Remove** function tab is selected, information about systems to which the selected update (or updates, if an update pool is selected from the Update View tree) have been applied is displayed. You can also select **Logs** (for information about previously completed Update Connector Manager tasks).

Figure 120. The Update Connector Manager Update View

When the **Apply** or **Remove** function tab is selected, a list of updates that are available for use on any of your defined systems appears in the main body of the window. If the **Apply** function tab is selected, checkboxes appear beside all of the updates that are listed that have not yet been applied to some or all of your systems. Updates that have already been applied to all defined systems will not have a checkbox, signifying that the update has been applied. Beside the checkbox is an information button. Select this information button to display a brief description of the update in your web browser.

The list of updates includes the following information:

Name The name of the update.

#Applic The number of systems (or the number of systems within the currently selected group) to which this update applies. To see a list of the system names to which the update applies, select the number that

	appears in the #Applic. column to the right of the update name.
Exists	The number of systems (or the number of systems within the currently selected group) to which the update has already been applied. To see a list of the system names to which the update has already been applied, select the number that appears in the Exists column to the right of the update name.
Selected	The number of systems to which an update that is selected will be applied.

The list of updates also features buttons at the bottom of the list that enable you to quickly select or deselect all of the listed updates.

Update Connector Manager Status View

Some updates can take a couple of minutes (or more) to complete. When an update is being applied, you can check the status of the update process at any time by clicking on the **Status** view tab.

Figure 121. The Update Connector Manager Status View

This view shows all current Update Connector Manager tasks and assorted information about each task is the status list. The following information is available in the **Status** list:

Task # — A count, beginning at 100, of the number of tasks that have been started or completed by Update Connector Manager since the interface was started.

Status — The status of the task (Scheduled, Completed, Running, Suspended, or Stopped).

Task — The task that Update Connector Manager completed performing or is in the process of performing (Discover Updates or Update Apply, for example).

Percent Complete — What percentage of the task is currently complete.

Object	The system, group, or update pool that is the primary focus of the task. For example, if you perform an update discovery on a group named "My Group," the **Object** would be **My Group**. However, if you create an update pool named "My Pool," the **Object** would be **My Pool**.

A series of 8 buttons are located below the **Status** list. Each button features tooltips to help you identify their function. Use the mouse to point to a button for a few seconds (but do not click on the button) and a small window will appear that described the purpose of the button.

The first group of 4 buttons controls the manner in which the contents of the window are displayed (large icons, small icons, list, or details views are available; details view is the default).

The second group of 4 buttons are action buttons that you can use to enable to suspend, resume, or stop tasks that Update Connector Manager is currently performing. You can also clear the contents of the Status list.

To suspend, resume, or stop a currently-active task:

1. Click in the **Status** list of the active task.
2. Click on the action button (**Suspend**, **Resume**, or **Stop**) that corresponds to action you want to perform on the selected task.

To clear the contents on the **Status** list, click on the **Clear List** action button.

Note: The Status list contains entries for tasks that have occurred only since you started the Update Connector Manager interface. If you close Update Connector Manager, all entries in the Status list are automatically deleted.

Update Connector Manager Group Functions

Before you can use Update Connector Manager to discover, apply, or remove updates from your client systems, you must first create groups. Groups created with Update Connector Manager also appear in the Remote System Manager System Group Management window.

Note: Once Update Connector Manager groups are created, you can use the Remote System Manager *Discovery* function to automatically discover and add mulstiple systems that are running the Update Connector Manager client to this group. For more information on using Remote System Manager with Update Connector Manager, see "Using Remote System Manager with Update Connector Manager" on page 417.

Instructions on how to create, edit, or remove Update Connector Manager groups follows.

Create Group

To create a group:

1. Select the **Client View** tab.
2. Select the **Apply** function tab.
3. Select **Create Group** from the Update Connector pulldown menu.

   The Create Group window opens.

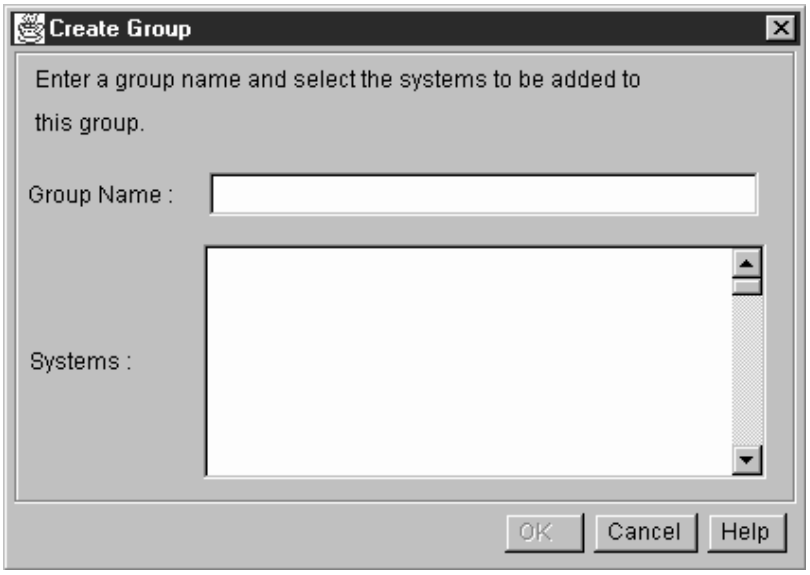

Figure 122. The Create Group window

4. Type in the **Group Name** field a name for your new group. The group name can be up to 32 characters long.
5. If you have previously created systems and added them to other groups, the systems will be listed in the **Systems** selection list. To add one (or more) systems to the new group, click in the **Systems** selection list on the names of the systems you want to add.

   Note: If you have not yet added any systems to other Update Connector Manager groups this list will be empty.
6. When you have typed a name for the group in the **Group Name** field and selected any systems that you want to include in the group from the **Systems** selection list, select OK to finish creating the new group.

The group will be added to the Update Connector Manager Client View tree and will also be added as a new Remote System Manager group.

Edit Group

You can use the Edit Group function to change the name of the group and to select systems to include in the group.

To edit a group:

1. Select the **Client View** tab.
2. Select the **Apply** function tab.
3. Select a group from the Client View tree.
4. Select **Edit Group** from the Update Connector pulldown menu.

   The Edit Group window opens.

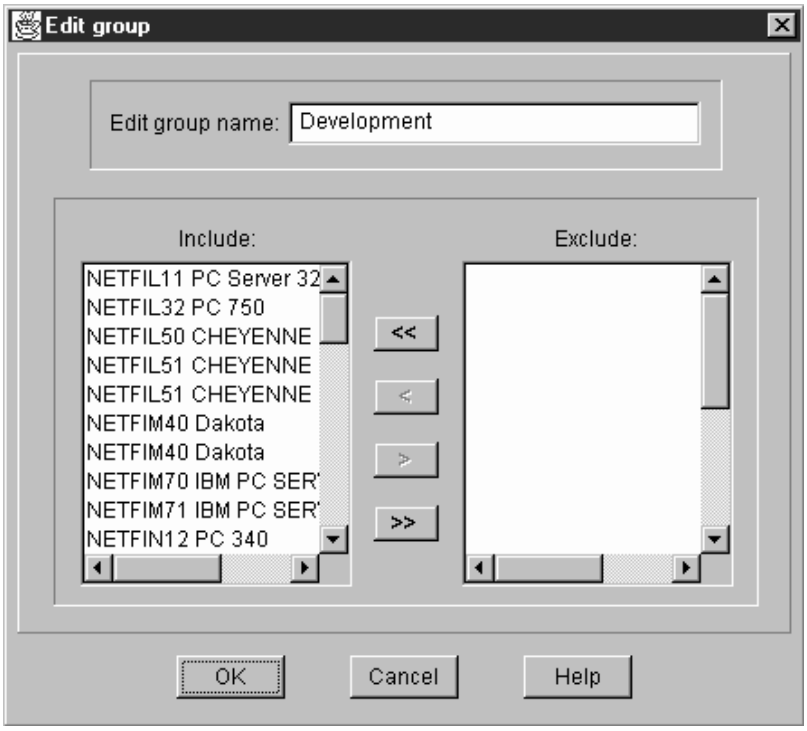

Figure 123. The Edit Group window

This window shows the current name of the group and a list of all systems that are currently included in the group (the **Include**

selection list) and systems that are currently no included in this group (the **Exclude** selection list).

5. Edit the group.
   - To change the name of the group, type in the **Group Name** field a new name for the group. The group name can be up to 32 characters long.
   - Add or remove systems from the group.

     To add systems that are currently excluded from the group, click on one or more system names in the **Exclude** selection list and the click on the < button. The selected system names are removed from the **Exclude** selection list and are added to the Include selection list.

     To remove systems that are currently included in the group, click on one or more system names in the **Include** selection list and then click on the > button. The selected systems are removed from the **Include** list and added to the **Exclude** list.

     You can use the << and >> buttons to move all systems between the lists.
6. When you have finished editing the group name or the list of systems that are included in or excluded from this group, select OK to finish editing the group. The group will be updated in the Update Connector Manager Client View tree and will also be updated in Remote System Manager.

Remove Group

To remove a group:

1. Select the **Client View** tab.
2. Select the **Apply** function tab.
3. Select from the Client View tree the group you want to remove.
4. Select **Remove Group** from the Update Connector pulldown menu.

The Delete Group window opens, with the group name that you selected from the Client View tree highlighted in the **Group** selection list.

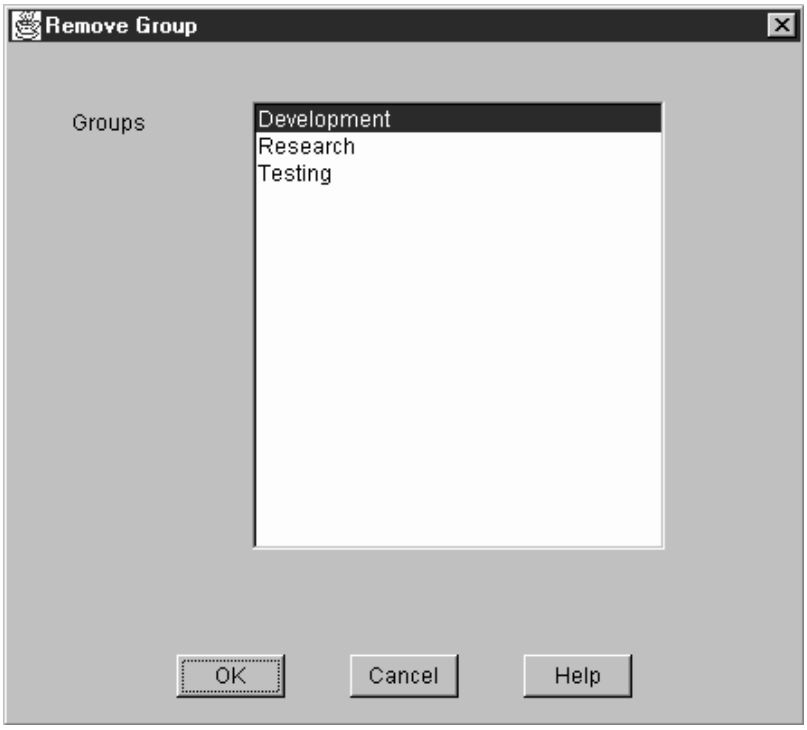

Figure 124. The Remove Group window

5. To delete multiple group simultaneously, select additional groups from the **Groups** selection list.
6. When you have selected all groups that you want to delete from the **Groups** selection list, select **OK** to delete all selected groups. All selected groups will be deleted from the Update Connector Manager Client View tree and will also be deleted in Remote System Manager.

Update Connector Manager System Functions

Use the Update Connector Manager system functions to add or remove client systems from your Update Connector Manager groups.

Note: You can use the Remote System Manager *Discovery* function to automatically discover and add multiple systems that are running the Update Connector Manager client to Update Connector Manager groups. For more information on using Remote System Manager with Update Connector Manager, see "Using Remote System Manager with Update Connector Manager" on page 417.

Add System

To add a system to a group:

1. Select a group (or a previously added system) from the Client View tree.
2. Select **Add System** from the Update Connector pulldown menu.

   The Add System window opens.

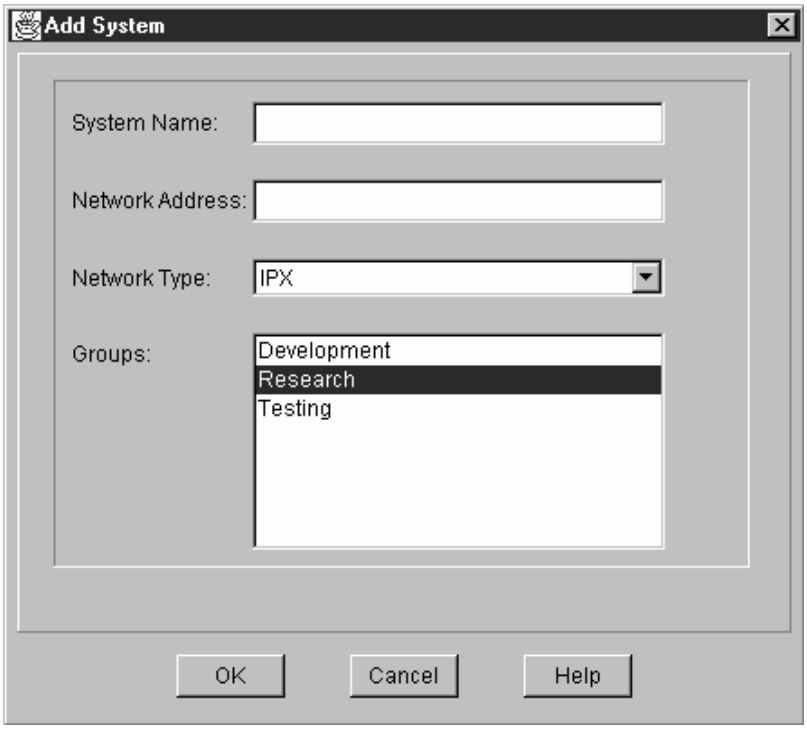

Figure 125. The Add System window

3. Type in the **System Name** field a name for the system you are adding. This name is for your use only and can be up to 32 characters in length.
4. Type in the **Network Address** field the network address of the system you are adding. This address can be up to 64 characters in length.

   Note: If no address is provided, the name you typed in the **System Name** field will be filled in automatically.
5. Select from the **Network Type** drop box the communications protocol that is used to communicate with the system you are adding.

   Note: Only communications protocols that are available for use by the system running the Update Connector Manager interface will be available.

6. Select from the **Groups** selection list one or more groups to which the newly created system will be added.
7. Select **OK** to finish adding the system to any selected groups.

This system will be added to the selected group in the Update Connector Manager Client View tree, and will also be added to the Remote System Manager group.

Remove System

To remove a system:

1. Select the **Client View** tab.
2. Select the **Apply** function tab.
3. Select from the Client View tree the system that you want to remove.
4. Select Remove System from the Update Connector pulldown menu.

   The Remove System window opens, with the system name that you selected from the Client View tree highlighted in the Systems selection list.

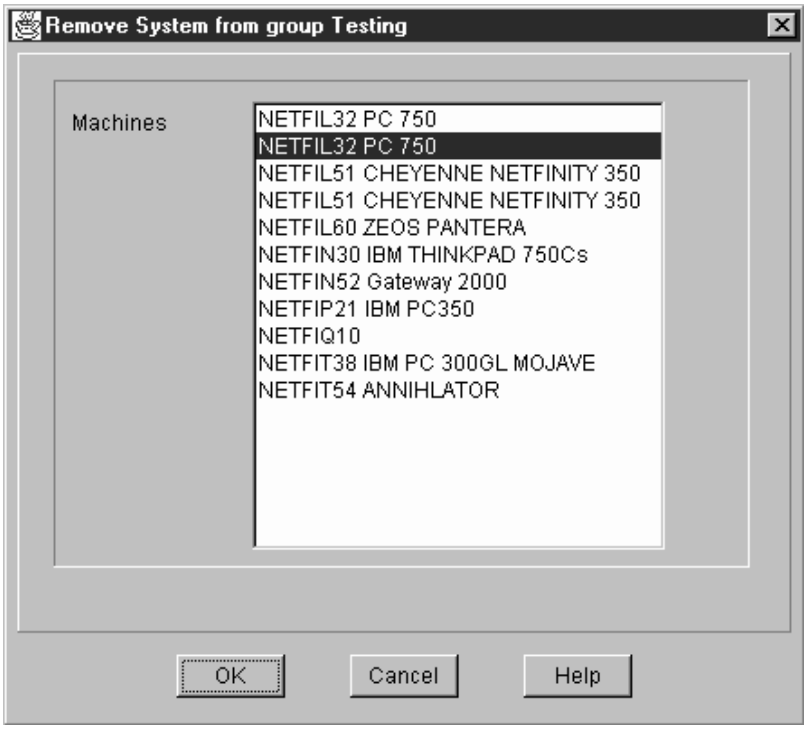

Figure 126. The Remove System window

5. To delete multiple systems simultaneously, select additional systems from the **Systems** selection list.
6. When you have selected all systems that you want to delete from the **Systems** selection list, select **OK** to delete all selected systems.

All selected systems will be deleted from all groups in which they are included in the Update Connector Manager Client View tree and will also be deleted in Remote System Manager.

Update Connector Manager Update Functions

After you have created at least one Update Connector Manager group and have added at least one client system to that group, you can use Update Connector Manager to:

- Discover updates for selected client systems.
- Apply updates to client systems.
- Remove previously applied updates from client systems.

Once updates are discovered they can be orgainized into *update pools*. Once updates are grouped into pools, you can simultaneously apply all updates in a selected pool to client systems to which the updates apply.

If you attempt to perform a task on a system that is not currently available, Update Connector Manager will finish all other portions of the current task. When the previously unavailable system comes back online, Update Connector Manager will attempt to perform the task again.

Discover Updates

To discover available updates:

1. Select the **Client View** tab.
2. Select the **Apply** function tab.
3. Select from the Client View tree the system or group for which you want to discover updates.
4. To discover updates now, select **Discover Updates** from the Actions pulldown menu.

   Note: You can use the Update Connector Manager scheduler to create a scheduled event for selected groups or systems. This will delay the discovery process until a later time, and will also enable you to create a scheduled task that will be repeated automatically on an hourly, daily, weekly, monthly, or yearly basis. For more information, see “Creating Scheduled Tasks” on page 410.

   The status bar at the bottom of the Update Connector Manager window indicates that update discovery is starting. During the update discovery process, system information about the system that you selected from the Client View tree (or, if you selected a group from the Client View tree, all systems that are included in the group) is gathered and then used to query the update database.

Updates that apply to the systems are identified and displayed in the Update Connector Manager window when update discovery completes. The Update Connector Manager Log contains additional information about the update discovery.

Apply Updates

To apply updates:

1. Select the **Client View** tab.
2. Select from the Client View tree a system or a group to which you will apply updates.
3. Select the **Apply** function tab.

   The Update Connector Manager window updates to display a list of all available updates for the selected systems or groups.

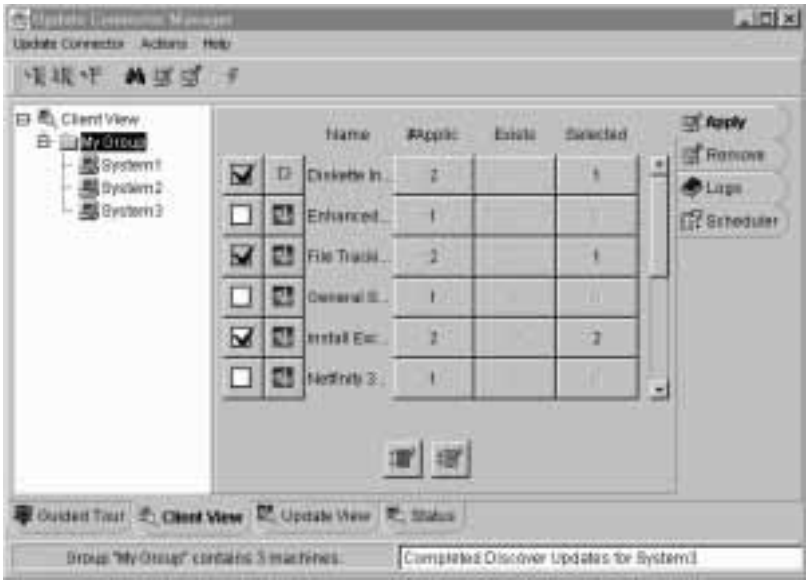

Figure 127. A list of available updates

4. Select any updates that you want to apply. To select an update, check the check box that appears beside the update.

5. To apply updates now, select **Apply Updates** from the Actions pulldown menu.

   Note: You can use the Update Connector Manager scheduler to create a scheduled event for selected groups or systems. This will delay the update application process until a later time, and will also enable you to create a scheduled task that will be repeated automatically on an hourly, daily, weekly, monthly, or yearly basis. For more information, see "Creating Scheduled Tasks" on page 410.

   The status bar at the bottom of the Update Connector Manager window indicates that update application process is starting. Update Connector Manager will then attempt to apply all selected updates to the system you selected from the Client View tree (or, if you selected a group from the Client View tree, to all systems in the selected group).

   At any time while updates are applied, you can check the status of the update apply process by selecting the **Status** tab.

   When the apply updates process completes, you can check the results by selecting the **Client View** tab and then selecting the **Logs** function tab.

Remove Updates

To remove previously applied updates:

1. Select the **Client View** tab.
2. Select from the Client View tree a system or group from which you want to remove previously applied updates.
3. Select the **Remove** function tab. P.The Update Connector Manager window updates to display a list of all updates that have been applied to the selected system (or to any systems contained in a selected group).

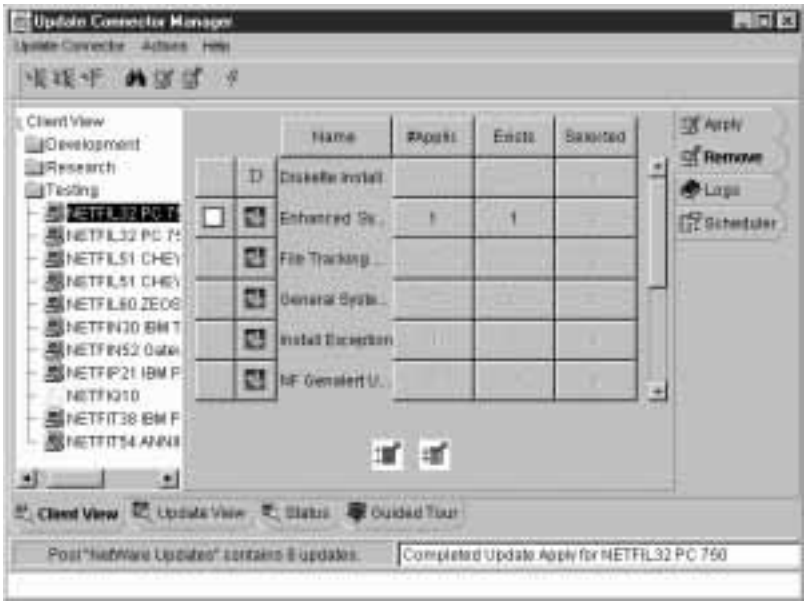

Figure 128. A list of previously applied updates

4. Select any previously applied updates that you want to remove. To select an update, uncheck the check box that appears beside the update.
5. To remove updates now, select **Remove Updates** from the Actions pulldown menu.

   Note: You can use the Update Connector Manager scheduler to create a scheduled event for selected groups or systems. This will delay the update removal process until a later time, and will also enable you to create a scheduled task that will be repeated automatically on an hourly, daily, weekly, monthly, or yearly basis. For more information, see "Creating Scheduled Tasks" on page 410.

The status bar at the bottom of the Update Connector Manager window indicates that update removal process is starting. Update Connector Manager will then attempt to remove all selected updates from the system you selected from the Client View tree (or, if you

selected a group from the Client View tree, from all systems in the selected group).

At any time while updates are being removed, you can check the status of the update removal process by selecting the **Status** tab.

When the update removal process completes, you can check the results by selecting the **Client View** tab and then selecting the **Logs** function tab.

Create Update Pools

Once you have discovered updates, you can create update pools. Update pools provide you with a simple way to organize updates into groups and apply multiple updates simultaneously. An individual update can be a part of multiple pools.

To create an update pool:

1. Select the **Update View** tab.
2. Select the **Apply** function tab.
3. Select **Create Pool** from the Update Connector pulldown menu.

   This opens the Create Pool window.

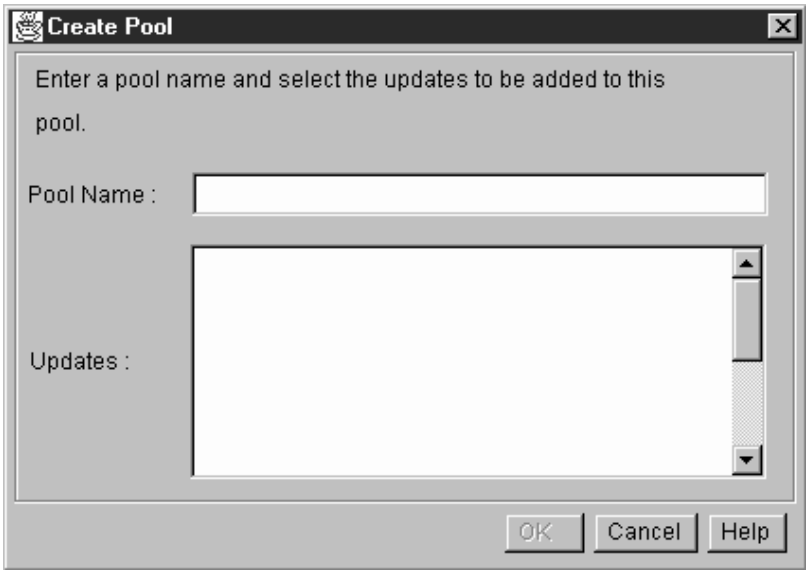

Figure 129. The Create Pool window

4. Type in the **Pool Name** field a name for this update pool. The update pool name can be up to 32 characters long.
5. All currently discovered and available updates are listed in the **Updates** selection list. To add updates to this pool, click on one (or more) update names.
6. When you have provided a name for the update pool and finished selecting updates to include in or exclude from this group, select **OK** to finish creating the update pool. The update pool will then be added to the Update Connector Manager Update View.

Edit Update Pools

To edit a previously created update pool:

1. Select the **Update View** tab.
2. Select the **Apply** function tab.
3. Select an update pool from the Update View tree.
4. Select **Edit Pool** from the Update Connector pulldown menu.

This opens the Edit Pool window.

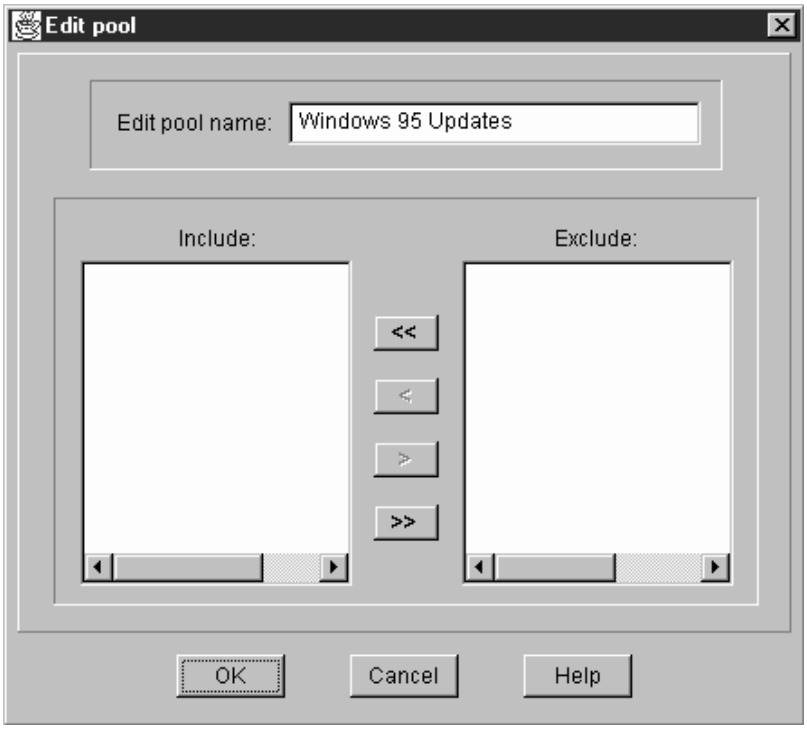

Figure 130. The Edit Pool window

5. Type in the **Edit Pool Name** field a new name for this update pool. The new update pool name can be up to 32 characters long.
6. All updates that are currently included in this update pool are listed in the **Include** selection list. All available updates that are not included in this update pool are listed in the **Exclude** selection list.
   - To add updates to this pool, click on one (or more) update names in the **Exclude** selection list and the click on the < button. The selected updates are removed from the **Exclude** selection list and are added to the **Include** selection list.

- To remove updates from the **Include** selection list, click on one (or more) update names in the **Include** selection list and click on the > button. The selected updates are removed from the **Include** selection list and are added to the **Exclude** selection list.
- You can use the << and >> buttons to move all updates between the lists.

7. When you have provided a new name for the update pool or finished selecting updates to include in or exclude from this group, select **OK** to finish editing the update pool. The update pool will be updated in the Update Connector Manager Update tree view.

Remove Update Pools

To remove an update pool:

1. Select the **Update View** tab.
2. Select the **Apply** function tab.
3. Select from the Update View tree the pool you want to delete.
4. Select **Remove Pool** from the Update Connector pulldown menu.

   The Remove Pool window opens, with the update pool name that you selected from the Client View tree highlighted in the Pools selection list.

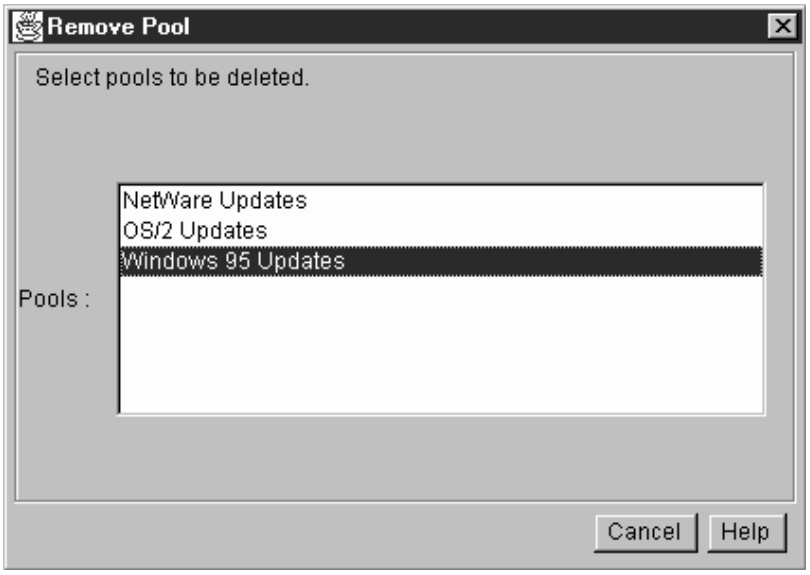

Figure 131. The Remove Pool window

5. To delete multiple pools simultaneously, select additional pools from the **Pools** selection list.
6. When you have selected all pools that you want to delete from the Pools selection list, select **OK** to delete all selected pools. All selected groups will be deleted in the Update Connector Manager Update tree view.

Creating Scheduled Tasks

You can use Update Connector Manager to schedule update discovery, apply update, or remove update processes so that they are performed at a later time. These automatically performed tasks can be scheduled to occur once only, or you can create a schedule that will repeat the scheduled task hourly, daily, weekly, monthly or yearly.

If you attempt to perform a task on a system that is not currently available, Update Connector Manager will finish all other portions of the current task. When the previously unavailable system comes

back online, Update Connector Manager will attempt to perform the task again.

To create a scheduled Update Connector Manager task:

1. Select systems or groups and configure any task-specific information.

   Before you can schedule a task, you must configure the task that will be performed.

   - To schedule an apply update process, select systems or groups from the Client View tree, select the **Apply** tab, and then select any updates you want to apply.
   - To schedule a remove update process, select systems or group from the Client View tree, select the **Remove** tab, and then select any updates you want to remove.
   - To schedule an update discovery, select systems or groups from the Client View tree.

2. Select the **Schedule** tab.

   The Update Connector Manager window will update to display any currently scheduled tasks that apply to the selected group. Currently scheduled task entries are displayed in a detail view with several columns of task-specific information.

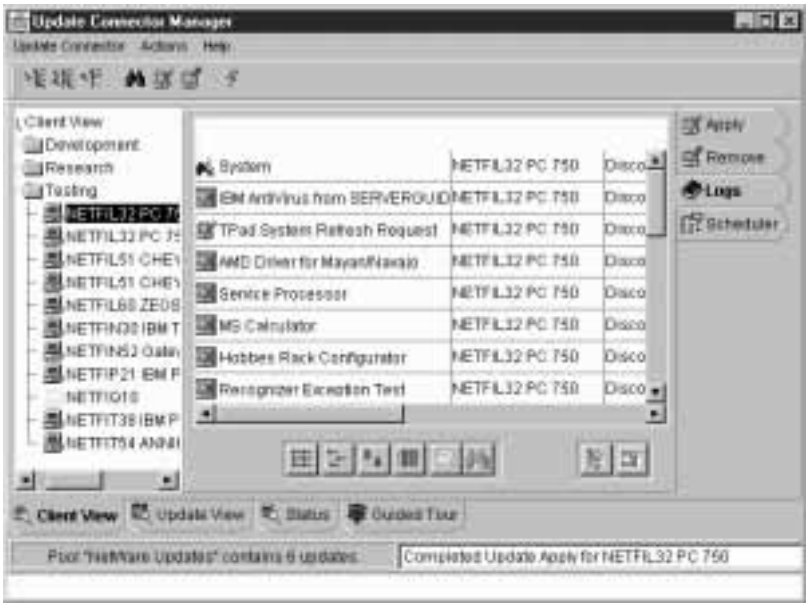

Figure 132. A list of scheduled tasks

The information displayed for each task is:

Name	The name of the scheduled task.
Task	The type of scheduled task that will be performed (Apply, Remove or Discover).
Target	The name of the groups or systems on which the scheduled task will be performed.
Time	The next time at which the scheduled task will be performed.
Frequency	How often the task will be performed (one-time, hourly, daily, weekly, monthly, or yearly).

A series of 7 buttons appear below the list of scheduled events. The first group of 3 buttons are scheduler action buttons that enable you to create new scheduled events, delete previously

created scheduled events, and edit previously created events. The second group of 4 buttons controls the manner in which the contents of the window are displayed (large icons, small icons, list, or details view are available; details view is the default).

Each button features tooltips to help you identify their function. Use the mouse to point to a button for a few seconds (but do not click on the button) and a small window will appear that described the purpose of the button.

3. Select the **Create Event** button (this is, when viewed from left to right, the first button at the bottom of the window). This opens the Scheduler window. You can also create a scheduled event by selecting **Schedule Discovery**, **Schedule Apply**, or **Schedule Remove** from the Actions pull-down menu.

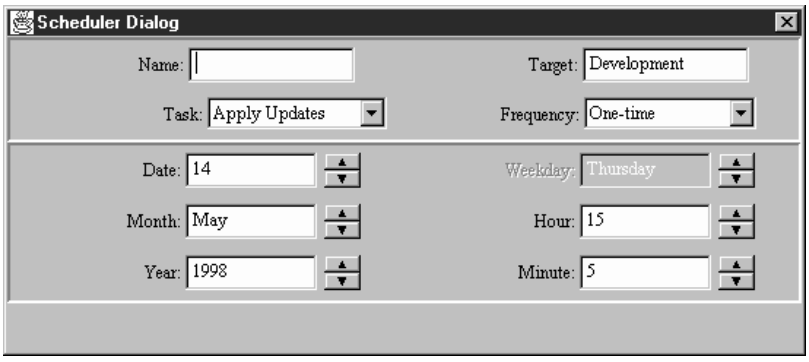

Figure 133. The Scheduler window

Use the Scheduler window to specify all of the information that determines what task will be performed, at what time the task will be performed, and how often (if at all) the task will be repeated.

The following fields appear in the top half of the Scheduler window and determine the name of the task, the Update Connector Manager group on which the task will be performed, the task that will be performed, and how often the task will be performed.

Name Type in this field a name for the scheduled task.

Target The name of the systems or groups you selected from the Client View tree appears in this field.

Task Select from this selection list the scheduled task that you want to create. You can select **Discover Update**, **Apply Updates**, or **Remove Updates**. If you opened the Scheduler window by selecting **Schedule Discovery**, **Schedule Apply**, or **Schedule Remove** from the Actions pull-down menu, the corresponding task will already be selected in this list.

Frequency Select from this selection list the frequency with which this scheduled task will be performed. You can select one time, hourly, daily, weekly, monthly, or yearly.

The following fields appear in the bottom half of the Scheduler window and determine the time at which the scheduled task will be performed.

Note: A field will only be available if it is needed to configure the task. For example, if you select Daily from the Frequency selection list, the Date, Month, Year, and Weekday fields will be disabled. This is because you do not need to enter any values in these fields to complete configuring the scheduled task.

Date Select from this selection list the date of the month on which the scheduled task will be performed.

Weekday Select from this selection list the day of the week on which the scheduled task will be performed.

Month	Select from this selection list the month of the year in which the scheduled task will be performed.
Hour	Select from this selection list the hour of the day at which the scheduled task will be performed.
Year	Select from this selection list the year in which the scheduled task will be performed.
Minute	Select from this selection list the minute of the selected hour at which the scheduled task will be performed.

4. When you have finished configuring all scheduling information, select Schedule to finish configuring the scheduled task. The task will be performed at the time you specified in the Scheduler window. If you selected any frequency other than one-time from the scheduler window Frequency field, the task will be repeated periodically.

Server Administration

Use Server Administration to change Update Connector Manager network communication settings.

Note: If the Server Administration settings are not configured correctly, Update Connector Manager will not function properly.

To use Server Administration:

1. Select **Server Administration** from the Update Connector pulldown menu.

   The Server Administration window opens.

Figure 134. The Server Administration window

2. Confiure your server settings.

   You can change any of the following Server Administration settings:

   Update Selection Server The IP address and port number that Update Connector Manager will use to communicate with the selection server. The selection server is where all approved and available updates are stored.

   Note: This value is pre-configured. Do not change this value unless you are instructed to so by service and support personnel. If this setting is incorrect, Update Connector Manager will be unable to discover and apply updates. If you change this or any other Server Configuration value in error, you can select **Restore** to

change all values back to their pre-configured state.

Network Proxies — If Update Connector Manager is installed in an environment that requires use of a SOCKS server to communicate with systems on the Internet, type in the SOCKS field the TCP/IP address of the SOCKS server. If you are uncertain of whether you need to supply a SOCKS server address, contact your network administrator for help.

3. Select **Save** to save changes to any of these values.

Select **Restore** at any time to change all values back to their pre-configured state.

Using Remote System Manager with Update Connector Manager

You can use Remote System Manager to quickly and easily add systems to your Update Connector Manager groups. When you use Update Connector Manager to create a group, a special Update Connector Manager group is added to the Remote System Manager. These special Remote System Manager groups are easily identified by their group image, which resembles the Update Connector Manager update symbol.

Once an Update Connector Manager group has been added to Remote System Manager, you can use the Remote System Manager Discovery function to quickly add multiple systems to the group.

To add multiple systems to an Update Connector Manager group using Remote System Manager:

1. Use Update Connector Manager to create a group.
2. Close Update Connector Manager.
3. Start Remote System Manager.

4. Open the Update Connector Manager group that appears in the System Group Management window.
5. Select **Discover Systems** from the System pulldown mdenu.

   Remote System Manager automatically adds all remote systems that are running the Update Connector Manager client to this group.
6. When Remote System Manager has finished adding systems, close the Update Connector Manager group window.
7. Close Remote System Manager.
8. Start Update Connector Manager.

All systems that were discovered using Remote System Manager have now been added to your Update Connector Manager group in the Client View tree.

Chapter 30. Web Manager Configuration

Netfinity Manager includes support for the Netfinity Manager for Web. Netfinity Manager for Web is a special-purpose web server specifically designed to work with the Netfinity services. You can use Netfinity Manager for Web to remotely access and manage the systems on your network from anywhere in the world, using the Internet and a World Wide Web (WWW) browser. For more information on the Netfinity Manager for Web, see Chapter 31, "Netfinity Manager for Web" on page 424.

You can use the Web Manager Configuration service to:

- Enable or disable Netfinity Manager for Web
- Specify the TCP/IP socket number that the Netfinity Manager for Web web server listens on
- Prevent unauthorized users from accessing your Netfinity services over the Internet
- Enable and disable logging

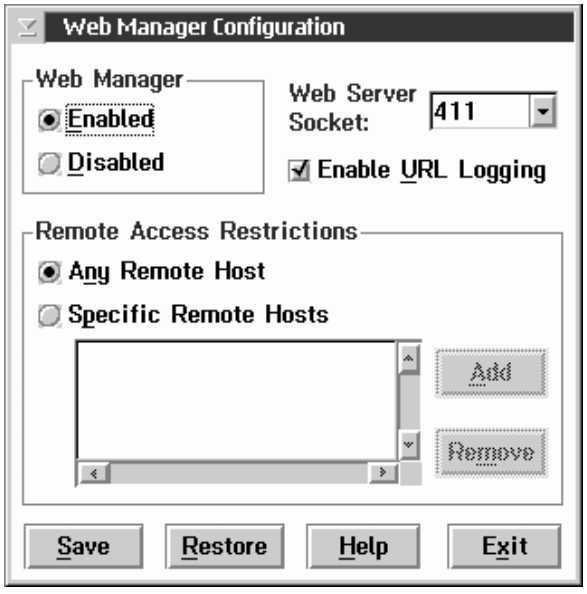

Figure 135. The Web Manager Configuration service

Enabling and Disabling Netfinity Manager for Web

To enable or disable Netfinity Manager for Web, select the **Enable** or **Disable** radio button in the Web Manager Configuration window and then select **Save**.

Specifying a TCP/IP Socket Number

By default, Netfinity Manager for Web web server uses TCP/IP socket number 411. However, you can configure the Netfinity Manager for Web web server to operate on any valid TCP/IP socket.

To specify a socket number, type the socket number in the **Web Server Socket** field, or select the arrow beside the field and select a socket number from the list and then select **Save**.

Enabling URL Logging

Select this checkbox to log all requests made to the web server. All URL logging information is stored in your Netfinity directory in a file named WEBFIN.LOG. The informations is recorded in the form of a plain text URL. In addition, the Intel byte order IP address of the requesting machine and the time/date stamp of the request are also logged.

Since many parameters are sent over the URL, sensitive data could potentially be logged (such as passwords). Users must be careful to secure the machine against possible tampering.

Note: The logging action takes care to remove passwords from the log that are entered through the security service. However this does not prevent a user from entering a password and having it logged by other services, such as while setting up an alert action to export alerts to a database.

Limiting Access to Netfinity Manager for Web

The Netfinity Manager for Web enables anyone with a web browser and a connection to the Internet (or any system using TCP/IP that can communicate with your network) to remotely access the Netfinity services on your Netfinity Manager system and on all other Netfinity systems in your network. When the Netfinity Manager is accessed over the Internet, the Security Manager service restricts access to individual services in the same way in which it restrict access by other Netfinity Managers on your own network. However, due to the highly open and unrestricted nature of the Internet, you might want to place firmer restrictions on access to your Manager system.

Web Manager Configuration adds an additional layer of security to your Netfinity Manager. You can use Web Manager Configuration to permit Netfinity Manager for Web access only to specified TCP/IP hosts and ranges of TCP/IP host addresses, preventing unauthorized Internet users from accessing your Netfinity Manager system at all.

- If you want to permit access to the Netfinity Manager for Web by any remote host to access the Netfinity Manager for Web, select **Any Remote Host** and then select **Save**.
- If you want to permit access to the Netfinity Manager for Web only by specified remote host addresses and ranges of host addresses, select **Specific Remote Hosts** and then select **Save**. Access to the Netfinity Manager for Web will now be permitted to only those host addresses or address ranges that appear in the **Specific Remote Hosts** field.

Note: If a remote user uses a SOCKS server to access the Internet, all attempts to access remote systems are actually made by their SOCKS server. If access is granted, the SOCKS server retrieves the requested information and then relays it back to the requesting system. In this case, access attempts will appear to originate from the TCP/IP address of the SOCKS server, **not** from the TCP/IP address of the remote user's system. If you use the Web Configuration service to limit access to specific TCP/IP addresses or address ranges and the TCP/IP address of the SOCKS server is not included in the

list of addresses or ranges, users configured to access the web using that SOCKS server will not be able to access Netfinity Manager for Web.

To add a specific TCP/IP host address to the **Specific Remote Hosts** field:

1. Select **Specific Remote Hosts**.
2. Select **Add**.

   The Add Authorized Host window appears (see Figure 136).
3. Select **Authorize Specific Host**.
4. Type in the **Host Name or Address** field the TCP/IP name or address of the host system you want to permit to access the Netfinity Manager for Web.
5. Select **OK** to close the Add Authorized Host window and add this address to the Specific Remote Hosts field in the Web Manager Configuration window.
6. Select **Save** from the Web Manager Configuration window to save these settings.

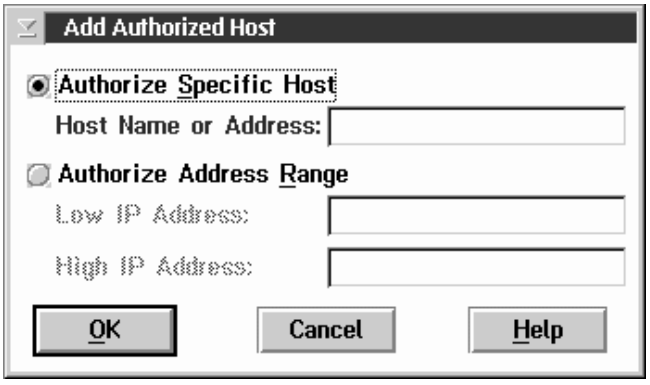

Figure 136. The Add Authorized Host window

To add a TCP/IP host address range to the **Specific Remote Hosts** field:

1. Select **Specific Remote Hosts**.

2. Select **Add**.

   The Add Authorized Host window appears.

3. Select **Authorize Address Range**.
4. Type in the **Low IP Address** field the TCP/IP address that will define the beginning of the range of host addresses that will be permitted access to the Netfinity Manager for Web.
5. Type in the **High IP Address** field the TCP/IP address that will define the end of the range of host addresses that will be permitted access to the Netfinity Manager for Web.
6. Select **OK** to close the Add Authorized Host window and add this address range to the Specific Remote Hosts filed in the Web Manager Configuration window.
7. Select **Save** from the Web Manager Configuration window to save these settings.

To delete a specific host address or a range of host addresses from the **Specific Remote Hosts** field:

1. Select the entry that you want to delete.
2. Select **Remove**.
3. Select **Save** to save these settings.

Chapter 31. Netfinity Manager for Web

With Netfinity Manager for Web, you can use a World Wide Web (WWW) browser, such as Netscape Navigator, to use the Internet to remotely access and control through the Internet any Netfinity Manager that has the Netfinity Manager for Web installed.

Netfinity Manager for Web is installed automatically when you select the Netfinity Manager with Web Enhancement installation configuration (see see "Installing Netfinity Manager" in *Netfinity Manager Quick Beginnings*). Netfinity Manager for Web installs the Netfinity web server, a limited function web server specifically designed to interact with the Netfinity services.

Once the Netfinity web server is installed and operational, you can use a web browser to remotely access and control the Netfinity Manager, from anywhere in the Internet with access to the Manager system's TCP/IP network. Once you have access to the Manager, you can use the Remote System Manager service to access and control other Netfinity systems in that Manager's network.

Simply put, you can monitor and manage all of the Netfinity systems in your network from *anywhere* in the world; all you need is an Internet connection, a web browser, and a system on your network that is running Netfinity Manager for Web and is accessible from the Internet.

System Requirements

There are no additional system requirements for a Netfinity Manager for Web.

There is no operating system requirement to use the Netfinity services remotely. However, your system must be running a web browser that supports Hypertext Markup Language (HTML) 2.0 or later.

Notes:

1. Netfinity Remote Session service is available only with a browser that supports the Java programming language (such as Netscape Navigator 2.02 or later).
2. Netfinity Manager for Web Guru requires support for Javascript and support for frames.
3. Netfinity web helps requires support for frames.

Accessing Netfinity through the World Wide Web

To access a Netfinity Manager for Web with your web browser, you must load the Netfinity Manager's *universal resource locator* (URL). The URL for a system running Netfinity Manager for Web is dependent on whether you are attempting to establish a secure or non-secure network connection with the Netfinity Manager.

- To establish a non-secure connection with a Netfinity Manager, use the following URL:

  `http://`*`TCPIPaddress`*`:`*`socket`*

  where *TCPIPaddress* is the TCP/IP address of the Netfinity Manager for Web and *socket* is the TCP/IP socket that the Netfinity Manager for Web is configured to operate on (the default socket value is 411). For more information, see Chapter 30, "Web Manager Configuration" on page 419. For example:

  `http://manager.my.domain.net:411`

  This opens the Netfinity Manager for Web Welcome Page. From here you can select the address of the Netfinity Manager you want to access.

- To establish a secure connection with a Netfinity Manager, use the following URL:

  `https://`*`TCPIPaddress`*`:`*`socket`*

  where *TCPIPaddress* is the TCP/IP address of the Netfinity Manager for Web and *socket* is the TCP/IP socket that the Netfinity Manager for Web is configured to operate on (the

default socket value is 411). For more information, see Chapter 30, “Web Manager Configuration” on page 419). For example:

```
https://manager.my.domain.net:411
```

This opens the Netfinity Manager for Web welcome page. From here you can select the address of the Netfinity Manager you want to access.

Secure web connections use a digital certificate and data encryption to protect the data that is exchanged between the web browser and the web server. Certificate installation occurs automatically when Netscape Navigator or Microsoft Internet Explorer version 4.0 attempts to make an secure connection to the Manager for the first time. When the first SSL connection is made, the browser will prompt you with a series of windows to ensure that the certificate should be installed into the browser.

If you are using a version of Microsoft Internet Explorer that was released prior to version 4.0, you must manually install the digital certificate and restart Internet Explorer before you establish a secure connection with Netfinity Manager for Web. To install a certificate on a system running an older version of Internet Explorer:

1. Open a connection to the Netfinity Manager for Web welcome page.
2. Open the Netfinity Manager for Web help.
3. Select the **Help for SSL** link.
4. Follow the instructions on how to download and accept the digital certificate.

Note: Web browsers indicate a secure connection in different ways. For example, Netscape Navigator indicates that a secure connection is active by changing the broken key image in the lower left-hand corner of the browser window to a solid key image. Microsoft Internet Explorer indicates that a secure connection is active by changing the open padlock image in the lower left hand corner of the browser window to a locked and illuminated padlock image. For more information on

how your browser indicates secure connections, refer to the browser documentation.

When you select an address from the welcome page, a web browser version of the Netfinity Service Manager appears (see Figure 137).

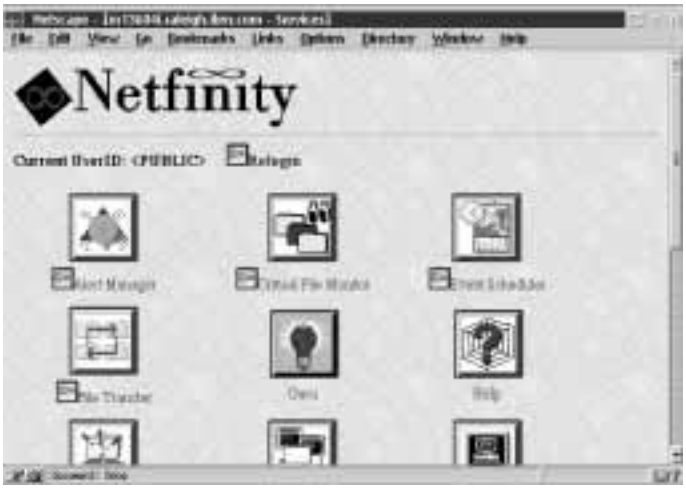

Figure 137. Using a web browser to access the Netfinity Service Manager

To use a Netfinity service, select the name of the service or the image for the service. Some services might be inaccessible because the user has restricted the access to them using Security Manager. The user ID that you are currently logged in as is displayed at the top of the Netfinity Service Manager page. Unlike the Netfinity Service Manager, which displays only the icons for services that are available for your use, the Netfinity Manager for Web displays icons for all Netfinity services that are supported by the system that you are accessing. All services that are unavailable for use because the system's user has used Security Manager to restrict access will have a small image of a padlock beside the image for the service.

To access a secured service, select the service and, when prompted by your web browser, provide a user ID/password combination. This user ID/password combination must match an incoming user ID/password combination that has been configured to enable access to some or all of the Netfinity Manager system's services. For more

information, see “Setting Incoming User ID/Password Combinations” on page 242.

Notes:

1. Due to the limitations of web pages, there are significant differences in some Netfinity service interfaces when accessed with a web browser. For more information, see “Netfinity Service Web Interfaces.”
2. Some web browsers keep web pages stored in cached memory. This can cause some Netfinity web pages to display inaccurate or expired data. To ensure that the data displayed is current and accurate, you should either manually reload or refresh your Netfinity web pages frequently or disable caching.

Netfinity Service Web Interfaces

The following Netfinity services are not available for use when accessing Netfinity Manager for Web:

- DMI Browser
- System Partition Access

  Note: Although the System Partition Access service is not available, the Event Scheduler service’s System Partition Access task is available for use with Netfinity Manager for Web.
- Remote Workstation Control
- Web Configuration Manager
- Cluster Manager
- Capacity Management
- System Diagnostics Manager

Web browsers do not support many of the basic interface features of OS/2, Windows, Windows 95, or Windows NT (such as context menus and nested windows). Because of this some of the Netfinity web interfaces differ significantly from the standard Netfinity user interfaces.

All Netfinity service functions that would ordinarily be selected from an object's context menu are instead available by selecting a radio button (where only one object can be selected) or check box (where multiple selections can be made) beside the object and then selecting an action button on the web page.

All database export features in Alert Manager, Event Scheduler, Software Inventory, System Information Tool, System Monitor, and System Profile are unavailable when accessing any system with Netfinity Manager for Web.

Service-specific user interface differences are detailed in the individual service's section that follows.

Alert Manager

All Alert Manager functions are available when using Netfinity Manager for Web. However, the user interface is significantly different. The following selections are available from the primary Alert Manager web interface (see Figure 138):

- Alert Log

  Select **Alert Log** to view the contents of the alert log and to configure alert log filters.

- Histograms of Alert Log

  Select **Histograms of Alert Log** to view the contents of the alert log in a histogram format. The contents of the alert log are broken down into groups based on alert-specific information, including severity, alert type, application ID, and the name of the system that generated the alert.

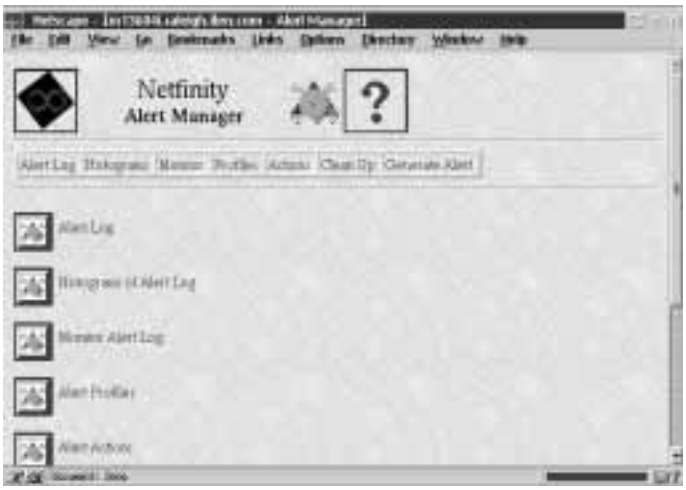

Figure 138. Using a web browser to access Alert Manager

- Monitor Alert Log

  Select **Monitor Alert Log** to begin to monitor for additions to the system's alert log. If your web browser supports automatic page updating (or *server pushes*), changes to the alert log will be automatically reported as long as this page is shown in the

browser. If your web browser does not support server pushes, this page will remain static and will only show changes if you select **Refresh**.

- Alert Profiles

  Select **Alert Profiles** to edit, define, or delete alert profiles.

- Alert Actions

  Select **Alert Actions** to edit, define, or delete alert actions.

- Clean Up

  As alerts are received, the number of entries that are available from the **Application ID**, **Application Alert Type**, and **Sender ID** selection lists can become too extensive to manage easily. Select **Clean Up** to remove selected entries from these selection lists.

- Generate Alert

  Select **Generate Alert** to configure and generate an alert on the system

Critical File Monitor

All Critical File Monitor functions are available when using Netfinity Manager for Web. Also, the Critical File Monitor web interface is functionally equivalent to the Critical File Monitor service interface.

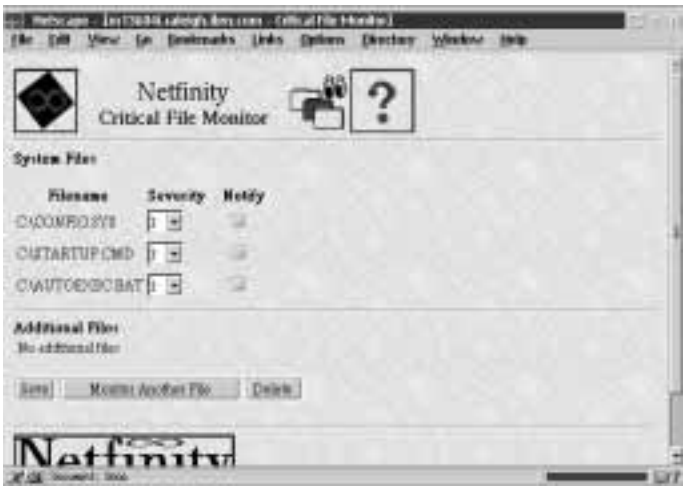

Figure 139. Using a web browser to access Critical File Monitor

ECC Memory Setup

All ECC Memory Setup functions are available when using Netfinity Manager for Web. Also, the ECC Memory Setup web interface is functionally equivalent to the ECC Memory Setup service interface.

Event Scheduler

All Event Scheduler functions and task-specific functions are available when using Netfinity Manager for Web.

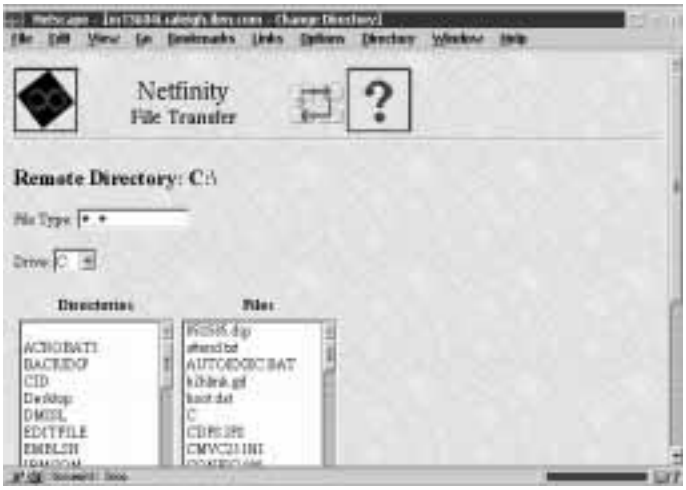

Figure 140. Using a web browser to access Event Scheduler

The Event Scheduler web interface (see Figure 140) is functionally equivalent to the Event Scheduler service interface. However, the task-specific data, date and time scheduling, and the group or system selection are all performed and defined on a single page, rather than in successive windows.

File Transfer

The following File Transfer functions are not available when using the File Transfer web service:

- Send File (available only if supported by browser)
- Send Directory

Also, when you use Netfinity Manager for Web to receive files, the files are received at the system from which you are running the web browser, not the system on which Netfinity Manager for Web is running.

Figure 141. Using a web browser to access File Transfer

Power-On Error Detect

Because web browsers do not support hierarchical windows, all information contained in each entry in the error log are displayed together on a single web page when the entry is selected. Otherwise, the Power-On Error Detect web interface is functionally equivalent to the Power-On Error Detect service interface.

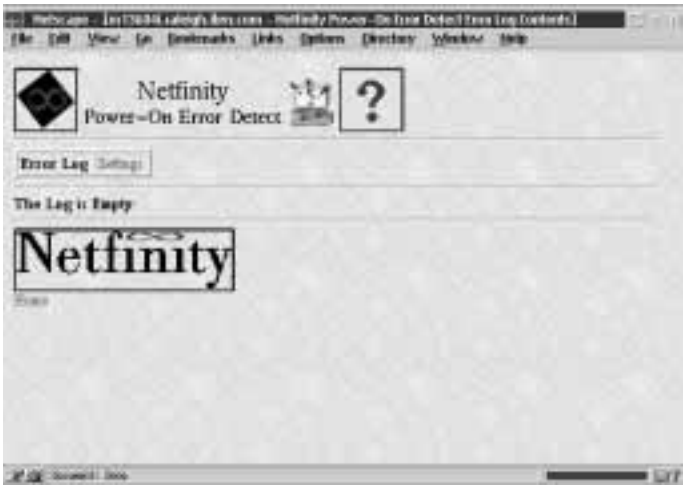

Figure 142. Using a web browser to access Power-On Error Detect

Predictive Failure Analysis

All Predictive Failure Analysis functions are available when using Netfinity Manager for Web. Also, the Predictive Failure Analysis web interface is functionally equivalent to the Predictive Failure Analysis service interface.

Process Manager

All Process Manager functions are available when using Netfinity Manager for Web. Also, the Process Manager web interface is functionally equivalent to the Process Manager service interface.

Figure 143. Using a web browser to access Process Manager

RAID Manager

The RAID Manager web service provides only RAID device and disk subsystem information. No RAID device configuration functions are available when using Netfinity Manager for Web to access the RAID Manager service.

Remote Session

The Remote Session web service will function only on Java-enabled web browsers. Also, you must select **Start** from the Remote Session web interface to initiate a command session. Otherwise, the Remote Session web interface is functionally equivalent to the Remote Session service interface.

Remote System Manager

All Remote System Manager functions are available when using Netfinity Manager for Web. The following differences are found in the Remote System Manager web service interface:

- All functions that would be accessed by using mouse button 2 to select a system or system group icon when using Remote System Manager are instead accessed by selecting the radio button beside the icon, and then selecting the button on the web page that corresponds to the function you want to perform. Buttons for all possible functions appear at the bottom of the web page. However, not all of these functions will be available on all systems.
- All systems images in a system group are identical. System status is represented as follows:
  - Systems that are online have a green background.
  - Systems that are offline have a red background.
  - Manager systems have a globe in the corner of the system image.
  - Systems that have reported an Error Condition have an exclamation point (“!”) image beside their system image.

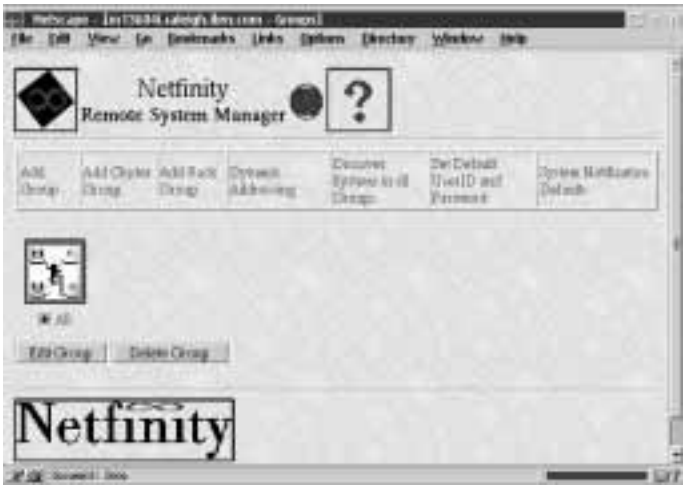

Figure 144. Using a web browser to access Remote System Manager

Screen View

All Screen View functions are available when using Netfinity Manager for Web. When you select the Screen View icon, a JPEG snapshot of the remote system's display will be sent in your web browser.

Security Manager

All Security Manager functions are available when using Netfinity Manager for Web. Also, the Security Manager web interface is functionally equivalent to the Security Manager service interface.

Figure 145. Using a web browser to access Security Manager

Serial Connection Control

All Serial Connection Control functions are available when using Netfinity Manager for Web. Also, the Serial Connection Control web interface is functionally equivalent to the Serial Connection Control service interface.

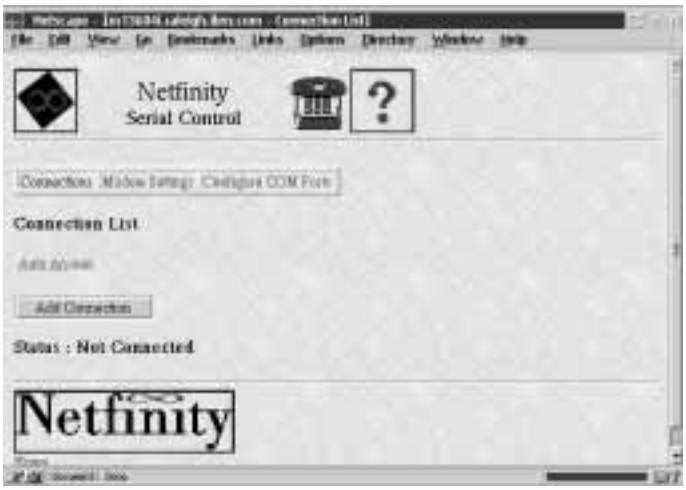

Figure 146. Using a web browser to access Serial Connection Control

Software Inventory

Only full dictionary searches can be performed when using Software Inventory with Netfinity Manager for Web. When you first access the Software Inventory service, a full dictionary search will be performed using the remote system's default Software Inventory Dictionary. All software discovered during the inventory process is displayed in a table on the web page. Other available dictionaries (if available) are displayed at the bottom of the web page. To perform a dictionary search using one of the additional dictionaries, select the dictionary name.

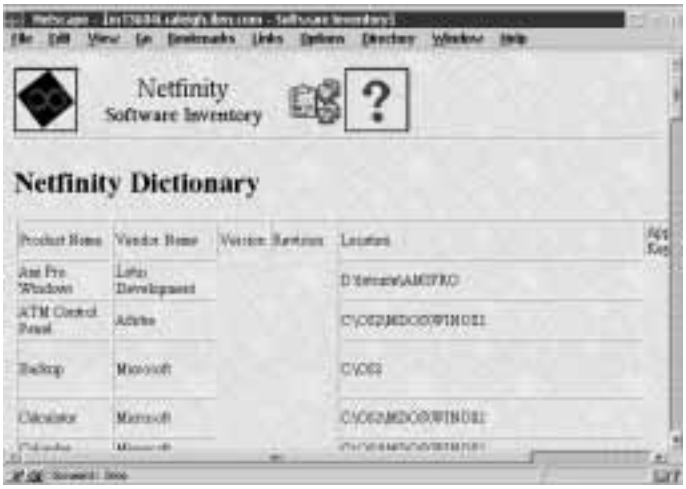

Figure 147. Using a web browser to access Software Inventory

System Information Tool

All System Information Tool functions are available when using Netfinity Manager for Web. However, all information gathered by the System Information Tool is displayed on a single web page.

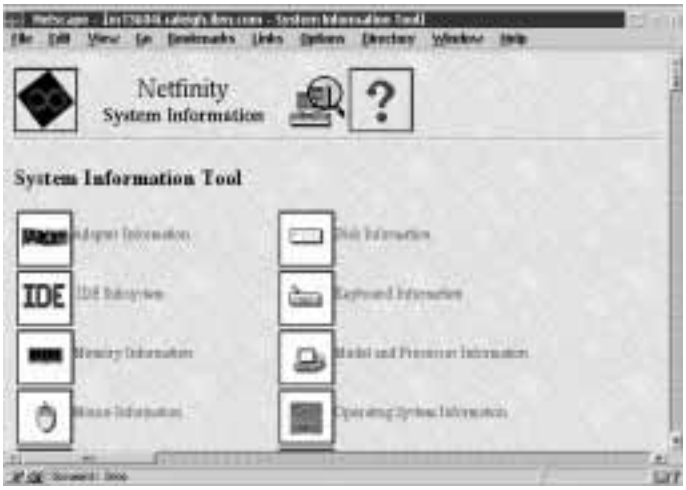

Figure 148. Using a web browser to access System Information Tool

System Monitor

When you use Netfinity Manager for Web to access System Monitor, the current value reported by **all** monitors supported by the remote system is reported in a single web page. Line-graph and real-time monitor views are not available. Otherwise, functions supported by the System Monitor service are available for use with the System Monitor web service.

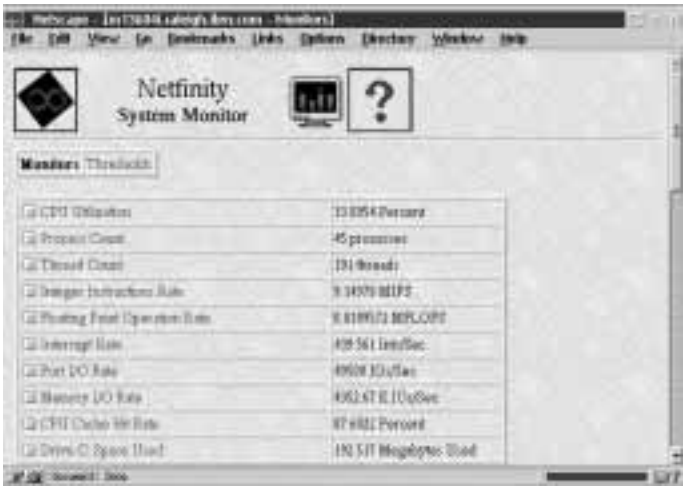

Figure 149. Using a web browser to access System Monitor

System Profile

All System Profile functions are available when using Netfinity Manager for Web. Also, the System Profile web interface is functionally equivalent to the System Profile service interface.

Figure 150. Using a web browser to access System Profile

Appendix A. Alert Manager on Downlevel Netfinity Systems

When remotely managing Netfinity or SystemView LAN systems, you will not have access to all of the features of Netfinity Alert Manager. Although these services are similar, neither the Netfinity Alert Manager nor the SystemView LAN Alert Manager support alert profiles or alert profile binding. Instead, you must configure each alert action separately, specifying alert conditions for each alert action that you want to create.

Remotely configuring actions on a Netfinity or SystemView LAN system is a two-step process. First, you must set the alert conditions that Alert Manager will look for. Then, you must set an Action Definition to define what action the Alert Manager will take in response to the received alert.

To configure alert actions on Netfinity or SystemView LAN systems:

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 perform 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.

   Alert Manager uses five alert conditions to determine appropriate action responses. For an alert to trigger an action, the alert must meet all of the alert conditions for the action. These five alert conditions are:

   - Alert Type
   - Severity
   - Application ID
   - Application Alert Type
   - Sender ID

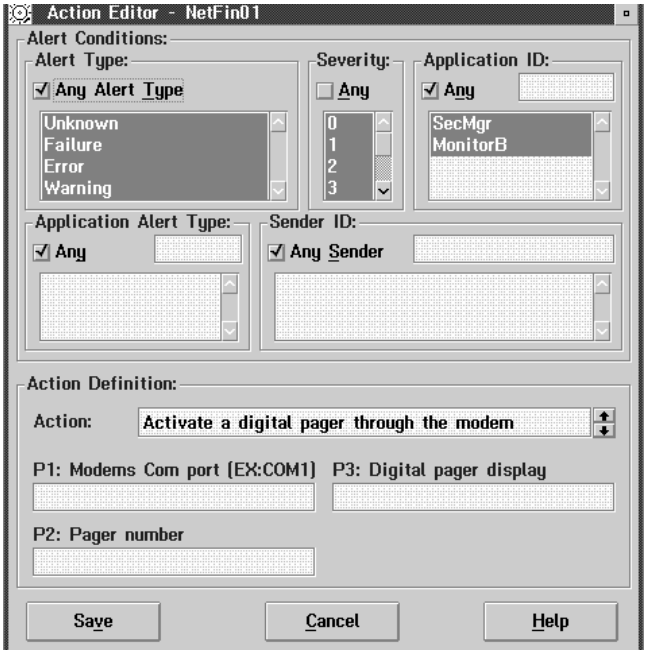

Figure 151. Alert Manager — Action Editor

To specify the **Alert Conditions**:

a. Select an Alert Type.

   The Alert Type is a brief description of the generated alert. It describes the nature of the alert (unknown, failure, error, warning, information), and can also contain a general description of the source of the alert (system, disk, network, operating system, application, device, or security).

   To check incoming alerts for specific Alert Types, select one or more Alert Types from the selection list. If you do not want to check for specific Alert Types, select the **Any** check box above the selection list.

b. Select a Severity.

   The Severity is a number from 0 through 7 that indicates how serious a generated alert is. A severity of 0 represents a very serious alert, while a severity of 7 is relatively minor.

   To check incoming alerts for specific Severity values, select one or more Severity values from the selection list. If you do not want to check for specific Severity values, select the **Any** check box above the selection list.

c. Select an Application ID.

   The Application ID is the alphanumeric identifier of the application that generated the alert.

   To check incoming alerts for specific Application IDs, you can choose one or more from the Application ID selection list. If an Application ID that you require is not available from the list, you can add it to the list by typing the ID in the entry field above the selection list and pressing **Enter**. If you do not want to check for specific Application IDs, select the **Any** check box above the selection list.

d. Select an Application Alert Type.

   The Application Alert Type is a numeric value assigned to an individual alert by the application that generated it. This value is often used by the application itself.

   To check incoming alerts for specific Application Alert Types, you can 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 can add it to the list by typing it in the entry field above the selection list and pressing **Enter**. If you do not want to check for specific Application Alert Types, select the **Any** check box above the selection list.

e. Select a Sender ID.

   The Sender ID is the network address of the system that generated the alert.

   To check incoming alerts for specific Sender IDs, you can choose one or more from the Sender ID selection list. If a

Sender ID that you require is not available from the list, you can add it to the list by typing it in the entry field above the selection list and pressing **Enter**. If you do not want to check for specific Sender IDs, select the **Any** check box above the selection list.

2. Set an Action Definition.

   You must select a specific alert action, and supply any necessary information for the completion of the action.

   a. Select an action.

      An action is an operation that is performed in response to an alert that meets the alert conditions that you have specified.

      Use the spin buttons at the right of the Action field to see the available actions.

   b. 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 appears for each required parameter, along with a brief description of the information that is required. Enter the appropriate information in each field.

3. Save the defined action.

   Once all alert conditions and action-definition information have been entered, select **Save** to save the configured action. This action will now appear in the **Available Actions** field of the Alert Actions window. After you select **Save**, the Alert Manager window closes automatically.

Appendix B. Cross-Platform Integration

Netfinity can help you manage your distributed desktop, notebook, and server systems with ease and efficiency. However, many networks are heterogeneous in nature and many systems administrators need to use a combination of offerings to lower the total cost of ownership and to effectively manage all of the various components of their networks.

Netfinity is designed to integrate with other systems management offerings with the same efficiency and simplicity that are characteristic of the Netfinity management framework. Netfinity includes many functions (such as custom inventory extensions, Netfinity alerts, and Netfinity Manager launch support) that enable you to harness Netfinity's powerful systems management capabilities to enhance the functionality of other systems management platforms.

Integrating with Microsoft SMS

When used with Microsoft Systems Management Server, Netfinity provides enhanced inventory capabilities, enhanced alerting functions, and integration with the SMS console.

Netfinity features custom hardware inventorying capabilities that enhance the information available to SMS administrators. This information includes such RAID information, PCI/EISA/MCA device information, serial numbers of IBM systems and other vital product data of components in your systems. This custom inventory provides SMS with a richer database of attributes which can then be queried and monitored by the SMS administrator console.

Netfinity is also capable of sharing all Netfinity alerts with the SMS Administrator console. Netfinity uses alert actions (configured using the Netfinity Alert Manager service) to define what actions a user would like to take in response to a monitor event. A monitor event takes place when a threshold has been met. Thresholds are set by selecting the item a user wants to monitor from the Netfinity Monitor service. Additional attributes that can be monitored are also available from within other Netfinity services. Netfinity features three alert actions that are especially useful to an SMS

administrator: **NT event log**, **Map Alert to a SNMP trap**, and **Send a SNMP trap**. For more information on alert actions and the Alert Manager service see Chapter 2, “Alert Manager” on page 11.

Netfinity’s alert management architecture also enhances SMS’s ability to notify administrators when problems are encountered. SMS alert actions only notify an administrator of potential problems if they are currently working at an administrator console on their network. However, with the Netfinity Alert Manager service you can configure alert actions that will notify you of problems when they occur using alternate methods such as pagers and email, thereby ensuring that the administrator is immediately informed when alerts are generated.

Netfinity also features Netfinity Service Manager launch support. With this feature, a SMS systems administrator who has Netfinity Manager installed along with his SMS Administrator console has access to the Netfinity management features from within the SMS environment.

System Requirements

The system requirements for Netfinity integration with Microsoft Systems Management Server are:

- Netfinity Manager 5.0 or later
- Netfinity Manager 5.0 or later installed on all SMS Administrator consoles that will manage systems as part of an integrated solution
- Microsoft Systems Management Server version 1.2 with Service Pack 2 or later
- Client Services for Netfinity Manager 5.0 or later installed on all SMS clients that will be managed as part of an integrated solution

Netfinity MIF Generator

The Netfinity Management Information Format (MIF) Generator is a utility that can generate a MIF containing data about your system configuration. MIF (Management Information Format) is a syntax

defined by the Desktop Management Task Force (DMTF) for use in its Desktop Management Interface (DMI) to describe components. SMS systems use data in this format to add or maintain items in a SMS database. The Netfinity 5.0 MIF Generator can be used to add custom inventory data to the Personal Computer Properties of a machine that is in an SMS network.

The Netfinity MIF Generator can be integrated into SMS in several ways. It can be scheduled to run using login scripts every time a user logs on, periodically using the Windows NT AT command or as a SMS job. For information on configuring SMS to perform these functions please refer to the documentation that came with your copy of Microsoft Systems Management Server.

The parameters for this utility are as follows:

```
SIMIFMAK SMS.MFT SISTATIC.MIF ffoptional“ /SMS
```

The template file SMS.MFT provides the Netfinity Custom MIF extensions for SMS. When the SMS.MFT template file is used, the /SMS parameter must be the second parameter and the output file will default to SISTATIC.MIF. SISTATIC.MIF will be created in the \MS\SMS\NOIDMIFS subdirectory, and the Netfinity extensions for SMS will be picked up during the next inventory cycle run by SMS.

Netfinity Alert Actions

The Netfinity Alert Actions that are of use within the SMS environment are the NT event log, Map Alert to a SNMP trap, and Send a SNMP trap actions. The alert actions are triggered by when Netfinity monitor thresholds are met or if Netfinity attribute monitors have been set to a particular state.

SMS version 1.2 provides an Event to Trap translator and a SNMP trap receiver. The Event to Trap translator must be configured to look for Netfinity as the NT event source. It will convert any NT event log entries from Netfinity into SNMP traps for SMS. The SMS SNMP trap receiver processes SNMP traps and inserts the information into the SQL database using the SNMP trap

architecture. Queries can then be run using parameters from the SNMP trap architecture.

To configure the SMS Event to Trap Translator:

1. Open the Site Properties window.
2. Select the SNMP Trap Filter screen.
3. Type in the **NT event source** field

   `Netfinity`
4. In the Machine Groups window, find the machine you want to configure and double-click on it to open the Personal Computer Properties window.
5. Scroll down to the Windows NT Administrative Tools and select **Event To Trap translator**.
6. Select **Edit** and look for Event Sources->Application->Netfinity.

   This will bring up a list on the right-hand side of the screen that lists all of our possible events.
7. Select **All**.
8. Select **Add**.
9. Select **Settings** and then select **Don't Apply Throttle**.

To configure the SNMP Trap Receiver:

1. Open the Site Properties window.
2. Select the SNMP Trap Filter screen.
3. Type in the **Enterprise OID** field 1.3.6.1.4.1.2.6.71.

   This is the SNMP OID for the Netfinity product.

Creating SMS Queries

Once SMS is configured to create SNMP trap entries in its SQL database, a SMS administrator can retrieve these entries by creating custom queries using the Queries window.

To view a list of SNMP traps converted from Netfinity Event Log entries, create a query using the SNMP Trap architecture where the

NT Event Source is Netfinity. To view a list of SNMP traps received directly from Netfinity, create a query using the SNMP trap architecture where the Enterprise OID is 1.3.6.1.4.1.2.6.71.

Netfinity Manager Launch Support

If SMS is detected on a system when Netfinity Manager is installed, Netfinity Service Manager is automatically added to the Tools Menu of the SMS Administrator Console. This enables an SMS administrator to launch the Netfinity Service Manager on any SMS machine in his network that is Netfinity-enabled.

Integrating with Intel LANDesk Server Manager or Client Manager

Netfinity Manager provides enhanced integration with LANDesk Server Manager in three key areas:

- Adding enhanced inventory capability to any LANDesk client using a DMI interface.

  With this enhancement, features such as RAID information, PCI/EISA/MCA device information, serial numbers of IBM systems and other vital product data of components in your system will be displayed via the LANDesk DMI browser.

- Sharing of Netfinity alerts with the LANDesk management console.

  Netfinity uses alert actions configured through the Alert Manager to define what actions will be taken in response to events. With Netfinity integration, an administrator can view alerts generated by Netfinity and bind LANDesk alert actions to them.

- Netfinity Manager launch support

  With Netfinity Manager launch support, you can now leverage the Netfinity management features that complement LANDesk management features within a LANDesk environment. For example, LANDesk Server Manager alert actions are more limited in number than those in Netfinity. Other complementing features include RAID management, Predictive

Failure Analysis, and various Netfinity extensions provided by third parties such as American Power Conversion, Vinca Corp., and Lexmark. With this integration, a system administrator can take full advantage of two very powerful management solutions.

Netfinity can also be used to enhance the management capapbilities of systems running LAN Desk Client Manager (LDCM). When you install Netfininty Manager or Client Services for Netfinity Manager on a system that has LDCM installed, Netfinity will automatically provide the following additional function to LDCM:

- Adding enhanced inventory capability to any LANDesk client using a DMI interface.
- Netfinity launch support

System Requirements

The system requirements for Netfinity integration with LANDesk Server Manager are:

The system requirements for this integration are and Netfinity

- Netfinity Manager or Client Services for Netfinity Manager version 5.1 or later
- LANDesk Server Manager (LDSM) version 2.52 or later
- Netfinity Manager or Client Services for Netfinity Manager *must* be installed on all LANDesk Server Manager clients you want to manage with LDSM and Netfinity.
- Netfinity Manager must be installed on all LDSM management consoles for launch support and sharing of management features

Configuration Setup

Use the following instructions to configure your system.

1. Inventory Integration

   Integration of inventory data occurs automatically during the installation of Netfinity Manager on a LANDesk management console. The data can be accessed via the LDSM console's DMI browser category for the selected system. After logging into the desired system:

a. Click on **DMI**.

b. Click on **Browser**.

c. Click on either Netfinity Manager or Client Services for Netfinity Manager.

A list of DMI components appear. Click on a coponent to display its attributes.

2. Alert Integration

   Netfinity alert actions that are compatible with the LDSM environment are

   - Add Event to Event Log
   - Map alert to SNMP trap
   - and Send SNMP Alert

   For Netfinity alerts configured with the Add Event to Event Log action to be available to LANDesk, the administrator must install the LANDesk SNMP Event forwarder on the client machine, and TCP/IP and SNMP must be installed on both the client and manager machines. The SNMP Event Forwarder translates NT event log entries into SNMP traps and displays them in the SNMP Event Viewer that also gets installed with the Event Forwarder.

   For Netfinity alerts configured with the Send SNMP Alert or Map alert to SNMP trap actions to be available to LANDesk, the administrator must install TCP/IP and SNMP on both the agent and manager console machines and configure the agent's SNMP service to send SNMP traps to the manager machine using the Windows NT SNMP Service configuration dialog. Then, when the administrator selects IBM from the list of SNMP Trap Receivers, traps received from Netfinity on the agent machine will be displayed in the LANDesk SNMP Trap log.

3. Configure the Event Forwarder

   The Event Forwarder application must be installed on a machine for translation capability to be available.

   a. Open the LANDesk Event Forwarder configuration utility (located in the LANDesk Server Manager group).

b. Select which NT Event log to receive traps from (i.e. Application, System or Security).

c. Select Netfinity from the list of sources.

d. Select events to include in the list to be translated to SNMP traps.

e. Click **OK**.

View the forwarded events with the LANDesk SNMP Event Viewer.

4. Configure the Windows NT SNMP service

   To perform this step, the system must have TCP/IP installed as a network protocol, and SNMP installed as a service.

   a. Open the Windows Control Panel and double-click the Network icon.

   b. Click on the **Services** tab.

   c. Select SNMP service.

   d. Click on **Properties** and then the **Traps** tab.

   e. Type in the Community Name filed

      `public`

      Type in the **Trap Destination** field the address or host name of the system to which the SNMP traps will be sent

      Note: This system should be an LDSM managing console.

   f. Restart the system, or stop and restart the SNMP service using the Control Panel **Services** application.

5. Configure the SNMP Trap Receiver

   Netfinity is added as an SNMP trap source for the LDSM trap receiver during Netfinity Manager installation on an LDSM management console. Accordingly, Netfinity alerts configured with the Send SNMP Alert action or Map alert to SNMP trap action will be displayed in the SNMP Trap Log when the IBM Enterprise icon is selected from the list of SNMP Trap Receivers.

6. Configure LANDesk Alert Actions for Netfinity Alerts

To configure a LANDesk alert action for an SNMP trap received from Netfinity:

a. Select the IBM Enterprise icon from the list of SNMP Trap Receivers

b. Right-click on the **Converted Netfinity Alert** parameter in the parameter selection pane and then select **Configure Alert Actions**.

c. Select **IBM:Converted Netfinity Alert** from the list of alerts and then select **Configure**.

Refer to the LANDesk documentation for configuring particular alert actions.

7. Launch Support Integration

The Netfinity Service Manager can be added as a category of a particular LDSM client system on the LDSM Management Console. This enables a LANDesk administrator to launch the Netfinity Service Manager against any LDSM client machine in his network that is Netfinity-enabled. Support for the Netfinity Manager launch integration will be added automatically during Netfinity Manager installation on a machine that is already configured as a LDSM Management Console. Then, Netfinity Service Manager will appear as a category of any Netfinity-enabled client machines and selecting it will launch Netfinity Manager against that machine. The administrator will need a Netfinity user ID and password for the machine just as if it were being accessed from the Netfinity Remote System Manager service.

Appendix C. Power-On Error Detect Enablement

This appendix contains instructions on how to install the Power-On Error Detect drivers on your system.

System Requirements

To support the Power-On Error Detect drivers (POED drivers), the system must be a LAN-attached Micro Channel system with:

- A System Partition
- A supported network adapter (see "Supported Network Adapters" on page 459)
- The NetBIOS communications protocol

Note: The system *does not* need the Netfinity Manager or Client Services for Netfinity Manager installed to support the Power-On Error Detect drivers. However, systems that are running Netfinity and that generate a Power-On Error Detect message can be identified more easily by the Netfinity Manager's Power-On Error Detect service.

Installing the Power-On Error Detect Drivers

To install the Power-On Error Detect drivers (POED drivers) on a LAN-attached system:

1. Insert the *Power-On Error Detect Installation Diskette* into drive A.
2. Restart the system.
3. Select an installation option.

   You can install or uninstall the Power-On Error Detect drivers with this diskette. Type

   1

   and press **Enter** to install the POED drivers. After a short time, the following message will appear on the system's display:

   ```
   Installation is complete.  Remove the diskette from
   the drive and press any key to restart the system.
   ```

   Remove the diskette and press a key. Installation is now complete.

Uninstalling the Power-On Error Detect Drivers

To uninstall the Power-On Error Detect drivers (POED drivers) on a system:

1. Insert the *Power-On Error Detect Installation Diskette* into drive A.
2. Restart the system.
3. Select an installation option.

   You can either install or uninstall the Power-On Error Detect drivers with this diskette. Type

   ```
   2
   ```

   and press **Enter** to uninstall the POED drivers. After a short time, the following message appears on the system's display:

   ```
   Uninstallation is complete.  Remove the diskette from
   the drive and press any key to restart the system.
   ```

   Remove the diskette and press a key. The system should restart as normal. All POED drivers have now been removed from the system.

Supported Network Adapters

The Power-On Error Detect drivers have been tested and found to function properly when used with the following network 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

Making a Power-On Error Detect Installation Diskette

The Power-On Error Detect Installation Diskette enables you to install the POED drivers to a system's reference partition. Once these drivers have been installed, the system will transmit SOS-style

messages over the LAN when it encounters errors during Power-On Self Test (POST).

Netfinity comes with a Power-On Error Detect Installation diskette. If you need to make an additional Power-On Error Detect enablement diskette:

1. Make a back-up copy of your Reference Diskette.

   Attention:
   Do not use your original Reference Diskette for this process: the contents of your Reference Diskette are permanently altered by this process.

2. Insert the newly created Reference Diskette backup copy into diskette drive A.
3. Place the Netfinity CD-ROM into your CD-ROM drive.
4. Open an OS/2 or a DOS command-line session.
5. Make the CD-ROM drive the current drive. For example, if the drive letter assigned to your CD-ROM is E, type

   ```
   E:
   ```

   at the command line and then press **Enter**.

6. Type

   ```
   CD POED\SERVICES
   ```

   and then press **Enter**.

7. Type

   ```
   POWRINST
   ```

   and then press Enter. This will start a batch program that will create the Power-On Error Detect Installation Diskette.

Appendix D. Supported PFA Hard Disk Drives

The following PFA-enabled hard disk drives are supported by Predictive Failure Analysis. Only the listed hard drives can be monitored or managed by the Predictive Failure Analysis service.

- IBM Type 0664 Hard Disk Drive
- IBM Type 0663 Hard Disk Drive
- IBM Type 0662 Hard Disk Drive
- IBM Type DPES-31080 Hard Disk Drive (product revision 531Q only)
- IBM Type DFHS Hard Disk Drive
- IBM Type DFMS Hard Disk Drive
- IBM Type XP31 Hard Disk Drive
- IBM Type XP32 Hard Disk Drive
- IBM Type XP34 Hard Disk Drive
- IBM Type DORS-3216DW Hard Disk Drive
- IBM Type FIREBALL12805 Hard Disk Drive (product revision 630N or later)

In addition to these hard disk drives, Netfinity Manager and Client Services for Netfinity Manager for OS/2 or Windows NT support PFA-enabled hard disk drives that conform to the self-monitoring analysis and reporting technology (SMART) standard. Support for SMART hard disk drives is available only on systems running Netfinity Manager or Client Services for Netfinity for OS/2 or Windows NT.

Appendix E. Supported RAID Adapters

The following RAID adapters are supported:

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

Appendix F. RAID Alerts

A RAID adapter (RAID means *redundant array of independent disks*) attaches to multiple physical disk drives, and enables you to treat these drives as up to eight system (or logical) drives. Although the System Monitor service does not display a monitor if a RAID system is present, it does monitor the status of all disk drives that are attached to the RAID adapter to ensure that they are online and functioning correctly.

The RAID adapter will detect when physical drives or system drive become active or inactive. This is called a drive's *state*.

System drives report one of three states. These states are:

- Online
- Critical
- Offline

Note: The Critical state can only be reported by RAID level 1, 2, 3, or 4 system disk drives. RAID level 0 system disk drives cannot report a Critical state. All RAID level 0 disk drives are either Online or Offline. For more information on RAID levels, see your RAID adapter documentation.

Physical drives report one of three states. These states are:

- Online
- Standby
- Defunct

RAID alerts are generated *only* when the RAID disk drive changes state. If the state remains unchanged, additional alerts will not be generated.

The alert text of all RAID alerts generated by System Monitor follow this format:

```
Alert: RAID Device state  Attribute typeandlocation
in subsystem set to state
```

where *state* is the state reported by the drive., *typeandlocation* is the type of RAID disk drive (Physical or System) and its designated

location (System Drive number or Physical Bay number), and *subsystem* is the name of the RAID subsystem reporting the state change.

The alert-specific information for each RAID alert follows.

RAID Physical Disk Drive State is Online

Description	Generated when a physical drive changes state from Standby or Defunct to Online.
Alert Type	Information
Severity	3
Application ID	MonitorB
Application Alert Type	130

RAID Physical Disk Drive State is Standby

Description	Generated when a physical drive changes state from Online or Defunct to Standby.
Alert Type	Error
Severity	2
Application ID	MonitorB
Application Alert Type	130

RAID Physical Disk Drive State is Defunct

Description	Generated when a physical drive changes state from Online or Standby to Defunct.
Alert Type	Failure
Severity	0
Application ID	MonitorB
Application Alert Type	130

RAID System Disk Drive State is Online

Description	Generated when a system drive changes state from Critical or Offline to Online.
Alert Type	Information
Severity	3
Application ID	MonitorB
Application Alert Type	131

RAID System Disk Drive State is Critical

Description	Generated when a system drive changes state from Online or Offline to Critical.
Alert Type	Warning
Severity	2
Application ID	MonitorB
Application Alert Type	131

RAID System Disk Drive State is Offline

Description	Generated when a system drive changes state from Critical or Online to Offline.
Alert Type	Failure
Severity	0
Application ID	MonitorB
Application Alert Type	131

Note: If a RAID physical disk drive generates an alert message, you will generally receive alert messages from all system drives that are associated with that physical drive.

Several of Netfinity's services can be accessed from your system's command line. The following sections describe how these services can be accessed from a command line, as well as the various parameters associated with their use.

Alert Manager Command Line Operations

The Alert Manager service does not have any command line operations. However, GENALERT.EXE is a program that causes an alert to be generated within your system. This alert may have a number of user-specified parameters, described below.

Note: If you want alerts generated using GENALERT to be forwarded to a host system using the "Send alert to host via APPC" alert action, see "Adding GENALERT Alert Descriptions to the NMVT.INI File" on page 467.

The command-line format for GENALERT.EXE is:

```
GENALERT /T:"text" /APP:id_name
/SEV:0..7 /TYPE:sssttt /ATYPE:hexnum
```

where:

/T:"*text*" Defines the text message describing the alert. The quotation marks are required.

/APP:*id_name* Defines the application ID for the alert (1—8 characters)

/SEV:*0...7* Defines the priority or severity of the alert (0=highest priority, 7=lowest priority).

/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. Values range from 0000 to FFFF.

Adding GENALERT Alert Descriptions to the NMVT.INI File

The NMVT.INI file, found in the Netfinity directory, contains alert descriptions that map standard Netfinity alerts to NMVT-style alerts that can then be properly passed to a host system using advanced program-to-program communications (APPC) and the "Send alert to host via APPC" alert action. However, because alerts generated using the GENALERT command are configured and defined by the user, they are not included in this file. As a result, if you do not add entries to the NMVT.INI file for GENALERT alerts, the "Send alert to host via APPC" alert action will not have the data it needs to build the NMVT (including alert description, failure causes, recommended actions, and so forth) and will be unable to pass this information to the host.

To enable a system to pass GENALERT-created alert information to the host, you must add an entry to the NMVT.INI file located in the Netfinity directory of the system generating the alert. This entry, like all other entries in the NMVT.INI file, must consist of information about the Netfinity alert (including application name, alert type, and alert severity) followed by configuration data for the NMVT that will be sent to the host.

For example, generate an alert using the following GENALERT command:

```
GENALERT /T:"Virus Detected" /APP:ANTVIR /SEV:0
/TYPE:SECWRN /ATYPE:000C
```

In order for this alert to be properly forwarded to the host, you must edit the NMVT.INI file and include an entry specifically created to translate the Netfinity alert information into NMVT-specific information. For example:

```
APP:ANTVIR TYPE:SECWRN SEV:0 ATYPE:000C GTYPE:01
DESC:C007 CAUSE:6700 USER:7199:1026 FAIL:0501:18003103
```

Once this entry is added to the NMVT.INI file, the Alert Manager will be able to use the "Send alert to host via APPC" alert action to convert this alert into an NMVT and forward it to the host system.

System Information Tool Command Line Operations

The System Information Tool can be started from a command line, and supports five command line parameters. The command line format for System Information Tool is:

SINFG30 /P:*filename* /H:*filename*
/F:*history filename* /NOLOGO /B

The command line parameters are as follows:

/P: *filename* This parameter is used to generate a report of all the information collected by the program. A logical printer name like LPT1 can be substituted for a file name, which will send the report to a printer. The program logo screen will be displayed while the information is being gathered, and the program will terminate after the report has been generated.

/H: *filename* This parameter is used to generate a binary history file that contains all of the information detected by the program, as well as the time and date that the report was generated. This file can then be used as an input source using the **/F** command-line parameter. The program logo screen will be displayed while the information is being gathered, and the program will terminate after the file is generated.

/F: *history filename*

This parameter causes the program to use a previously generated history file as the source for information gathering, rather use than the physical system the program is being executed on. You can use this option to view a history file from another system.

/NOLOGO When this parameter is used, the program logo will not be displayed. This parameter can be used in conjunction with any of the other parameters.

/B This parameter causes the program to bypass all warning and informational messages while the program is starting. This could be used for unattended system startups. This parameter can be used in conjunction with any of the other parameters.

ECC Memory Setup Command Line Operations

All functions of the ECC Memory Setup can also be accessed from your OS/2 command line, using ECCMEM.EXE.

Note: ECCMEM.EXE is available for use only on systems running OS/2.

The command line format for ECCMEM.EXE is:

```
ECCMEM /INIT /SCRUB:ON or OFF /THRESH:ON or OFF
/COUNT:ON or OFF /QUIET  /COUNTVAL:number
/THRESHVAL:number
```

where:

/INIT	Causes the ECC memory to be initialized to the saved settings
/SCRUB*ON or OFF*[1]	Enables or disables single-bit error scrubbing
/THRESH:*ON or OFF*[1]	Enables or disables single-bit error threshold nonmaskable interrupt (NMI)
/COUNT:*ON or OFF*[1]	Enables or disables single-bit error counting
/QUIET	Causes ECCMEM.EXE to generate no textual output
/COUNTVAL:*number*	Sets the single-bit error count to a given value
/THRESHVAL:*number*[1]	Sets the single-bit error threshold to a given value

[1] These options update the saved settings to the value provided. When the system is restarted, the saved settings will configure the ECC memory.

Starting and Stopping Service Base Programs Remotely

You can use the Netfinity STRTBASE.EXE and STOPBASE.EXE command-line programs to remotely start or stop the base program of most Netfinity services.

Note: STRTBASE.EXE and STOPBASE.EXE can start and stop the base programs only for individual Netfinity services. These programs cannot be used to remotely start or stop the Netfinity Network Interface, the Netfinity Support Program, or any base program that is started by the Netfinity Network Interface or the Netfinity Support Program (these include the base programs for Alert Manager, Power-On Error Detect, System Monitor, and Serial Connection Control). One of these programs **must** be running on the remote system for STRTBASE.EXE or STOPBASE.EXE to function properly.

Starting Service Base Programs Remotely

From your system, use STRTBASE.EXE to start a Netfinity service's base program on a remote system. The command line format for STRTBASE.EXE is:

```
STRTBASE \N:networktype::networkaddress
\BASE:servicebase [\BATCH] [\?]
```

Variable	Definition
networktype	Name of the protocol to be used to send the message (for example, TCPIP)
networkaddress	Protocol-specific address of the remote system on which the base program will be started (for example, user.network.com)
servicebase	The service connection name of the program base to be started on the remote system. For a list of the service connection names that must be used with this command, see "Service Connection Names" on page 473.
BATCH	Program runs with no output. When STRTBASE.EXE is run in BATCH mode, a file named SYSNAME.OUT that contains

	the remote system's name is created in the same directory as STRTBASE.EXE
?	Displays command line help.

Stopping Service Base Programs Remotely

From your system, use STOPBASE.EXE to stop a Netfinity service's base program on a remote system. The command line format for STOPBASE.EXE is:

```
STOPBASE \N:networktype::networkaddress
\BASE:servicebase [\BATCH] [\?]
```

Variable	Definition
networktype	Name of the protocol to be used to send the message (for example, TCPIP)
networkaddress	Protocol-specific address of the remote system on which the base program will be stopped (for example, user.network.com)
servicebase	The service connection name of the program base to be stopped on the remote system. For a list of the service connection names that must be used with this command, see "Service Connection Names" on page 473.
BATCH	Program runs with no output. When STOPBASE.EXE is run in BATCH mode, a file named SYSNAME.OUT that contains the remote system's name is created in the same directory as STOPBASE.EXE
?	Displays command line help.

Service Connection Names

A list of the service connection names that must be used with the STRTBASE.EXE and STOPBASE.EXE programs follows.

Service Connection Name	Service Name
CFMBase	Critical File Monitor
ProcMgr	Process Manager
ECCMemory	ECC Memory Setup
Gatherer3.0	System Information Tool (Version 3.0 or later)
Gatherer	System Information Tool (all other versions)
PFAServiceBase	Predictive Failure Analysis
ScreenID	Screen View
DMIBrowserBase	DMI Browser
RAID_BASE	RAID Manager
RCSHD	Remote Session
SoftInvB	Software Inventory
FileBase	File Transfer
PartionBase	System Partition Access
SCH_BASE_NODE	Event Scheduler
ProfileBase	System Profile
CAPMGT	Capacity Management
RWCService	Remote Workstation Control
DiagMgr	System Diagnostic Manager
SCFMgr	Service Configuration Manager
ServiceProcessorBase	Service Processor Manager
UpdateConnector	Update Connector Manager (interface)

UpdateConnectorClient	Update Connector Manager (interface or client)

Appendix H. Installation Options

This appendix describes methods by which you can perform automated installations of Netfinity and create customized Netfinity installations.

Automated Installation

If you have a CID-enabled (CID stands for customization, installation, and distribution) software distribution manager utility (such as LAN CID, included with IBM Network Transport Services/2), you can install Netfinity on systems within your network by using the Netfinity installation program command line parameters and response file. First, you must create a source directory for the installation.

To create a source directory for a Client Services for Netfinity Manager installation:

1. Create a source directory for the program files.
2. Copy the files from the appropriate *Netfinity Services* subdirectory on the Netfinity CD-ROM.

   For example, if you are creating a source directory to distribute Client Services for Netfinity Manager for OS/2, copy all of the files from the OS2\SERVICES subdirectory on the Netfinity CD-ROM into the directory.

To create a source directory for a Netfinity Manager installation:

1. Create a source directory for the program files.
2. Copy the files from the appropriate *Netfinity Manager* subdirectory on the Netfinity CD-ROM.

   For example, if you are creating a source directory to distribute Netfinity Manager for OS/2, copy all of the files from the OS2\MANAGER subdirectory on the Netfinity CD-ROM into the directory.

Once you have created an installation source directory, use a response file and the Netfinity installation program's command line parameters. The Netfinity installation program supports the following command line parameters:

/R: *drive+path+filename* Specifies the drive, path, and file name of the response file. See the NETFBASE.RSP file (located in the directory in which you installed Netfinity) for an example of a response file with comments on the included parameters.

/S: *drive+path* Specifies the drive and path to install *from*. This is the directory to which you copied the program files from the Netfinity CD-ROM.

/T: *drive* Specifies the drive to install *to*. Default is the current startup drive.

/TU: *drive+path* Specifies the drive and path of the CONFIG.SYS file to update. The default is to change the CONFIG.SYS in the root directory of the drive specified in the /T parameter (or the startup drive). This parameter is ignored if the *ChangeConfig* parameter in the response file is FALSE.

For example, the line:

```
NETFINST /R:NETFBASE.RSP /S:Y:\NETFIN
/T:C /TU:D:\
```

will install Netfinity using the options in the response file NETFBASE.RSP, using the program files from the directory Y:\NETFIN, to drive C: (the directory to which the files are installed is taken from the response file), and will modify the CONFIG.SYS file in the D:\ directory.

Note: For information on how to use a CID-enabled software distribution manager, refer to the publications provided with the individual CID-enabled product.

Customized Installation

For security reasons, all users may not need to have access to all services. User access can be restricted by creating a customized installation that will prevent some services from being installed.

To create a customized installation, the INSTALL.INI file must be edited. For example, when creating a customized Netfinity Manager for Windows 95 or NT installation, edit the INSTALL.INI file that is found on Netfinity Manager directory.

The INSTALL.INI file has three sections, separated by the line

[==]

The first section contains the installation configuration that can be selected during installation. There can be no more than eight choices. Each choice takes up two lines. The first line is the text that is displayed next to the installation configuration radio button. The second line is a list of the options in the third section that will be installed when this choice is selected for installation.

For example:

```
;IBM SysMgt Install Script, Version 2 (Do not remove this comment line)
Netfinity Manager Installation [Manager 16900]
    Advanced System Management Support [ServProc 450]
    Capacity Manager Enhancement [CapMgt 5600]
    Remote Workstation Control [RWC 2000]
    World Wide Web Enhancement (TCPIP Required) [WebManager 3000] IsTcpip
[==]
Netfinity Manager CD for Windows 95/NT
[==]
NetFinity Admin
NULL Manager
    CL 0 1 NETFBASE.EXE
    CCL 0 1 NETDOM.INI
    CCL 0 1 NETNODES.INI
    CCL 0 1 INSTALL.BAT
    CCL 0 1 NETFINST.EXE
    CCL 0 1 INSTALL.INI
    CCL 0 1 WININST.HLP
    CL 0 1 APCKINST.DLL
;Screen Capture GUI
;NULL Manager
;    CL 0 1 SAVEG.EXE
;    CL 0 1 SAVEG.HLP
```

This INSTALL.INI would create a Netfinity Manager installation configuration that also installs Advanced System Management, Capacity Manager, Remote Workstation Control, and Netfinity World Wide Web enhancement.

The second section contains the names of the CD that this installation script will use.

The third section contains the list of options that can be installed. These are the options that are selected by the choices in the first section. The options are consecutively numbered starting at 1, so any inserted options will change the number of all following options. Each option uses the following format:

```
Option Name
Dll-entrypoint
    option file
    option file
    ...
install command
install command
...
```

Option Name	An identifying comment by the installation program. All options must have a different Option Name. This is only used for identification.
Dll-entrypoint	Used to determine whether an option is valid for a given target machine. In most cases, it should be the reserved string "NULL."

The easiest way to customize an installation is to simply put a semi-colon in front of any service that you want to remove from the installation.

To add a line item in a specific section, add all the necessary item information in the format shown in the following example.

Before:

```
Screen Capture GUI
NULL Manager
    CL 0 1 SAVEG.EXE
    CL 0 1 SAVEG.HLP
```

After:

```
Screen Capture GUI
NULL Manager
    CL 0 1 SAVEG.EXE
    CL 0 1 SAVEG.HLP
    CL 0 1 CUSTOM.INI
```

Appendix I. Netfinity Relational Database Tables

Notes:

1. Database management systems that do not support the *date* or *time* data type will assign it an SQL-type time stamp (for example, *datetime*).
2. The varchar datatype has a maximum value of 255 characters on Microsoft SQL Server databases (and others). This value may be up to 256 characters on DB2 databases.

Netfinity System Information Tables

The following database configuration tables contain the name, type, and description of database entries for information gathered and exported by the System Information Tool.

BASE Table

Table 1 (Page 1 of 2). BASE Configuration Table. Base system configuration information.

Name	Type	Description
SYSTEM_ID	char(32) not null	Identifies unique system ID
MANAGING_ID	char(32)	Netfinity system manager for group
GROUP_NAME	char(32)	Netfinity Logical Group Name
OPERATING_SYSTEM	char(32)	Operating system
VERSION	char(8)	Version of operating system
MEMORY_OPERATING	dec(10,2)	Total memory detected by operating system (megabytes)
MEMORY_BASE	dec(10,2)	Base memory (megabytes)
MEMORY_USABLE	dec(10,2)	Usable memory (megabytes)
MEMORY_BOARD	dec(10,2)	Memory board memory (kilobytes)
MEMORY_ADAPTER	dec(10,2)	Adapter card memory (megabytes)
MEMORY_CACHEABLE	dec(10,2)	Cacheable memory (megabytes)
REFERENCE_DISK	smallint	Reference disk type
NVRAM	smallint	NVRAM size
DEDICATED_IRQ	char(38)	Dedicated IRQ levels

Table 1 (Page 2 of 2). BASE Configuration Table. Base system configuration information.

Name	Type	Description
SHARED_IRQ	char(38)	Shared IRQ levels
PARALLEL_PORTS	smallint	Number of parallel ports
SERIAL_PORTS	smallint	Number of serial ports
SYSTEM_SERIAL	char(20)	Serial number of system
PLANAR_ID	char(4)	ID of planar board
PLANAR_SERIAL	char(20)	Serial number of planar board
PROCESSOR_CARD_SER	char(20)	Serial number of processor card
BASE_DATE	date not null	Date of update
BASE_TIME	time not null	Time of update

Note: The primary key is SYSTEM_ID, unique index on SYSTEM_ID.

DISKETTE Table

Table 2. DISKETTE Table. Diskette information, one entry per diskette drive.

Name	Type	Description
SYSTEM_ID	char(32) not null	Identifies unique system ID
LOGICAL_DRIVE	char(2)	Identifies logical drive. For example, A:
DEVICE_TYPE	char(40)	Type of device. For example, Direct Access Device

Note: Foreign key (SYSTEM_ID), references BASE.

DISPLAY Table

Table 3. DISPLAY Table. Display information, one entry per display

Name	Type	Description
SYSTEM_ID	char(32) not null	Identifies unique system ID
DISPLAY_ADAPTER	char(40)	Type of adapter in use.
DISPLAY_TYPE	char(40)	Type of display in use.
VIDEO_MEMORY	dec(10,2)	Amount of memory in kilobytes
COLORS	int	Number of colors displayed
HORIZONTAL_RES	smallint	Horizontal resolution of screen
VERTICAL_RES	smallint	Vertical resolution of screen
HORIZONTAL_SIZE	smallint	Horizontal size of screen in millimeters
VERTICAL_SIZE	smallint	Vertical size of screen in millimeters
VIDEO_SUBSYSTEM	smallint	Video subsystem, 0 = primary
SLOT_LOCATION	smallint	Video adapter slot location number

Note: Foreign key (SYSTEM_ID), references BASE.

EXPANSION_SLOT Table

Table 4. EXPANSION_SLOT Table. Expansion slot information, one entry per slot.

Name	Type	Description
SYSTEM_ID	char(32) not null	Identifies unique system ID
SLOT	smallint	Identifies slot number
BUS_TYPE	char(16)	Type of bus used
BUS_NUMBER	smallint	Bus number
ADAPTER_ID	char(10)	Adapter ID number
ADAPTER_TYPE	char(70)	Type of adapter card

Note: Foreign key (SYSTEM_ID), references BASE.

FIXED_DISK Table

Table 5. FIXED_DISK Table. Fixed disk information, one entry per physical unit.

Name	Type	Description
SYSTEM_ID	char(32) not null	Identifies unique system ID
DISK_CAPACITY	dec(10,2)	Capacity in megabytes
DISK_CYLINDERS	int	Number of cylinders
SECTORS_PER_CYL	int	Number of sectors per cylinder
DISK_HEADS	int	Number of heads
DISK_TOTAL_SECTORS	int	Total number of sectors
PHYSICAL_DRIVE	char(8)	Physical drive ID. For example, 1:

Note: Foreign key (SYSTEM_ID), references BASE.

LOGICAL_DRIVE Table

Table 6. LOGICAL_DRIVE Table. Logical drive information, one entry per logical unit.

Name	Type	Description
SYSTEM_ID	char(32) not null	Identifies unique system ID
LOGICAL_NAME	char(32)	For example, G: Remote Disk Attached by LAN
VOLUME_NAME	char(16)	Volume name
FILE_SYSTEM	char(8)	File system name
FILE_ATTACH	char(32)	File system attach name
DRIVE_TYPE	char(1)	Local (L) or remote (R) drive
SECTORS_CLUSTER	smallint	Number of sectors per cluster
SECTORS_BYTES	smallint	Number of bytes per sector
DEVICE_CAPACITY	dec(10,2)	Capacity in megabytes
AVAILABLE_SPACE	dec(10,2)	Space available in megabytes
PHYSICAL_DRIVE	char(8)	Physical drive ID. For example, 1:

Note: Foreign key (SYSTEM_ID), references BASE.

KEYBOARD Table

Table 7. KEYBOARD Table. KEYBOARD information, one entry per system.

Name	Type	Description
SYSTEM_ID	char(32) not null	Identifies unique system ID
KEYBOARD_TYPE	char(30)	Type of keyboard
COUNTRY_CODE	char(3)	Identifies country code. For example, US
SUBCOUNTRY_CODE	char(3)	Identifies sub-country code. For example, 103
CODE_PAGE	smallint	code page. For example, 437

Note: Foreign key (SYSTEM_ID), references BASE.

MODEL Table

Table 8. MODEL Configuration Table. Model dependent information, one entry per system.

Name	Type	Description
SYSTEM_ID	char(32) not null	Identifies unique system ID
MODEL_NAME	char(30)	Model name of system
EXPANSION_BUS	char(30)	Expansion bus type
MODEL_NUMBER	char(2)	Model number
SUBMODEL_NUMBER	char(2)	Sub-model number
BIOS_REVISION	char(2)	BIOS revision level
BIOS_DATE	date	BIOS ROM date

Note: Foreign key (SYSTEM_ID), references BASE.

MOUSE Table

Table 9. MOUSE Table. MOUSE information, one entry per system.

Name	Type	Description
SYSTEM_ID	char(32) not null	Identifies unique system ID
MOUSE_TYPE	char(30)	Type of mouse
MOUSE_BUTTONS	smallint	Number of buttons on the mouse

Note: Foreign key (SYSTEM_ID), references BASE.

PRINTER Table

Table 10. PRINTER Table. PRINTER information, one entry per installed printer.

Name	Type	Description
SYSTEM_ID	char(32) not null	Identifies unique system ID
PRINTER_PORT	char(4)	Name of logical printer port
PRINT_QUEUE	char(8)	Name of print queue
PRINTER_DRIVER	char(16)	Name of printer driver
PRINTER_MODEL	char(32)	Name of printer model

Note: Foreign key (SYSTEM_ID), references BASE.

PROCESSOR Table

Table 11. PROCESSOR Configuration Table. Processor information, one entry per processor.

Name	Type	Description
SYSTEM_ID	char(32) not null	Identifies unique system ID
PROCESSOR	char(16)	Processor type
CO_PROCESSOR	char(16)	Co_Processor type
PROCESSOR_SPEED	int	Speed of installed processor in MHz
INTERNAL_CACHE	char(1)	Internal processor cache enabled (E), disabled (D), not installed (N)
EXTERNAL_CACHE	char(1)	External processor cache enabled (E), disabled (D), not installed (N), or unsupported (U)
PLANAR_SPEED	int	Speed of planar in MHz
PROCESSOR_NUMBER	smallint	Processor number. Multi-Processor use only.

Note: Foreign key (SYSTEM_ID), references BASE.

SYSLEVEL Table

Table 12. SYSLEVEL Table. SYSLEVEL information, one entry per installed product.

Name	Type	Description
SYSTEM_ID	char(32) not null	Identifies unique system ID
PRODUCT_NAME	char(80)	Name of software product
PRODUCT_VERSION	char(5)	Version of software product
COMPONENT_ID	char(9)	ID number of installed component
CURRENT_CSD	char(8)	Current install CSD level.
PREVIOUS_CSD	char(8)	Previous install CSD level.

Note: Foreign key (SYSTEM_ID), references BASE.

MEMORY Table

Table 13. MEMORY Table. MEMORY information, one entry per connector.

Name	Type	Description
SYSTEM_ID	char(32) not null	Identifies unique system ID
CONNECTOR_ID	char(8)	ID number of installed connector
MEMORY_SIZE	dec(10,2)	Memory size in megabytes.
MEMORY_SPEED	dec(10,2)	Memory speed in nanoseconds
MEMORY_TYPE	char(10)	Memory type. For example, Parity, ECC

Note: Foreign key (SYSTEM_ID), references BASE.

DASD_ADAPTER Table

Table 14 (Page 1 of 2). DASD_ADAPTER Table. DASD adapter information, one entry per adapter

Name	Type	Description
SYSTEM_ID	char(32) not null	Identifies unique system ID
PHYSICAL_UNIT	smallint	Physical unit number
LOGICAL_UNIT	smallint	Logical unit number
DASD_BUS_TYPE	char(10)	Type of bus used. For example, SCSI
DASD_SLOT	smallint	Adapter slot location
BUS_ATTRIBUTES	char(20)	Bus attributes
IO_ACCESS	char(20)	Vehicle for I/O access. For example, bus master
HOST_BUS	char(20)	Host bus
HOST_BUS_WIDTH	smallint	Host bus width
MAX_SCATTER	smallint	Maximum scatter gather list
MAX_CDB	smallint	Maximum CDB length
ADD_MAJOR	smallint	ADD major level
ADD_MINOR	smallint	ADD minor level

Table 14 (Page 2 of 2). DASD_ADAPTER Table. DASD adapter information, one entry per adapter

Name	Type	Description
DASD_DEVICES	smallint	Number of devices on DASD adapter

Note: Foreign key (SYSTEM_ID), references BASE.

DASD_DEVICE Table

Table 15. DASD_DEVICE Table. DASD_DEVICE information, one entry per device on DASD adapter card.

Name	Type	Description
SYSTEM_ID	char(32) not null	Identifies unique system ID
DASD_SIZE	dec(10,2)	DASD Device capacity in megabytes
DASD_TYPE	char(40)	DASD Device type
UNIT_PUN	smallint	Device unit PUN
UNIT_LUN	smallint	Device unit LUN
ANSI_LEVEL	char(20)	ANSI level supported
UNIT_STATUS	char(1)	Unit status, A = active, D = disabled, U = unknown
VENDOR_ID	char(8)	Vendor ID
PRODUCT_ID	char(16)	Product ID numbers
PRODUCT_REVISION	char(4)	Product revision level

Note: Foreign key (SYSTEM_ID), references BASE.

Netfinity System Profile Tables

The following database configuration tables contain the name, type, and description of database entries for information gathered and exported by the System Information Tool from System Profile.

SYSTEM_PROFILE Table

Table 16. SYSTEM_PROFILE Table. System profile information, one entry per system_id

Name	Type	Description
SYSTEM_ID	char(32) not null	Identifies unique system ID
MODEL_NAME	char(32)	Model name of system
MODEL_NUMBER	char(32)	Model number of system
SYSTEM_SERIAL	char(32)	System serial number
SYSTEM_BOARD_SER	char(32)	System board serial number
PROCESSOR_CARD_SER	char(32)	System processor card serial number
SYSTEM_PURCHASED	date	Date the system was purchased
DISPLAY_MODEL	char(32)	Display model name
DISPLAY_SERIAL	char(32)	Display serial number
DISPLAY_PURCHASED	date	Date display was purchased
PRINTER_MODEL	char(32)	Printer model name
PRINTER_SERIAL	char(32)	Printer serial number
PRINTER_PURCHASED	date	Date printer was purchased
MODEM_MODEL	char(32)	Modem model name
MODEM_SERIAL	char(32)	Modem serial number
MODEM_PURCHASED	date	Date modem was purchased

Note: The primary key is SYSTEM_ID, unique index on SYSTEM_ID.

SYSTEM_USER Table

Table 17. SYSTEM_USER Table. System profile user information, one entry per system_id

Name	Type	Description
SYSTEM_ID	char(32) not null	Identifies unique system ID
FIRST_NAME	char(32)	First name
MIDDLE_NAME	char(32)	Middle name
LAST_NAME	char(32)	Last name
EMPLOYEE_ID	char(32)	Employee ID
TITLE	char(32)	Title
DEPT_NAME	char(32)	Department name
DEPT_NUMBER	char(32)	Department number
DIVISION	char(32)	Division
START_DATE	date	Start date
SHIFT	char(32)	Shift
SCHEDULED_START	time	Scheduled start time
SCHEDULED_END	time	Scheduled end time
HOME_PHONE	char(32)	Home phone
HOME_STREET1	char(32)	Home street - line 1
HOME_STREET2	char(32)	Home street - line 2
HOME_CITY	char(32)	Home city
HOME_STATE	char(32)	Home state
HOME_ZIP	char(32)	Home zip code
HOME_COUNTRY	char(32)	Home country
EMERGENCY_NAME	char(32)	Emergency contact name
EMERGENCY_PHONE	char(32)	Emergency contact phone number

Note: On some database management systems (such as Microsoft SQL Server), SYSTEM_USER is a reserved keyword. On these systems, the name of this table is SYSTEM_USER1.

Note: Foreign key (SYSTEM_ID), references SYSTEM_PROFILE.

SYSTEM_LOCATION Table

Table 18. SYSTEM_LOCATION Table. System profile location information, one entry per system_id

Name	Type	Description
SYSTEM_ID	char(32) not null	Identifies unique system ID
COMPANY_NAME	char(32)	Name of the company
ADDRESS	char(32)	Internal location of user
CITY	char(32)	Location City
STATE	char(32)	Location State
ZIP_CODE	char(32)	Location zip code
COUNTRY	char(32)	Country of location
SITE_NAME	char(32)	Name of site
OFFICE_NUMBER	char(32)	Internal office number of user
BUILDING	char(32)	Building location
FLOOR	char(32)	Building floor

Note: Foreign key (SYSTEM_ID), references SYSTEM_PROFILE.

SYSTEM_CONTACTS Table

Table 19 (Page 1 of 2). SYSTEM_CONTACTS Table. System profile contact information, one entry per system_id

Name	Type	Description
SYSTEM_ID	char(32) not null	Identifies unique system ID
INTERNAL_PHONE	char(32)	Internal phone number
EXTERNAL_PHONE	char(32)	External phone number
CELLULAR_PHONE	char(32)	Cellular phone number
PAGER_NUMBER	char(32)	Pager number
FAX_NUMBER	char(32)	Fax number
EMAIL_ADDRESS	char(32)	E-mail address
BACKUP_NAME	char(32)	Backup name
BACKUP_PHONE	char(32)	Backup phone number

Table 19 (Page 2 of 2). SYSTEM_CONTACTS Table. System profile contact information, one entry per system_id

Name	Type	Description
TECHNICAL_NAME	char(32)	Name of technical contact
TECHNICAL_PHONE	char(32)	Phone number of technical contact
MANAGER_NAME	char(32)	Name of manager
MANAGER_PHONE	char(32)	Phone number of manager
SECRETARY_NAME	char(32)	Name of secretary
SECRETARY_PHONE	char(32)	Phone number of secretary

Note: Foreign key (SYSTEM_ID), references SYSTEM_PROFILE.

SYSTEM_MISC Table

Table 20. MISC Table. System profile miscellaneous information, one entry for each miscellaneous slot containing information.

Name	Type	Description
SYSTEM_ID	char(32) not null	Identifies unique system ID
ENTRY_SLOT *x*	smallint	Slot number of entry
MISC_INFO	char(32)	Miscellaneous entry data

Note: Foreign key (SYSTEM_ID), references SYSTEM_PROFILE.

Netfinity System Monitor Tables

MONITOR_STATE Table

Table 21 (Page 1 of 2). MONITOR_STATE Table. Monitors containing state information

Name	Type	Description
SYSTEM_ID	char(32) not null	Identifies unique system ID
MONITOR_NAME	varchar(128) not null	Name of monitor

Table 21 (Page 2 of 2). MONITOR_STATE Table. Monitors containing state information

Name	Type	Description
MONITOR_STATE	varchar(64) not null	State reported by monitor
MONITOR_DATETIME	timestamp not null	Date/time stamp

Note: The primary key is SYSTEM_ID, MONITOR_NAME, MONITOR_DATETIME unique. No duplicates.

MONITOR_VALUE Table

Table 22. MONITOR_VALUE Table. Monitors containing quantitative data points.

Name	Type	Description
SYSTEM_ID	char(32) not null	Identifies unique system ID
MONITOR_NAME	char(128) not null	Name of monitor
MONITOR_DATA	float not null	Data point sent from monitor
MONITOR_INTERVAL	int not null	Time interval for data point in seconds
MONITOR_DATETIME	timestamp not null	Date/time stamp

Note: The primary key is SYSTEM_ID, MONITOR_NAME, MONITOR_DATETIME unique. No duplicates.

Netfinity Software Inventory Tables

SOFTWARE_INVENTORY Table

Table 23 (Page 1 of 2). SOFTWARE_INVENTORY Table. Software Inventory information.

Name	Type	Description
SYSTEM_ID	char(32) not null	Identifies unique system ID
MANAGING_ID	char(32)	Netfinity system manager for group
GROUP_NAME	char(32)	Netfinity logical group name
PROGRAM_TITLE	varchar(64)	Text title of program

Table 23 (Page 2 of 2). SOFTWARE_INVENTORY Table. Software Inventory information.

Name	Type	Description
VERSION_ID	char(16)	Identifies unique version
RELEASE_LEVEL	char(12)	Identifies release level of product
VENDOR_NAME	char(32)	Name of software vendor
LOCATION	varchar(256)	Location of installed product
SOFT_INV_DATETIME	timestamp	Date/time stamp

Netfinity Alert Table

ALERT_LOG Table

Table 24. ALERT_LOG Table. Alert log information, one entry per alert.

Name	Type	Description
SYSTEM_ID	char(32) not null	Identifies unique system ID
ALERT_TEXT	varchar(128)	Text of alert
ALERT_ID	char(32)	ID of alert (type of alert)
ALERT_CLASS	char(32)	Class of Alert (type of alert)
SEVERITY	smallint	Severity of alert
APPLICATION_ID	char(8)	Application ID
APPL_ALERT_TYPE	char(4)	Application alert type
RECEIVED_FROM	varchar(256)	Received from (path)
SYSTEM_NAME	varchar(64)	System generating the alert
ALERT_DATETIME	timestamp	Date/time of alert

Row Deletion in DB2 Databases

The database is set up using referential integrity to ensure data integrity. If a row is deleted in the BASE table on a DB2 database management system, all tables in the System Information group

using the same SYSTEM_ID will be deleted. However if a row is deleted in any other table, only that row is deleted.

- BASE Table
  - DISKETTE Table
  - DISPLAY Table
  - EXPANSION_SLOT Table
  - FIXED_DISK Table
  - LOGICAL_DRIVE Table
  - KEYBOARD Table
  - MODEL Table
  - MOUSE Table
  - PRINTER Table
  - PROCESSOR Table
  - SYSLEVEL Table
  - MEMORY Table
  - DASD_ADAPTER Table
  - DASD_DEVICE Table

The database is set up using referential integrity to ensure data integrity. If a row is deleted in the SYSTEM_PROFILE table on a DB2 database management system, the same will happen to all tables in the System Profile group. However if a row is deleted in any other table, only that row is deleted.

- SYSTEM_PROFILE Table
  - SYSTEM_USER Table
  - SYSTEM_LOCATION Table
  - SYSTEM_CONTACTS Table
  - SYSTEM_MISC

General Database Query Information and Examples

Use any query tool that has the ability to access your relational database tables to retrieve information from the Netfinity database. This section features some simple queries for each table to help you get started. These queries are contained in the file QUERY.SQL, found on *Netfinity Manager for OS/2, Diskette #1*. Create views on the tables or columns you are most interested in. A NULL is used to represent the absence of any value for a column. The presence of a NULL value usually means that the information is not available from the system in question.

- BASE Table
  - Select all columns from BASE table

    ```
    SELECT * FROM NETFIN.BASE
    ORDER BY SYSTEM_ID
    ```

  - Delete all rows from the BASE table over 30 days old

    ```
    DELETE FROM NETFIN.BASE
    WHERE BASE_DATE < CURRENT DATE - 30 DAYS
    ```

- DISKETTE Table
  - Select all columns for a system from DISKETTE table

    ```
    SELECT * FROM NETFIN.DISKETTE
    WHERE SYSTEM_ID = XXXXXX
    ORDER BY LOGICAL_DRIVE
    ```

  - Delete a row from the DISKETTE table

    ```
    DELETE FROM NETFIN.DISKETTE
    WHERE SYSTEM_ID = 'XXXXXX'
    ```

- DISPLAY Table
  - Select all columns for a system from DISPLAY table

    ```
    SELECT * FROM NETFIN.DISPLAY
    WHERE SYSTEM_ID = XXXXXX
    ORDER BY VIDEO_SUBSYSTEM
    ```

  - Delete a row from the DISPLAY table

```
DELETE FROM NETFIN.DISPLAY
WHERE SYSTEM_ID = 'XXXXXX'
```

- EXPANSION_SLOT Table
  - Select all columns for a system from EXPANSION_SLOT table

    ```
    SELECT * FROM NETFIN.EXPANSION_SLOT
    WHERE SYSTEM_ID = XXXXXX
    ORDER BY SLOT
    ```

  - Delete a row from the expansion_slot table

    ```
    DELETE FROM NETFIN.EXPANSION_SLOT
    WHERE SYSTEM_ID = 'XXXXXX'
    ```

- FIXED_DISK Table
  - Select all columns for a system from FIXED_DISK table

    ```
    SELECT * FROM NETFIN.FIXED_DISK
    WHERE SYSTEM_ID = XXXXXX
    ORDER BY PHYSICAL_DRIVE
    ```

  - Delete a row from the FIXED_DISK table

    ```
    DELETE FROM NETFIN.FIXED_DISK
    WHERE SYSTEM_ID = 'XXXXXX'
    ```

- LOGICAL_DRIVE Table
  - Select all columns for a system from LOGICAL_DRIVE table

    ```
    SELECT * FROM NETFIN.LOGICAL_DRIVE
    WHERE SYSTEM_ID = XXXXXX
    ORDER BY LOGICAL_NAME
    ```

  - Delete a row from the LOGICAL_DRIVE table

    ```
    DELETE FROM NETFIN.LOGICAL_DRIVE
    WHERE SYSTEM_ID = 'XXXXXX'
    ```

- KEYBOARD Table
  - Select the column for a system from KEYBOARD table

    ```
    SELECT * FROM NETFIN.KEYBOARD
    WHERE SYSTEM_ID = XXXXXX
    ```

  - Delete a row from the KEYBOARD table

```
DELETE FROM NETFIN.KEYBOARD
WHERE SYSTEM_ID = 'XXXXXX'
```

- MODEL Table
  - Select the column for a system from MODEL table

    ```
    SELECT * FROM NETFIN.MODEL
    WHERE SYSTEM_ID = XXXXXX
    ```

  - Delete a row from the MODEL table

    ```
    DELETE FROM NETFIN.MODEL
    WHERE SYSTEM_ID = 'XXXXXX'
    ```

- MOUSE Table
  - Select the column for a system from MOUSE table

    ```
    SELECT * FROM NETFIN.MOUSE
    WHERE SYSTEM_ID = XXXXXX
    ```

  - Delete a row from the MOUSE table

    ```
    DELETE FROM NETFIN.MOUSE
    WHERE SYSTEM_ID = 'XXXXXX'
    ```

- PRINTER Table
  - Select all columns for a system from PRINTER table

    ```
    SELECT * FROM NETFIN.PRINTER
    WHERE SYSTEM_ID = XXXXXX
    ```

  - Delete a row from the PRINTER table

    ```
    DELETE FROM NETFIN.PRINTER
    WHERE SYSTEM_ID = 'XXXXXX'
    ```

- PROCESSOR Table
  - Select all columns for a system from PROCESSOR table

    ```
    SELECT * FROM NETFIN.PROCESSOR
    WHERE SYSTEM_ID = XXXXXX
    ```

  - Find the fastest processors from PROCESSOR table

    ```
    SELECT * FROM NETFIN.PROCESSOR
    WHERE PROCESSOR_SPEED =
      (SELECT MAX(PROCESSOR_SPEED)
       FROM NETFIN.PROCESSOR)
    ```

- Delete a row from the PROCESSOR table

```
DELETE FROM NETFIN.PROCESSOR
WHERE SYSTEM_ID = 'XXXXXX'
```

- SYSLEVEL Table
  - Select all columns for a system from SYSLEVEL table

```
SELECT * FROM NETFIN.SYSLEVEL
WHERE SYSTEM_ID = XXXXXX
ORDER BY PRODUCT_ID
```

  - Delete a row from the SYSLEVEL table

```
DELETE FROM NETFIN.SYSLEVEL
WHERE SYSTEM_ID = 'XXXXXX'
```

- MEMORY Table
  - Select all columns for a system from MEMORY table

```
SELECT * FROM NETFIN.MEMORY
WHERE SYSTEM_ID = XXXXXX
ORDER BY CONNECTOR_ID
```

  - Get total memory and type for all machines from MEMORY table

```
SELECT SYSTEM_ID SUM(MEMORY_SIZE) MEMORY_TYPE
FROM NETFIN.MEMORY GROUP BY SYSTEM_ID,
MEMORY_TYPE
```

  - Delete a row from the MEMORY table

```
DELETE FROM NETFIN.MEMORY
WHERE SYSTEM_ID = 'XXXXXX'
```

- DASD_ADAPTER Table
  - Select all columns for a system from DASD_ADAPTER table

```
SELECT * FROM NETFIN.DASD_ADAPTER
WHERE SYSTEM_ID = XXXXXX
ORDER BY PHYSICAL_UNIT
```

  - Delete a row from the DASD_ADAPTER table

```
DELETE FROM NETFIN.DASD_ADAPTER
WHERE SYSTEM_ID = 'XXXXXX'
```

- DASD_DEVICE Table

- Select all columns for a system from DASD_DEVICE table

  ```
  SELECT * FROM NETFIN.DASD_DEVICE
  WHERE SYSTEM_ID = XXXXXX
  ORDER BY PHYSICAL_UNIT
  ```

- Delete a row from the DASD_DEVICE table

  ```
  DELETE FROM NETFIN.DASD_DEVICE
  WHERE SYSTEM_ID = 'XXXXXX'
  ```

- SYSTEM_PROFILE Table
  - Select all columns for a system from SYSTEM_PROFILE table

    ```
    SELECT * FROM NETFIN.SYSTEM_PROFILE
    WHERE SYSTEM_ID = XXXXXX
    ORDER BY SYSTEM_ID
    ```

  - Delete all rows from the SYSTEM_PROFILE table

    ```
    DELETE FROM NETFIN.SYSTEM_PROFILE
    WHERE SYSTEM_ID = 'XXXXXX'
    ```

- SYSTEM_USER Table
  - Select all columns for a system from SYSTEM_USER table

    ```
    SELECT * FROM NETFIN.SYSTEM_USER
    WHERE SYSTEM_ID = XXXXXX
    ORDER BY SYSTEM_ID
    ```

  - Delete all rows from the SYSTEM_USER table

    ```
    DELETE FROM NETFIN.SYSTEM_USER
    WHERE SYSTEM_ID = 'XXXXXX'
    ```

- SYSTEM_LOCATION Table
  - Select all columns for a system from SYSTEM_LOCATION table

    ```
    SELECT * FROM NETFIN.SYSTEM_LOCATION
    WHERE SYSTEM_ID = XXXXXX
    ORDER BY SYSTEM_ID
    ```

  - Delete all rows from the SYSTEM_LOCATION table

    ```
    DELETE FROM NETFIN.SYSTEM_LOCATION
    WHERE SYSTEM_ID = 'XXXXXX'
    ```

- SYSTEM_CONTACTS Table
  - Select all columns for a system from SYSTEM_CONTACTS table

    ```
    SELECT * FROM NETFIN.SYSTEM_CONTACTS
    WHERE SYSTEM_ID = XXXXXX
    ORDER BY SYSTEM_ID
    ```

  - Delete all rows from the SYSTEM_CONTACTS table

    ```
    DELETE FROM NETFIN.SYSTEM_CONTACTS
    WHERE SYSTEM_ID = 'XXXXXX'
    ```

- SYSTEM_MISC Table
  - Select all columns for a system from SYSTEM_MISC table

    ```
    SELECT * FROM NETFIN.SYSTEM_MISC
    WHERE SYSTEM_ID = XXXXXX
    ORDER BY SYSTEM_ID
    ```

  - Delete all rows from the SYSTEM_MISC table

    ```
    DELETE FROM NETFIN.SYSTEM_MISC
    WHERE SYSTEM_ID = 'XXXXXX'
    ```

- ALERT_LOG Table
  - Select all columns for a system from ALERT_LOG table

    ```
    SELECT * FROM NETFIN.ALERT_LOG
    WHERE SYSTEM_ID = XXXXXX
    ORDER BY SYSTEM_ID
    ```

  - Delete all rows from the ALERT_LOG table

    ```
    DELETE FROM NETFIN.ALERT_LOG
    WHERE SYSTEM_ID = 'XXXXXX'
    ```

- MONITOR_STATE Table
  - Select all columns for a system from MONITOR_STATE table

    ```
    SELECT * FROM NETFIN.MONITOR_STATE
    WHERE SYSTEM_ID = XXXXXX
    ORDER BY SYSTEM_ID
    ```

  - Delete all rows from the MONITOR_STATE table

```
DELETE FROM NETFIN.MONITOR_STATE
WHERE SYSTEM_ID = 'XXXXXX'
```

- MONITOR_VALUE Table
  - Select all columns for a system from MONITOR_VALUE table

    ```
    SELECT * FROM NETFIN.MONITOR_VALUE
    WHERE SYSTEM_ID = XXXXXX
    ORDER BY SYSTEM_ID
    ```

  - Delete all rows from the MONITOR_VALUE table

    ```
    DELETE FROM NETFIN.MONITOR_VALUE
    WHERE SYSTEM_ID = 'XXXXXX'
    ```

Appendix J. Netfinity Alerts

All Netfinity Alerts include the time and date at which the Alert was generated. The other information depends on which service generated the Alert and the circumstances that caused the Alert to be generated.

Some Alerts have values that can be assigned by the user. This often applies to Severity values, although there are some exceptions. In this case, the Alert information will be signified with a variable, and a note below the alert data will provide any clarification necessary.

Some alerts support macro parameter strings. These strings (%P1–%P9) can be passed through to and used by other programs.

Each alert and its alert-specific information are listed beneath the heading of the service that generates the alert.

Power On Error Detect

Explanation	Generated by the Power-On Error Detect service when a Power-On Error is detected on a remote system. The Power-On Error Detect will generate this alert only if the service's **Generate Alert on Error** option is enabled.
Alert Text	Netfinity Power-On Error Detect Alert
Type of Alert	Failure
Severity	4
Application ID	Power-On Error Detect
Application Alert Type	0201

This alert does not support additional parameter strings.

Predictive Failure Analysis

Explanation	Generated by the Predictive Failure Analysis service when the service receives notification from a PFA-enabled hard disk drive that a drive failure will occur within 24 hours. The Predictive Failure Analysis service will generate this alert only if the service's **Generate Alert** option is enabled.
Alert Text	Predictive Failure Analysis has detected an imminent failure on PUN *w*, LUN *x* hard drive. Back up physical drive *y* and call your service provider for a replacement.
Type of Alert	Disk Failure
Severity	*z*
Application ID	PFA
Application Alert Type	0000

This alert does not support additional parameter strings.

Notes:

1. The Alert Text variables *w*, *x*, and *y* are determined by the Predictive Failure Analysis service, and represent the PUN, LUN, and drive letter assigned to the failing PFA-enabled hard disk drive, respectively.
2. You can add additional text to this alert. For more information, see "The PFA Options for Drive Window" on page 175.
3. You can specify the Severity variable *z*. For more information, see "The PFA Options for Drive Window" on page 175.

Critical File Monitor

Alerts generated by the Critical File Monitor follow.

File Changed Alert

Explanation	Generated by Critical File Monitor when a monitored file changes size, date, or time.
Alert Text	The following file has changed: '*filename*'.
Type of Alert	Application Warning
Severity	*x*
Application ID	MonCritF
Application Alert Type	0

This alert does not support additional parameter strings.

Notes:

1. The Alert Text variable *filename* is the name of the file that has changed.
2. You can set the Severity variable *x*. The default Severity value for this alert is 3.

File Deleted Alert

Explanation	Generated by Critical File Monitor when a monitored file is deleted.
Alert Text	The following file has been deleted: '*filename*'.
Type of Alert	Warning
Severity	*x*
Application ID	MonCritF
Application Alert Type	1

This alert does not support additional parameter strings.

Notes:

1. The Alert Text variable *filename* is the name of the file that has been deleted.
2. You can set the Severity variable *x*. The default Severity value for this alert is 3.

File Created Alert

Explanation	Generated by Critical File Monitor when a monitored file is created.
Alert Text	The following file has been created: '*filename*'.
Type of Alert	Warning
Severity	*x*
Application ID	MonCritF
Application Alert Type	2

This alert does not support additional parameter strings.

Notes:

1. The Alert Text variable *filename* is the name of the file that has been created.
2. You can set the Severity variable *x*. The default Severity value for this alert is 3.

Process Manager

Alerts generated by Process Manager follow.

Process Terminated Alert

Explanation	Generated by Process Manager when a monitored process is stopped.
Alert Text	Process '*%P1*' has terminated.
Type of Alert	Application Information
Severity	*x*
Application ID	ProcMgr
Application Alert Type	0901

Notes:

1. This alert supports the following macro parameter string:

   %P1 Name of the process that has been terminated.

2. You can set the Severity variable *x*.

Process Started Alert

Explanation	Generated by Process Manager when a monitored process is started.
Alert Text	Process '*%P1*' has started.
Type of Alert	Application Information
Severity	*x*
Application ID	ProcMgr
Application Alert Type	0900

Notes:

1. This alert supports the following macro parameter string:

   %P1 Name of the process that has been started.

2. You can set the Severity variable *x*.

Process Failed to Start Alert

Explanation	Generated by Process Manager when a monitored process fails to start within a specified time of system startup.
Alert Text	Process '*%P1*' has failed to start.
Type of Alert	Application Information
Severity	*x*
Application ID	ProcMgr
Application Alert Type	0902

Notes:

1. This alert supports the following macro parameter string:

   %P1 Name of the process that has failed to start.

2. You can set the Severity variable *x*.

Remote System Manager

Alerts generated by the Remote System Manager follow.

System Online Notification Alert

Explanation	Generated when the Remote System Manager receives notification from a remote system that the system is online and reachable. The Remote System Manager service will generate this alert only if the service's System Notifications: Notify When Online option has been enabled for a system within a system group.
Alert Text	Alert Text: System '*%P1*' (Address '*%P2*' on Network '*%P3*') is active and online.
Type of Alert	System Information
Severity	*x*
Application ID	NetMgr
Application Alert Type	000A

Notes:

1. This alert supports the following macro parameter strings:

   %P1 System Name of active system. This is set to indicate the system that has come online.

   %P2 Network Address of active system. This is set to indicate the system that has come online.

   %P3 Network Type of active system.

2. You can set the Severity variable *x*.

System Offline Notification Alert

Explanation	Generated when the Remote System Manager is incapable of reaching a remote system. The Remote System Manager service will generate this alert only if the service's System Notifications: Notify When Offline option has been enabled for a system within a system group.
Alert Text	Alert Text: System '*%P1*' (Address '*%P2*' on Network '*%P3*') is offline or unreachable.
Type of Alert	System Information
Severity	*x*
Application ID	NetMgr
Application Alert Type	000B

Notes:

1. This alert supports the following macro parameter strings:

%P1	System Name of inactive system. This is set to indicate the system that has gone offline.
%P2	Network Address of inactive system. This is set to indicate the system that has gone offline.
%P3	Network Type of inactive system.

2. You can set the Severity variable *x*.

Security Manager

Access Granted Alert

Explanation Generated by the Security Manager service when access to one or more services is granted to a remote user who has used a UserID / Password combination to gain access.

Alert Text User ID '*%P1*' from Address '*%P2*' on Network '*%P3*' has been granted system access.

Type of Alert Security Information

Severity 7

Application ID SecMgr

Application Alert Type 14

Note: This alert supports the following macro parameter strings:

%P1 User ID requesting system access

%P2 Network Address of system requesting access

%P3 Network Type of system requesting access

Public Access Granted Alert

Explanation Generated by the Security Manager service when Public access to one or more services is granted to a remote user.

Alert Text User ID '*%P1*' from Address '*%P2*' on Network '*%P3*' has been granted public system access.

Type of Alert Security Information

Severity 6

Application ID SecMgr

Application Alert Type 15

Note: This alert supports the following macro parameter strings:

%P1 User ID requesting system access

%P2 Network Address of system requesting access

%P3 Network Type of system requesting access

System Access Denied Alert

Explanation Generated by the Security Manager service when access to the system is denied to a remote user.

Alert Text Logon attempt by User ID '*%P1*' from Address '*%P2*' on Network '*%P3*' has been rejected.

Type of Alert Security Warning

Severity 5

Application ID SecMgr

Application Alert Type 16

Note: This alert supports the following macro parameter strings:

%P1 User ID requesting system access

%P2 Network Address of system requesting access

%P3 Network Type of system requesting access

System Restart Initiated Alert

Explanation Generated by the Security Manager service when a remote Netfinity Manager uses the Remote System Manager's Restart System option to restart your system.

Alert Text System Restart initiated by User ID '*%P1*' from Address '*%P2*' on Network '*%P3*'.

Type of Alert Security Information

Severity 5

Application ID SecMgr

Application Alert Type 41

Note: This alert supports the following macro parameter strings:

%P1 User ID requesting system restart

%P2 Network Address of system requesting restart

%P3 Network Type of system requesting restart

System Restart Request Rejected Alert

Explanation Generated by the Security Manager service when a remote Netfinity Manager attempts to use the Remote System Manager's Restart System option to restart your system, but does not have adequate security access to do so.

Alert Text System Restart request by User ID '*%P1*' from Address '*%P2*' on Network '*%P3*' rejected.

Type of Alert Security Error

Severity 3

Application ID SecMgr

Application Alert Type 40

Note: This alert supports the following macro parameter strings:

%P1	User ID requesting system restart
%P2	Network Address of system requesting restart
%P3	Network Type of system requesting restart

Service Manager

Alerts generated by the Service Manager follow.

Service Start Request Alert

Explanation	Generated by the Service Manager when a remote Netfinity Manager attempts to use one of your Netfinity services.
Alert Text	User ID '*%P1*' from Address '*%P2*' on Network '*%P3*' requested start of '*%P4*' service.
Type of Alert	Security Information
Severity	7
Application ID	SvcMgr
Application Alert Type	0900

Note: This alert supports the following macro parameter strings:

%P1	User ID requesting service start
%P2	Network Address of system requesting service start
%P3	Network Type of system requesting service start
%P4	Name of service requested to be started

Service Start Request Rejected Alert

Explanation	Generated by the Service Manager when a remote Netfinity Manager's request to use one of your Netfinity services is rejected.
Alert Text	User ID '*%P1*' from Address '*%P2*' on Network '*%P3*' request to start '*%P4* rejected.'
Type of Alert	Security Warning
Severity	5
Application ID	SvcMgr
Application Alert Type	0901

Note: This alert supports the following macro parameter strings:

%P1	User ID requesting service start
%P2	Network Address of system requesting service start
%P3	Network Type of system requesting service start
%P4	Name of service requested to be started

System Monitor

Alerts generated by System Monitor follow.

Upper-Range Threshold Error Alert

Explanation	Generated by the System Monitor service when the value of a monitored system component exceeds the upper-range Error value for greater than the specified time.
Alert Text	Error Alert *%P1*: Monitor '*%P2*' has been above or equal to *%P3* for *%P4*.
Type of Alert	Error
Severity	*x*
Application ID	MonitorB
Application Alert Type	0000

Notes:

1. This alert supports the following macro parameter strings:

%P1	Name of the threshold
%P2	Name of the monitor
%P3	Threshold value
%P4	Duration of threshold violation

2. You can set the Severity variable *x*. The default value for this variable is 3.

Upper-Range Threshold Warning Alert

Explanation	Generated by the System Monitor service when the value of a monitored system component exceeds the upper-range Warning value for greater than the specified time.
Alert Text	Warning Alert *%P1*: Monitor '*%P2*' has been above or equal to *%P3* for *%P4*.
Type of Alert	Warning
Severity	*x*
Application ID	MonitorB
Application Alert Type	0000

Notes:

1. This alert supports the following macro parameter strings:

   %P1 Name of the threshold

   %P2 Name of the monitor

   %P3 Threshold value

   %P4 Duration of threshold violation

2. You can set the Severity variable *x*. The default value for this variable is 4.

Lower-Range Threshold Warning Alert

Explanation	Generated by the System Monitor service when the value of a monitored system component falls below the lower-range Warning value for greater than the specified time.
Alert Text	Warning Alert *%P1*: Monitor '*%P2*' has been below or equal to *%P3* for *%P4*.
Type of Alert	Warning
Severity	*x*
Application ID	MonitorB
Application Alert Type	0000

Notes:

1. This alert supports the following macro parameter strings:

   %P1 Name of the threshold

   %P2 Name of the monitor

   %P3 Threshold value

   %P4 Duration of threshold violation

2. You can set the Severity variable *x*. The default value for this variable is 4.

Lower-Range Threshold Error Alert

Explanation	Generated by the System Monitor service when the value of a monitored system component falls below the lower-range Error value for greater than the specified time.
Alert Text	Error Alert *%P1*: Monitor '*%P2*' has been below or equal to *%P3* for *%P4*.
Type of Alert	Error
Severity	*x*
Application ID	MonitorB
Application Alert Type	0000

Notes:

1. This alert supports the following macro parameter strings:

   %P1 Name of the threshold

   %P2 Name of the monitor

   %P3 Threshold value

   %P4 Duration of threshold violation

2. You can set the Severity variable *x*. The default value for this variable is 2.

Threshold Return To Normal Alert

Explanation	Generated by the System Monitor service when the value of a monitored system component returns from a threshold exception state to a specified “normal” state or range.
Alert Text	Informational Alert *%P1*: Monitor '*%P2*' has returned to normal.
Type of Alert	Error
Severity	*x*
Application ID	MonitorB
Application Alert Type	10

Notes:

1. This alert supports the following macro parameter strings:

   %P1 Name of the threshold

   %P2 Name of the monitor

2. You can set the Severity variable *x*. The default value for this variable is 6.

Physical RAID Device Online Alert

Explanation	Generated by the System Monitor service when a physical RAID drive changes state to Online.
Alert Text	RAID Device Online: Attribute Physical Drive *x* in *y* set to online.
Type of Alert	Information
Severity	3
Application ID	MonitorB
Application Alert Type	130

Notes:

1. Alert Text variable *x* is the physical drive's designated location (Physical Bay number), and *y* is the name of the RAID subsystem reporting the state change.
2. This alert will be generated only by systems that have a supported RAID adapter (see Appendix E, "Supported RAID Adapters" on page 462).

Physical RAID Device Standby Alert

Explanation	Generated by the System Monitor service when a physical RAID drive changes state to Standby.
Alert Text	RAID Device Standby: Attribute Physical Drive *x* in *y* set to standby.
Type of Alert	Information
Severity	2
Application ID	MonitorB
Application Alert Type	130

Notes:

1. Alert Text variable *x* is the physical drive's designated location (Physical Bay number), and *y* is the name of the RAID subsystem reporting the state change.
2. This alert will be generated only by systems that have a supported RAID adapter (see Appendix E, "Supported RAID Adapters" on page 462).

Physical RAID Device Dead Alert

Explanation	Generated by the System Monitor service when a physical RAID drive changes state to Dead.
Alert Text	RAID Device Dead: Attribute Physical Drive *x* in *y* set to dead.
Type of Alert	Failure
Severity	0
Application ID	MonitorB
Application Alert Type	130

Notes:

1. Alert Text variable *x* is the physical drive's designated location (Physical Bay number), and *y* is the name of the RAID subsystem reporting the state change.
2. This alert will be generated only by systems that have a supported RAID adapter (see Appendix E, "Supported RAID Adapters" on page 462).

Logical RAID Device Online Alert

Explanation	Generated by the System Monitor service when a logical RAID system drive changes state to Online.
Alert Text	RAID Device Online: Attribute System Drive *x* in *y* set to online.
Type of Alert	Information
Severity	3
Application ID	MonitorB
Application Alert Type	131

Notes:

1. Alert Text variable *x* is the system drive's designated location (System Drive number), and *y* is the name of the RAID subsystem reporting the state change.
2. This alert will be generated only by systems that have a supported RAID adapter (see Appendix E, "Supported RAID Adapters" on page 462).

Logical RAID Device Critical Alert

Explanation	Generated by the System Monitor service when a logical RAID system drive changes state to Critical.
Alert Text	RAID Device Critical: Attribute System Drive *x* in *y* set to critical.
Type of Alert	Warning
Severity	2
Application ID	MonitorB
Application Alert Type	131

Notes:

1. Alert Text variable *x* is the system drive's designated location (System Drive number), and *y* is the name of the RAID subsystem reporting the state change.
2. This alert will be generated only by systems that have a supported RAID adapter (see Appendix E, "Supported RAID Adapters" on page 462).

Logical RAID Device Offline Alert

Explanation	Generated by the System Monitor service when a logical RAID system drive changes state to Offline.
Alert Text	RAID Device Offline: Attribute System Drive *x* in *y* set to offline.
Type of Alert	Failure
Severity	0
Application ID	MonitorB
Application Alert Type	131

Notes:

1. Alert Text variable *x* is the system drive's designated location (System Drive number), and *y* is the name of the RAID subsystem reporting the state change.
2. This alert will be generated only by systems that have a supported RAID adapter (see Appendix E, "Supported RAID Adapters" on page 462).

Appendix K. Troubleshooting Wake-On-LAN Systems

The following flowchart is designed to help you determine causes of and solutions to problems you may encounter when using Netfinity's Wake on LAN functions with your Netfinity systems.

MAP 0100: Check System Hardware

001

Do you have an Ethernet card or Token Ring card which includes the Wake on LAN function in the target system?

Yes **No**

002

The network card must be capable of detecting the Wake on LAN *magic packet* to initiate a wake up.

003

Is the target system a Wake on LAN enabled system unit?

Yes **No**

004

The system must be capable of reacting to the wake up signal from the network adapter.

005

Continue at "MAP 0110: Check Hardware Configuration" on page 526.

MAP 0110: Check Hardware Configuration

001

Is the target system configured to permit Wake on LAN?

– In SurePath Setup, check to see if Advanced Power Management/Automatic Power On/LAN Wake Up is enabled.
Yes No

002

The wake-up function must be enabled using the system setup program.

003

Continue at "MAP 0120: Check System Software" on page 527.

MAP 0120: Check System Software

001

Is Netfinity version 3.05 or later installed on the remote system?

Yes **No**

002

Older versions of Netfinity are not Wake on LAN aware and will not notify the Netfinity Manager that this capability is supported on the system.

003

Is WAKONLAN.DLL properly installed on the remote system?

Yes **No**

004

This DLL tells Netfinity whether the feature is available or not (see note 1 on page 534).

005

If the remote system is running OS/2, is the PNPDRV.SYS device driver installed?

– Check the remote system's CONFIG.SYS.

Yes **No**

006

WAKONLAN.DLL requires this device driver (see note 1 on page 534).

007

(Step **007** continues)

007 (continued)

Is Netfinity version 3.06 or later installed on the administrator system (the system attempting to send wake up magic packet)?

Yes **No**

008

Older versions of Netfinity do not know how to send the "magic packet."

009

Can the remote system determine its own media access control (MAC) address?

Answer Yes if any of the following are true:

- **a) You intend to manage the remote system using IPX and the Netfinity IPX protocol device driver is enabled in the remote system**
- **b) You intend to manage the remote system using NETBIOS and the Netfinity NETBIOS protocol device driver is enabled at the remote system**
- **c) You intend to manage the remote system using TCP/IP, the Netfinity TCP/IP protocol device driver is enabled at the remote system, the remote system is running Netfinity version 3.06 or later, and either the Netfinity IPX or NETBIOS protocol device drivers are enabled at the remote system.**
- **d) You intend to manage the remote system using TCP/IP, the Netfinity TCP/IP protocol device driver is enabled at the remote system, the remote system is running OS/2, and the remote system is running Netfinity version 5.0 or later**
- **e) You intend to manage the remote system using TCP/IP, the Netfinity TCP/IP protocol device driver is enabled at the remote system, the remote system is running Windows NT, and the remote system is running Netfinity version 5.0 or later**

Yes **No**

010

The TCP/IP protocol does not provide an application programming interface (API) that enables Netfinity to determine the MAC address of the network adapter (which must be known to send a wake up magic packet). Starting with Netfinity version 3.06, the TCP/IP device driver can acquire this information from IPX or NETBIOS if one of those device drivers is also enabled.

011

Can the administrator system generate a wake up "magic packet"?

Answer Yes if any of the following are true:

- **The administrator system is using Netfinity version 3.06 or later and the IPX protocol device driver is enabled**
- **The administrator system is using Netfinity version 4.0 or later and the TCP/IP protocol device driver is enabled**

Yes No

012

NETBIOS broadcasts are not true broadcasts in the sense that IPX and IP broadcasts are. The NETBIOS APIs do not provide a method for sending the type of broadcast that Wake on LAN requires. Netfinity will use IPX or IP to send a wake-up packet to a NETBIOS system if they are available at the administrator's system.

013

(Step **013** continues)

013 (continued)

Is the token-ring format of the MAC address being sent to the target system in the wake up magic packet if needed?

Answer Yes if any of the following are true:

- **The target system is using the token-ring version of the Wake on LAN adapter (as opposed to Ethernet).**
- **The target system is not running Windows 3.1 or Windows 95.**
- **The administrator system is using Netfinity version 4.0 or later.**

Yes **No**

014

Under 16 bit Windows, NETBIOS might report the token-ring format of the MAC address instead of the real burned-in MAC address that is needed to wake the card. Starting with version 4.0, Netfinity sends the wake-up magic packet using both the reported MAC addresses and the token-ring format of the reported address.

015

If the target system is running Windows 95, does the MAC address in the Windows 95 configuration match the actual address of the card?

To check this:

- **a) Using mouse-button 2, click on Network Neighborhood.**
- **b) Select Properties.**
- **c) Find and select the network card that has wake-up capabilities.**
- **d) Select Properties.**
- **e) Select Advanced.**
- **f) Verify or correct the value of the Network Address. It must match the value reported by the LANAID configuration utility that came with the card.**

Yes **No**

016

The MAC address that is reported to Netfinity is the one that appears in **Network Neighborhood**. If the address does not match the real address burned into the network card, the card will not respond to the "magic packets" when they are sent.

017

Continue at "MAP 0130: Check the Network Setup" on page 532.

MAP 0130: Check the Network Setup

001

Are *Locally Administered Addresses* **(LAAs) being used on the target system?**

Yes **No**

002

Will IP or IPX broadcast frames sent from the administrator's system be able to pass through the network to the portion of the network where the target system resides?

Yes **No**

003

Some equipment in the network (hubs, bridges, or routers, for example) might be configured to pass only selected protocols or to block broadcasts.

004

Continue at "MAP 0140: Other Potential Reasons" on page 533.

005

The use of LAAs interferes with Netfinity's ability to determine the real MAC address of the network adapter (see note 3 on page 535).

MAP 0140: Other Potential Reasons

001

Did you wait one presence check interval (the default value is 10 minutes but can be changed) or perform a presence check on the system after it was discovered into a group (see note 2 on page 535)?

Yes **No**

002

Netfinity Manager does not learn about a system's ability to support wake-up during the initial discovery. This capability is detected only during subsequent presence checks.

- Using the Netfinity Remote System Manager, find the target system icon in the appropriate groups. Multiple icons for the target system might be present in the group if the system is accessible through more than one network protocol.
- Find the icon that represents the target system through the IPX or NETBIOS network. Select **Detail View** from the View pull-down menu in the Group window, open the system's context menu (using mouse-button 2, click on the target system's icon or name). The **Wake Up** option appears in this menu. It will be gray and non-selectable if the system is currently online and selectable if the system is offline.
- If the target system is running Netfinity version 3.06 or later and has both TCP/IP and IPX protocol support (or TCP/IP and NETBIOS), the icon representing the target system through the TCP/IP network will also present the **Wake Up** option on the context menu.

003

(Step **003** continues)

003 (continued)

See "Other Potential Problems."

Other Potential Problems

If the **Wake Up** function still does not appear on the menu or does not work, carefully review your answers to the questions asked in the previous sections, and then suspect a hardware or installation problem. The network adapter must be properly cabled to the system board.

Attention: Some older systems had a problem with a two conductor wire between the network card and the system board being reversed. If this cable is reversed, the main power button will not power on and off the system correctly. If it is necessary to reverse the cable, be sure to pull the power plug from the wall before reversing the cable as these systems remain partially powered on internally even when they appear to be off.

Notes:

1. The WAKONLAN.DLL is used by Netfinity to determine whether the network card in the target system is capable of being awakened. If you do not have the WAKONLAN.DLL (or if the version of the DLL which you have does not support the network card which you are using), you can override the result returned from the DLL using an environment variable:

   ```
   SET NFWAKEONLAN=ON
   ```

   or

   ```
   SET NFWAKEONLAN=YES
   ```

   These variables will cause Netfinity to act as if the function is available regardless of WAKONLAN.DLL. Likewise,

   ```
   SET NFWAKEONLAN=OFF
   ```

   or

   ```
   SET NFWAKEONLAN=NO
   ```

will disable the feature. If the environment variable is used, WAKONLAN.DLL and PNPDRV.SYS are not required on the target system.

Make sure there are no spaces or other characters after the environment variable. Additional characters on the SET NFWAKEONLAN line will prevent Remote System Manager from being able to recognize this function. The way in which you set this environment variable depends on your operating system.

- To set this environment variable on an OS/2 or Windows 95 system, add the variable to your CONFIG.SYS file and then restart your system.
- On NT systems:
  a. Open the Windows NT Control Panel, then double-click on **System**.
  b. Click on the **Environment** tab.
  c. Click anywhere in the **System Environment Variable** field.
  d. Type in the **Variable** field

     `NFWAKEONLAN`

  e. Type in the **Value** field the value (YES, ON, NO, or OFF).
  f. Select **Set**.
  g. Select **Apply**.
  h. Select **OK**.
  i. Shutdown and restart the Netfinity Support Program.

2. The default interval between presence checks is 10 minutes. To verify or change the value, using mouse-button 2 click on a system icon and select **System Notifications** from the menu. To initiate a Presence Check manually, select **Presence Check** from the same menu.
3. Systems running Netfinity Manager or Services for Windows NT version 5.0 or later can properly report the MAC address,

regardless of whether Locally Administered Addresses are in use.

4. When setting environment variables on systems using Windows NT, the environment variable needs to be set in **System Environment Variables**, *not* in **User Environment Variables**. Environment variable are only visible to Netfinity if they are configured in **System Environment Variables**.

Appendix L. Notices

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 that IBM product, program, or service may be used. Subject to IBM's valid intellectual property or other legally protectable rights, any functionally equivalent product, program, or service may be used instead of the IBM product, program, or service. The evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, are the responsibility of the user.

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:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594
U.S.A.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact IBM Corporation, Department 80D, P.O. Box 12195, 3039 Cornwallis, Research Triangle Park, NC 27709, U.S.A. Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

Alert on LAN	DB2
FFST	First Failure Support Technology
IBM	Micro Channel
MVS	Netfinity
NetView	OS/2
Predictive Failure Analysis	Presentation Manager
PS/2	SurePath
SystemView	Wake on LAN

The following terms are trademarks of other companies:

3Com	3Com Corporation
cc:Mail	cc:Mail, Inc. division of Lotus Development Corporation
EtherLink/MC	3Com Corporation
DMI	Desktop Management Task Force
IPX	Novell, Incorporated
Lotus Notes	Lotus Development Corporation
Netscape	Netscape Communications Corporation
NetWare	Novell, Incorporated
Novell	Novell, Incorporated
SMC	Standard Microsystems Corporation
Sportster	U. S. Robotics Corporation
U. S. Robotics	U. S. Robotics Corporation

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

LANDesk and Pentium are registered trademarks of Intel Corporation.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Tivoli is a trademark of Tivoli Systems.

Other company, product, and service names may be trademarks or service marks of others.

Portions of this product include Corel clipart.

Portions of this software product are based in part on the work of the Independent JPEG Group.

Appendix M. Index

A

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

Part Number: 10L9271

Printed in U.S.A.